The specifications and information regarding the products in this manual are subject to change without notice. All statements, information, and recommendations in this manual are believed to be accurate but are presented without warranty of any kind, express or implied. Users must take full responsibility for their application of any products.

The software license and limited warranty for the accompanying product are set forth in the information packet that shipped with the product and are incorporated herein by this reference. If you are unable to locate the software license or limited warranty, contact your Cisco representative for a copy.

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

Notwithstanding any other warranty herein, all document files and software of these suppliers are provided “as is” with all faults. Cisco and the above-named suppliers disclaim all warranties, expressed or implied, including, without limitation, those of merchantability, fitness for a particular purpose and noninfringement or arising from a course of dealing, usage, or trade practice. In no event shall Cisco or its suppliers be liable for any indirect, special, consequential or incidental damages, including, without limitation, lost profits or loss or damage to data arising out of the use or inability to use this manual, even if Cisco or its suppliers have been advised of the possibility of such damages.

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

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2016 Cisco Systems, Inc. All rights reserved.
# CONTENTS

## Preface

Changes to This Document  xiii
Obtaining Documentation and Submitting a Service Request  xiii

## Chapter 1

**IGMP Commands on Cisco ASR 9000 Series Router**  1

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-group (IGMP)</td>
<td>3</td>
</tr>
<tr>
<td>clear igmp counters</td>
<td>4</td>
</tr>
<tr>
<td>clear igmp group</td>
<td>6</td>
</tr>
<tr>
<td>clear igmp reset</td>
<td>8</td>
</tr>
<tr>
<td>explicit-tracking</td>
<td>9</td>
</tr>
<tr>
<td>join-group</td>
<td>11</td>
</tr>
<tr>
<td>maximum groups</td>
<td>13</td>
</tr>
<tr>
<td>maximum groups-per-interface</td>
<td>16</td>
</tr>
<tr>
<td>nsf lifetime (IGMP)</td>
<td>20</td>
</tr>
<tr>
<td>query-interval</td>
<td>22</td>
</tr>
<tr>
<td>query-max-response-time</td>
<td>24</td>
</tr>
<tr>
<td>query-timeout</td>
<td>26</td>
</tr>
<tr>
<td>robustness-count</td>
<td>28</td>
</tr>
<tr>
<td>router</td>
<td>29</td>
</tr>
<tr>
<td>router igmp</td>
<td>31</td>
</tr>
<tr>
<td>show igmp groups</td>
<td>33</td>
</tr>
<tr>
<td>show igmp interface</td>
<td>35</td>
</tr>
<tr>
<td>show igmp nsf</td>
<td>39</td>
</tr>
<tr>
<td>show igmp nsr</td>
<td>41</td>
</tr>
<tr>
<td>show igmp summary</td>
<td>43</td>
</tr>
<tr>
<td>show igmp ssm map</td>
<td>46</td>
</tr>
</tbody>
</table>
Multicast Source Discovery Protocol Commands 57

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>show igmp traffic</td>
<td>47</td>
</tr>
<tr>
<td>ssm map</td>
<td>50</td>
</tr>
<tr>
<td>static-group</td>
<td>52</td>
</tr>
<tr>
<td>version</td>
<td>54</td>
</tr>
<tr>
<td>vrf (igmp)</td>
<td>56</td>
</tr>
</tbody>
</table>

**CHAPTER 2**

**Multicast Source Discovery Protocol Commands** 57

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>cache-sa holdtime</td>
<td>58</td>
</tr>
<tr>
<td>cache-sa-state</td>
<td>59</td>
</tr>
<tr>
<td>clear msdp peer</td>
<td>61</td>
</tr>
<tr>
<td>clear msdp sa-cache</td>
<td>62</td>
</tr>
<tr>
<td>clear msdp stats</td>
<td>64</td>
</tr>
<tr>
<td>connect-source</td>
<td>65</td>
</tr>
<tr>
<td>default-peer</td>
<td>67</td>
</tr>
<tr>
<td>description (peer)</td>
<td>68</td>
</tr>
<tr>
<td>global maximum external-sa</td>
<td>69</td>
</tr>
<tr>
<td>maximum external-sa</td>
<td>70</td>
</tr>
<tr>
<td>maximum peer-external-sa</td>
<td>72</td>
</tr>
<tr>
<td>mesh-group (peer)</td>
<td>74</td>
</tr>
<tr>
<td>originator-id</td>
<td>75</td>
</tr>
<tr>
<td>password (peer)</td>
<td>76</td>
</tr>
<tr>
<td>peer (MSDP)</td>
<td>78</td>
</tr>
<tr>
<td>remote-as (multicast)</td>
<td>79</td>
</tr>
<tr>
<td>sa-filter</td>
<td>80</td>
</tr>
<tr>
<td>show msdp globals</td>
<td>82</td>
</tr>
<tr>
<td>show msdp peer</td>
<td>84</td>
</tr>
<tr>
<td>show msdp rpf</td>
<td>86</td>
</tr>
<tr>
<td>show msdp nsr</td>
<td>88</td>
</tr>
<tr>
<td>show msdp sa-cache</td>
<td>89</td>
</tr>
<tr>
<td>show msdp statistics peer</td>
<td>93</td>
</tr>
<tr>
<td>show msdp summary</td>
<td>95</td>
</tr>
<tr>
<td>show msdp vrf context</td>
<td>97</td>
</tr>
<tr>
<td>shutdown (MSDP)</td>
<td>99</td>
</tr>
<tr>
<td>ttl-threshold (MSDP)</td>
<td>100</td>
</tr>
</tbody>
</table>
Multicast Routing and Forwarding Commands

accounting per-prefix
accounting per-prefix forward-only
address-family (multicast)
boundary
clear mfib counter
clear mfib database
clear mfib hardware resource-counters
clear mfib hardware route statistics
disable (multicast)
enable (multicast)
forwarding-latency
interface (multicast)
interface all enable
interface-inheritance disable
log-traps
maximum disable
mdt c-multicast-routing
mdt data
mdt data ingress replication
mdt default
mdt mtu
mdt source
migration route-policy
multicast-routing
multipath
nsf (multicast)
oom-handling
rate-per-route
shared-tree-prune delay
show mfib bvi
show mfib connections
show mfib counter
### IGMP and MLD Snooping Commands on Cisco ASR 9000 Series Routers

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-group (snooping profile)</td>
<td>245</td>
</tr>
<tr>
<td>clear igmp snooping bridge-domain</td>
<td>246</td>
</tr>
<tr>
<td>clear igmp snooping group</td>
<td>248</td>
</tr>
<tr>
<td>clear igmp snooping port</td>
<td>250</td>
</tr>
<tr>
<td>clear igmp snooping summary</td>
<td>252</td>
</tr>
<tr>
<td>clear l2vpn forwarding bridge-domain mroute</td>
<td>253</td>
</tr>
<tr>
<td>group limit</td>
<td>254</td>
</tr>
<tr>
<td>group policy</td>
<td>256</td>
</tr>
<tr>
<td>igmp snooping profile</td>
<td>258</td>
</tr>
<tr>
<td>immediate-leave</td>
<td>261</td>
</tr>
<tr>
<td>internal-querier</td>
<td>263</td>
</tr>
<tr>
<td>internal-querier (MLD)</td>
<td>265</td>
</tr>
<tr>
<td>internal-querier max-response-time</td>
<td>266</td>
</tr>
<tr>
<td>internal-querier query-interval</td>
<td>268</td>
</tr>
<tr>
<td>internal-querier robustness-variable</td>
<td>270</td>
</tr>
<tr>
<td>internal-querier tcn query count</td>
<td>272</td>
</tr>
<tr>
<td>internal-querier tcn query interval</td>
<td>274</td>
</tr>
<tr>
<td>internal-querier timer expiry</td>
<td>276</td>
</tr>
<tr>
<td>internal-querier version</td>
<td>278</td>
</tr>
<tr>
<td>last-member-query count</td>
<td>280</td>
</tr>
<tr>
<td>last-member-query count (MLD)</td>
<td>282</td>
</tr>
<tr>
<td>last-member-query interval</td>
<td>283</td>
</tr>
<tr>
<td>last-member-query interval (MLD)</td>
<td>285</td>
</tr>
<tr>
<td>minimum-version</td>
<td>286</td>
</tr>
<tr>
<td>minimum version (MLD)</td>
<td>288</td>
</tr>
<tr>
<td>mld snooping profile</td>
<td>289</td>
</tr>
<tr>
<td>mrouter</td>
<td>290</td>
</tr>
<tr>
<td>nv satellite offload ipv4 multicast enable</td>
<td>292</td>
</tr>
<tr>
<td>querier query-interval</td>
<td>293</td>
</tr>
<tr>
<td>querier robustness-variable</td>
<td>295</td>
</tr>
<tr>
<td>redundancy iccp-group report-standby-state disable</td>
<td>297</td>
</tr>
<tr>
<td>report-suppression disable</td>
<td>299</td>
</tr>
</tbody>
</table>
report-suppression disable(MLD) 301
router-alert-check disable 302
router-guard 304
show igmp snooping bridge-domain 306
show igmp snooping group 313
show igmp snooping port 321
show igmp snooping profile 327
show igmp snooping redundancy 332
show igmp snooping summary 335
show igmp snooping trace 340
show l2vpn forwarding bridge-domain mroute 342
show l2vpn forwarding bridge-domain mroute detail 344
show l2vpn forwarding bridge-domain mroute hardware ingress detail 346
show mld snooping bridge-domain 353
show mld snooping group 359
show mld snooping port 363
show mld snooping profile 367
show mld snooping summary 372
show mld snooping trace 376
startup query count 378
startup query iccp-group 379
startup query interval 381
startup query max-response-time 382
startup query port-up disable 383
startup query process start 384
startup query topology-change 385
static group 386
system-ip-address 388
tcn flood disable 390
tcn flood query count 392
tcn flood query count (MLD) 394
tcn query solicit 396
tcn query solicit (MLD) 398
ttl-check disable 399
CHAPTER 5  Multicast PIM Commands  403

unsolicited-report-interval  401

accept-register  405
auto-rp candidate-rp  406
bsr candidate-bsr  408
bsr candidate-rp  410
clear pim counters  412
clear pim topology  415
clon source  417
dr-priority  418
global maximum  420
global maximum bsr crp-cache threshold  421
global maximum group-mappings bsr threshold  423
hello-interval (PIM)  425
interface (PIM)  427
join-prune-interval  429
join-prune-mtu  430
maximum register-states  431
maximum route-interfaces  432
maximum routes  433
mofrr  434
neighbor-check-on-recv enable  436
neighbor-check-on-send enable  437
neighbor-filter  438
nsf lifetime (PIM)  439
old-register-checksum  440
router pim  441
rp-address  443
rpf topology route-policy  445
rpf-redirect  446
rpf-vector  447
rp-static-deny  448
show auto-rp candidate-rp  449
Multicast Tool and Utility Commands 515

mrinfo 516
mtrace 518
sap cache-timeout 520
sap listen 521
show sap 522
Preface

The Preface contains these topics:

- Changes to This Document, on page xiii
- Obtaining Documentation and Submitting a Service Request, on page xiii

Changes to This Document

This table lists the technical changes made to this document since it was first printed.

<table>
<thead>
<tr>
<th>Date</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 2015</td>
<td>Initial release of this document for the Release 5.3.0</td>
</tr>
<tr>
<td>September 2015</td>
<td>Documentation updates for the Release 5.3.2</td>
</tr>
</tbody>
</table>

Obtaining Documentation and Submitting a Service Request

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

To receive new and revised Cisco technical content directly to your desktop, you can subscribe to the What's New in Cisco Product Documentation RSS feed. RSS feeds are a free service.
IGMP Commands on Cisco ASR 9000 Series Router

This chapter describes the commands used to configure and monitor IPv4 multicast protocol on Cisco ASR 9000 Series Routers.

The commands in this chapter apply to the Internet Group Management Protocol (IGMP), versions 1, 2, and 3.

For detailed information about multicast routing concepts, configuration tasks, and examples, refer to the Implementing Multicast Routing on Cisco IOS XR Software configuration module in Multicast Configuration Guide for Cisco ASR 9000 Series Routers.

- access-group (IGMP), on page 3
- clear igmp counters, on page 4
- clear igmp group, on page 6
- clear igmp reset, on page 8
- explicit-tracking, on page 9
- join-group, on page 11
- maximum groups, on page 13
- maximum groups-per-interface, on page 16
- nsf lifetime (IGMP), on page 20
- query-interval, on page 22
- query-max-response-time, on page 24
- query-timeout, on page 26
- robustness-count, on page 28
- router, on page 29
- router igmp, on page 31
- show igmp groups, on page 33
- show igmp interface, on page 35
- show igmp nsf, on page 39
- show igmp nsr, on page 41
- show igmp summary, on page 43
- show igmp ssm map, on page 46
- show igmp traffic, on page 47
- ssm map, on page 50
- static-group, on page 52
- version, on page 54
- vrf (igmp), on page 56
access-group (IGMP)

To set limits on an interface for multicast-group join requests by hosts, use the **access-group** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

```
access-group access-list
no access-group access-list
```

### Syntax Description

- **access-list**: Number or name of a standard IP access list. Range is 1 to 99.

### Command Default

No default behavior or values

### Command Modes

IGMP interface configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If this command is not specified in router Internet Group Management Protocol (IGMP) configuration mode, the interface accepts all multicast join requests by hosts.

### Examples

In the following example, hosts serviced by GigabitEthernet interface 0/1/0/1 can join only group 225.2.2.2:

```
RP/0/RSP0/CPU0# configure
RP/0/RSP0/CPU0(config)# ipv4 access-list mygroup permit 225.2.2.2 0.0.0.0
RP/0/RSP0/CPU0(config)# router igmp
RP/0/RSP0/CPU0(config-igmp)# interface GigE 0/1/0/1
RP/0/RSP0/CPU0(config-igmp-if)# access-group mygroup
RP/0/RSP0/CPU0(config-igmp)# configure
RP/0/RSP0/CPU0(config)# ipv4 access-list mygroup permit 225.2.2.2 0.0.0.0
RP/0/RSP0/CPU0(config)# router igmp
RP/0/RSP0/CPU0(config-igmp)# interface GigE 0/1/0/1
RP/0/RSP0/CPU0(config-igmp-if)# access-group mygroup
```

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4 access-list</td>
<td>Defines a standard IP access list. For information, see <em>IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers</em></td>
</tr>
</tbody>
</table>
clear igmp counters

To clear IGMP traffic statistics, use the `clear igmp counters` command in EXEC mode.

```
clear igmp [ipv4 [vrf vrf-name] | vrf vrf-name] counters
```

**Syntax Description**
- `ipv4` (Optional) Specifies IPv4 addressing. IPv4 is the default for Internet Group Management Protocol (IGMP) groups.
- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.

**Command Default**
No default behavior or values

**Command Modes**
EXEC

**Command History**
- **Release** 3.7.2  This command was introduced.

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

After IGMP statistics are cleared, statistics begin incrementing again.

**Task ID**
- **Task ID**
- **Operations**
  - `multicast` `execute`

**Examples**
The following example shows sample output before and after clearing IGMP traffic statistics:

```
RP/0/RSP0/CPU0:router# show igmp traffic
IGMP Traffic Counters
Elapsed time since counters cleared: 00:00:19

<table>
<thead>
<tr>
<th>Received</th>
<th>Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid IGMP Packets</td>
<td>0</td>
</tr>
<tr>
<td>Queries</td>
<td>0</td>
</tr>
<tr>
<td>Reports</td>
<td>0</td>
</tr>
<tr>
<td>Leaves</td>
<td>0</td>
</tr>
<tr>
<td>Mtrace packets</td>
<td>0</td>
</tr>
<tr>
<td>DVNRF packets</td>
<td>0</td>
</tr>
<tr>
<td>PIM packets</td>
<td>0</td>
</tr>
</tbody>
</table>

Errors:
- Malformed Packets: 0
- Bad Checksums: 0
- Socket Errors: 0
- Bad Scope Errors: 0
- Auxiliary Data Len Errors: 0
- Subnet Errors: 0
```
Packets dropped due to invalid socket 0
Packets which couldn't be accessed 0
Other packets drops 0

RP/0/RSP0/CPU0:router# clear igmp counters

RP/0/RSP0/CPU0:router# show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 00:00:12

<table>
<thead>
<tr>
<th>Received</th>
<th>Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid IGMP Packets</td>
<td>0</td>
</tr>
<tr>
<td>Queries</td>
<td>0</td>
</tr>
<tr>
<td>Reports</td>
<td>0</td>
</tr>
<tr>
<td>Leaves</td>
<td>0</td>
</tr>
<tr>
<td>Mtrace packets</td>
<td>0</td>
</tr>
<tr>
<td>DVMRP packets</td>
<td>0</td>
</tr>
<tr>
<td>PIM packets</td>
<td>0</td>
</tr>
</tbody>
</table>

Errors:
Malformed Packets 0
Bad Checksums 0
Socket Errors 0
Bad Scope Errors 0
Auxiliary Data Len Errors 0
Subnet Errors 0
Packets dropped due to invalid socket 0
Packets which couldn't be accessed 0
Other packets drops 0

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show igmp traffic, on page 47</td>
<td>Displays all the Internet Group Management Protocol (IGMP) traffic-related counters.</td>
</tr>
</tbody>
</table>
clear igmp group

To clear Internet Group Management Protocol (IGMP) groups on one or all interfaces, use the `clear igmp group` command in EXEC mode.

```
clear igmp [{ipv4 | vrf vrf-name}] group [{ip-address | type interface-path-id}]
```

**Syntax Description**
- **ipv4** (Optional) Specifies IPv4 addressing. IPv4 is the default for IGMP groups.
- **vrf vrf-name** (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- **ip-address** (Optional) IP hostname or group address.
- **type** (Optional) Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id** (Optional) Physical interface or virtual interface.

**Note**
Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**
If no group address is specified, all IGMP groups are cleared.

**Command Modes**
EXEC

**Command History**
Release 3.7.2  This command was introduced.

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

To clear all IGMP groups, use the `clear igmp group` command without using an argument. To clear a particular group, use the `ip-address` or `type interface-path-id` arguments.

The following groups cannot be cleared:
- 224.0.0.2
- 224.0.0.13
- 224.0.0.22
- 224.0.0.40

**Task ID**
```
Task ID  Operations
multicast  execute
```
Examples

The following example uses the `show igmp groups` command to display the IGMP Connected Group Membership, the `clear igmp group` command to clear address 239.1.1.1, and the `show igmp groups` command again to display the updated list.

RP/0/RSP0/CPU0:router# show igmp groups tenGigE 0/4/0/0

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Interface</th>
<th>Uptime</th>
<th>Expires</th>
<th>Last Reporter</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.0.2</td>
<td>TenGigE0/4/0/0</td>
<td>3w6d</td>
<td>never</td>
<td>10.114.8.44</td>
</tr>
<tr>
<td>224.0.0.5</td>
<td>TenGigE0/4/0/0</td>
<td>3w6d</td>
<td>never</td>
<td>10.114.8.44</td>
</tr>
<tr>
<td>224.0.0.6</td>
<td>TenGigE0/4/0/0</td>
<td>3w6d</td>
<td>never</td>
<td>10.114.8.44</td>
</tr>
<tr>
<td>224.0.0.13</td>
<td>TenGigE0/4/0/0</td>
<td>3w6d</td>
<td>never</td>
<td>10.114.8.44</td>
</tr>
<tr>
<td>224.0.0.22</td>
<td>TenGigE0/4/0/0</td>
<td>3w6d</td>
<td>never</td>
<td>10.114.8.44</td>
</tr>
</tbody>
</table>

RP/0/RSP0/CPU0:router# clear igmp groups tenGigE 0/4/0/0

RP/0/RSP0/CPU0:router# show igmp groups tenGigE 0/4/0/0

<table>
<thead>
<tr>
<th>Group Address</th>
<th>Interface</th>
<th>Uptime</th>
<th>Expires</th>
<th>Last Reporter</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.0.2</td>
<td>TenGigE0/4/0/0</td>
<td>3w6d</td>
<td>never</td>
<td>10.114.8.44</td>
</tr>
<tr>
<td>224.0.0.5</td>
<td>TenGigE0/4/0/0</td>
<td>3w6d</td>
<td>never</td>
<td>10.114.8.44</td>
</tr>
<tr>
<td>224.0.0.6</td>
<td>TenGigE0/4/0/0</td>
<td>3w6d</td>
<td>never</td>
<td>10.114.8.44</td>
</tr>
<tr>
<td>224.0.0.13</td>
<td>TenGigE0/4/0/0</td>
<td>3w6d</td>
<td>never</td>
<td>10.114.8.44</td>
</tr>
<tr>
<td>224.0.0.22</td>
<td>TenGigE0/4/0/0</td>
<td>3w6d</td>
<td>never</td>
<td>10.114.8.44</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show igmp groups, on page 33</td>
<td>Displays the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP).</td>
</tr>
</tbody>
</table>
clear igmp reset

To clear all Internet Group Management Protocol (IGMP) membership entries and reset connection in the Multicast Routing Information Base (MRIB), use the **clear igmp reset** command in EXEC mode.

```
clear igmp [{ipv4 vrf vrf-name} vrf vrf-name}]] reset
```

**Syntax Description**

- **ipv4** (Optional) Specifies IPv4 addressing. IPv4 is the default for IGMP groups.
- **vrf vrf-name** (Optional) Specifies a VPN routing and forwarding (VRF) instance.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Every IGMP group membership that IGMP learns is downloaded to the MRIB database. The **clear igmp reset** command is used to clear all information from the IGMP topology table and reset the MRIB connection.

**Note**

This command is reserved to force synchronization of IGMP and MRIB entries when communication between the two components is malfunctioning.

**Task ID**

- **Task ID** Operations
  - multicast execute

**Examples**

The following example shows how to clear the group memberships in MRIB:

```
RP/0/RSP0/CPU0:router# clear igmp reset
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show igmp groups, on page 33</td>
<td>Displays the multicast groups that are directly connected to the router and that were learned through IGMP</td>
</tr>
<tr>
<td>show mrib route</td>
<td>Displays all route entries in the MRIB table.</td>
</tr>
</tbody>
</table>
explicit-tracking

To configure explicit host tracking under Internet Group Management Protocol (IGMP) Version 3, use the `explicit-tracking` command in the appropriate configuration mode. To disable explicit host tracking, use the `no` form of this command.

```
explicit-tracking  [{access-list|disable}]
no  explicit-tracking
```

**Syntax Description**

- **access-list** (Optional) Access list that specifies the group range for host tracking.
- **disable** (Optional) Disables explicit host tracking on a specific interface. This option is available only in interface configuration mode.

**Command Default**

If this command is not specified in IGMP configuration mode, then explicit host tracking is disabled.

**Command Modes**

- IGMP VRF configuration
- IGMP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

By default, IGMP supports Version 3, unless a Version 2 or Version 1 IGMP host message is detected in the network. For backward compatibility, IGMP downgrades to run at the IGMP version level that is installed.

This feature allows the router to achieve minimal leave latencies when hosts leave a multicast group or channel. To monitor IGMP membership of hosts, use the `show igmp groups` command in EXEC mode.

In router configuration mode, the `explicit-tracking` command enables explicit host tracking for all interfaces. To disable explicit tracking for all interfaces, use the `no` form of the command from IGMP configuration mode. To disable the feature on specific interfaces, use the `explicit-tracking` command in interface configuration mode with the `disable` keyword, as shown in the following example.

```
no  explicit-tracking
```

**Note**

If you configure this command in IGMP VRF configuration mode, parameters are inherited by all new and existing interfaces. However, you can override these parameters on individual interfaces from IGMP interface configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read,  write</td>
</tr>
</tbody>
</table>
The following example shows how to enable explicit host tracking for the access list named router1 on all interfaces and how to disable explicit host tracking for a specific GigabitEthernet interface:

```
RP/0/RSP0/CPU0:router(config)# router igmp
RP/0/RSP0/CPU0:router(config-igmp)# explicit-tracking router1
RP/0/RSP0/CPU0:router(config-igmp)# interface GigabitEthernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-igmp-default-if)# explicit-tracking disable
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show igmp groups, on page 33</td>
<td>Displays the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP).</td>
</tr>
</tbody>
</table>
**join-group**

To have the router join a multicast group, use the `join-group` command in the appropriate configuration mode. To return to the default behavior, use the `no` form of this command.

```
join-group  group-address  [source-address]
no  join-group  group-address  [source-address]
```

**Syntax Description**

- `group-address`: Address of the multicast group. This is a multicast IP address group in IPv4 format
  - IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format `A.B.C.D`.
- `source-address`: (Optional) Source address of the multicast group to include in IPv4 prefixing format
  - IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format `A.B.C.D`.

**Command Default**

No multicast group memberships are predefined. If not specified, include is the default.

**Command Modes**

IGMP interface configuration

**Command History**

**Release**  | **Modification**
---|---
Release 3.7.2 | This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `join-group` command permits the IP packets that are addressed to the group address to pass to the IP client process in the Cisco IOS XR software.

If all the multicast-capable routers that you administer are members of a multicast group, pinging that group causes all routers to respond. This command can be a useful administrative and debugging tool.

Another reason to have a router join a multicast group is when other hosts on the network are prevented from correctly answering IGMP queries. When the router joins the multicast group, upstream devices learn multicast routing table information for that group and keep the paths for that group active.

**Caution**

Joining a multicast group can result in a significant performance impact, because all subscribed multicast packets are punted to the route processor.
Examples

In the following example, the router joins multicast group 225.2.2.2:

```
RP/0/RSP0/CPU0:router(config)# router igmp
RP/0/RSP0/CPU0:router(config-igmp)# interface GigabitEthernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-igmp-default-if)# join-group 225.2.2.2
```

The `join-group` command can have an include/exclude mode for IGMPv3 interfaces as shown in the following example:

```
RP/0/RSP0/CPU0:router(config)# router igmp
RP/0/RSP0/CPU0:router(config-igmp)# int gigabitEthernet 0/5/0/1
RP/0/RSP0/CPU0:router(config-igmp-default-if)# join-group ?
A.B.C.D IP group address
RP/0/RSP0/CPU0:router(config-igmp-default-if)# join-group 225.0.0.0 ?
A.B.C.D Source address to include
exclude Exclude the only following source address include Include only the following source address <cr>
RP/0/RSP0/CPU0:router(config-igmp-default-if)# join-group 225.0.0.0 10.10.10.10 ?
<cr>
RP/0/RSP0/CPU0:router(config-igmp-default-if)# join-group 225.0.0.0 ?
A.B.C.D Source address to include
exclude Exclude the only following source address include Include only the following source address <cr>
RP/0/RSP0/CPU0:router(config-igmp-default-if)# join-group 225.0.0.0
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ping</td>
<td>Checks host reachability and network connectivity on IP networks. For information, see <em>IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers</em>.</td>
</tr>
</tbody>
</table>
maximum groups

To configure the maximum number of groups used by Internet Group Management Protocol (IGMP) and accepted by a router, use the `maximum groups` command in the appropriate configuration mode. To return to the default behavior, use the `no` form of this command.

```
maximum groups number
no maximum groups
```

**Syntax Description**

- `number` Maximum number of groups accepted by a router. Range is 1 to 75000.

**Command Default**

- `number`: 50000

**Command Modes**

- IGMP configuration
- IGMP VRF configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When configuring this command within IGMP VRF configuration mode, you may either use the default (unspecified) VRF or a specific VRF by specifying its name.

The maximum combined number of groups on all interfaces can be 75000. After the maximum groups value is met, all additional memberships learned are ignored. The maximum number includes external and local membership.

The following groups obtain local membership on each interface when multicast is enabled and are added into the group totals for each interface: 224.0.0.13 (for PIM), 224.0.0.22 and 224.0.0.2 (for IGMP).

You cannot use the `maximum groups` command to configure the maximum number of groups below the number of existing groups. For instance, if the number of groups is 39, and you set the maximum number of groups to 10, the configuration is rejected.

Although Cisco IOS XR Software Release 3.9.0 supports 40,000 groups per interface, the ASR9000 router supports a maximum of 16,000 multicast routes per system.

Furthermore, you can use the `maximum groups per-interface` command to configure the maximum number of groups for each interface accepted by a router.
The following example shows how to display the number of groups (39) and the maximum number of groups configured (50000). Through use of the maximum groups command, a configuration is committed to change the maximum number of groups to 40. Before and after configuration, the show igmp summary command is used to confirm the configuration change:

```
RP/0/RSP0/CPU0:router# show igmp summary
IGMP summary

Robustness Value 2
No. of Group x Interfaces 61
Maximum number of Group x Interfaces 50000

Supported Interfaces : 18
Unsupported Interfaces : 2
Enabled Interfaces : 18
Disabled Interfaces : 2

Interface Grp No Max Grp No
MgmtEth0/RSP0/CPU0/0 0 25000
Loopback0 4 25000
Bundle-Ether24 3 25000
Bundle-Ether28 3 25000
Bundle-Ether28.1 3 25000
Bundle-Ether28.2 3 25000
Bundle-Ether28.3 3 25000
MgmtEth0/RP1/CPU0/0 0 25000
GigabitEthernet0/1/5/0 3 25000
GigabitEthernet0/1/5/1 5 25000
GigabitEthernet0/1/5/2 5 25000
GigabitEthernet0/1/0/1 5 25000
GigabitEthernet0/1/4/2 3 25000
GigabitEthernet0/6/5/1 3 25000
GigabitEthernet0/6/5/2 3 25000
GigabitEthernet0/6/5/7 3 25000
GigabitEthernet0/6/0/1 3 25000
GigabitEthernet0/6/4/4 3 25000
GigabitEthernet0/6/4/5 3 25000
GigabitEthernet0/6/4/6 3 25000

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router igmp
RP/0/RSP0/CPU0:router(config-igmp)# maximum groups 65
RP/0/RSP0/CPU0:router(config-igmp)# commit

RP/0/RSP0/CPU0:router:May 13 12:26:59.108 : config[65704]: %LIBTARCFG-6-COMMIT : Configuration committed by user 'cisco'. Use 'show commit changes 1000000025' to view the changes.

RP/0/RSP0/CPU0:router# show igmp summary
IGMP summary

Robustness Value 2
No. of Group x Interfaces 61
Maximum number of Group x Interfaces 65

Supported Interfaces : 18
Unsupported Interfaces : 2
Enabled Interfaces : 18
Disabled Interfaces : 2

Interface Grp No Max Grp No
MgmtEth0/RSP0/CPU0/0 0 25000
```
<table>
<thead>
<tr>
<th>Interface</th>
<th>Groups</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback0</td>
<td>4</td>
<td>25000</td>
</tr>
<tr>
<td>Bundle-Ether28</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>Bundle-Ether28.1</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>Bundle-Ether28.2</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>Bundle-Ether28.3</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>MgmtEth0/RP1/CPU0/0</td>
<td>0</td>
<td>25000</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5/0</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5/1</td>
<td>5</td>
<td>25000</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5/2</td>
<td>5</td>
<td>25000</td>
</tr>
<tr>
<td>GigabitEthernet0/6/5/1</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>GigabitEthernet0/6/5/2</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>GigabitEthernet0/6/5/7</td>
<td>3</td>
<td>25000</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maximum groups-per-interface, on page 16</td>
<td>Configures the maximum number of groups for each interface accepted by a router.</td>
</tr>
<tr>
<td>show igmp summary, on page 43</td>
<td>Displays group membership information for Internet Group Management Protocol (IGMP).</td>
</tr>
</tbody>
</table>
maximum groups-per-interface

To configure the maximum number of groups for each interface accepted by a router, use the **maximum groups-per-interface** command in the appropriate configuration mode. To return to the default behavior, use the **no** form of this command.

```
maximum groups-per-interface number
no maximum groups-per-interface
```

**Syntax Description**

- `number`: Maximum number of groups accepted by a router for each interface. Range is 1 to 16000.

**Command Default**

`number : 20000`

**Command Modes**

- IGMP configuration
- IGMP VRF configuration
- IGMP interface configuration

**Command History**

- **Release 3.7.2**: This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The following groups obtain local membership on each interface when multicast is enabled and are added into the group totals for each interface: 224.0.0.13 (for Protocol Independent Multicast [PIM]), 224.0.0.22 and 224.0.0.2 (for Internet Group Management Protocol [IGMP]). The number of groups for each interface reflects both external and local group membership.

**Note**

You cannot use the `maximum groups-per-interface` command to configure the maximum number of groups for each interface below the number of existing groups on an interface. For example, if the number of groups is 39, and you set the maximum number of groups to 10, the configuration is rejected.

When you use the `maximum groups-per-interface` command for a specific interface, it overrides the inheritance property of this command specified under IGMP configuration mode.

**Task ID**

- `multicast`: read, write

**Examples**

The following example shows how to display the maximum number of groups for each interface. A configuration is committed to change the maximum number of groups for each interface to 12. Before
and after configuration, use the `show igmp summary` command to confirm the configuration change:

RP/0/RSP0/CPU0# show igmp summary

IGMP summary

Robustness Value 2
No. of Group x Interfaces 61
Maximum number of Group x Interfaces 50000

Supported Interfaces : 18
Unsupported Interfaces : 2
Enabled Interfaces : 18
Disabled Interfaces : 2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Grp No</th>
<th>Max Grp No</th>
</tr>
</thead>
<tbody>
<tr>
<td>MgmtEth0/RSP0/CPU0/0</td>
<td>0</td>
<td>25000</td>
</tr>
<tr>
<td>Loopback0</td>
<td>4</td>
<td>25000</td>
</tr>
<tr>
<td>Bundle-Ether28</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>Bundle-Ether28.1</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>Bundle-Ether28.2</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>Bundle-Ether28.3</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>MgmtEth0/RP1/CPU0/0</td>
<td>0</td>
<td>25000</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5/0</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5/1</td>
<td>5</td>
<td>25000</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5/2</td>
<td>5</td>
<td>25000</td>
</tr>
<tr>
<td>GigabitEthernet0/6/5/1</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>GigabitEthernet0/6/5/2</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>GigabitEthernet0/6/5/7</td>
<td>3</td>
<td>25000</td>
</tr>
</tbody>
</table>

RP/0/RSP0/CPU0# configure
RP/0/RSP0/CPU0(config)# router igmp
RP/0/RSP0/CPU0(config-igmp)# maximum groups-per-interface 5
RP/0/RSP0/CPU0(config-igmp)# commit

RP/0/RSP0/CPU0# show igmp summary

Robustness Value 2
No. of Group x Interfaces 61
Maximum number of Group x Interfaces 65

Supported Interfaces : 18
Unsupported Interfaces : 2
Enabled Interfaces : 18
Disabled Interfaces : 2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Grp No</th>
<th>Max Grp No</th>
</tr>
</thead>
<tbody>
<tr>
<td>MgmtEth0/RSP0/CPU0/0</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Loopback0</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Bundle-Ether28</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Bundle-Ether28.1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Bundle-Ether28.2</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Bundle-Ether28.3</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>MgmtEth0/RP1/CPU0/0</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5/0</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5/1</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5/2</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>GigabitEthernet0/6/5/1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>GigabitEthernet0/6/5/2</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>GigabitEthernet0/6/5/7</td>
<td>3</td>
<td>5</td>
</tr>
</tbody>
</table>
The following example shows how to configure all interfaces with 3000 maximum groups per interface except GigabitEthernet interface 0/4/0/0, which is set to 4000:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router igmp
RP/0/RSP0/CPU0:router(config-igmp)# maximum groups-per-interface 3000
RP/0/RSP0/CPU0:router(config-igmp)# interface GigabitEthernet 0/4/0/0
RP/0/RSP0/CPU0:router(config-igmp-default-if)# maximum groups-per-interface 4000
```

IGMP summary

Robustness Value 2
No. of Group x Interfaces 61
Maximum number of Group x Interfaces 50000

Supported Interfaces : 18
Unsupported Interfaces : 2
Enabled Interfaces : 18
Disabled Interfaces : 2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Grp No</th>
<th>Max Grp No</th>
</tr>
</thead>
<tbody>
<tr>
<td>MgmtEth0/RP0/CPU0/0</td>
<td>0</td>
<td>25000</td>
</tr>
<tr>
<td>Loopback0</td>
<td>4</td>
<td>25000</td>
</tr>
<tr>
<td>Bundle-POS24</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>Bundle-Ether28</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>Bundle-Ether28.1</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>Bundle-Ether28.2</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>Bundle-Ether28.3</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>MgmtEth0/RP1/CPU0/0</td>
<td>0</td>
<td>25000</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5/0</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5/1</td>
<td>5</td>
<td>25000</td>
</tr>
<tr>
<td>GigabitEthernet0/1/5/2</td>
<td>5</td>
<td>25000</td>
</tr>
<tr>
<td>POS0/1/0/1</td>
<td>5</td>
<td>25000</td>
</tr>
<tr>
<td>POS0/1/4/2</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>GigabitEthernet0/6/5/1</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>GigabitEthernet0/6/5/2</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>GigabitEthernet0/6/5/7</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>POS0/6/0/1</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>POS0/6/4/4</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>POS0/6/4/5</td>
<td>3</td>
<td>25000</td>
</tr>
<tr>
<td>POS0/6/4/6</td>
<td>3</td>
<td>25000</td>
</tr>
</tbody>
</table>

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router igmp
RP/0/RSP0/CPU0:router(config-igmp)# maximum groups-per-interface 5
RP/0/RSP0/CPU0:router(config-igmp)# commit
RP/0/RSP0/CPU0:router# show igmp summary
```

Robustness Value 2
No. of Group x Interfaces 61
Maximum number of Group x Interfaces 65

Supported Interfaces : 18
Unsupported Interfaces : 2
Enabled Interfaces : 18
Disabled Interfaces : 2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Grp No</th>
<th>Max Grp No</th>
</tr>
</thead>
<tbody>
<tr>
<td>MgmtEth0/RP0/CPU0/0</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Loopback0</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Bundle-POS24</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Bundle-Ether28</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Bundle-Ether28.1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Bundle-Ether28.2</td>
<td>3</td>
<td>5</td>
</tr>
</tbody>
</table>
Bundle-Ether28.3  3  5
MgmtEth0/RP1/CP00/0  0  5
GigabitEthernet0/1/5/0  3  5
GigabitEthernet0/1/5/1  5  5
GigabitEthernet0/1/5/2  5  5
POS0/1/0/1  5  5
POS0/1/4/2  3  5
GigabitEthernet0/6/5/1  3  5
GigabitEthernet0/6/5/2  3  5
GigabitEthernet0/6/5/7  3  5
POS0/6/0/1  3  5
POS0/6/4/4  3  5
POS0/6/4/5  3  5
POS0/6/4/6  3  5

RP/0/RSP0/CP00:router# configure
RP/0/RSP0/CP00:router(config)# router igmp
RP/0/RSP0/CP00:router(config-igmp)# maximum groups-per-interface 3000
RP/0/RSP0/CP00:router(config-igmp)# interface POS 0/4/0/0
RP/0/RSP0/CP00:router(config-igmp-default-if)# maximum groups-per-interface 4000

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maximum groups, on page 13</td>
<td>Configures the maximum number of groups used by Internet Group Management Protocol (IGMP).</td>
</tr>
<tr>
<td>show igmp summary, on page 43</td>
<td>Displays group membership information for Internet Group Management Protocol (IGMP).</td>
</tr>
</tbody>
</table>
nsf lifetime (IGMP)

To configure the maximum time for the nonstop forwarding (NSF) timeout on the Internet Group Management Protocol (IGMP) process, use the `nsf lifetime` command in the appropriate configuration mode. To return to the default behavior, use the `no` form of this command.

```
nsf lifetime seconds
no nsf lifetime
```

**Syntax Description**

- `seconds` Maximum time for NSF mode. Range is 10 to 3600 seconds.

**Command Default**

- `seconds`: 60

**Command Modes**

- IGMP configuration
- IGMP VRF configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The IGMP NSF process is triggered by the restart of the IGMP process. While in IGMP NSF mode, the Multicast Routing Information Base (MRIB) purges the routes installed by the previous IGMP process when the IGMP NSF process times out.

The IGMP NSF lifetime is the period for IGMP to relearn all the host membership of the attached network through membership queries and reports. During this NSF period, PIM continues to maintain forwarding state for the local members while IGMP recovers their membership reports.

Additionally, IGMP recovers the internal receiver state from Local Packet Transport Services (LPTS) for IP group member applications (including the Session Announcement Protocol (SAP) Listener) and updates the MRIB.

**Task ID**

```
Task ID Operations
multicast read,
            write
```

**Examples**

The following example shows how to set the IGMP NSF timeout value to 120 seconds:

```
RP/0/RSP0/CPU0:router(config)# router igmp
RP/0/RSP0/CPU0:router(config-igmp)# nsf lifetime 120
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nsf (multicast)</td>
<td>Enables NSF capability for the multicast routing system.</td>
</tr>
<tr>
<td>nsf lifetime (PIM)</td>
<td>Configures the NSF timeout value for the PIM process.</td>
</tr>
<tr>
<td>show igmp nsf, on page 39</td>
<td>Displays the state of NSF operation in IGMP.</td>
</tr>
<tr>
<td>show mfib nsf</td>
<td>Displays the state of NSF operation for the MFIB line cards.</td>
</tr>
</tbody>
</table>
query-interval

To configure the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) host-query messages, use the `query-interval` command in the appropriate configuration mode. To return to the default frequency, use the `no` form of this command.

```
query-interval  seconds
no  query-interval
```

**Syntax Description**

`seconds` Frequency used to send IGMP host-query messages. Range is 1 to 3600.

**Command Default**

If this command is not specified in interface configuration mode, the interface adopts the query interval parameter specified in IGMP configuration mode.

If this command is not specified in IGMP configuration mode, the query interval time is 60 seconds.

**Command Modes**

IGMP VRF configuration

IGMP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Multicast routers send host membership query messages (host-query messages) to discover which multicast groups have members on the attached networks of the router. Hosts respond with IGMP report messages indicating that they want to receive multicast packets for specific groups (that is, that the host wants to become a member of the group). Host-query messages are addressed to the all-hosts multicast group, which has the address 224.0.0.1, and has an IP time-to-live (TTL) value of 1.

The designated router for a LAN is the only router that sends IGMP host-query messages:

- For IGMP Version 1 (only), the designated router is elected according to the multicast routing protocol that runs on the LAN.
- For IGMP Versions 2 and 3, the designated querier is the lowest IP-addressed multicast router on the subnet.

If the router hears no queries for the timeout period (controlled by the query-timeout command), it becomes the querier.

**Note**

Changing the value of the `seconds` argument may severely impact network performance. A short query interval may increase the amount of traffic on the attached network, and a long query interval may reduce the querier convergence time.
If you configure the **query-interval** command in IGMP configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces from interface configuration mode.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to change the frequency at which the designated router sends IGMP host-query messages to 2 minutes:

```
RP/0/RSP0/CPU0:router(config)# router igmp
RP/0/RSP0/CPU0:router(config-igmp)# interface gigabitEthernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-igmp-default-if)# query-interval 120
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>hello-interval (PIM)</strong></td>
<td>Configures the frequency of PIM hello messages.</td>
</tr>
<tr>
<td>query-timeout</td>
<td>Configures the timeout value before the router takes over as the querier for the interface.</td>
</tr>
<tr>
<td>show igmp groups, on page 33</td>
<td>Displays the multicast groups that are directly connected to the router and that were learned through IGMP.</td>
</tr>
</tbody>
</table>
query-max-response-time

To configure the maximum response time advertised in Internet Group Management Protocol (IGMP) queries, use the `query-max-response-time` command in the appropriate configuration mode. To return to the default behavior, use the `no` form of this command.

```plaintext
query-max-response-time  seconds
no  query-max-response-time
```

**Syntax Description**
- `seconds` Maximum response time, in seconds, advertised in IGMP queries. Range is 1 to 12.

**Command Default**
- If this command is not specified in interface configuration mode, the interface adopts the maximum response time parameter specified in IGMP configuration mode.
- If this command is not specified in IGMP configuration mode, the maximum response time is 10 seconds.

**Command Modes**
- IGMP VRF configuration
- IGMP interface configuration

**Command History**
- **Release** 3.7.2  This command was introduced.

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `query-max-response-time` command is not supported on IGMP Version 1.

This command is used to control the maximum response time for hosts to answer an IGMP query message. Configuring a value less than 10 seconds enables the router to prune groups much faster, but this action results in network burstiness because hosts are restricted to a shorter response time period.

If you configure this command in IGMP configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces in interface configuration mode.

**Note**
If the hosts do not read the maximum response time in the query message correctly, group membership might be pruned inadvertently. Therefore, the hosts must know to respond faster than 10 seconds (or the value you configure).

**Task ID**
- **Task ID** Operations
  - multicast  read, write

**Examples**
The following example shows how to configure a maximum response time of 8 seconds:
RP/0/RSP0/CPU0:router(config)# router igmp
RP/0/RSP0/CPU0:router(config-igmp)# interface gigabitEthernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-igmp-default-if)# query-max-response-time 8

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hello-interval (PIM)</td>
<td>Configures the frequency of PIM hello messages.</td>
</tr>
<tr>
<td>show igmp groups, on page 33</td>
<td>Displays the multicast groups that are directly connected to the router and that were learned through IGMP.</td>
</tr>
</tbody>
</table>
query-timeout

To configure the timeout value before the router takes over as the querier for the interface, use the `query-timeout` command in the appropriate configuration mode. To return to the default behavior, use the `no` form of this command.

```
query-timeout seconds
no query-timeout
```

**Syntax Description**

- **seconds**: Number of seconds that the router waits after the previous querier has stopped querying before it takes over as the querier. Range is 60 to 300.

**Command Default**

If this command is not specified in interface configuration mode, the interface adopts the timeout value parameter specified in IGMP VRF configuration mode. If this command is not specified in IGMP VRF configuration mode, the maximum response time is equal to twice the query interval set by the `query-interval` command.

**Command Modes**

- IGMP VRF configuration
- IGMP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `query-timeout` command is not supported on Internet Group Management Protocol (IGMP) Version 1.

By default, the router waits twice the query interval specified by the `query-interval` command, after which, if the router has heard no queries, it becomes the querier. By default, the query interval is 60 seconds, which means that the `query-timeout` value defaults to 120 seconds.

If you configure a query timeout value less than twice the query interval, routers in the network may determine a query timeout and take over the querier without good reason.

**Note**

If you configure this command in IGMP configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces in interface configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>
Examples

The following example shows how to configure the router to wait 30 seconds from the time it received the last query before it takes over as the querier for the interface:

```
RP/0/RSP0/CPU0:router(config)# router igmp
RP/0/RSP0/CPU0:router(config-igmp)# interface gigabitEthernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-igmp-default-if)# query-timeout 30
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>query-interval, on page 22</td>
<td>Configures the frequency at which the Cisco IOS XR Software sends Internet Group Management Protocol (IGMP) host-query messages.</td>
</tr>
</tbody>
</table>
robustness-count

To set the robustness variable to tune for expected packet loss on a network, use the robustness-count command in the appropriate configuration mode. To return to the default setting, use the no form of this command.

robustness-count count
no robustness-count

Syntax Description

| count | Value of the robustness count variable. Range is 2 to 10 packets. |

Command Default

Default is 2 packets.

Command Modes

IGMP VRF configuration
IGMP interface configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

IGMP is a soft-state protocol. State must be periodically refreshed or it times out. At a robustness-count command setting, for example, of 4, a network might lose three IGMP packets related to some specific state yet still maintain the state. If, however, a network lost more than three IGMP packets in the sequence, the state would time out. You might then consider changing the robustness-count setting to maintain state.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example illustrates the use of the robustness-count command:

```
RP/0/RSP0/CPU0:router(config)# configure
RP/0/RSP0/CPU0:router(config)# router igmp
RP/0/RSP0/CPU0:router(config-igmp)# robustness-count 2
```
**router**

To disable or enable Internet Group Management Protocol (IGMP) membership tracking, use the `router` command in the appropriate configuration mode. To return to the default behavior, use the `no` form of this command.

```
router {disable|enable}
no router {disable|enable}
```

**Syntax Description**
- `disable`  
  Turns off IGMP membership tracking.
- `enable`  
  Turns on IGMP membership tracking.

**Command Default**
If this command is not specified in IGMP VRF configuration mode, router functionality is enabled on all interfaces.

**Command Modes**
IGMP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `router` command is used to enable and disable the IGMP router functionality on a specific interface. For instance, IGMP stops queries from an interface when the router functionality is disabled on that interface. Disabling IGMP router functionality does not prevent local group membership from being announced through the group membership report.

**Note**
This command is useful if you want to disable or enable IGMP interfaces that have been previously enabled through the `multicast-routing` command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to enable IGMP membership tracking functionality on all multicast enabled interfaces, except Packet-over-SONET/SDH (POS) interface 0/1/0/0:

```
RP/0/RSP0/CPU0:router(config)# router igmp
RP/0/RSP0/CPU0:router(config-igmp)# interface gigabitEthernet 0/1/0/0
RP/0/RSP0/CPU0:router(config-igmp-default-if)# router enable
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast routing</td>
<td>Enables multicast routing and forwarding on all enabled interfaces of the router and enters multicast routing configuration mode.</td>
</tr>
</tbody>
</table>
**router igmp**

To enter Internet Group Management Protocol (IGMP) configuration mode, use the `router igmp` command in global configuration mode. To return to the default behavior, use the `no` form of this command.

```
router igmp
no router igmp
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

No default behavior or values

**Command Default**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

From IGMP VRF configuration mode, you can configure the maximum response time advertised in IGMP queries and modify the host query interval.

**Note**

The IGMP process is turned on when the `router igmp` command or the `multicast-routing` command is initiated.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enter IGMP configuration mode:

```
RP/0/RSP0/CPU0:router(config)# router igmp
RP/0/RSP0/CPU0:router(config-igmp)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface all disable</code></td>
<td>Disables IGMP membership tracking on all interfaces.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td><code>multicast routing</code></td>
<td>Enables multicast routing and forwarding on all enabled interfaces of the router and enters multicast routing configuration mode.</td>
</tr>
</tbody>
</table>
**show igmp groups**

To display the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP), use the `show igmp groups` command in EXEC mode.

```
show igmp [vrf vrf-name] groups [{group-address|type interface-path-id|not-active|summary}] [detail] [explicit]
```

**Syntax Description**

- `vrf vrf-name`: (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `group-address`: (Optional) Address or name of the multicast group. An address is a multicast IP address in four-part dotted-decimal notation. A name is as defined in the Domain Name System (DNS) hosts table.
- `type`: (Optional) Interface type. For more information, use the question mark (?) online help function.
- `interface-path-id`: (Optional) Displays group joinsthatarenotprocessed.
- `not-active`: (Optional) Displays the total number of (*, G) and (S, G) states in IGMP.
- `summary`: (Optional) Displays detail information such as IGMP Version 3 source list, host, and router mode.
- `detail`: (Optional) Displays explicit tracking information.
- `explicit`: (Optional) Displays explicit tracking information.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

- **Release** **Modification**
  - Release 3.7.2  This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
If you omit all optional arguments, the `show igmp groups` command displays (by group address and interface name) all the multicast memberships that the directly connected networks have subscribed.

### Examples

The following is sample output from the `show igmp groups` command on a specific (tenGigE) interface:

```
RP/0/RSP0/CPU0:router# show igmp groups tenGigE 0/4/0/0

IGMP Connected Group Membership
Group Address Interface Uptime Expires Last Reporter
224.0.0.2    TenGigE0/4/0/0       3w6d  never  10.114.8.44
224.0.0.5    TenGigE0/4/0/0       3w6d  never  10.114.8.44
224.0.0.6    TenGigE0/4/0/0       3w6d  never  10.114.8.44
224.0.0.13   TenGigE0/4/0/0       3w6d  never  10.114.8.44
224.0.0.22   TenGigE0/4/0/0       3w6d  never  10.114.8.44
```

This table describes the significant fields shown in the display.

### Table 1: `show igmp groups` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Address</td>
<td>Address of the multicast group.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface through which the group is reachable.</td>
</tr>
<tr>
<td>Uptime</td>
<td>How long (in hours, minutes, and seconds) this multicast group has been known.</td>
</tr>
<tr>
<td>Expires</td>
<td>How long (in hours, minutes, and seconds) until the entry is removed from the IGMP groups table.</td>
</tr>
<tr>
<td>Last Reporter</td>
<td>Last host to report being a member of the multicast group.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show igmp interface</code>, on page 35</td>
<td>Displays Internet Group Management Protocol (IGMP) multicast-related information about an interface.</td>
</tr>
</tbody>
</table>
**show igmp interface**

To display Internet Group Management Protocol (IGMP) multicast-related information about an interface, use the `show igmp interface` command in EXEC mode.

```
show igmp [vrf vrf-name] interface [{type interface-path-id|state-on|state-off}]
```

**Syntax Description**

- **vrf vrf-name** (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- **type** (Optional) Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id** (Optional) Either a physical interface or a virtual interface.
  
  **Note** Use the `show interfaces` command in EXEC mode to see a list of all interfaces currently configured on the router.
  
  For more information about the syntax for the router, use the question mark (?) online help function.
- **state-on** (Optional) Displays all interfaces with IGMP enabled.
- **state-off** (Optional) Displays all interfaces with IGMP disabled.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If you omit the optional arguments, the `show igmp interface` command displays information about all interfaces.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show igmp interface` command:

```
RP/0/RSP0/CPU0:router# show igmp interface
```
Loopback0 is up, line protocol is up
Internet address is 10.144.144.144/32
IGMP is enabled on interface
Current IGMP version is 3
IGMP query interval is 60 seconds
IGMP querier timeout is 125 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1 seconds
IGMP activity: 3 joins, 0 leaves
IGMP querying router is 10.144.144.144 (this system)
TenGigE0/4/0/0 is up, line protocol is up
Internet address is 10.114.8.44/24
IGMP is enabled on interface
Current IGMP version is 3
IGMP query interval is 60 seconds
IGMP querier timeout is 125 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1 seconds
IGMP activity: 9 joins, 4 leaves
IGMP querying router is 10.114.8.11
Bundle-Ether16.162 is up, line protocol is up
Internet address is 10.194.8.44/24
IGMP is enabled on interface
Bundle-Ether16.163 is up, line protocol is up
Internet address is 10.194.12.44/24
IGMP is disabled on interface
GigabitEthernet0/1/0/2 is up, line protocol is up
Internet address is 10.147.4.44/24
IGMP is enabled on interface
Current IGMP version is 3
IGMP query interval is 60 seconds
IGMP querier timeout is 125 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1 seconds
IGMP activity: 6 joins, 0 leaves
IGMP querying router is 10.147.4.44 (this system)
GigabitEthernet0/1/0/8 is up, line protocol is up
Internet address is 10.146.4.44/24
IGMP is enabled on interface
Current IGMP version is 3
IGMP query interval is 60 seconds
IGMP querier timeout is 125 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1 seconds
IGMP activity: 5 joins, 0 leaves
IGMP querying router is 10.146.4.44 (this system)
GigabitEthernet0/1/0/18 is up, line protocol is up
Internet address is 10.194.4.44/24
IGMP is enabled on interface
Current IGMP version is 3
IGMP query interval is 60 seconds
IGMP querier timeout is 125 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1 seconds
IGMP activity: 7 joins, 2 leaves
IGMP querying router is 10.194.4.19
GigabitEthernet0/1/0/23 is up, line protocol is up
Internet address is 10.114.4.44/24
IGMP is enabled on interface
Current IGMP version is 3
IGMP query interval is 60 seconds
IGMP querier timeout is 125 seconds
IGMP max query response time is 10 seconds
Last member query response interval is 1 seconds
IGMP activity: 9 joins, 4 leaves
IGMP querying router is 10.114.4.11
GigabitEthernet0/1/0/27 is up, line protocol is up
  Internet address is 10.145.4.44/24
  IGMP is enabled on interface
  Current IGMP version is 3
  IGMP query interval is 60 seconds
  IGMP querier timeout is 125 seconds
  IGMP max query response time is 10 seconds
  Last member query response interval is 1 seconds
IGMP activity: 7 joins, 2 leaves
IGMP querying router is 10.145.4.44 (this system)

This table describes the significant fields shown in the display.

Table 2: show igmp interface Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback0 is up, line protocol is up</td>
<td>Interface type, number, and status.</td>
</tr>
<tr>
<td>Internet address is</td>
<td>Internet address of the interface and subnet mask being applied to the interface, as specified with the address command.</td>
</tr>
<tr>
<td>IGMP is enabled on interface</td>
<td>Indicates whether IGMP router functionality has been enabled on the interface. Note Multicast protocols do not run on Management Ethernet interfaces even if they are enabled with the CLI.</td>
</tr>
<tr>
<td>IGMP query interval is 60 seconds</td>
<td>Interval at which the Cisco IOS XR software software sends Protocol Independent Multicast (PIM) query messages, as specified with the query-interval command.</td>
</tr>
<tr>
<td>IGMP querier timeout is...</td>
<td>Timeout that is set by nonquerier routers. When this timeout expires, the nonquerier routers begin to send queries.</td>
</tr>
<tr>
<td>IGMP max query response time is...</td>
<td>Query response time, in seconds, that is used by administrators to tune the burstiness of IGMP messages on the network. This is the maximum time within which a response to the query is received.</td>
</tr>
<tr>
<td>Last member query response is...</td>
<td>Query response time in seconds since a host replied to a query that was sent by the querier.</td>
</tr>
<tr>
<td>IGMP activity:</td>
<td>Total number of joins and total number of leaves received.</td>
</tr>
<tr>
<td>IGMP querying router is 239.122.41.51 (this system)</td>
<td>Indicates the elected querier on the link.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Sets a primary or secondary IP address for an interface.</td>
</tr>
<tr>
<td>query-interval, on page 22</td>
<td>Configures the frequency at which Cisco IOS XR software sends IGMP host-query messages.</td>
</tr>
</tbody>
</table>
### IGMP Commands on Cisco ASR 9000 Series Router

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>router, on page 29</td>
<td>Disables or enables IGMP membership tracking.</td>
</tr>
</tbody>
</table>
**show igmp nsf**

To display the state of the nonstop forwarding (NSF) operation in Internet Group Management Protocol (IGMP), use the `show igmp nsf` command in EXEC mode.

```
show igmp [vrf vrf-name] nsf
```

**Syntax Description**
- `old-output` (Optional) Displays the old show output—available for backward compatibility.
- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.

**Command Default**
No default behavior or values

**Command Modes**
EXEC

**Command History**
- Release 3.7.2 This command was introduced.

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `show igmp nsf` command displays the current multicast NSF state for IGMP. The NSF state that is displayed may be either normal or activated for NSF. The activated state indicates that recovery is in progress due to an IGMP failure. The total NSF timeout and time remaining are displayed until NSF expiration.

**Task ID**
```
Task ID Operations
multicast read
```

**Examples**
The following is sample output from the `show igmp nsf` command:

```
RP/0/RSP0/CPU0:router# show igmp nsf
IGMP_AFD
Non-Stop Forwarding Status: Multicast routing state: Normal

NSF Lifetime
: 00:01
:00
```
This table describes the significant fields shown in the display.

### Table 3: show igmp nsf Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast routing state</td>
<td>Multicast NSF status of IGMP (Normal or Non-Stop Forwarding Activated).</td>
</tr>
<tr>
<td>NSF Lifetime</td>
<td>Timeout for IGMP NSF. IGMP remains in the NSF state, recovering the IGMP route state through IGMP reports for this period of time, before making the transition back to the normal state and signaling the Multicast Routing Information Base (MRIB).</td>
</tr>
<tr>
<td>NSF Time Remaining</td>
<td>If IGMP NSF state is activated, the time remaining until IGMP reverts to Normal mode displays.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>nsf (multicast)</code></td>
<td>Enables NSF capability for the multicast routing system.</td>
</tr>
<tr>
<td><code>nsf lifetime (IGMP)</code>, on page 20</td>
<td>Configures the NSF timeout value for the IGMP or MLD process. Configures the NSF timeout value for the IGMP process.</td>
</tr>
<tr>
<td><code>nsf lifetime (PIM)</code></td>
<td>Configures the NSF timeout value for the PIM process.</td>
</tr>
<tr>
<td><code>show mfib nsf</code></td>
<td>Displays the state of NSF operation for the MFIB line cards.</td>
</tr>
<tr>
<td><code>show mrib nsf</code></td>
<td>Displays the state of NSF operation in the MRIB.</td>
</tr>
<tr>
<td><code>show pim nsf</code></td>
<td>Displays the state of NSF operation for PIM.</td>
</tr>
</tbody>
</table>
show igmp nsr

To display the nonstop routing (NSR) information in Internet Group Management Protocol (IGMP), use the show igmp nsr command in EXEC mode.

\[ \text{show igmp ipv4|ipv6 nsr} \]

**Syntax Description**
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `ipv6` (Optional) Specifies IPv6 address prefixes

**Command Default**
No default behavior or values

**Command Modes**
EXEC

**Command History**
- Release 5.2.2 This command was introduced.

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `show igmp nsr` command displays the current multicast NSR information for IGMP. The NSR state that is displayed may be either normal or activated for NSR. The activated state indicates that recovery is in progress due to an IGMP failure. The total NSR timeout and time remaining are displayed until NSR expiration.

**Task ID**
- **Task ID**
- **Operations**
  - multicast read

**Examples**
The following is sample output from the `show igmp nsr` command:

```
RP/0/RSP0/CPU0:router# show igmp nsr
IGMP NSR Data :
 NSR State : Not Ready (uptime 4w0d)
 Converged with collaborators : Y
 Partner connection state : Not-coverged/Down
 RMF Notif done : Y
 Last RMF ready notified : Never [0]
 Last RMF not ready notified : 4w0d [1]
 Last partner process conn up : Never [0]
 Last partner process conn down : Never [0]
```
This table describes the significant fields shown in the display.

### Table 4: show igmp nsr Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSR State</td>
<td>Multicast Non-Stop Routing State: Ready or Not Ready</td>
</tr>
<tr>
<td>Converged with collaborators</td>
<td>Yes or No</td>
</tr>
<tr>
<td>Partner connection state</td>
<td>Converged/Yes or Non-converged/No</td>
</tr>
<tr>
<td>RMF Notif done</td>
<td>RMF notification whether activated: Yes or No</td>
</tr>
<tr>
<td>Last RMF ready notified</td>
<td>The Time when the last RMF ready notification was received: Yes, No, or Never.</td>
</tr>
<tr>
<td></td>
<td>The number in the brackets indicate the number of times the RMF ready notification was received.</td>
</tr>
<tr>
<td>Last RMF not ready notified</td>
<td>The Time when the last RMF not ready notification was received: Yes, No, or Never.</td>
</tr>
<tr>
<td></td>
<td>The number in the brackets indicate the number of times the RMF ready notification was received.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show msdp nsr</td>
<td>Displays the state of NSR operation for MSDP.</td>
</tr>
<tr>
<td>show mrib nsr</td>
<td>Displays the state of NSR operation in MRIB.</td>
</tr>
<tr>
<td>show pim nsr</td>
<td>Displays the state of NSR operation for PIM.</td>
</tr>
</tbody>
</table>
show igmp summary

To display group membership information for Internet Group Management Protocol (IGMP), use the `show igmp summary` command in EXEC mode.

```
show igmp [vrf vrf-name] summary
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>old-output</code></td>
<td>(Optional) Displays the old show output—available for backward compatibility.</td>
</tr>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Specifies a VPN routing and forwarding (VRF) instance.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `show igmp summary` command is used to display the total group membership. The value for number of groups is the total number of group members on all interfaces. The value for maximum number of groups is the total number of external and local members possible for all interfaces. The maximum number of groups and the default value for the maximum number of groups is 50000 members. The maximum number of groups for each interface, and the default value for the maximum number of groups for each interface, is 25000 members.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows the number of groups for each interface that are IGMP members and the maximum number of groups that can become members on each interface:

```
RP/0/RSP0/CPU0:router# show igmp summary

IGMP summary
Robustness Value 2
No. of Group x Interfaces 61
Maximum number of Group x Interfaces 65

Supported Interfaces : 18
Unsupported Interfaces : 2
Enabled Interfaces : 18
```
show igmp summary

Disabled Interfaces : 2

<table>
<thead>
<tr>
<th>Interface</th>
<th>Grp No</th>
<th>Max Grp No</th>
<th>Bundle-Ether28.1</th>
<th>3</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>MgmtEth0/RSP0/CPU0/0</td>
<td>0</td>
<td>5</td>
<td>Loopback0</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>MgmtEth0/RP1/CPU0/0</td>
<td>0</td>
<td>5</td>
<td>Bundle-Ether28</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Bundle-Ether28</td>
<td>3</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bundle-Ether28.1</td>
<td>3</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bundle-Ether28.2</td>
<td>3</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bundle-Ether28.3</td>
<td>3</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MgmtEth0/RP1/CPU0/0</td>
<td>0</td>
<td>5</td>
<td>GigabitEthernet0/1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GigabitEthernet0/1</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GigabitEthernet0</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GigabitEthernet0/1</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GigabitEthernet0</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GigabitEthernet0/1</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>GigabitEthernet0</td>
<td>3</td>
<td>5</td>
</tr>
</tbody>
</table>
This table describes the significant fields shown in the display.

**Table 5: show igmp summary Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of Group x Interfaces</td>
<td>Number of multicast groups that are joined through the interface.</td>
</tr>
<tr>
<td>Maximum number of Group x Interfaces</td>
<td>Maximum number of multicast groups that can be joined through the interface.</td>
</tr>
<tr>
<td>Supported Interfaces</td>
<td>Interfaces through which the multicast groups are reachable.</td>
</tr>
<tr>
<td>Unsupported Interfaces</td>
<td>Number of unsupported interfaces.</td>
</tr>
<tr>
<td>Enabled Interfaces</td>
<td>Number of enabled interfaces.</td>
</tr>
<tr>
<td>Disabled Interfaces</td>
<td>Number of disabled interfaces.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show igmp groups, on page 33</td>
<td>Displays the multicast groups that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP).</td>
</tr>
</tbody>
</table>
show igmp ssm map

To query the source-specific mapping (SSM) state, use the show igmp ssm map command in EXEC mode.

```
show igmp [vrf vrf-name] ssm map [group-address] [detail]
```

**Syntax Description**

- **vrf** (Optional) Specifies a VPN routing and forwarding (VRF) instance to be queried.
- **vrf-name** (Optional) Specifies the name of the specific VRF instance.
- **group-address** (Optional) Specifies the address of the SSM group for which to obtain the mapping state.
- **detail** (Optional) Displays detailed source information.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following example illustrates the use of the show igmp ssm map command:

```
RP/0/RSP0/CPU0:router# show igmp ssm map 232.1.1.1

232.1.1.1 is static with 1 source
```
show igmp traffic

To display all the Internet Group Management Protocol (IGMP) traffic-related counters, use the `show igmp traffic` command in EXEC mode.

```
show igmp [vrf vrf-name] traffic
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `show igmp traffic` command is used to display the state of all counters for IGMP traffic. It gives information about the length of time the counters have been active and the count of different types of IGMP packets received, such as queries, leaves, and reports. Also, this command keeps a count of all the erroneous IGMP packets received.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show igmp traffic` command:

```
RP/0/RSP0/CPU0:router# show igmp traffic
IGMP Traffic Counters
Elapsed time since counters cleared: 15:27:38

Received  Sent
Valid IGMP Packet 2784 5576
Queries 0 2784
Reports 2784 2792
Leaves 0 0
Mtrace packets 0 0
DVMRP packets 0 0
PIM packets 0 0

Errors:
Malformed Packets 0
Bad Checksums 0
```
This table describes the significant fields shown in the display for the `show igmp traffic` command.

### Table 6: show igmp traffic Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid IGMP Packet</td>
<td>Total number of valid protocol packets sent and received. Valid packet types include:</td>
</tr>
<tr>
<td></td>
<td>- Queries</td>
</tr>
<tr>
<td></td>
<td>- Membership reports</td>
</tr>
<tr>
<td></td>
<td>- Leaves</td>
</tr>
<tr>
<td>Queries</td>
<td>Total number of query packets sent and received. IP Multicast routers send queries to determine the multicast reception state of neighboring interfaces.</td>
</tr>
<tr>
<td>Reports</td>
<td>Total number of membership report packets received. Membership reports indicate either the current multicast reception state of a neighboring interface or a change to that state.</td>
</tr>
<tr>
<td>Leaves</td>
<td>Total number of leaves received. A leave group packet indicates a neighboring interface no longer has multicast reception state for a particular group.</td>
</tr>
<tr>
<td>Mtrace packets</td>
<td>Total number of Mtrace packets sent and received. Mtrace traces the route from a receiver to a source using a particular multicast address.</td>
</tr>
<tr>
<td>DVMRP packets</td>
<td>Total number of Distance Vector Multicast Routing Protocol (DVMRP) packets sent and received. DVMRP is an Internet routing protocol that provides a mechanism for connectionless datagram delivery to a group of hosts across an internetwork. This protocol dynamically generates IP multicast delivery trees using Reverse Path Multicasting. Packet type 0x13 indicates a DVMRP packet.</td>
</tr>
<tr>
<td>PIM packets</td>
<td>Total number of sent and received Protocol Independent Multicast (PIM) packets.</td>
</tr>
<tr>
<td>Malformed Packets</td>
<td>Total number of malformed packets received. A malformed packet is a packet smaller than the smallest valid protocol packet.</td>
</tr>
<tr>
<td>Bad Checksums</td>
<td>Total number of packets received with a bad protocol header checksum.</td>
</tr>
<tr>
<td>Socket Errors</td>
<td>Total number of read and write failures on the protocol socket.</td>
</tr>
<tr>
<td>Bad Scope Errors</td>
<td>Total number of packets received with an invalid multicast scope.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> IGMP has no invalid scopes; this counter, therefore, never increments in IGMP.</td>
</tr>
<tr>
<td>Auxiliary Data Len Errors</td>
<td>Total number of packets received with a non-zero auxiliary data length.</td>
</tr>
</tbody>
</table>
### Subnet Errors

Total number of packets received that were not sourced on the same subnet as the router.

DVMRP and MTRACE packets received are not checked for this error as they may be validly sourced from a different subnet.

### Packets dropped due to invalid socket

Total number of packets dropped due to an invalid socket.

### Packets which couldn’t be accessed

Total number of packets that could not be sent or received. This might occur if:

- Packet buffer does not form a valid protocol packet.
- IP header is not written to the packet.
- Outgoing packet interface handle was not set.
- Errors occurred calculating the protocol checksum.

### Other Packet Drops

Packets dropped for any other reason.

---

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show pim traffic</td>
<td>Displays PIM traffic counter information.</td>
</tr>
</tbody>
</table>
ssm map

To map group memberships from legacy hosts in Source-Specific Multicast (SSM) groups accepted by an access control list (ACL) to a Protocol Independent Multicast (PIM)-SSM source or to configure DNS mapping for PIM-SSM sources to a set of SSM groups, use the `ssm map` command in the appropriate configuration mode. To revert to default behavior, use the `no` form of this command.

```
ssm map { static source-address access-list | query dns }
no ssm map { static source-address access-list | query dns }
```

**Syntax Description**

- `source-address`  PIM-SSM source address to be used to create a static mapping.
- `access-list`  ACL specifying the groups to be used to create a static mapping.
- `query`  Configure a mapping of sources to groups querying external database.
- `dns`  Configure a DNS mapping for sources to a set of SSM groups.

**Command Default**

Legacy host membership reports in the SSM group range are discarded and DNS-based SSM mapping is not enabled.

**Command Modes**

IGMP VRF configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 5.3.2</td>
<td>The keywords &quot;query&quot; and &quot;DNS&quot; were introduced to configure DNS-based SSM mapping.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

PIM-SSM requires the use of IGMPv3 (IPv4) to determine local memberships. Under normal operating conditions, IGMP discards older version group membership reports for groups in the SSM group range. This means that a host with a legacy group membership protocol is unable to receive data from a PIM-SSM source.

The `ssm map static` command maps an older group membership report to a set of PIM-SSM sources. If the ACL associated with a configured source accepts the SSM group, then that source is included in its set of sources for the SSM group.

**Examples**

The following example shows PIM-SSM mapping in IGMP routing configuration mode:

```
RP/0/RSP0/CPU0:router(config)# configuration
```
RP/0/RSP0/CPU0:router(config)# **router igmp**
RP/0/RSP0/CPU0:router(config-igmp)# **ssm map static 10.0.0.1 mc2**
RP/0/RSP0/CPU0:router(config-igmp)#

Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference, Release 5.3.x
static-group

To configure the router to be a statically configured member of the specified group on the interface, or to statically forward for a multicast group onto the interface, use the `static-group` command in the appropriate configuration mode. To return to the default behavior, use the `no` form of this command.

`static-group`  
`group-address`  
`[inc-mask mask count cnt]`  
`[source-address [inc-mask mask count cnt]]`

`no static-group`  
`group-address`  
`[inc-mask mask count cnt]`  
`[source-address [inc-mask mask count cnt]]`

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>group-address</th>
<th>IP address of the multicast group in IPv4 prefixing format:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>• IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format A.B.C.D.</td>
</tr>
<tr>
<td></td>
<td>inc-mask mask</td>
<td>(Optional) Specifies a mask for the increment range. This is an IP address expressed range in IPv4 format. This mask is used with the group address to generate subsequent group addresses:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format A.B.C.D.</td>
</tr>
<tr>
<td></td>
<td>count cnt</td>
<td>(Optional) Specifies a number of group addresses to generate using the increment mask. Range is 1 to 512.</td>
</tr>
<tr>
<td></td>
<td>source address</td>
<td>(Optional) Source address of the multicast group to include in IPv4 prefixing format:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• IP address as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format A.B.C.D.</td>
</tr>
</tbody>
</table>

| Command Default | A router is not a statically connected member of an IP multicast group. |
| Command Modes | IGMP interface configuration |
| Command History | Release 3.7.2 This command was introduced. |

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When you configure the `static-group` command, packets to the group are switched out the interface, provided that packets were received on the correct Reverse Path Forwarding (RPF) interface.

The `static-group` command differs from the `join-group` command. The `join-group` command allows the router to join the multicast group and draw traffic to an IP client process (that is, the route processor). If you
configure both the `join-group` and `static-group` command for the same group address, the `join-group` command takes precedence and the group behaves like a locally joined group.

**Note**
The `static-group` command has no impact on system performance. Configuring a static-group on a loopback interface has no effect on the ASR 9000 Series Aggregation Services Router.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast read, write</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

In the following example, the router statically joins two multicast groups 225.2.2.2 and 225.2.2.4 for the specific source 1.1.1.1:

```
RP/0/RSP0/CPU0:router(config)# router igmp
RP/0/RSP0/CPU0:router(config-igmp)# interface GigE 0/1/0/0
RP/0/RSP0/CPU0:router(config-igmp-default-if)# static-group 225.2.2.2 inc-mask 0.0.0.2 count 2 1.1.1.1
```
version

To configure an Internet Group Management Protocol (IGMP) version for the router, use the `version` command in the appropriate configuration mode. To restore the default value, use the `no` form of this command.

```
version \{1|2|3\}
no version
```

**Syntax Description**


**Command Default**

If this command is not specified in interface configuration mode, the interface adopts the IGMP version parameter specified in IGMP VRF configuration mode.

If this command is not specified in IGMP configuration mode, IGMP uses Version 3.

**Command Modes**

IGMP configuration

IGMP VRF configuration

IGMP interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

All routers on the subnet must be configured with the same version of IGMP. For example, a router running Cisco IOS XR software does not automatically detect Version 1 systems and switch to Version 1. Hosts can have any IGMP version and the router will correctly detect their presence and query them appropriately.

The `query-max-response-time` and `query-timeout` commands require IGMP Version 2 or 3.

**Note**

If you configure this command in IGMP configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces from interface configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>
The following example shows how to configure the router to use IGMP Version 3:

```
RP/0/RSP0/CPU0:router(config)# router igmp
RP/0/RSP0/CPU0:router(config-igmp)# version 3
```
vrf (igmp)

To configure a virtual private network (VRF) instance, use the `vrf` command in IGMP routing configuration mode. To remove the VRF instance from the configuration file and restore the system to its default condition, use the `no` form of this command.

```
vrf vrf-name
no vrf vrf-name
```

**Syntax Description**

| vrf-name | Name of the VRF instance. |

**Command Default**

No default behavior or values.

**Command Modes**

IGMP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When you use the `vrf` command from the IGMP routing configuration mode to configure a VRF instance, you enter the IGMP VRF configuration submode.

A VRF instance is a collection of VPN routing and forwarding tables maintained at the provider edge (PE) router.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a VRF instance in IGMP configuration submode and to enter VRF configuration submode:

```
RP/0/RSP0/CPU0:router(config)# router igmp
RP/0/RSP0/CPU0:router(config-igmp)# vrf
vrf_1
RP/0/RSP0/CPU0:router(config-igmp-vrf_1)#
```
Multicast Source Discovery Protocol Commands

This chapter describes the commands used to configure and monitor the Multicast Source Discovery Protocol (MSDP) on the Cisco ASR 9000 Series Router.

For detailed information about multicast routing concepts, configuration tasks, and examples, refer to the Implementing Multicast Routing on the Cisco ASR 9000 Series Router configuration module in Multicast Configuration Guide for Cisco ASR 9000 Series Routers.

- cache-sa holdtime, on page 58
- cache-sa-state, on page 59
- clear msdp peer, on page 61
- clear msdp sa-cache, on page 62
- clear msdp stats, on page 64
- connect-source, on page 65
- default-peer, on page 67
- description (peer), on page 68
- global maximum external-sa, on page 69
- maximum external-sa, on page 70
- maximum peer-external-sa, on page 72
- mesh-group (peer), on page 74
- originator-id, on page 75
- password (peer), on page 76
- peer (MSDP), on page 78
- remote-as (multicast), on page 79
- sa-filter, on page 80
- show msdp globals, on page 82
- show msdp peer, on page 84
- show msdp rpf, on page 86
- show msdp nsr, on page 88
- show msdp sa-cache, on page 89
- show msdp statistics peer, on page 93
- show msdp summary, on page 95
- show msdp vrf context, on page 97
- shutdown (MSDP), on page 99
- ttl-threshold (MSDP), on page 100
cache-sa holdtime

To configure the cache source-active (SA) state hold-time period on a router, use the `cache-sa-holdtime` command in MSDP configuration mode. To return to the default behavior, use the `no` form of this command.

**Syntax**

```
cache-sa-holdtime  holdtime-number
no cache-sa-holdtime  holdtime-number
```

**Syntax Description**

- `holdtime-number`  Hold-time period (in seconds). Range is 150 to 3600.

**Command Default**

`holdtime-number`  : 150 seconds

**Command Modes**

- MSDP configuration

**Command History**

- **Release** 3.7.2  This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `cache-sa-holdtime` command is used to increase the cache SA state hold time. Any cache entry that is created usually expires after 150 seconds. For troubleshooting purposes, you may need Multicast Source Discovery Protocol (MSDP) to keep SA cache entries for a longer period.

**Task ID**

- Task ID  Operations
  - multicast  read, write

**Examples**

The following example shows how to set the cache SA state hold-time period to 200 seconds:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router
msdp
RP/0/RSP0/CPU0:router(config-msdp)# cache-sa-holdtime
200
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cache-sa-state, on page 59</td>
<td>Controls cache source-active (SA) state on a router.</td>
</tr>
</tbody>
</table>
cache-sa-state

To control cache source-active (SA) state on a router, use the `cache-sa-state` command in MSDP configuration mode. To return to the default behavior, use the `no` form of this command.

```
cache-sa-state {list access-list-number|rp-list access-list-name}
no cache-sa-state {list access-list-number|rp-list access-list-name}
```

**Syntax Description**
- `list access-list-number` Specifies an IP access list that defines which (S, G) pairs to cache.
- `rp-list access-list-name` Specifies an access list name for the originating rendezvous point (RP).

**Command Default**
The router creates SA state.

**Command Modes**
MSDP configuration

**Command History**
- **Release 3.7.2** This command was introduced.

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When a new member joins a group immediately after an SA message arrives, latency may occur and an SA message may be missed. To overcome this problem, you can configure this command and the router will supply SA information (from cache memory) to the new member instead of requiring that the member wait until the next SA message is received.

The `cache-sa-state` command is required in every Multicast Source Discovery Protocol (MSDP) speaker, to cache SA messages received from peers.

**Examples**
The following example shows how to configure the cache state for all sources in 10.0.0.0/16 sending to groups 224.2.0.0/16:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# MSDP
RP/0/RSP0/CPU0:router(config-madp)# cache-sa-state list 100
RP/0/RSP0/CPU0:router(config-madp)# exit
RP/0/RSP0/CPU0:router(config)# ipv4
access-list 100 permit 10.0.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```
The source and destination fields in the access list matches on the (S,G) fields in the SA messages. We recommend that the first address and mask field in the access list is used for the source and the second field in the access list is used for the group or destination.

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show msdp sa-cache</code>, on page 89</td>
<td>Displays the (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers.</td>
</tr>
</tbody>
</table>
clear msdp peer

To clear the TCP connection of the specified Multicast Source Discovery Protocol (MSDP) peer, use the `clear msdp peer` command in EXEC mode.

```
clear msdp [ipv4] peer peer-address
```

**Syntax Description**

- **ipv4** (Optional) Specifies IPv4 address prefixes.
- **peer-address** IPv4 address or hostname of the MSDP peer to which the TCP connection is cleared.

**Command Default**
IPv4 addressing is the default.

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `clear msdp peer` command closes the TCP connection to the MSDP peer, resets all the MSDP peer statistics, and clears the input and output queues to and from the MSDP peer.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear the TCP connection of the MSDP peer at address 224.15.9.8:

```
RP/0/RSP0/CPU0:router# clear msdp peer 224.15.9.8
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer (MSDP), on page 78</td>
<td>Configures a Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
</tbody>
</table>
clear msdp sa-cache

to clear external Multicast Source Discovery Protocol (MSDP) source-active (SA) cache entries, use the clear msdp sa-cache command in EXEC mode.

clear msdp [ipv4] sa-cache [group-address]

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ipv4</strong></td>
<td>(Optional) Specifies IPv4 address prefixes.</td>
</tr>
<tr>
<td><strong>group-address</strong></td>
<td>(Optional) Multicast group address or name for which external SA entries are cleared from the SA cache.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Note**

SA caching is enabled by default on Cisco IOS XR software.

If you do not specify a multicast group by group address or group name with the group-address argument, the clear msdp sa-cache command clears all external SA cache entries.

**Note**

Local SA cache entries can be cleared using the clear pim topology command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear the external SA entries for the multicast group at address 224.5.6.7 from the cache:
clear msdp sa-cache

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show msdp sa-cache, on page 89</td>
<td>Displays the (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers.</td>
</tr>
</tbody>
</table>
clear msdp stats

To reset Multicast Source Discovery Protocol (MSDP) peer statistic counters, use the `clear msdp stats` command in EXEC mode.

```
clear msdp [ipv4] stats [peer peer-address] [allvalues]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IPv4 address prefixes.</td>
</tr>
<tr>
<td>peer peer-address</td>
<td>(Optional) Clears MSDP peer statistic counters for the specified IPv6 MSDP peer address or peer name.</td>
</tr>
<tr>
<td>allvalues</td>
<td>(Optional) Clears all statistic counters for all MSDP peers.</td>
</tr>
</tbody>
</table>

| Command Default                  | No default behavior or values                                              |
| Command Modes                    | EXEC                                                                        |
| Command History                  | Release 3.7.2  This command was introduced.                                |

| Usage Guidelines                 | To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance. |

The `clear msdp stats` command resets MSDP peer statistic counters such as the number of keepalives sent and received and the number of Source Active (SA) entries sent and received.

If you do not specify an MSDP peer with the `peer` keyword and `peer-address` argument, this command clears statistic counters for all MSDP peers.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID  Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>multicast execute</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Examples</th>
<th>The following example shows how to clear all statistics for all peers:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>RP/0/RSP0/CPU0:router# clear msdp stats peer 224.0.1.1</code></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show msdp statistics peer, on page 93</td>
<td>Displays Multicast Source Discovery Protocol (MSDP) peer statistic counters.</td>
</tr>
</tbody>
</table>
connect-source

To configure a source address used for a Multicast Source Discovery Protocol (MSDP) connection, use the `connect-source` command in the appropriate configuration mode. To return to the default behavior, use the `no` form of this command.

`connect-source type [interface-path-id]`
`no connect-source type [interface-path-id]`

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>type</code></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>(Optional) Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

| Note | Use the `show interfaces` command in EXEC mode to see a list of all interfaces currently configured on the router. |

For more information about the syntax for the router, use the question mark (?) online help function.

Command Default

If a source address is not configured for the MSDP connection, the IP address of the interface toward the peer is used as a source address.

Command Modes

- MSDP configuration
- MSDP peer configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `connect-source` command:

- Specifies the interface type and path ID whose primary address becomes the source IP address for the TCP connection.
- Is recommended for MSDP peers that peer with a router inside the remote domain.
- Can be configured globally for MSDP (and is inheritable by MSDP peers). This global configuration can be overridden if the command is issued again in peer configuration mode.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to configure a loopback interface source address for an MSDP connection:
RP/0/RSP0/CPU0:router(config)# interface loopback 0
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 10.1.1.1/24
RP/0/RSP0/CPU0:router(config-if)# exit
RP/0/RSP0/CPU0:router(config)# router msdp
RP/0/RSP0/CPU0:router(config-msdp)# connect-source loopback 0
default-peer

To define a default peer from which to accept all Multicast Source Discovery Protocol (MSDP) source-active (SA) messages, use the `default-peer` command in MSDP configuration mode. To return to the default behavior, use the `no` form of this command.

```
default-peer ip-address
no default-peer
```

### Syntax Description

- **ip-address**: IP address or Domain Name System (DNS) name of the MSDP default peer.

### Command Default

No default MSDP peer exists.

### Command Modes

MSDP configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

A default peer configuration accepts all MSDP Source-Active (SA) messages, as a last Reverse Path Forwarding (RPF) rule, when all other MSDP RPF rules fail.

Use the `default-peer` command if you do not want to configure your MSDP peer to be a BGP peer also.

When the `prefix-list list` keyword and argument are not specified, all SA messages received from the configured default peer are accepted.

Remember to configure a BGP prefix list to configure the `prefix-list list` keyword and argument with the `default-peer` command.

### Examples

The following example shows how to configure the router 172.16.12.0 as the default peer to the local router:

```
RP/0/RSP0/CPU0:router(config)# router msdp
RP/0/RSP0/CPU0:router(config-msdp)# default-peer 172.16.12.0
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>peer (MSDP)</code>, on page 78</td>
<td>Configures a Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
</tbody>
</table>
description (peer)

To add descriptive text to the configuration for a Multicast Source Discovery Protocol (MSDP) peer, use the `description` command in peer configuration mode. To return to the default behavior, use the `no` form of this command.

```
description peer-address text
no description peer-address text
```

**Syntax Description**

- `peer-address`: IP address or hostname for the peer to which this description applies.
- `text`: Description of the MSDP peer. Use up to 80 characters to describe this peer.

**Command Default**

No description is associated with an MSDP peer.

**Command Modes**

MSDP peer configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Configure a description to make the MSDP peer easier to identify. This description is visible in the `show msdp peer` command output.

**Examples**

The following example shows how to configure the router at the IP address 10.0.5.4 with a description indicating that it is a router at customer site A:

```
RP/0/RSP0/CPU0:router(config)# router msdp
RP/0/RSP0/CPU0:router(config-msdp)# peer 10.0.5.4
RP/0/RSP0/CPU0:router(config-msdp-peer)# description 10.0.5.4 router_at_customer_site_A
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer (MSDP), on page 78</td>
<td>Configures a Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
<tr>
<td>show msdp peer, on page 84</td>
<td>Displays information about the Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
</tbody>
</table>
**global maximum external-sa**

To limit the total number of source active (SA) messages across all VRFs, use the `global maximum external-sa` command in the MSDP configuration mode. To remove the set SA messages limit use the `no` form of the command.

```
global maximum external-sa  value
no global maximum external-sa
```

**Syntax Description**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>value</strong></td>
<td>Specifies the maximum-limit for the source active messages. Range is 1 to 75000.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

MSDP configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The value configured using the `global maximum external-sa` command must be greater than the maximum value of any VRF, which, in turn, must be greater than the maximum value of any peer in that VRF. When the set limit is reached, a syslog message is issued.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

This example shows the maximum-limit value for the source active messages, set to 100:

```
RP/0/RSP0/CPU0:router (config-masd) # global maximum external-sa 100
```
**maximum external-sa**

To configure the maximum number of external Multicast Source Discovery Protocol (MSDP) source-active (SA) entries that can be learned by the router or by a specific MSDP peer, use the `maximum external-sa` command in the appropriate configuration mode. To return to the default behavior, use the `no` form of this command.

```plaintext
maximum external-sa entries
no maximum external-sa
```

**Syntax Description**

- `entries` Maximum number of SA entries that can be learned by the router or a specific MSDP peer. Range is 1 to 75000.

**Command Default**

- `entries : 20000`

**Command Modes**

- MSDP peer configuration
- MSDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When issued from MSDP configuration mode, the `maximum external-sa` command configures the total number of external SA entries (that is, the total cumulative SA state for all peers) that can be learned by the router. This command is used to control router resource utilization under heavy traffic conditions.

**Note**

The configuration fails if you configure the maximum number of external SA entries to be lower than the current accumulated SA state.

When issued from MSDP peer configuration mode, the `maximum external-sa` command configures the total number of external SA entries that can be learned by a specific MSDP peer. From MSDP configuration mode, this command can also be used to configure a specific MSPD peer to override the maximum external SA entry value configured with the `maximum peer-external-sa` command.

**Note**

The configuration fails if you configure the maximum number of external SA entries for a specific MSDP peer to be higher than the maximum number of external SA entries that can be learned by the router.
### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

This example shows how to configure the maximum number of external SA entries that can be learned by the router to 30000 SA entries:

```
RP/0/RSP0/CPU0:router(config)# router msdp
RP/0/RSP0/CPU0:router(config-msdp)# maximum external-sa 30000
```

This example shows how to configure the maximum number of external SA entries that can be learned by the MSDP peer at address 10.1.5.3 to 25000 SA entries:

```
RP/0/RSP0/CPU0:router(config)# router msdp
RP/0/RSP0/CPU0:router(config-msdp)# peer 10.1.5.3
RP/0/RSP0/CPU0:router(config-msdp-peer)# maximum external-sa 25000
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maximum peer-external-sa, on page 72</td>
<td>Configures the maximum number of external Multicast Source Discovery Protocol (MSDP) Source-Active (SA) entries that can be learned from MSDP peers.</td>
</tr>
<tr>
<td>show msp summary, on page 95</td>
<td>Displays Multicast Source Discovery Protocol (MSDP) peer status.</td>
</tr>
</tbody>
</table>
# maximum peer-external-sa

To configure the maximum number of external Multicast Source Discovery Protocol (MSDP) Source-Active (SA) entries that can be learned from MSDP peers, use the `maximum peer-external-sa` command in MSDP configuration mode. To return to the default behavior, use the `no` form of this command.

```plaintext
maximum peer-external-sa entries
no maximum peer-external-sa
```

## Syntax Description

| entries | Maximum number of SA entries to be learned by MSDP peers. Range is 1 to 75000. |

## Command Default

`entries : 20000`

## Command Modes

MSDP configuration

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `maximum peer-external-sa` command configures the maximum number of external SA entries that can be learned for each configured MSDP peer, whereas the `maximum external-sa` command (in MSDP configuration mode) configures the maximum number of SA entries accepted by the router as a cumulative total.

## Note

The configuration fails if you attempt to configure the maximum number of external SA entries for MSDP peers to be higher than the maximum number of external SA entries that can be learned by the router.

## Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

## Examples

This example shows how to configure the maximum number of external SA entries that each MSDP peer can learn to 27000 SA entries:
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>maximum external-sa, on page 70</td>
<td>Configures the maximum number of external Multicast Source Discovery Protocol (MSDP) source-active (SA) entries that can be learned by the router or by a specific MSDP peer.</td>
</tr>
<tr>
<td>show msdp summary, on page 95</td>
<td>Displays Multicast Source Discovery Protocol (MSDP) peer status.</td>
</tr>
</tbody>
</table>
**mesh-group (peer)**

To configure a Multicast Source Discovery Protocol (MSDP) peer to be a member of a mesh group, use the `mesh-group` command in peer configuration mode. To return to the default behavior, use the *no* form of this command.

```
mesh-group name
no mesh-group name
```

**Syntax Description**

- `name` Name of the mesh group.

**Command Default**

MSDP peers do not belong to a mesh group.

**Command Modes**

MSDP peer configuration

**Command History**

- **Release** Modification
  - Release 3.7.2 This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

A mesh group is a group of MSDP speakers that have fully meshed MSDP connectivity among themselves. Any Source-Active (SA) messages received from a peer in a mesh group are not forwarded to other peers in the same mesh group.

Mesh groups can be used to:

- Reduce SA message flooding
- Simplify peer Reverse Path Forwarding (RPF) flooding (no need to run Border Gateway Protocol [BGP] among MSDP peers)

**Task ID**

**Task ID** | **Operations**
---|---
multicast | read, write

**Examples**

The following example shows how to configure the MSDP peer at address 10.0.5.4 to be a member of the mesh group named internal:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router msdp
RP/0/RSP0/CPU0:router(config-msdp)# peer 10.0.5.4
RP/0/RSP0/CPU0:router(config-msdp-peer)# mesh-group internal
```
originator-id

To identify an interface type and instance to be used as the rendezvous point (RP) address in a Multicast Source Discovery Protocol (MSDP) Source-Active (SA) message, use the **originator-id** command in MSDP configuration mode. To return to the default behavior, use the **no** form of this command.

```
originator-id type interface-path-id
no originator-id type interface-path-id
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>type</strong></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><strong>interface-path-id</strong></td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note:** Use the **show interfaces** command in EXEC mode to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

### Command Default

The RP address is used as the originator ID.

### Command Modes

MSDP configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **originator-id** command allows an MSDP speaker that originates an SA message to use the IP address of the interface as the RP address in the SA message.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to configure Gigabit Ethernet interface 0/1/1/0 to be used as the RP address in SA messages:

```
RP/0/RSP0/CPU0:router(config)# router msdp
RP/0/RSP0/CPU0:router(config-msdp)# originator-id GigE0/1/1/0
```
**password (peer)**

To enable Message Digest 5 (MD5) authentication on a TCP connection between two Multicast Source Discovery Protocol (MSDP) peers, use the `password` command in MSDP peer configuration mode. To return to the default behavior, use the `no` form of this command.

```
password {clear|encrypted} password
no password {clear|encrypted} password
```

**Syntax Description**

- **clear** Specifies that an unencrypted password follows. The password must be a case-sensitive, clear-text unencrypted password.
- **encrypted** Specifies that an encrypted password follows. The password must be a case-sensitive, encrypted password.
- **password** Password of up to 80 characters. The password can contain any alphanumeric characters. However, if the first character is a number or the password contains a space, the password must be enclosed in double quotation marks; for example, “2 password.”

**Command Default**

No password is configured.

**Command Modes**

MSDP peer configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `password` command supports MD5 signature protection on a TCP connection between two MSDP peers. When MD5 authentication is enabled between two MSDP peers, each segment sent on the TCP connection between the peers is verified. MD5 authentication must be configured with the same password on both MSDP peers; otherwise, the connection between them is not made. Configuring MD5 authentication causes the Cisco IOS XR software to generate and verify the MD5 digest of every segment sent on the TCP connection.

Use the `show msdp peer` command to check if a password has been configured on a peer.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the MSDP password on a peer:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router msdp
```
RP/0/RSP0/CPU0:router(config-msdp)# peer 10.0.5.4
RP/0/RSP0/CPU0:router(config-msdp-peer)# password encrypted a34bi5m

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show msdp peer, on page 84</td>
<td>Displays information about the Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
</tbody>
</table>
peer (MSDP)

To configure a Multicast Source Discovery Protocol (MSDP) peer, use the `peer` command in MSDP configuration mode. To return to the default behavior, use the `no` form of this command.

```
peer peer-address
no peer peer-address
```

**Syntax Description**
- `peer-address`: IP address or Domain Name System (DNS) name of the router that is to be the MSDP peer.

**Command Default**
No MSDP peer is configured.

**Command Modes**
MSDP configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Configure the specified router as a Border Gateway Protocol (BGP) neighbor.

If you are also BGP peering with this MSDP peer, use the same IP address for MSDP as you do for BGP. However, you are not required to run BGP with the MSDP peer, as long as there is a BGP path between the MSDP peers. If there is no path, you must configure the `default-peer` command from MSDP configuration mode.

**Task ID**
- Task ID: Operations
  - multicast: read,
  - write

**Examples**
The following example shows how to configure the router at the IP address 172.16.1.2 as an MSDP peer to the local router and enter MSDP peer configuration mode:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# router msdp
RP/0/RSP0/CPU0:router(config-msdp)# peer 172.16.1.2
RP/0/RSP0/CPU0:router(config-msdp-peer)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>default-peer</code>, on page 67</td>
<td>Defines a default peer from which to accept all Multicast Source Discovery Protocol (MSDP) source-active (SA) messages.</td>
</tr>
</tbody>
</table>
## remote-as (multicast)

To configure the remote autonomous system number of this peer, use the `remote-as` command in peer configuration mode. To return to the default behavior, use the `no` form of this command.

```
remote-as  as-number
no remote-as  as-number
```

### Syntax Description

| as-number | Autonomous system number of this peer. Range for 2-byte numbers is 1 to 65535. Range for 4-byte numbers is 1.0 to 65535.65535. |

### Command Default

If this command is not issued during peer configuration, the remote autonomous system value is derived from BGP (if also configured) or initialized to zero, when only Interior Gateway Protocol (IGP) is present.

### Command Modes

MSDP peer configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `remote-as` command to configure remote autonomous system if deriving the autonomous system value from the configured Border Gateway Protocol (BGP) is not required.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to set the autonomous system number for the specified peer to 250:

```
RP/0/RSP0/CPU0:router(config)# router msdp
RP/0/RSP0/CPU0:router(config-msdp)# peer 172.16.5.4
RP/0/RSP0/CPU0:router(config-msdp-peer)# remote-as 250
```
To configure an incoming or outgoing filter list for Source-Active (SA) messages received from the specified Multicast Source Discovery Protocol (MSDP) peer, use the `sa-filter` command in the appropriate configuration mode. To return to the default behavior, use the `no` form of this command.

```
sa-filter {in|out} {list access-list-name|rp-list access-list-name}
no sa-filter {in|out} {list access-list-name|rp-list access-list-name}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>in</th>
<th>out</th>
<th>Specifies incoming or outgoing SA filtering.</th>
</tr>
</thead>
<tbody>
<tr>
<td>list access-list-name</td>
<td>Specifies an IP access list number or name. If no access list is specified, no (S, G) pairs from the peer are filtered.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>rp-list access-list-name</td>
<td>Specifies an originating rendezvous point (RP) access list in SA messages.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**
If the `sa-filter` command is not configured, no incoming or outgoing messages are filtered; all incoming SA messages are accepted from the peer, and all outgoing SA messages received are forwarded to the peer.

**Command Modes**
- MSDP configuration
- MSDP peer configuration

**Command History**
- **Release 3.7.2** This command was introduced.

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Note**
You can configure the `sa-filter` command globally for MSDP (and is inheritable by MSDP peers); however, this global configuration can be overridden if it is issued again in peer configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
In the following example, only (S, G) pairs that pass access list 10 are forwarded in an SA message to the peer with IP address 131.107.5.4:

```
RP/0/RSP0/CPU0:router(config)# router msdp
RP/0/RSP0/CPU0:router(config-msdp)# peer 131.107.5.4
RP/0/RSP0/CPU0:router(config-msdp-peer)# sa-filter out list_10
```
In the following example, only (S, G) pairs for the rendezvous point that passes access list 151 are forwarded in an SA message to the peer with the IP address 131.107.5.4:

```bash
RP/0/RSP0/CPU0:router(config)# router msdp
RP/0/RSP0/CPU0:router(config-msdp)# peer 131.107.5.4
RP/0/RSP0/CPU0:router(config-msdp-peer)# sa-filter out rp-list list_151
```

**Note**
The source and destination fields in the access list matches on the (S,G) fields in the SA messages. We recommend that the first address and mask field in the access list is used for the source and the second field in the access list is used for the group or destination.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>peer (MSDP), on page 78</code></td>
<td>Configures a Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
</tbody>
</table>
show msdp globals

To display the Multicast Source Discovery Protocol (MSDP) global variables, use the `show msdp globals` command in

EXEC mode

```
show msdp [ipv4] globals
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IPv4 address prefixes.</td>
</tr>
</tbody>
</table>

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 3.9.0</td>
<td>Asplain format for 4-byte Autonomous system numbers notation was supported. The input parameters and output were modified to display 4-byte autonomous system numbers and extended communities in either asplain or asdot notations.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Some global variables associated with MSDP sessions are displayed, such as the originator ID, default peer, and connection state with Protocol Independent Multicast (PIM), Source.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show msdp globals` command:

```
RP/0/RSP0/CPU0:router# show msdp globals
Multicast Source Discovery Protocol - msdp[405672]
  AS: 10, caching, originator: not set, default peer: not set
  Connected to PIM: yes
  Active RP Grange/len Source Count
  10.10.2.1  224.0.0.0/4  0,0
  10.10.10.3  0.0.0.0  1,1

  Max/active group count:  1/1
  Max/active SA count:     1/1
```
General stats
Current lists allocated/free:  2/0
Total list items allocated/free:  9/1
Total source buffers allocated/free:  1/0
Total group buffers allocated/free:  1/0
Total RP buffers allocated/free:  2/0
TLV buffers allocated/free:  1/1

This table describes the significant fields shown in the display.

Table 7: show msdp globals Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AS</td>
<td>Local autonomous system.</td>
</tr>
<tr>
<td>caching</td>
<td>SA caching that is enabled.</td>
</tr>
<tr>
<td>originator</td>
<td>Local rendezvous point (RP).</td>
</tr>
<tr>
<td>default peer</td>
<td>Default peer to accept Source Active (SA) messages from when all Reverse Path Forwarding (RPF) rules fail.</td>
</tr>
<tr>
<td>Active RP</td>
<td>All RPs involved in sending SA messages to this router.</td>
</tr>
<tr>
<td>Grange/len</td>
<td>Multicast Group Range or Multicast Group Mask. The field is visible only when there is a specified group range for the local RP. If a group range is unspecified (for example, for RPs that advertise SAs) only the Advertiser address and the RPF information is displayed (see ADV/RPF below).</td>
</tr>
<tr>
<td>Source Count</td>
<td>Total and active SA messages advertised by the respective RP.</td>
</tr>
<tr>
<td>ADV/RPF</td>
<td>Advertiser and RPF entry.</td>
</tr>
<tr>
<td>Max/active group count</td>
<td>Maximum group count since router was booted and number of active groups.</td>
</tr>
<tr>
<td>Max/active SA count</td>
<td>Maximum SA message count since router was booted, and number of active SA messages.</td>
</tr>
<tr>
<td>Total source buffers allocated/free</td>
<td>Number of internal source buffers allocated and freed after allocation.</td>
</tr>
<tr>
<td>Total group buffers allocated/free</td>
<td>Number of internal group buffers allocated and freed after allocation.</td>
</tr>
<tr>
<td>Total RP buffers allocated/free</td>
<td>Number of internal RP buffers allocated and freed after allocation.</td>
</tr>
<tr>
<td>TLV buffers allocated/free</td>
<td>Number of internal time-to-live buffers allocated and freed after allocation.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show msdp peer, on page 84</td>
<td>Displays information about the Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
<tr>
<td>show msdp sa-cache, on page 89</td>
<td>Displays the (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers.</td>
</tr>
</tbody>
</table>
show msdp peer

To display information about the Multicast Source Discovery Protocol (MSDP) peer, use the `show msdp peer` command in EXEC mode.

```
show msdp [ipv4] peer [peer-address]
```

**Syntax Description**

- **ipv4**: (Optional) Specifies IPv4 address prefixes.
- **peer-address**: (Optional) IP address or hostname of the MSDP peer for which information is displayed.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>3.9.0</td>
<td>Asplain format for 4-byte Autonomous system numbers notation was supported. The input parameters and output were modified to display 4-byte autonomous system numbers and extended communities in either asplain or asdot notations.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

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

```
RP/0/RSP0/CPU0:router# show msdp peer 10.10.10.2

MSDP Peer 10.10.10.2 (?), AS 20
Description:
    Connection status:
        State: Up, Resets: 0, Connection Source: 10.10.10.12
        Uptime(Downtime): 00:00:26, SA messages received: 0
        TLV messages sent/received: 1/1
        Output messages discarded: 0
        Connection and counters cleared 00:00:26 ago
    SA Filtering:
        Input (S,G) filter: none
        Input RP filter: none
        Output (S,G) filter: none
```
Output RP filter: none
SA-Requests:
  Input filter: none
  Sending SA-Requests to peer: disabled
Password: None
Peer ttl threshold: 0
Input queue size: 0, Output queue size: 0

This table describes the significant fields shown in the display.

**Table 8: show msdp peer Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSDP Peer</td>
<td>IP address of the MSDP peer.</td>
</tr>
<tr>
<td>AS</td>
<td>Autonomous system to which the peer belongs.</td>
</tr>
<tr>
<td>State</td>
<td>State of the peer.</td>
</tr>
<tr>
<td>Uptime (Downtime)</td>
<td>Days and hours the peer is up or down, per state shown in previous column.</td>
</tr>
<tr>
<td></td>
<td>If less than 24 hours, it is shown in terms of hours:minutes:seconds.</td>
</tr>
<tr>
<td>Msgs Sent/Received</td>
<td>Number of Source-Active (SA) messages sent to peer/number of SA messages</td>
</tr>
<tr>
<td></td>
<td>received from peer.</td>
</tr>
<tr>
<td>Peer Name</td>
<td>Name of peer.</td>
</tr>
<tr>
<td>TCP connection source</td>
<td>Interface used to obtain IP address for TCP local connection address.</td>
</tr>
<tr>
<td>SA input filter</td>
<td>Name of the access list filtering SA input (if any).</td>
</tr>
<tr>
<td>SA output filter</td>
<td>Name of the access list filtering SA output (if any).</td>
</tr>
<tr>
<td>SA-Request filter</td>
<td>Name of the access list filtering SA request messages (if any).</td>
</tr>
<tr>
<td>Sending SA-Requests to peer</td>
<td>There are no peers configured to send SA request messages to.</td>
</tr>
<tr>
<td>Password</td>
<td>Information on the password. If the password is set on an active peer,</td>
</tr>
<tr>
<td></td>
<td>“Configured, set on active socket” is displayed.</td>
</tr>
<tr>
<td>Peer ttl threshold</td>
<td>Multicast packets with an IP header that shows time-to-live greater than or</td>
</tr>
<tr>
<td></td>
<td>equal to this value are sent to the MSDP peer.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer (MSDP), on page 78</td>
<td>Configures a Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
<tr>
<td>show msdp sa-cache, on page 89</td>
<td>Displays the (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers.</td>
</tr>
</tbody>
</table>
show msdp rpf

To display the Multicast Source Discovery Protocol (MSDP) Reverse Path Forwarding (RPF) rule that governs whether an Source-Active (SA) from an originating RP will be accepted, use the `show msdp rpf` command in EXEC mode.

```
show msdp [ipv4] rpf rpf-address
```

**Syntax Description**

- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `rpf-address` IP address or hostname of the RPF next hop.

**Command Default**
IPv4 addressing is the default.

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| 3.7.2   | This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `show msdp rpf` command displays the peer interface and autonomous system to which the SAs are sent and forwarded based on the MSDP RPF rule. The rule is displayed and applied on the RP address field of the arriving SAs.

**Examples**

The following is sample output from the `show msdp rpf` command for RP peer 10.1.1.1:

```
RP/0/RSP0/CPU0:router# show msdp rpf 10.1.1.1
RP peer for 172.16.1.1 is 10.1.1.1 AS 200, rule: 1
bgp/rib lookup: nexthop: 10.1.1.1, asnum: 200
```

This table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RP peer for 172.16.1.1 is 10.1.1.1</td>
<td>IP address of the MSDP RPF peer.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>AS 200</td>
<td>Autonomous system to which the peer belongs.</td>
</tr>
<tr>
<td>rule: 1</td>
<td>MSDP RPF rule that matches what was learned from SAs.</td>
</tr>
<tr>
<td>bgp/rib lookup:</td>
<td>Multicast RPF routing table lookup.</td>
</tr>
<tr>
<td>nexthop: 10.1.1.1</td>
<td>Router where the SA is sent to reach the final destination.</td>
</tr>
<tr>
<td>asnum: 200</td>
<td>Autonomous system number for the next-hop neighbor router.</td>
</tr>
</tbody>
</table>
show msdp nsr

To display nonstop routing (NSR) information in the Multicast Source Discovery Protocol (MSDP), use the `show mrib nsr` command in the appropriate mode.

```
show msdp [ipv4|ipv6] nsr
```

**Syntax Description**
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `ipv6` (Optional) Specifies IPv6 address prefixes.

**Command Default**
IPv4 addressing is the default.

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `show msdp nsr` command displays the current multicast NSR state for the MSDP. The state may be normal or activated for NSR. The activated state indicates that recovery is in progress due to a failure in MRIB or Protocol Independent Multicast (PIM). The total NSR timeout and time remaining are displayed until NSR expiration.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**
The following is sample output from the `show msdp nsr` command:

```
RP/0/RSP0/CPU0:router# show msdp nsr
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mrib nsr</td>
<td>Displays the state of NSR operation in the MRIB.</td>
</tr>
<tr>
<td>show igmp nsr</td>
<td>Displays the state of NSR operation for IGMP.</td>
</tr>
<tr>
<td>show pim nsr</td>
<td>Displays the state of NSR operation for PIM.</td>
</tr>
</tbody>
</table>
show msdp sa-cache

To display the (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers, use the `show msdp sa-cache` command in EXEC mode.

```
show msdp [ipv4] sa-cache [source-address] [group-address] [all] [asnum as-number] [peer peer-address] [rpaddr rp-address] [summary]
```

**Syntax Description**

- **ipv4** (Optional) Specifies IPv4 address prefixes.
- **source-address** (Optional) Source address or hostname of the source about which (S, G) information is displayed.
- **group-address** (Optional) Group address or name of the group about which (S, G) information is displayed.
- **all** (Optional) Displays all Source Active (SA) entries with PI (PIM Interested) flags.
- **asnum as-number** (Optional) Displays SA entries of the specified autonomous system number. Range for 2-byte Autonomous system numbers (ASNs) is 1 to 65535. Range for 4-byte Autonomous system numbers (ASNs) in asplain format is 1 to 4294967295. Range for 4-byte Autonomous system numbers (ASNs) in asdot format is 1.0 to 65535.65535.
- **peer peer-address** (Optional) Displays peer entry information, including peer name and peer address.
- **rpaddr rp-address** (Optional) Displays SA entries that match the specified rendezvous point (RP) address.
- **summary** (Optional) Displays the count of all SA entries, RPs, sources, and groups.

**Command Default**
IPv4 addressing is the default.

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 3.9.0</td>
<td>Asplain format for 4-byte Autonomous system numbers notation was supported. The input parameters and output were modified to display 4-byte autonomous system numbers and extended communities in either asplain or asdot notations.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `show msdp sa-cache` command is used to examine the (S, G) entries and the attributes, flags (L, E, EA), uptime, autonomous system number, and RP addresses that are stored in the SA cache.
These guidelines apply when this command is used:

- The `cache-sa-state` command is enabled by default.
- When you specify the `summary` keyword, the total number of cache, group, and source entries, and entries advertised by each RP and autonomous system are displayed.
- When you specify two addresses or names, an (S, G) entry corresponding to those addresses is displayed.
- When you specify a single group address, all sources for that group are displayed.
- When you specify no options, the entire SA cache is displayed, excluding the PI flag entries.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>multicast read</td>
</tr>
</tbody>
</table>

### Examples

This is a sample output from the `show msdp sa-cache` command:

```
RP/0/RSP0/CPU0:router# show msdp sa-cache

MSDP Flags:
E - set MRIB E flag, L - domain local source is active,
EA - externally active source, PI - PIM is interested in the group,
DE - SAs have been denied.
Cache Entry:
(10.10.5.102, 239.1.1.1), RP 10.10.4.3, AS 20, 15:44:03/00:01:17
Learned from peer 10.10.2.2, RPF peer 10.10.2.2
SA's recv'd 1049, Encapsulated data received: 0
grp flags: PI, src flags: E, EA, PI
```

This table describes the significant fields shown in the display.

### Table 10: `show msdp sa-cache` Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(10.10.5.102, 239.1.1.1)</td>
<td>The first address (source) is sending to the second address (group).</td>
</tr>
<tr>
<td>RP 10.10.4.3</td>
<td>Rendezvous point (RP) address in the originating domain where the SA messages started.</td>
</tr>
</tbody>
</table>
| MBGP/AS 20 | RP is in autonomous system AS 20 according to the unicast RPF table:  
- If Multiprotocol Border Gateway Protocol (MBGP) is not configured—RIB table 1.  
- If MBGP is configured—RIB table 2 or multicast table. |
| 15:44:03/00:01:17 | The route has been cached for 15 hours, 44 minutes, and 3 seconds. If no SA message is received in 1 minute and 17 seconds, the route is removed from the SA cache. |
| Encapsulated data received: 0 | MSDP SA captures any data information when the source starts so that the receiver does not miss data when the SA path is established. |

The following is sample output using the `all` keyword option:

```
RP/0/RSP0/CPU0:router# show msdp sa-cache all
```
MSDP Flags:
E - set MRIB E flag, L - domain local source is active,
EA - externally active source, PI - PIM is interested in the group,
DE - SAs have been denied. Timers age/expiration,

Cache Entry:
(*, 239.1.1.1), RP 0.0.0.0, AS 0, 06:32:18/expired
Learned from peer local, RPF peer local
SAs recvd 0, Encapsulated data received: 0 grp flags: PI, src flags:

This table describes the significant fields shown in the display.

### Table 11: show msdp sa-cache all Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(*, 239.1.1.1)</td>
<td>Protocol Independent Multicast (PIM) interest in the group due to a local Internet Group Management Protocol (IGMP) join.</td>
</tr>
<tr>
<td>RP 0.0.0.0</td>
<td>There is no RP associated with this entry.</td>
</tr>
<tr>
<td>AS 0</td>
<td>This entry is 0, autonomous system (AS) rendezvous point (RP) is null.</td>
</tr>
<tr>
<td>06:32:18/expired</td>
<td>Route is alive in hours, minutes, and seconds. Note that MSDP does not monitor this route as it is received from the MRIB and PIM.</td>
</tr>
</tbody>
</table>

The following is sample output using the `summary` keyword option:

```
RP/0/RSP0/CPU0:router# show msdp sa-cache summary

Total # of SAs = 3
Total # of RPs = 2
Total # of Sources = 1
Total # of Groups = 3

Originator-RP      SA total     RPF peer
172.16.1.1       0     0.0.0.0
172.17.1.1       3     172.17.1.1

AS-num        SA total
200            3
```

This table describes the significant fields shown in the display.

### Table 12: show msdp sa-cache summary Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total # of SAs</td>
<td>Total number of SAs that are currently active in the system.</td>
</tr>
<tr>
<td>Total # of RPs</td>
<td>Total number of RPs that have distributed the SA information to this system.</td>
</tr>
<tr>
<td>Total # of Sources</td>
<td>Total number of sources that are active from all domains.</td>
</tr>
<tr>
<td>Total # of Groups</td>
<td>Total number of groups to which sources are sending data from all domains.</td>
</tr>
</tbody>
</table>
show msdp sa-cache

### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Originator-RP</td>
<td>SA information based on the individual RPs and the originating domains that distributed them.</td>
</tr>
<tr>
<td>AS-num</td>
<td>SA information based on the originating autonomous system.</td>
</tr>
</tbody>
</table>

The following is sample output using the `asnum` keyword option:

```
RP/0/RSP0/CPU0:router# show msdp sa-cache asnum 200

MSDP Flags:
E - set MRIB E flag, L - domain local source is active,
EA - externally active source, PI - FIM is interested in the group,
DE - SAs have been denied. Timers age/expiration,
Cache Entry:

(172.31.1.1, 239.1.1.1), RP 5.1.1.1, AS 200, 00:00:25/00:02:04
Learned from peer 5.1.1.1, RPF peer 172.17.1.1
SAs recvd 1, Encapsulated data received: 100
grp flags: none, src flags: EA

(172.31.1.1, 239.1.1.2), RP 172.17.1.1, AS 200, 00:00:16/00:02:13
Learned from peer 172.17.1.1, RPF peer 172.17.1.1
SAs recvd 1, Encapsulated data received: 100
grp flags: none, src flags: EA

(172.31.1.1, 239.1.1.3), RP 172.17.1.1, AS 200, 00:00:13/00:02:16
Learned from peer 172.17.1.1, RPF peer 172.17.1.1
SAs recvd 1, Encapsulated data received: 100
grp flags: none, src flags: EA
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cache-sa-state, on page 59</td>
<td>Controls cache source-active (SA) state on a router.</td>
</tr>
<tr>
<td>peer (MSDP), on page 78</td>
<td>Configures a Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
</tbody>
</table>
show msdp statistics peer

To display Multicast Source Discovery Protocol (MSDP) peer statistic counters, use the `show msdp statistics peer` command in EXEC mode.

```
show msdp [ipv4] statistics peer [peer-address]
```

**Syntax Description**

- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `peer-address` (Optional) IP address or name of the MSDP peer.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

- **Release**
  - 3.7.2 This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `show msdp statistics peer` command displays MSDP peer statistics such as the number of keepalive messages sent and received and the number of Source-Active (SA) entries sent and received.

If you do not specify an MSDP peer with the `peer-address` argument, this command displays statistics for all MSDP peers.

**Task ID**

```
Task ID  Operations
multicast  read
```

**Examples**

The following is sample output from the `show msdp statistics peer` command:

```
RP/0/RSP0/CPU0:router# show msdp statistics peer

MSDP Peer Statistics :-

Peer 10.1.2.3 : AS is 10, State is Up, 0 active SAs
TLV Rcvd : 57 total
57 keepalives, 0 notifications
0 SAs, 0 SA Requests
0 SA responses, 0 unknowns
TLV Sent : 57 total
54 keepalives, 0 notifications
3 SAs, 0 SA Requests
0 SA responses
SA msgs : 0 received, 3 sent
```
Peer 10.2.3.4: AS is 0, State is Connect, 0 active SAs

TLV Rcvd: 0 total
  0 keepalives, 0 notifications
  0 SAs, 0 SA Requests
  0 SA responses, 0 unknowns

TLV Sent: 0 total
  0 keepalives, 0 notifications
  0 SAs, 0 SA Requests
  0 SA responses

SA msgs: 0 received, 0 sent

This table describes the significant fields shown in the display.

Table 13: show msdp statistic peer Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer 10.1.2.3</td>
<td>All statistics are displayed for MSDP peer.</td>
</tr>
<tr>
<td>AS 10</td>
<td>Peer belongs to autonomous system (AS) 10.</td>
</tr>
<tr>
<td>State is UP</td>
<td>Peer state is established.</td>
</tr>
<tr>
<td>0 active SAs</td>
<td>There are no active SAs from this peer.</td>
</tr>
<tr>
<td>TLV Rcvd</td>
<td>Information about the time-to-lives (TLVs) received from this peer.</td>
</tr>
<tr>
<td>TLV Sent</td>
<td>Information about the TLVS sent to this peer.</td>
</tr>
<tr>
<td>SA msgs</td>
<td>Information about the SA messages for this peer.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear msdp stats, on page 64</td>
<td>Resets Multicast Source Discovery Protocol (MSDP) peer statistic counters.</td>
</tr>
</tbody>
</table>
**show msdp summary**

To display Multicast Source Discovery Protocol (MSDP) peer status, use the `show msdp summary` command in EXEC mode.

```
show msdp summary
```

**Syntax Description**

```
ipv4 (Optional) Specifies IPv4 address prefixes.
```

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `show msdp summary` command displays peer status such as the following:

- Peer address
- Peer autonomous system
- Peer state
- Uptime and downtime
- Number of Source-Active (SA) messages sent or received

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

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

```
RP/0/RSP0/CPU0>show msdp summary
Out of Resource Handling Enabled
Maximum External SA's Global : 20000
Current External Active SAs : 0

MSDP Peer Status Summary
Peer Address   AS   State  Uptime/ Downtime  Reset  Peer  Active Cfg.Max TLV recv/sent
10.1.1.1       0   NoIntf 00:10:07   0      ?     0  0      0/0
```
This table describes the significant fields shown in the display.

**Table 14: show msdp summary Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Peer Address</td>
<td>Neighbor router address from which this router has MSDP peering established.</td>
</tr>
<tr>
<td>AS</td>
<td>Autonomous system to which this peer belongs.</td>
</tr>
<tr>
<td>State</td>
<td>State of peering, such as UP, inactive, connect, and NoIntf.</td>
</tr>
<tr>
<td>Uptime/Downtime</td>
<td>MSDP peering uptime and downtime in hours, minutes, and seconds.</td>
</tr>
<tr>
<td>Reset Count</td>
<td>Number of times the MSDP peer has reset.</td>
</tr>
<tr>
<td>Peer Name</td>
<td>DNS name of peer (if available).</td>
</tr>
<tr>
<td>Active SA Cnt</td>
<td>Total number of SAs that are active on this router.</td>
</tr>
<tr>
<td>Cfg. Max Ext. SAs</td>
<td>Total number of maximum external SAs after the SAs are dropped. If 0, nothing is configured.</td>
</tr>
<tr>
<td>TLV recv/sent</td>
<td>Total number of time-to-lives (TLVs) sent and received.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show msdp peer, on page 84</td>
<td>Displays information about the Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
<tr>
<td>show msdp sa-cache, on page 89</td>
<td>Displays the (S, G) state learned from Multicast Source Discovery Protocol (MSDP) peers.</td>
</tr>
</tbody>
</table>
show msdp vrf context

To show the MSDP information configured for a VPN routing and forwarding (VRF) context, use the `show msdp vrf context` command in EXEC mode.

```plaintext
show msdp vrf vrf-name context
```

**Syntax Description**

t | vrf-name | VPN routing and forwarding (VRF) interface.

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to use the `show msdp vrf context` command:

```plaintext
RP/0/RSP0/CPU0:router # show msdp vrf red context
Fri Feb 8 18:13:51.599 PST
MSDP context information for red
  VRF ID : 0x60000002
  Table ID : 0xe0000002
  Table Count (Active/Total) : 1/1
Inheritable Configuration
  TTL : 2
  Maximum SAs : 0
  Keepalive Period : 30
  Peer Timeout Period : 75
  Connect Source : 
  SA Filter In : 
  SA Filter Out : 
  RP Filter In : 
  RP Filter Out :
Configuration
  Originator Address : 0.0.0.0
  Originator Interface Name : 
  Default Peer Address : 0.0.0.0
  SA Holdtime : 150
  Allow Encaps Count : 0
```
show msdp vrf context

Context Maximum SAs : 20000
SA Cache Counts (Current/High Water Mark)
  Groups : 0/0
  Sources : 0/0
  RPs : 2/0
  External SAs : 0/0
MRIB Update Counts
  Total updates : 2
  With no changes : 0
  (*,G) routes : 2
  (S,G) routes : 0
MRIB Update Drops
  Invalid group : 0
  Invalid group length : 0
  Invalid source : 0
  Auto-RP Address : 2
shutdown (MSDP)

To shut down a Multicast Source Discovery Protocol (MSDP) peer, use the `shutdown` command in peer configuration mode. To return to the default behavior, use the `no` form of this command.

```
shutdown
no shutdown
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

No default behavior or values

**Command Modes**

MSDP peer configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `shutdown` command to shut down the peer. To configure many MSDP commands for the same peer, shut down the peer, configure it, and activate the peer later.

You might also want to shut down an MSDP session without losing configuration information for the peer.

When a peer is shut down, the TCP connection is terminated and is not restarted.

**Examples**

The following example shows how to shut down the peer with the address 172.16.5.4:

```
RP/0/RSP0/CPU0:router(config)# router msdp
RP/0/RSP0/CPU0:router(config-msdp)# peer 172.16.5.4
RP/0/RSP0/CPU0:router(config-msdp-peer)# shutdown
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show msdp peer</code>, on page 84</td>
<td>Displays information about the Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
</tbody>
</table>
**ttl-threshold (MSDP)**

To limit which multicast data packets are sent in Source-Active (SA) messages to a Multicast Source Discovery Protocol (MSDP) peer, use the `ttl-threshold` command in MSDP configuration mode or peer configuration mode. To return to the default behavior, use the `no` form of this command.

```
    ttl-threshold ttl
    no ttl-threshold ttl
```

**Syntax Description**

- `ttl`: Time to live value. Range is 1 to 255.

**Command Default**

`ttl`: 1

**Command Modes**

- MSDP configuration
- MSDP peer configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `ttl-threshold` command limits which multicast data packets are sent in data-encapsulated Source-Active (SA) messages. Only multicast packets with an IP header time-to-live (TTL) greater than or equal to the `ttl` argument are sent to the MSDP peer specified by the IP address or name.

Use the `ttl-threshold` command to use TTL to examine your multicast data traffic. For example, you can limit internal traffic to a TTL of 8. If you want other groups to go to external locations, send the packets with a TTL greater than 8.

**Note**

This command can be configured globally for MSDP (and to be inheritable by MSDP peers). However this global configuration can be overridden if issued again in peer configuration mode.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a TTL threshold of eight hops:
```
RP/0/RSP0/CPU0:router(config)# router msdp
RP/0/RSP0/CPU0:router(config-msdp)# ttl-threshold 8
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer (MSDP), on page 78</td>
<td>Configures a Multicast Source Discovery Protocol (MSDP) peer.</td>
</tr>
</tbody>
</table>
ttl-threshold (MSDP)
Multicast Routing and Forwarding Commands

This module describes the commands used to configure and monitor multicast routing.

For detailed information about multicast routing concepts, configuration tasks, and examples, refer to the Implementing Multicast Routing on Cisco IOS XR Software configuration module in the Multicast Configuration Guide for Cisco ASR 9000 Series Routers.

- accounting per-prefix, on page 105
- accounting per-prefix forward-only, on page 107
- address-family (multicast), on page 109
- boundary, on page 112
- clear mfib counter, on page 113
- clear mfib database, on page 114
- clear mfib hardware resource-counters, on page 115
- clear mfib hardware route statistics, on page 116
- disable (multicast), on page 118
- enable (multicast), on page 120
- forwarding-latency, on page 122
- interface (multicast), on page 123
- interface all enable, on page 125
- interface-inheritance disable, on page 127
- log-traps, on page 129
- maximum disable, on page 130
- mdt c-multicast-routing, on page 131
- mdt data, on page 132
- mdt data ingress replication, on page 134
- mdt default, on page 135
- mdt mtu, on page 137
- mdt source, on page 138
- migration route-policy, on page 140
- multicast-routing, on page 141
- multipath, on page 142
- nsf (multicast), on page 143
- oom-handling, on page 145
- rate-per-route, on page 146
- shared-tree-prune delay, on page 147
- show mfib bvi, on page 148
- show mfib connections, on page 149
- show mfib counter, on page 151
- show mfib enca-info, on page 153
- show mfib hardware interface, on page 155
- show mfib hardware ltrace, on page 160
- show mfib hardware resource-counters, on page 164
- show mfib hardware route accept-bitmap, on page 167
- show mfib hardware route logical, on page 169
- show mfib hardware route location, on page 172
- show mfib hardware route mofrr, on page 174
- show mfib hardware route olist, on page 180
- show mfib hardware route statistics, on page 191
- show mfib hardware route summary, on page 195
- show mfib hardware table, on page 198
- show mfib interface, on page 200
- show mfib nsf, on page 202
- show mfib route, on page 204
- show mfib table-info, on page 210
- show mrib client, on page 212
- show mrib bvi, on page 215
- show mrib nsf, on page 216
- show mrib nsr end, on page 218
- show mrib platform trace location standby, on page 220
- show mrib route, on page 222
- show mrib route-collapse, on page 224
- show mrib route outgoing-interface, on page 226
- show mrib table-info, on page 228
- show mrib tlc, on page 230
- static-rpf, on page 231
- source-tree-prune-delay, on page 233
- suppress-pim-data-signaling, on page 234
- suppress-shared-tree-join, on page 235
- til-threshold (multicast), on page 236
- unicast-reachability, on page 238
- vrf (multicast), on page 239
- cef platform lsm frr-holdtime, on page 241
accounting per-prefix

To enable accounting for multicast routing, use the `accounting per-prefix` command in the appropriate configuration mode. To return to the default behavior, use the `no` form of this command.

```
accounting per-prefix
no accounting per-prefix
```

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
This feature is disabled by default.

**Command Modes**
Multicast routing configuration
Multicast routing address family IPv4 configuration
Multicast VRF configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `accounting per-prefix` command is used to enable per-prefix counters only in hardware. Cisco IOS XR Software counters are always present. When enabled, every existing and new (S, G) route is assigned forward, punt, and drop counters on the ingress route and forward and punt counters on the egress route. The (*, G) routes are assigned a single counter.

There are a limited number of counters on all nodes. When a command is enabled, counters are assigned to routes only if they are available.

To display packet statistics, use the `show mfib route` and the `show mfib hardware route statistics` commands. These commands display “N/A” for counters when no hardware statistics are available or when the `accounting per-prefix` command is disabled.

**Task ID**
```
Task ID  Operations
multicast  read,
           write
```

**Examples**
The following example shows how to enable accounting for multicast routing:
RP/0/RSP0/CPU0:router(config)# **multicast-routing**
RP/0/RSP0/CPU0:router(config-mcast)# **accounting per-prefix**

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>show mfib hardware route statistics, on page 191</strong></td>
<td>Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the packet and byte counters for each route.</td>
</tr>
<tr>
<td><strong>show mfib route, on page 204</strong></td>
<td>Displays route entries in the Multicast Forwarding Information Base (MFIB).</td>
</tr>
</tbody>
</table>
accounting per-prefix forward-only

To reduce hardware statistics resource allocations when enabling accounting, particularly for multicast VPN (MVPN), use the `accounting per-prefix forward-only` command under multicast routing configuration mode. To return to the default mode of accounting per-prefix, on page 105, use the `no` form of this command.

```
accounting per-prefix forward-only
no accounting per-prefix forward-only
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

If no counters were configured, there is no default.

If the accounting per-prefix counter was previously configured, it becomes the default.

If no accounting was configured for multicast routing, forwarding-only is the default mode and triggers a data MDT transition in the case of MVPN deployment.

**Command Modes**

- Multicast routing configuration
- Multicast routing address family IPv4 and IPv6 configuration
- Multicast VRF configuration

**Command History**

```
Release  Modification
3.8.0      This command was introduced.
```

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Note**

The `accounting per-prefix forward-only` command has only one `fwd-only` counter. In other words, there is no `punt` or `drop` counter allocated.

We recommended this command for configuration of multicast VPN routing or for any line card that has a route-intensive configuration. Each individual router can support up to 150,000 routes.

**Note**

To verify the number of statistics allocated or free on a line card, use the `show mfib hardware resource-counters, on page 164` command in EXEC mode.

There are a limited number of counters on all nodes. When accounting on a prefix is enabled, counters are assigned to routes only if they are available.

To display packet statistics, use the `show mfib route` and the `show mfib hardware route statistics` commands. These commands display “N/A” for counters when no hardware statistics are available or when
neither the accounting per-prefix, on page 105 command nor the accounting per-prefix forward-only command are enabled.

You may switch between accounting-perprefix and accounting per-prefix forward-only statistics for ipv4 or ipv6 multicast family. However, be aware that only one set of counters is supported on the (*,G) routes (with fwd/punt/drop on ingress and fwd/drop on egress) regardless of whether you enabled the accounting-perprefix or accounting-perprefix fwd-only command.

Although you can switch accounting modes, this involves freeing the hardware statistics and reallocating them, thereby resulting in a loss of any previously collected data. Therefore, it is preferable to decide which statistics mode you want to use at the start to avoid the resource cost entailed by resetting the statistics counter values with a change in mode.

### Examples

The following example shows how to enable accounting per-prefix forward-only for MVPN routing:

```
RP/0/RSP0/CPU0:router (config) # multicast-routing
RP/0/RSP0/CPU0:router (config-mcast) # accounting per-prefix forward-only
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting per-prefix, on page 105</td>
<td>Enables accounting for multicast routing.</td>
</tr>
<tr>
<td>clear mfib hardware resource-counters, on page 115</td>
<td>Clears global resource counters.</td>
</tr>
</tbody>
</table>
# address-family (multicast)

To display available IP prefixes to enable multicast routing and forwarding on all router interfaces, use the `address-family` command in multicast-routing configuration mode or multicast VRF configuration submode. To disable use of an IP address prefix for routing, use the `no` form of this command.

```plaintext
address-family [vrf vrf-name] {ipv4|ipv6}
no address-family [vrf vrf-name] {ipv4|ipv6}
```

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Specifies a VPN routing and forwarding (VRF) instance.</td>
</tr>
<tr>
<td><code>ipv4</code></td>
<td>Specifies IPv4 address prefixes.</td>
</tr>
<tr>
<td><code>ipv6</code></td>
<td>Specifies IPv6 address prefixes.</td>
</tr>
</tbody>
</table>

## Command Default

No default behavior or values

## Command Modes

Multicast routing configuration

Multicast VRF configuration

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>4.2.0</td>
<td>The <code>ipv6</code> keyword was added.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `address-family` command either from multicast routing configuration mode or from multicast VRF configuration sub to enter either the multicast IPv4 or IPv6 address family configuration submode, depending on which keyword was chosen. Use the `address-family` command with the `multicast-routing`, on page 141 command to start the following multicast processes:

- Multicast Routing Information Base (MRIB)
- Multicast Forwarding Engine (MFWD)
- Protocol Independent Multicast Sparse mode (PIM-SM)
- Internet Group Management Protocol (IGMP)
- Multicast Listener Discovery Protocol (MLD)

Basic multicast services start automatically when the multicast PIE is installed, without any explicit configuration required. The following multicast services are started automatically:

- Multicast Routing Information Base (MRIB)
- Multicast Forwarding Engine (MFWD)
- Protocol Independent Multicast Sparse mode (PIM-SM)
- Internet Group Management Protocol (IGMP)
Other multicast services require explicit configuration before they start. For example, to start the Multicast Source Discovery Protocol (MSDP) process, you must enter the `router msdp` command and explicitly configure it.

To enable multicast routing and protocols on interfaces, you must explicitly enable the interfaces using the `interface` command in multicast routing configuration mode. This action can be performed on individual interfaces or by configuring a wildcard interface using the `alias` command.

To enable multicast routing on all interfaces, use the `interface all enable` command in multicast routing configuration mode. For any interface to be fully enabled for multicast routing, it must be enabled specifically (or configured through the `interface all enable` command for all interfaces) in multicast routing configuration mode, and it must not be disabled in the PIM and IGMP configuration modes.

**Note**

The `enable` and `disable` keywords available under the IGMP and PIM interface configuration modes have no effect unless the interface is enabled in multicast routing configuration mode—either by default or by explicit interface configuration.

To allow multicast forwarding functionality, while turning multicast routing functionality off, `interface-inheritance disable, on page 127` command on a per interface or `interface all enable` basis in PIM or IGMP configuration mode.

**Examples**

This example shows how to enter IPv4 and IPv6 multicast routing configuration mode:

```
RP/0/RSP0/CPU0:router(config)# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# address-family ipv4
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)#
```

```
RP/0/RSP0/CPU0:router(config-mcast)# address-family ipv6
RP/0/RSP0/CPU0:router(config-mcast-default-ipv6)#
```

This example shows how to enter IPv4 and IPv6 VRF multicast routing configuration submode:

```
RP/0/RSP0/CPU0:router(config)# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# vrf vrf-name address-family ipv4
RP/0/RSP0/CPU0:router(config-mcast-vrf-name-ipv4)#
```

```
RP/0/RSP0/CPU0:router(config-mcast)# vrf vrf-name address-family ipv6
RP/0/RSP0/CPU0:router(config-mcast-vrf-name-ipv6)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alias</td>
<td>Creates a command alias.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>interface all enable, on page 125</td>
<td>Enables multicast routing and forwarding on all new and existing interfaces.</td>
</tr>
<tr>
<td>interface all disable</td>
<td>Disables PIM processing on all new and existing interfaces.</td>
</tr>
<tr>
<td>interface-inheritance disable, on page 127</td>
<td>Separates the disabling of multicast routing and forwarding.</td>
</tr>
<tr>
<td>interface (multicast), on page 123</td>
<td>Configures multicast interface properties.</td>
</tr>
</tbody>
</table>
**boundary**

To configure the multicast boundary on an interface for administratively scoped multicast addresses, use the `boundary` command in the appropriate configuration mode. To return to the default behavior, use the `no` form of this command.

```
boundary access-list
no boundary access-list
```

**Syntax Description**

- `access-list` Access list specifying scoped multicast groups. The name cannot contain a space or quotation mark; it may contain numbers.

**Command Default**

A multicast boundary is not configured.

**Command Modes**

- Multicast routing interface configuration
- Multicast routing VRF interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `boundary` command is used to set up a boundary to keep multicast packets from being forwarded. The boundary acl can specify a mcast source address in addition to a mcast group address. The keyword "any" can be added before the mcast group range.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set up a boundary for all administratively scoped addresses:

```
RP/0/RSP0/CPU0:router(config) # ipv4 access-list myboundary2
RP/0/RSP0/CPU0:router(config) # 10 deny ipv4 any 239.0.0.0 0.255.255.255
RP/0/RSP0/CPU0:router(config) # 20 permit ipv4 any 224.0.0.0 15.255.255.255
RP/0/RSP0/CPU0:router(config)# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast) # address-family ipv4
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# interface GigE 0/2/0/2

RP/0/RSP0/CPU0:router(config-mcast-default-ipv4-if)# boundary myboundary2
```
**clear mfib counter**

To clear Multicast Forwarding Information Base (MFIB) route packet counters, use the `clear mfib counter` command in the appropriate mode.

```
clear mfib [vrf vrf-name] ipv4 counter [{group-address|source-address}] [location {node-id|all}]
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `group-address` (Optional) IP address of the multicast group.
- `source-address` (Optional) IP address of the source of the multicast route.
- `location node-id` (Optional) Clears route packet counters from the designated node.
- `all` The `all` keyword clears route packet counters on all nodes.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Note**

This command only clears MFIB route packet software counters. To clear MFIB hardware statistics counters use the `clear mfib hardware route statistics` command.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear MFIB route packet counters on all nodes:

```
RP/0/RSP0/CPU0:router# clear mfib counter location all
```
clear mfib database

To clear the Multicast Forwarding Information Base (MFIB) database, use the **clear mfib database** command in the appropriate mode.

```
clear mfib [{ipv4|ipv6}] database [location {node-id|all}]
```

**Syntax Description**

- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `location node-id` (Optional) Clears global resource counters from the designated node.
- `all` The `all` keyword clears all global resource counters.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write, execute</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to clear the Multicast Forwarding Information Base (MFIB) database on all nodes:

```
RP/0/RSP0:CPU0:router# clear mfib database location all
```
clear mfib hardware resource-counters

To clear global resource counters, use the `clear mfib hardware resource-counters` command in EXEC mode.

```
clear mfib [vrf vrf-name] [{ipv4|ipv6}] hardware resource-counters [location {node-id|all}]
```

**Command Syntax Description**

- **vrf vrf-name** (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- **ipv4** (Optional) Specifies IPv4 address prefixes.
- **ipv6** (Optional) Specifies IPv6 address prefixes.
- **location node-id** (Optional) Clears global resource counters from the designated node.
- **all** The `all` keyword clears all global resource counters.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

```
Release    Modification
----------- ------------
3.7.2       This command was introduced.
```

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `clear mfib hardware resource-counters` to estimate resource usage for an operation.

**Task ID**

```
Task ID  Operations
--------  ------------------
        multicast  read, write, execute
```

**Examples**

The following example shows how to clear all global resource counters:

```
RP/0/RSP0/CPU0:router# clear mfib hardware resource-counters location all
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mfib hardware resource-counters, on page 164</code></td>
<td>Displays the allocated and freed hardware resources for the Multicast Forwarding Information Base (MFIB) process.</td>
</tr>
</tbody>
</table>
clear mfib hardware route statistics

To reset all allocated counter values regardless of the Multicast Forwarding Information Base (MFIB) hardware statistics mode (accounting per-prefix or accounting per-prefix forward-only), use the clear mfib hardware route statistics command in EXEC mode.

clear mfib [vrf vrf-name] [ipv4|ipv6] hardware route statistics {egress|ingress|ingress-and-egress} [{*source-address}] [group-address [/prefix-length]] [location {node-id|all}]

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a VPN routing and forwarding (VRF) instance.</td>
</tr>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IPv4 address prefixes.</td>
</tr>
<tr>
<td>ipv6</td>
<td>(Optional) Specifies IPv6 address prefixes.</td>
</tr>
<tr>
<td>ingress-and-egress</td>
<td>(Optional) Clears hardware statistics on both the incoming (ingress) and outgoing (egress) routes.</td>
</tr>
<tr>
<td>*</td>
<td>(Optional) Clears shared tree route statistics.</td>
</tr>
<tr>
<td>source-address</td>
<td>(Optional) IP address or hostname of the multicast route source.</td>
</tr>
<tr>
<td>group-address</td>
<td>(Optional) IP address or hostname of the multicast group.</td>
</tr>
<tr>
<td>/ prefix-length</td>
<td>(Optional) Prefix length of the multicast group. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash must precede the decimal value.</td>
</tr>
<tr>
<td>location</td>
<td>(Optional) Clears route packet counters from the designated node.</td>
</tr>
<tr>
<td>node-id</td>
<td>The node-id argument is entered in the rack/slot/module notation.</td>
</tr>
<tr>
<td>all</td>
<td>The all keyword clears route packet counters on all nodes</td>
</tr>
</tbody>
</table>

**Command Default**

If not specified, IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes the proper task IDs.

The Multicast Forwarding (MFWD) process exists on each line card and assigns hardware counters to each (S, G) route. Additionally, one global counter is assigned for all (*, G) routes, depending on resource availability.
To clear the set of counters for (*) G) routes, the MFWD process assigns a single set of counters to count packets that match (*) G) routes. Consequently, the clear mfib hardware route statistics command must be used in a form that either clears counters on all routes or matches all (*) G) routes.

**Note**

This command only clears MFIB hardware statistics counters. To clear MFIB route packet software counters, use the clear mfib counter command.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>multicast read, write, execute</td>
</tr>
</tbody>
</table>

**Examples**

The following command shows how to clear counters by route statistics for all multicast routes on both ingress and egress forwarding engines for the line card 0/1/CPU0:

```
RP/0/RSP0/CPU0/router# clear mfib ipv4 hardware route statistics ingress-and-egress location 0/1/CPU0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mfib hardware route statistics, on page 191</td>
<td>Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the packet and byte counters for each route.</td>
</tr>
</tbody>
</table>
disable (multicast)

To disable multicast routing and forwarding on an interface, use the disable command in the appropriate configuration mode. To return to the default behavior, use the no form of this command.

```
disable
no disable
```

Syntax Description
This command has no keywords or arguments.

Command Default
Multicast routing and forwarding settings are inherited from the global interface enable all command. Otherwise, multicast routing and forwarding is disabled.

Command Modes
Multicast routing interface configuration
Multicast routing VRF interface configuration

Command History
Release 3.7.2 This command was introduced.

Usage Guidelines
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The disable command modifies the behavior of a specific interface to disabled. This command is useful if you want to disable multicast routing on specific interfaces, but leave it enabled on all remaining interfaces.

The following guidelines apply when the enable and disable commands (and the no forms) are used in conjunction with the interface all enable command:

- If the interface all enable command is configured:
  - The enable and no forms of the command have no additional effect on a specific interface.
  - The disable command disables multicast routing on a specific interface.
  - The no disable command enables a previously disabled interface.

- If the interface all enable command is not configured:
  - The enable command enables multicast routing on a specific interface.
  - The no enable command enables the previously disabled interface.
  - The disable and no forms of the command have no additional effect on a specific interface.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>
The following example shows how to enable multicast routing on all interfaces and disable the feature only on GigabitEthernet interface 0/1/0/0:

```
RP/0/RSP0/CPU0:router(config)# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# interface all enable
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# interface GigE 0/1/0/0
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4-if)# disable
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable (multicast), on page 120</td>
<td>Enables multicast routing and forwarding on an interface.</td>
</tr>
<tr>
<td>interface all enable, on page 125</td>
<td>Enables multicast routing and forwarding on all new and existing interfaces.</td>
</tr>
</tbody>
</table>
**enable (multicast)**

To enable multicast routing and forwarding on an interface, use the `enable` command in the appropriate configuration mode. To return to the default behavior, use the `no enable` form of this command.

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

Multicast routing and forwarding settings are inherited from the global `interface enable all` command. Otherwise, multicast routing and forwarding is disabled.

**Command Modes**

Multicast routing interface configuration

Multicast routing VRF interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `enable` command modifies the behavior of a specific interface to enabled. This command is useful if you want to enable multicast routing on specific interfaces, but leave it disabled on all remaining interfaces.

The following guidelines apply when the `enable` and `disable` commands (and the `no` forms) are used in conjunction with the `interface all enable` command:

- If the `interface all enable` command is configured:
  - The `enable` and `no` forms of the command have no additional effect on a specific interface.
  - The `disable` command disables multicast routing on a specific interface.
  - The `no disable` command enables a previously disabled interface.

- If the `interface all enable` command is not configured:
  - The `enable` command enables multicast routing on a specific interface.
  - The `no enable` command enables a previously enabled interface.
  - The `disable` and `no` forms of the command have no additional effect on a specific interface.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>
The following example shows how to enable multicast routing on a specific interface only:

```
RP/0/RSP0/CPU0:router(config)# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# interface GigE 0/1/0/0
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4-if)# enable
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable (multicast), on page 118</td>
<td>Disables multicast routing and forwarding on an interface.</td>
</tr>
<tr>
<td>interface all enable, on page 125</td>
<td>Enables multicast routing and forwarding on all new and existing interfaces.</td>
</tr>
</tbody>
</table>
forwarding-latency

To delay traffic being forwarded on a route, use the **forwarding-latency** command. To return to the default behavior, use the **no** form of this command.

```
forwarding-latency [delay milliseconds]
no forwarding-latency
```

**Syntax Description**
- `delay milliseconds` (Optional) Specifies the delay time in milliseconds. Range is 5 - 500.

**Command Default**
The default delay time is 30 milliseconds.

**Command Modes**
- Multicast routing configuration
- IPv4 and IPv6 multicast routing configuration

**Command History**
- **Release 3.8.0** This command was introduced.

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the **forwarding-latency** command when you expect a receiver to leave and rejoin the same multicast group within a very short period such as 20 or 30 milliseconds. The delay may be required to provide the router sufficient time to update its Multicast Forwarding Information Base (MFIB) table.

When the **forwarding-latency** command is enabled, each interface is allocated a separate table lookup unit (TLU) block in the output interface list (olist), thereby increasing TLU hardware resource usage, and, for this reason, it should be used with caution when many multicast routes are present.

When the **forwarding-latency** command is disabled, up to three interfaces may share a single TLU block in the olist.

**Task ID**
- Task ID: multicast
  - Operations: read, write

**Examples**
The following example shows how to delay traffic from being forwarded for 120 milliseconds:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# multicast-routing
RP/0/RSP0/CPU0:router# forwarding-latency delay 120
```
interface (multicast)

To configure multicast interface properties, use the `interface` command in the appropriate configuration mode. To disable multicast routing for interfaces, use the no form of this command.

```
interface type interface-path-id
no interface type interface-path-id
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>type</code></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note**

- Use the `show interfaces` command in EXEC mode to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark ( ? ) online help function.

**Command Default**

No default behavior or values

**Command Modes**

- Multicast routing configuration
- IPv4 or multicast routing configuration
- Multicast VRF configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `interface` command to configure multicast routing properties for specific interfaces.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable multicast routing on all interfaces and disable the feature only on GigabitEthernet interface 0/1/0/0:

```
RP/0/RSP0/CPU0:router(config)# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# interface all enable
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4-if)# interface GigE 0/1/0/0
```
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4-if)# **disable**

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>disable (multicast), on page 118</strong></td>
<td>Disables multicast routing and forwarding on an interface.</td>
</tr>
<tr>
<td><strong>enable (multicast), on page 120</strong></td>
<td>Enables multicast routing and forwarding on an interface.</td>
</tr>
<tr>
<td><strong>interface all enable, on page 125</strong></td>
<td>Enables multicast routing and forwarding on all new and existing interfaces.</td>
</tr>
</tbody>
</table>
interface all enable

To enable multicast routing and forwarding on all new and existing interfaces, use the `interface all enable` command in the appropriate configuration mode. To return to the default behavior, use the `no interface all enable` form of this command.

```
interface all enable
no interface all enable
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

Multicast routing and forwarding is disabled by default.

**Command Modes**

Multicast routing configuration

Multicast VRF configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command modifies the default behavior for all new and existing interfaces to enabled unless overridden by the `enable` or `disable` keywords available in interface configuration mode.

The following guidelines apply when the `enable` and `disable` commands (and the `no` forms) are used in conjunction with the `interface all enable` command:

- If the `interface all enable` command is configured:
  - The `enable` and `no` forms of the command have no additional effect on a specific interface.
  - The `disable` command disables multicast routing on a specific interface.
  - The `no disable` command enables a previously disabled interface.

- If the `interface all enable` command is not configured:
  - The `enable` command enables multicast routing on a specific interface.
  - The `no enable` command enables a previously enabled interface.
  - The `disable` and `no` forms of the command have no additional effect on a specific interface.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

---

*Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference, Release 5.3.x*
Examples

The following example shows how to enable multicast routing on all interfaces and disable the feature only on GigabitEthernet interface 0/1/0/0:

```
RP/0/RSP0/CPU0:router(config)# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# interface all enable
RP/0/RSP0/CPU0:router(config-mcast)# interface GigE 0/1/0/0
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4-if)# disable
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable (multicast), on page 118</td>
<td>Disables multicast routing and forwarding on an interface.</td>
</tr>
<tr>
<td>enable (multicast), on page 120</td>
<td>Enables multicast routing and forwarding on an interface.</td>
</tr>
</tbody>
</table>
**interface-inheritance disable**

To separate PIM and IGMP routing from multicast forwarding on all interfaces, use the **interface-inheritance disable** command under multicast routing address-family IPv4 submode. To restore the default functionality, use the **no** form of the command.

```plaintext
interface-inheritance disable
no interface-inheritance disable
```

### Syntax Description

This command has no keywords or arguments.

### Command Default

This feature is not enabled by default.

### Command Modes

Multicast routing configuration

Address-family IPv4 configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use of the **interface-inheritance disable** command together with the **interface type interface-path-id** or **interface all enable** command under multicast routing address-family IPv4 submode separates PIM and IGMP routing functionality from multicast forwarding on specified interfaces. You can nonetheless enable multicast routing functionality explicitly under PIM or IGMP routing configuration mode for individual interfaces.

**Note**

Although you can explicitly configure multicast routing functionality on individual interfaces, you cannot explicitly disable the functionality. You can only disable the functionality on all interfaces.

Used from the address-family ipv4 configuration submode, it prevents IGMP and PIM from inheriting the multicast-routing interface configuration.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>read,</td>
</tr>
<tr>
<td></td>
<td>write</td>
</tr>
</tbody>
</table>

### Examples

The following configuration disables PIM and IGMP routing functionality on all the interfaces using the **interface-inheritance disable** command, but multicast forwarding is still enabled on all the interfaces in the example, based on use of the keywords **interface all enable**.
PIM is enabled on Loopback 0 based on its explicit configuration (interface Loopback0 enable) under router pim configuration mode.

IGMP protocol is enabled on GigabitEthernet0/6/0/3, because it too has been configured explicitly under router igmp configuration mode (interface GigabitEthernet0/6/0/3 router enable):

```
RP/0/RSP0/CPU0:router(config)# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# address-family ipv4
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# interface-inheritance disable
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# interface loopback 1 enable

RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# show run router pim
```

With the interface-inheritance disable command in use, IGMP and PIM configuration are enabled in the protocol configuration as follows:

```
router igmp
  interface loopback 0
    router enable

router pim
  interface loopback 0
    enable

router pim vrf default address-family ipv4
  interface Loopback0
    enable

RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# show run router igmp
```

```
router igmp
  vrf default
    interface GigabitEthernet0/6/0/3
      router enable
```
**log-traps**

To enable logging of trap events, use the **log-traps** command in the appropriate configuration mode. To remove this functionality, use the **no** form of this command.

```
log-traps
no log-traps
```

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
This command is disabled by default.

**Command Modes**
- Multicast routing configuration
- Multicast routing address family IPv4 configuration
- Multicast VRF configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to enable logging of trap events:

```
RP/0/RSP0/CPU0:router# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# log-traps
```
**maximum disable**

To disable maximum state limits, use the `maximum disable` command in the appropriate configuration mode. To remove this functionality, use the `no` form of this command.

```
maximum disable
no maximum disable
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

Maximum state limits are enabled.

**Command Modes**

- Multicast routing configuration
- Multicast routing address family IPv4 configuration
- Multicast VRF configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `maximum disable` command to override the default software limit on the number of multicast routes.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to disable maximum state limits:

```
RP/0/RSP0/CPU0:router# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# maximum disable
```
**mdt c-multicast-routing**

To configure customer multicast routing (c-multicast-routing) for multicast distribution trees (MDT) and to enter the c-multicast-routing mode, use the `mdt c-multicast-routing` command in the appropriate mode. To delete the configuration, use the `no` form of the command.

```
mdt c-multicast-routing [ bgp | pim ]
no mdt c-multicast-routing [ bgp | pim ]
```

**Syntax Description**

- `bgp` Enables customer multicast routing for BGP.
- `pim` Enables customer multicast routing for PIM.

**Command Default**

None

**Command Modes**

PIM VRF address-family configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

- **multicast** read, write

**Example**

This example show how to run the `mdt c-multicast-routing`:

```
RP/0/RSP0/CPU0:router(config-pim-v1-ipv4) # mdt c-multicast-routing bgp
```
**mdt data**

To configure multicast data to be part of a multicast distribution tree (MDT) data group for multicast VPN (MVPN), use the `mdt data` command in the appropriate configuration mode. To remove this functionality, use the `no` form of this command.

```
mdt data mdt-group-address / [mask] [threshold threshold-value] [acl-name]
no mdt data mdt-group-address /prefix-length [threshold threshold-value] [acl-name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mdt-group-address</code></td>
<td>IP address of the MDT group.</td>
</tr>
<tr>
<td><code>/ mask</code></td>
<td>A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash must precede the decimal value.</td>
</tr>
<tr>
<td><code>threshold threshold-value</code></td>
<td>Specifies the traffic rate threshold to trigger data MDT. Range is 1 to 4294967295.</td>
</tr>
<tr>
<td><code>acl-name</code></td>
<td>Access list (ACL) for the customer’s VRF groups allowed to perform data MDT.</td>
</tr>
</tbody>
</table>

**Command Default**

`threshold : 1`

**Command Modes**

Multicast routing configuration

Multicast routing address family IPv4 and IPv6 configuration

Multicast VRF configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.5.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>3.7.0</td>
<td>Additional keyword information was added to the command.</td>
</tr>
<tr>
<td></td>
<td>The bottom of the threshold value range was increased by 1.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When certain multicast streams exceed a configured bandwidth, the multicast data is moved to an MDT data group that is dynamically chosen from an available pool of multicast addresses. If the traffic bandwidth falls below the threshold, the source is switched back to the default MDT. To avoid transitions between the MDTs, traffic only reverts to the default MDT if traffic below the data MDT threshold is at least one minute old.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the data MDT group:
RP/0/RSP0/CPU0:router# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# mdt data 172.23.2.2/24 threshold 1200 acl_A

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mdt default, on page 135</td>
<td>Configures the default group address of the multicast VPN (MVPN) multicast distribution tree (MDT).</td>
</tr>
<tr>
<td>mdt mtu, on page 137</td>
<td>Configures the maximum transmission unit (MTU) configuration of the multicast VPN (MVPN) multicast distribution tree (MDT).</td>
</tr>
<tr>
<td>mdt source, on page 138</td>
<td>Configures the interface used to set the multicast VPN (MVPN) data multicast distribution tree (MDT) source address.</td>
</tr>
</tbody>
</table>
**mdt data ingress replication**

To configure ingress replication (IR) data for Multicast Distribution Trees (MDT), use the `mdt data ingress replication` command in the appropriate mode. To remove the configuration, use the `no` form of the command.

```shell
mdt data ingress replication [ acl_name | immediate-switch | number value | threshold value ]
no mdt data ingress replication [ acl_name | immediate-switch | number value | threshold value ]
```

**Syntax Description**

- `immediate-switch` Enables switching to data MDT immediately.
- `acl_name` ACL for vrf groups that are enabled for data MDT
- `number value` Maximum number of data MDTs to be triggered. Range is 1 to 262143.
- `immediate-switch value` Traffic rate threshold (in kbps) to trigger data MDT. Range is 1 to 4294967.

**Command Default**

None

**Command Modes**

Multicast routing VRF address-family configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to run the `mdt data ingress replication` command:

```shell
RP/0/RSP0/CP0:router (config-mcast-v1-ipv4) # mdt data ingress-replication immediate-switch
```
**mdt default**

To configure the default group address of the multicast VPN (MVPN) multicast distribution tree (MDT), use the `mdt default` command in the appropriate configuration mode. To remove this functionality, use the `no` form of this command.

```
mdt default {mdt-default-group-address|ipv4 mdt-default-address}
no mdt default {mdt-default-group-address|ipv4 mdt-default-address}
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mdt-default-group-address</code></td>
<td>IP address of the MDT default group entered in <code>A.B.C.D.</code> format.</td>
</tr>
<tr>
<td><code>ipv4</code></td>
<td>Specifies IPv4-encapsulated MDT.</td>
</tr>
<tr>
<td><code>mdt-default-address</code></td>
<td>MDT IPv4 default address entered in <code>A.B.C.D.</code> format</td>
</tr>
</tbody>
</table>

**Command Default**
The MDT default group address must be unique.

**Command Modes**
Multicast routing configuration  
Multicast routing address family IPv4 and IPv6 configuration  
Multicast VRF configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.5.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>3.7.0</td>
<td>Additional keyword information was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The default MDT has a unique group address used to create MVPN multicast tunnel interfaces.

Although within the multicast VRF configuration submode, the MDT configuration uses either the `ipv4` or `ipv6` keyword to distinguish the appropriate multicast VPN, the MDT core tree is IPv4.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to configure the MDT default group address from multicast routing configuration mode:

```
RP/0/RSP0/CPU0:router# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# mdt default
172.16.10.1
```
The following example shows how to configure the MDT default group address from multicast VRF configuration submode for an IPv6 address family:

```
RP/0/RSP0/CPU0:router# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# vrf vrf-name address-family ipv6
RP/0/RSP0/CPU0:router(config-mcast-vrf-name-ipv6)# mdt default 172.16.10.1
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mdt data, on page 132</td>
<td>Configures multicast data to be part of a multicast distribution tree (MDT) data group for multicast VPN (MVPN).</td>
</tr>
<tr>
<td>mdt mtu, on page 137</td>
<td>Configures the maximum transmission unit (MTU) configuration of the multicast VPN (MVPN) multicast distribution tree (MDT).</td>
</tr>
<tr>
<td>mdt source, on page 138</td>
<td>Configures the interface used to set the multicast VPN (MVPN) data multicast distribution tree (MDT) source address.</td>
</tr>
</tbody>
</table>
**mdt mtu**

To configure the maximum transmission unit (MTU) configuration of the multicast VPN (MVPN) multicast distribution tree (MDT), use the `mdt mtu` command in multicast VPN configuration mode. To remove this functionality, use the `no` form of this command.

```
mdt mtu  value
no mdt mtu  value
```

**Syntax Description**

- `value` Specifies the MTU value and ranges between 401 to 65535. The configured mdt mtu value includes 24 bytes of GRE encapsulation.

**Command Default**

The MDT tunnel default size is 1376.

**Command Modes**

Multicast VRF configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.5.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Examples**

The following example shows how to configure the MTU of the multicast distribution tree:

```
RP/0/RSP0/CPU0:router# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# vrf vrf_A
RP/0/RSP0/CPU0:router(config-mcast-vrf_A-ipv4)# mdt mtu 2345
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mdt data</code>, on page 132</td>
<td>Configures multicast data to be part of a multicast distribution tree (MDT) data group for multicast VPN (MVPN).</td>
</tr>
<tr>
<td><code>mdt default</code>, on page 135</td>
<td>Configures the default group address of the multicast VPN (MVPN) multicast distribution tree (MDT).</td>
</tr>
<tr>
<td><code>mdt source</code>, on page 138</td>
<td>Configures the interface used to set the multicast VPN (MVPN) data multicast distribution tree (MDT) source address.</td>
</tr>
</tbody>
</table>
**mdt source**

To configure the interface used to set the multicast VPN (MVPN) data multicast distribution tree (MDT) source address, use the `mdt source` command in the appropriate configuration mode. To remove this functionality, use the `no` form of this command.

```markdown
**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>type</td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note** Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

No default behavior or values

**Command Modes**

- Multicast routing configuration
- Multicast routing address family IPv4 configuration
- Multicast VRF configuration

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `mdt source` command to identify the root of the multicast distribution tree in the service provider network. This address is used to update all MVPN peers through multiprotocol BGP.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the interface used to set the MDT source address:

```plaintext
RP/0/RSP0/CPU0:router# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# mdt source POS 0/1/0/0
```

**Note** Per VRF MDT Source is a new feature introduced in IOS XR Software Release 3.9.0 apart from the existing default MDT source. Each VRF can have its own MDT source interface co-existing with the default MDT source to achieve core diversity.
The following example shows how to configure a per VRF MDT source:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# address-family ipv4
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4)# mdt source loopback0
RP/0/RSP0/CPU0:router(config-mcast)# vrf foo
RP/0/RSP0/CPU0:router(config-mcast-foo)# address-family ipv4
RP/0/RSP0/CPU0:router(config-mcast-foo-ipv4)# mdt source loopback1
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mdt data, on page 132</td>
<td>Configures multicast data to be part of a multicast distribution tree (MDT) data group for multicast VPN (MVPN).</td>
</tr>
<tr>
<td>mdt default, on page 135</td>
<td>Configures the default group address of the multicast VPN (MVPN) multicast distribution tree (MDT).</td>
</tr>
<tr>
<td>mdt mtu, on page 137</td>
<td>Configures the maximum transmission unit (MTU) configuration of the multicast VPN (MVPN) multicast distribution tree (MDT).</td>
</tr>
</tbody>
</table>
migration route-policy

To support PIM And BGP c-multicast joins over the same or different MDTs, use the `migration route-policy` command in the appropriate mode. To disable the migration, use the `no` form of the command.

```
migration route-policy policy-name
nomigration route-policy policy-name
```

**Syntax Description**

- `policy-name` Name of the policy.

**Command Default**

None

**Command Modes**

C-multicast routing configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The policy name is used to match the upstream PEs (nexthop) and send joins through BGP or PIM.

**Task ID**

```
read, write
```

**Example**

This example shows how to use the `migration route-policy` command:

```
RP/0/RSP0/CPU0:router (config-pim-v1-ipv4-mdt-cmcast) # migration route-policy pl
```
**multicast-routing**

To enter multicast routing configuration mode, use the `multicast-routing` command in global configuration mode. To return to the default behavior, use the `no` form of this command.

```
multicast-routing
no multicast-routing
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

No default behavior or values.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Examples**

The following example shows how to enter multicast routing configuration mode:

```
RP/0/RSP0/CPU0:router(config)# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)#
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting per-prefix, on 105</td>
<td>Enables per-prefix counters only in hardware.</td>
</tr>
<tr>
<td>alias</td>
<td>Creates a command alias.</td>
</tr>
<tr>
<td>interface (multicast), on 123</td>
<td>Configures multicast interface properties.</td>
</tr>
<tr>
<td>interface all enable, on 125</td>
<td>Enables multicast routing and forwarding on all new and existing interfaces.</td>
</tr>
</tbody>
</table>
**multipath**

To enable Protocol Independent Multicast (PIM) to divide the multicast load among several equal cost paths, use the `multipath` command in the appropriate configuration mode. To return to the default behavior, use the `no` form of this command.

```
[address-family ipv4] multipath [hash {source|source next-hop}]
no multipath
```

**Syntax Description**
- `hash` (Optional) Enables multipath hashing.
- `source` Enables source-based multipath hashing.
- `source-next-hop` (Optional) Enables source with next-hop hashing.

**Command Default**
This command is disabled by default.

**Command Modes**
- Multicast routing configuration
- Multicast routing address-family ipv4
- Multicast VRF configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

By default, equal-cost multipath (ECMP) paths are not load balanced. A single path from each unicast route is used for all multicast routes (which is the equivalent of the `no` form of the `multipath` command).

**Task ID**
```
Task ID  Operations
multicast  read, write
```

**Examples**
The following example shows how to enable multipath functionality:

```
RP/0/RSP0/CPU0:router(config)# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# multipath hash
```
nsf (multicast)

To turn on the nonstop forwarding (NSF) capability for the multicast routing system, use the `nsf` command in multicast routing configuration mode. To turn off this function, use the `no` form of this command.

```
nsf [lifetime seconds]
nof nsf [lifetime]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>lifetime seconds</th>
<th>(Optional) Specifies the maximum time (in seconds) for NSF mode. Range is 30 to 3600.</th>
</tr>
</thead>
</table>

**Command Default**

This command is disabled by default.

**Command Modes**

- Multicast routing configuration
- Multicast routing address family ipv4 configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `nsf` command does not enable or disable the multicast routing system, but just the NSF capability for all the relevant components. When the `no` form of this command is used, the NSF configuration is returned to its default disabled state.

Enable multicast NSF when you require enhanced availability of multicast forwarding. When enabled, failures of the control-plane multicast routing components Multicast Routing Information Base (MRIB) or Protocol Independent Multicast (PIM) will not cause multicast forwarding to stop. When these components fail or communication with the control plane is otherwise disrupted, existing Multicast Forwarding Information Base (MFIB) entries continue to forward packets until either the control plane recovers or the MFIB NSF timeout expires.

Enable multicast NSF when you upgrade control-plane Cisco IOS XR Software packages so that the live upgrade process does not interrupt forwarding.

When the MFIB partner processes enter NSF mode, forwarding on stale (nonupdated) MFIB entries continues as the control-plane components attempt to recover gracefully. Successful NSF recovery is signaled to the Multicast Forwarding Engine (MFWD) partner processes by MRIB. MRIB remains in NSF mode until Internet Group Management Protocol (IGMP) has recovered state from the network and host stack and until PIM has recovered state from the network and IGMP. When both PIM and IGMP have recovered and fully updated the MRIB, MRIB signals the MFIBs that NSF is ending, and begins updating the stale MFIB entries. When all updates have been sent, the MFWD partner processes delete all remaining stale MFIB entries and returns to normal operation, ending the NSF mode. MFIB NSF timeout prior to the signal from MRIB may cause NSF to end, and thus forwarding to stop.

When forwarding is in NSF mode, multicast flows may continue longer than necessary when network conditions change due to multicast routing protocols, unicast routing protocol reachability information, or local sender and receiver changes. The MFWD partner processes halt forwarding on stale MFIB entries when the potential
for a multicast loop is detected by receipt of incoming data on a forwarding interface for the matching MFIB entry.

**Note** For NSF to operate successfully in your multicast network, you must also enable NSF for the unicast protocols (such as Intermediate System-to-Intermediate System [IS-IS], Open Shortest Path First [OSPF] and Border Gateway Protocol [BGP]) that PIM relies on for Reverse Path Forwarding (RPF) information. See the appropriate configuration modules to learn how to configure NSF for unicast protocols.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to enable NSF for the multicast routing system:

```
RP/0/RSP0/CPU0:router(config)# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# nsf
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>nsf lifetime (IGMP)</code></td>
<td>Configures the maximum time for the NSF timeout value under IGMP.</td>
</tr>
<tr>
<td><code>nsf lifetime (PIM)</code></td>
<td>Configures the NSF timeout value for the PIM process.</td>
</tr>
<tr>
<td><code>show igmp nsf</code></td>
<td>Displays the state of NSF operation in IGMP.</td>
</tr>
<tr>
<td><code>show mfib nsf</code></td>
<td>Displays the state of NSF operation for the MFIB line cards.</td>
</tr>
<tr>
<td><code>show mrib nsf, on page 216</code></td>
<td>Displays the state of NSF operation in the MRIB.</td>
</tr>
<tr>
<td><code>show pim nsf</code></td>
<td>Displays the state of NSF operation for PIM.</td>
</tr>
</tbody>
</table>
oom-handling

To enable the out-of-memory (OOM) functionality on multicast routing software components, use the oom-handling command in multicast routing configuration mode. To remove this functionality, use the no form of this command.

oom-handling
no oom-handling

Syntax Description
This command has no keywords or arguments.

Command Default
This command is disabled by default.

Command Modes
Multicast routing configuration
Multicast routing address family ipv4 configuration

Command History
Release Modification
Release 3.7.2 This command was introduced.

Usage Guidelines
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When the oom-handling command is enabled, and the router memory is low or in a warning state, the following states are not created:

- Protocol Independent Multicast (PIM) route states in response to PIM join and prune messages, and register messages
- Internet Group Management Protocol (IGMP) group states
- External Source-Active (SA) states in Multicast Source Discovery Protocol (MSDP)

Multicast routing show commands such as the show pim topology command indicate when the router is running low on memory and that new state creation has stopped.

Task ID
Task ID Operations
multicast read, write

Examples
The following example shows how to enable the out-of-memory functionality:

RP/0/RSP0/CPU0:router# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# oom-handling

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show pim topology</td>
<td>Displays PIM topology table information.</td>
</tr>
</tbody>
</table>
# rate-per-route

To enable individual (source, group [S, G]) rate calculations, use the **rate-per-route** command in the appropriate configuration mode. To remove this functionality, use the **no** form of this command.

```plaintext
rate-per-route
no rate-per-route
```

## Syntax Description

This command has no keywords or arguments.

## Command Default

This command is disabled by default.

## Command Modes

Multicast routing configuration

Multicast routing address family ipv4 configuration

Multicast VRF configuration

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

## Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

## Examples

The following example shows how to enable individual route calculations:

```plaintext
RP/0/RSP0/CPU0:router# multicast-routing vrf vpn12 address-family ipv4
RP/0/RSP0/CPU0:router(config-mcast)# rate-per-route
```

## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mfib route, on page 204</td>
<td>Displays route entries in the Multicast Forwarding Information Base (MFIB).</td>
</tr>
</tbody>
</table>
shared-tree-prune delay

To set or change the prune installation time, use the `shared-tree-prune-delay` command in the appropriate mode. To disable the set time, use the `no` form of the command.

```
shared-tree-prune-delay  time
no shared-tree-prune-delay  time
```

**Syntax Description**

- `time`  Delay in seconds. Range is 0 to 1800.

**Command Default**

60 seconds (for upstream prune)

**Command Modes**

C-multicast-routing configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command is used to change the prune installation time (C-S, C-G, RPT). This is required on PEs connected to the C-RP (under certain conditions), when a Type-5 route is received. This is applicable only to BGP C-multicast Routing.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to use the `shared-tree-prune-delay` command:

```
RP/0/RSP0/CPU0:router (config-pim-v1-ipv4-mdt-cmcast) # shared-tree-prune-delay 100
```
show mfib bvi

To display the Bridge Virtual Interface (BVI) details in the Multicast Forwarding Information Base (MFIB), use the `show mfib bvi` command in EXEC mode.

`show mfib bvi [interface | route] bvi_number`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>MFIB BVI interface.</td>
</tr>
<tr>
<td>route</td>
<td>BVI route entry.</td>
</tr>
<tr>
<td>bvi_number</td>
<td>BVI interface number. Range is from 1 to 65535.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.1.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to run the `show mfib bvi` command:

```
RP/0/RSP0/CPU0:router # show mfib bvi route bvi 200
```
show mfib connections

To display the status of Multicast Forwarding Information Base (MFIB) connections to servers, use the `show mfib connections` command in the appropriate mode.

### Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IPv4 address prefixes.</td>
</tr>
<tr>
<td>ipv6</td>
<td>(Optional) Specifies IPv6 address prefixes.</td>
</tr>
<tr>
<td>location node-id</td>
<td>(Optional) Specifies MFIB connections associated with an interface of the designated node.</td>
</tr>
</tbody>
</table>

### Command Default

IPv4 addressing is the default.

### Command Modes

EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `show mfib connections` command to display a list of servers connected to the MFIB and the status of the connections.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>multicast</td>
</tr>
<tr>
<td></td>
<td>read</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `show mfib connections` command:

```
RP/0/RSP0/CPU0:router# show mfib connections

Netio         : connected
IM            : connected
Pakman        : connected
MRIB          : connected
IFH           : connected
SysDB-Global  : connected
SysDB-Local   : connected
SysDB-NSF     : connected
SYSDB-EDM     : connected
SYSDB-Action  : connected
AIB           : connected
MLIB          : connected
IDB           : connected
IIR           : connected
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mfib interface, on page 200</code></td>
<td>Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.</td>
</tr>
<tr>
<td><code>show mfib route, on page 204</code></td>
<td>Displays route entries in the Multicast Forwarding Information Base (MFIB).</td>
</tr>
</tbody>
</table>
show mfib counter

To display Multicast Forwarding Information Base (MFIB) counter statistics for packets that have dropped, use the `show mfib counter` command in the appropriate mode.

```
show mfib [vrf vrf-name] ipv4 counter [location node-id]
```

**Syntax Description**
- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `location node-id` (Optional) Specifies MFIB counter statistics associated with an interface of the designated node.

**Command Default**
IPv4 addressing is the default.

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `show mfib counter` command displays packet drop statistics for packets that cannot be accounted for under route counters.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show mfib counter` command:

```
RP/0/RSP0/CPU0:router# show mfib counter location 0/1/CPU0

MFIB global counters are :
* Packets [no input idb] : 0
* Packets [failed route lookup] : 0
* Packets [Failed idb lookup] : 0
* Packets [Mcast disabled on input I/F] : 0
* Packets [encap drops due to ratelimit] : 0
* Packets [MC disabled on input I/F (iarm nfn)] : 0
```
This table describes the significant fields shown in the display.

### Table 15: show mfib counter Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets [no input idb]</td>
<td>Packets dropped because no input interface information was found in the packet.</td>
</tr>
<tr>
<td>Packets [failed route lookup]</td>
<td>Packets dropped because of failure to match any multicast route.</td>
</tr>
<tr>
<td>Packets [Failed idb lookup]</td>
<td>Packets dropped because the descriptor block was not found for an interface (incoming or outgoing).</td>
</tr>
<tr>
<td>Packets [Mcast disabled on input I/F]</td>
<td>Packets dropped because arriving on an interface that was not enabled for the multicast routing feature.</td>
</tr>
<tr>
<td>Packets [encap drops due to ratelimit]</td>
<td>Packets dropped because of rate limit.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mfib interface, on page 200</td>
<td>Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.</td>
</tr>
<tr>
<td>show mfib route, on page 204</td>
<td>Displays route entries in the Multicast Forwarding Information Base (MFIB).</td>
</tr>
</tbody>
</table>
**show mfib encap-info**

To display the status of encapsulation information for Multicast Forwarding Information Base (MFIB), use the `show mfib encap-info` command in the appropriate mode.

```
show mfib [vrf vrf-name] [{ipv4|ipv6}] encap-info [location node-id]
```

**Syntax Description**

- **vrf vrf-name** (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- **ipv4** (Optional) Specifies IPv4 address prefixes.
- **ipv6** (Optional) Specifies IPv6 address prefixes.
- **location node-id** (Optional) Specifies MFIB connections associated with an interface of the designated node.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show mfib encap-info` command:

```
RP/0/RSP0/CPU0:router# show mfib vrf vrf_a encap-info

----------------------------
Encaps String          Dependent Routes #  Encaps Table ID  MDT Name/Handle
(192.168.5.203, 255.1.1.1)  5               0xe0000000  mdtA1 (0x100a480)
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mfib interface</code>, on page 200</td>
<td>Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>show mfib route, on page 204</td>
<td>Displays route entries in the Multicast Forwarding Information Base (MFIB).</td>
</tr>
</tbody>
</table>
show mfib hardware interface

To display hardware switching interface information for the Multicast Forwarding Information Base (MFIB) process, use the `show mfib hardware interface` command in EXEC mode.

```
show mfib [vrf vrf-name] [ipv4|ipv6] hardware interface [detail] [type interface-path-id] [location node-id]
```

**Syntax Description**

- **vrf vrf-name**  
  (Optional) Specifies a VPN routing and forwarding (VRF) instance.

- **ipv4**  
  (Optional) Specifies IPv4 address prefixes.

- **ipv6**  
  (Optional) Specifies IPv6 address prefixes.

- **detail**  
  (Optional) Displays detailed information about the MFIB interface.

- **type**  
  (Optional) Interface type. For more information, use the question mark (?) online help function.

- **interface-path-id**  
  (Optional) Physical interface or virtual interface.

  **Note**  
  Use the `show interfaces` command to see a list of all interfaces currently configured on the router.

  For more information about the syntax for the router, use the question mark (?) online help function.

- **location node-id**  
  (Optional) Specifies an MFIB-designated node.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `show mfib hardware interface` command displays multicast-specific information about the software switching interfaces of the router hardware. This command will not display any useful output if only RSP is specified or if no location is specified.
The following is sample output from the `show mfib hardware interface` command.

```
RP/0/RSP0/CPU0:router# show mfib hardware interface location 0/0/CPU0

LC Type: Trident

<table>
<thead>
<tr>
<th>Interface Handle</th>
<th>RefCnt</th>
<th>TTL</th>
<th>Routes uIDB</th>
<th>Enbld</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/0/0/4</td>
<td>0x180</td>
<td>5</td>
<td>0</td>
<td>2</td>
<td>True</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>success</td>
</tr>
<tr>
<td>Gi0/0/0/5</td>
<td>0x1c0</td>
<td>27</td>
<td>0</td>
<td>6</td>
<td>True</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>success</td>
</tr>
<tr>
<td>Gi0/0/0/6</td>
<td>0x200</td>
<td>5</td>
<td>0</td>
<td>2</td>
<td>True</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>success</td>
</tr>
<tr>
<td>Gi0/0/0/7</td>
<td>0x240</td>
<td>25</td>
<td>0</td>
<td>8</td>
<td>True</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>success</td>
</tr>
<tr>
<td>Gi0/0/0/8</td>
<td>0x280</td>
<td>30</td>
<td>0</td>
<td>9</td>
<td>True</td>
</tr>
</tbody>
</table>

ROUTE INFORMATION:
Legend:
  S: Source, G: Group, P: Prefix length, PI: Packets cn, PO: packets out,
  RF: RPF failures, TF: TTL failures, OF: OLIST failures, F: Other failures
Route flags - (Ingress)
  C: Chip ID, IC: BACL check, IP: Punt this packet to LC CPU,
  ID: Directly connected, IS: RPF interface signal, IU: Punt copy to RP,
  IF: Punt to LC CPU if forwarded, IM: Result match, IV: Valid entry,
  IR: RPF IF, IA: Fabric slotmask, IG: Multicast group ID
Route flags - (Egress)
  ET: Table ID to be used for OLIST lookup, EO: OLIST count bit,
  ER: Route MGID to be used for OLIST/NRPF lookup, EM: Result match,
  EV: Valid entry, EC: Count of OLIST members on this chip,
  BS: Base of the statistics pointer

Interface: Gi0/0/0/4
S: 4.0.0.2  G: 227.0.0.1  P: 32  PI: 1  PO: 0  RF: 0  TF: 0  OF: 0  F: 0

| C | IC | IP | ID | IS | IU | IF | IM | IV | IR | IA | ET | EO | ER | EM | EV | EC | BS     |
|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|------|
| 0 | F  | F  | F  | F  | F  | T  | T  | 0x180 | 0x1 | 0x8006 | 0 | F  | 6  | T  | T  | 0   | 0x5518a  |
| 1 | F  | F  | F  | F  | F  | T  | T  | 0x180 | 0x1 | 0x8006 | 0 | F  | 6  | T  | T  | 0   | 0x5518a  |
| 2 | F  | F  | F  | F  | F  | T  | T  | 0x180 | 0x1 | 0x8006 | 0 | F  | 6  | T  | T  | 0   | 0x5518a  |
| 3 | F  | F  | F  | F  | F  | T  | T  | 0x180 | 0x1 | 0x8006 | 1 | T  | 6  | T  | T  | 3   | 0x555c2  |

Interface: Gi0/0/0/5
This interface is not part of the olist of any route

Interface: Gi0/0/0/6
S: 4.0.0.2  G: 227.0.0.1  P: 32  PI: 1  PO: 0  RF: 0  TF: 0  OF: 0  F: 0

<table>
<thead>
<tr>
<th>C</th>
<th>IC</th>
<th>IP</th>
<th>ID</th>
<th>IS</th>
<th>IU</th>
<th>IM</th>
<th>IV</th>
<th>IR</th>
<th>IA</th>
<th>ET</th>
<th>EO</th>
<th>ER</th>
<th>EM</th>
<th>EV</th>
<th>EC</th>
<th>BS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x1</td>
<td>0x8004</td>
<td>0</td>
<td>F</td>
<td>5</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x1</td>
<td>0x8004</td>
<td>0</td>
<td>F</td>
<td>5</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x1</td>
<td>0x8004</td>
<td>0</td>
<td>F</td>
<td>5</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x1</td>
<td>0x8004</td>
<td>1</td>
<td>T</td>
<td>5</td>
<td>T</td>
<td>T</td>
<td>3</td>
</tr>
</tbody>
</table>
The following example shows a sample output for `show mfib hardware interface` command on the Cisco ASR 9000 Series SIP-700 line card:

```
RP/0/RSP0/CPU0# show mfib hardware interface serial 0/4/0/0/1 location 0/4/CPU0
LC Type: A9K-SIP-700

Hardware Interface Information

Interface Handle Type TTL Number of Routes Multicast Enabled Num bundles
Se0/4/0/0/1 0xc000ec0 0 0 2 True 0
```

Header : IDB Route Information
Source : Source address
Group : Group Address
M : Mask Length
show mfib hardware interface

<table>
<thead>
<tr>
<th>PI</th>
<th>Packets in</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO</td>
<td>Packets out</td>
</tr>
<tr>
<td>RF</td>
<td>RPF failures</td>
</tr>
<tr>
<td>TF</td>
<td>TTL failures</td>
</tr>
<tr>
<td>OF</td>
<td>OLIST failures</td>
</tr>
<tr>
<td>F</td>
<td>Other failures</td>
</tr>
<tr>
<td>C</td>
<td>Directly connected check flag</td>
</tr>
<tr>
<td>RPF</td>
<td>Accepting interface for non-bidir entries</td>
</tr>
<tr>
<td>S</td>
<td>Signal if packet arrived on RPF interface</td>
</tr>
<tr>
<td>IC</td>
<td>Aggregated Internal copy flag</td>
</tr>
<tr>
<td>PR</td>
<td>Punt to RP flag for Internal copy in the Loopback interface</td>
</tr>
<tr>
<td>PK</td>
<td>PEEK flag</td>
</tr>
<tr>
<td>FGID</td>
<td>Fabric Group ID</td>
</tr>
<tr>
<td>MGID</td>
<td>Multicast Group ID</td>
</tr>
</tbody>
</table>

Interface: Se0/4/0/0/1

Source: 12.12.12.2 Group: 225.0.0.0 M: 64 PI: 1 PO: 0 RF: 0 TF: 0 OF: 0 F: 0
C: F RPF: Se0/4/0/0/1 S: F IC: F PR: F PK: F FGID: 64 MGID: 17024

Ingress CPP Prefix Information
-----------------------------------

--- QFP Multicast prefix info ---
Root: 9dcbcfb0, Flags: 0 First leaf: 9dcbccfc
Number of nodes: 0x000001, leaves: 0x000001 RPF i/f: 0x007fff
RPF Fast Convergence flags: 00000000 Secondary RPF: 00000000
RPF Fast Convergence timer: 0 ext_leaf: 0x8b900200

Egress CPP Prefix Information
-----------------------------------

--- QFP Multicast prefix info ---
Root: 9dcbcfb0, Flags: 0 First leaf: 9dcbccfc
Number of nodes: 0x000001, leaves: 0x000001 RPF i/f: 0x007fff
RPF Fast Convergence flags: 00000000 Secondary RPF: 00000000
RPF Fast Convergence timer: 0 ext_leaf: 0x8ce80200

Route OCE Entry Information
-----------------------------------

**** Leaf Info (in cp): [9dcbccfc]
oce flags = 0x2 next obj type : 11 next obj handle : a73e9104
**** Leaf Info (in cpp): [0]
leaf_flags= 0x1 oce_flags: 0 oce_ptr: 0x8c5800c0

Source: 0.0.0.0 Group: 225.0.0.0 M: 32 PI: 1 PO: 0 RF: 0 TF: 0 OF: 0 F: 0
C: T RPF: Se0/4/0/0/1 S: F IC: F PR: F PK: F FGID: 64 MGID: 17013

Ingress CPP Prefix Information
-----------------------------------

--- QFP Multicast prefix info ---
Root: 9dcbd530, Flags: 2 First leaf: 9dcbd9bc
Number of nodes: 0x000001, leaves: 0x000001 RPF i/f: 0x007fff
RPF Fast Convergence flags: 00000000 Secondary RPF: 00000000
RPF Fast Convergence timer: 0 ext_leaf: 0x8b900080

Egress CPP Prefix Information
-----------------------------------

--- QFP Multicast prefix info ---
Root: 9dcbd530, Flags: 2 First leaf: 9dcbd9bc
Number of nodes: 0x000001, leaves: 0x000001 RPF i/f: 0x007fff

Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference, Release 5.3.x
RPF Fast Convergence flags: 00000000 Secondary RPF: 00000000
RPF Fast Convergence timer: 0 ext_leaf: 0x8ce80080

Route OCE Entry Information

---------------------------------------------

**** Leaf Info (in cp) : [9dcbd9bc]
oce flags = 0x6 next obj type : 11 next obj handle : a73e9104
**** Leaf Info (in cpp): [0]
leaf_flags= 0x1 oce_flags: 0 oce_ptr: 0x8c5800c0

This table describes the significant fields shown in the display.

Table 16: show mfib hardware interface Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>MFIB interface name.</td>
</tr>
<tr>
<td>Handle</td>
<td>A 32-bit system-wide identifier of the MFIB interface.</td>
</tr>
<tr>
<td>RefCnt</td>
<td>Number of times various data structures referred to this MFIB interface.</td>
</tr>
<tr>
<td>TTL</td>
<td>Multicast time-to-live threshold that was configured on this MFIB interface.</td>
</tr>
<tr>
<td>Routes</td>
<td>The number of routes that include this interface as a member.</td>
</tr>
<tr>
<td>uIDB</td>
<td>The ucode Interface Descriptor Block index.</td>
</tr>
<tr>
<td>Enbld</td>
<td>If true, multicast is enabled on the MFIB interface.</td>
</tr>
<tr>
<td>Comment</td>
<td>Indicates whether there were problems when reading hardware information.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mfib interface, on page 200</td>
<td>Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.</td>
</tr>
</tbody>
</table>
**show mfib hardware ltrace**

To display IP Multicast platform specific trace information for the Multicast Forwarding Information Base (MFIB) process, use the `show mfib hardware ltrace` command in EXEC mode.

```
show mfib [vrf vrf-name] [ipv4|ipv6] hardware ltrace
[{{error|event|frequent-event|hexdump|init|last|netio|reverse|stats|tail|unique|verbose|wrapping}}] file
file-name location node-id
```

**Syntax Description**

- **vrf vrf-name** (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- **ipv4** (Optional) Specifies IPv4 address prefixes.
- **ipv6** (Optional) Specifies IPv6 address prefixes.
- **error** (Optional) Displays error events.
- **event** (Optional) Displays non-frequent events.
- **frequent-event** (Optional) Displays frequent events.
- **hexdump** (Optional) Displays traces in hexadecimal output.
- **init** (Optional) Displays initiation and configuration events.
- **last** (Optional) Displays the last n entries.
- **netio** (Optional) Displays the netio events.
- **reverse** (Optional) Displays the traces in the reverse order starting with the latest events.
- **stats** (Optional) Displays the statistics.
- **tail** (Optional) Displays the new traces as they are added.
- **unique** (Optional) Displays the unique entries with the counts.
- **verbose** (Optional) Displays the internal debugging information.
- **wrapping** (Optional) Displays the wrapping entries.
- **file file-name** (Optional) Specifies the file name.
- **location node-id** Specifies an MFIB-designated node.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC
Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Note

This command will not display any useful output if only RSP is specified or if no location is specified.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>multicast</td>
</tr>
<tr>
<td></td>
<td>read</td>
</tr>
</tbody>
</table>

Examples

The following is sample output from the **show mfib hardware ltrace** command:

```
RP/0/RSP0/CPU0:router# show mfib hardware ltrace error location 0/1/cpu

3079 wrapping entries (4096 possible, 0 filtered, 4242 total)
May 21 01:45:32.865 ipmcast/error 0/1/CPU0 t1 Traffic Loss msg rxed, Null Route
, cntid=0x705f0
May 21 01:45:32.877 ipmcast/error 0/1/CPU0 t1 Traffic Loss msg rxed, Null Route
, cntid=0x705f2
May 21 01:58:37.019 ipmcast/error 0/1/CPU0 t1 Traffic Loss msg rxed, Null Route
, cntid=0x705f0
May 21 01:58:37.019 ipmcast/error 0/1/CPU0 t1 Traffic Loss msg rxed, Null Route
, cntid=0x705f2
```

The following is a sample output for the **show mfib hardware ltrace** command on the Cisco ASR 9000 Series SIP-700 line card:

```
RP/0/RSP0/CPU0:router# show mfib hardware ltrace location 0/4/CPU0

438 wrapping entries (88064 possible, 0 filtered, 438 total)
Aug 25 00:22:02.978 mfwd_ipv4_hw/init 0/4/CPU0 t1 ===> Proc started jid=199, pid=163944
Aug 25 00:22:02.978 mfwd_ipv4_hw/event 0/4/CPU0 t1 ===> Proc started jid=199, pid=163944
Aug 25 00:22:02.978 mfwd_ipv4_hw/error 0/4/CPU0 t1 ===> Proc started jid=199, pid=163944
Aug 25 00:22:02.978 mfwd_ipv4_hw/event 0/4/CPU0 t1 ===> Proc started jid=199, pid=163944
Aug 25 00:22:02.978 mfwd_ipv4_hw/netio 0/4/CPU0 t1 ===> Proc started jid=199, pid=163944
Aug 25 00:22:03.001 mfwd_ipv4_hw/init 0/4/CPU0 t1 MFWD: Platform lib initialization started
```
Aug 25 00:22:03.001 mfwd_ipv4_hw/init 0/4/CPU0 t1 Successfully got shared memory window header
Aug 25 00:22:03.001 mfwd_ipv4_hw/init 0/4/CPU0 t1 Platform extension does not exist - cold boot
Aug 25 00:22:03.042 mfwd_ipv4_hw/init 0/4/CPU0 t1 CPP IPMC Gtrie Lib Init done: rc=0
Aug 25 00:22:03.075 mfwd_ipv4_hw/init 0/4/CPU0 t1 Library not initialized previously, establishing connections
Aug 25 00:22:23.990 mfwd_ipv4_hw/init 0/4/CPU0 t1 CPP IPMC PAL Lib Init done: rc=0
Aug 25 00:22:24.851 mfwd_ipv4_hw/init 0/4/CPU0 t1 CPP IPMC iox Init done: rc=0
Aug 25 00:22:24.852 mfwd_ipv4_hw/init 0/4/CPU0 t1 Successfully initiated thread ctx and API ctx
Aug 25 00:22:24.871 mfwd_ipv4_hw/init 0/4/CPU0 t1 Successfully done binding with CPP GIC Server
Aug 25 00:22:24.906 mfwd_ipv4_hw/init 0/4/CPU0 t1 Successfully binded with CPP Tx Adjacency APIs Lib
Aug 25 00:22:24.904 mfwd_ipv4_hw/init 0/4/CPU0 t1 Successfully binded with CPP Rx Adjacency APIs Lib
Aug 25 00:22:24.902 mfwd_ipv4_hw/init 0/4/CPU0 t1 Successfully binded with CPP Tx Adjacency APIs Lib
Aug 25 00:22:24.906 mfwd_ipv4_hw/init 0/4/CPU0 t1 Successfully binded with CPP Rx Adjacency APIs Lib
Aug 25 00:22:25.000 mfwd_ipv4_hw/init 0/4/CPU0 t1 Initialized interface lib
Aug 25 00:22:25.000 mfwd_ipv4_hw/init 0/4/CPU0 t1 MFWD: Platform lib initialization completed
Aug 25 00:22:26.046 mfwd_ipv4_hw/event 0/4/CPU0 t1 table: table id -536870912 vrf id 1610612736 got created/commit table_ext 0x9dc89c10
Aug 25 00:22:26.098 mfwd_ipv4_hw/init 0/4/CPU0 t1 gtrie: Platform gtrie lib init started
Aug 25 00:22:26.099 mfwd_ipv4_hw/init 0/4/CPU0 t1 gtrie: successfully initiated gtrie 0xa6039dec for protocol 0, table id 0, use shmem 1, shmem id 1
Aug 25 00:24:25.780 mfwd_ipv4_hw/event 0/4/CPU0 t1 CPP Create adj cpp 1 adj handle 0xa73e90c0 ifh 98 link 1 enctype 0 flags 1 hw addr 0x8c580010
Aug 25 00:24:25.876 mfwd_ipv4_hw/event 0/4/CPU0 t1 CPP Create adj cpp 1 adj handle 0xa73e907c ifh 91 link 1 enctype 0 flags 0 hw addr 0x8c580000
Aug 25 21:43:55.784 mfwd_ipv4_hw/init 0/4/CPU0 t1 Platform extension exists - warm boot
Aug 25 21:43:55.784 mfwd_ipv4_hw/init 0/4/CPU0 t1 CPP IPMC Gtrie Lib Init done: rc=0
Aug 25 21:43:55.784 mfwd_ipv4_hw/init 0/4/CPU0 t1 CPP IPMC gtrie lib re-init started for gtrie 0xa6039dec, shmem ld 1
Aug 25 21:43:55.784 mfwd_ipv4_hw/init 0/4/CPU0 t1 CPP IPMC gtrie lib re-init done prot=2 tab=0 rc=0
Aug 25 21:43:55.784 mfwd_ipv4_hw/init 0/4/CPU0 t1 Platform extension does not exist - cold boot
Aug 25 21:43:55.784 mfwd_ipv4_hw/init 0/4/CPU0 t1 CPP IPMC Gtrie Lib Init done: rc=0
Aug 25 21:43:55.784 mfwd_ipv4_hw/init 0/4/CPU0 t1 CPP IPMC Gtrie Lib Init done: rc=0
Aug 25 21:43:55.784 mfwd_ipv4_hw/init 0/4/CPU0 t1 CPP IPMC Gtrie Lib Init done: rc=0
Aug 25 21:43:55.784 mfwd_ipv4_hw/init 0/4/CPU0 t1 CPP IPMC Gtrie Lib Init done: rc=0
Aug 25 21:43:56.442 mfwd_ipv4_hw/init 0/4/CPU0 t1 Successfully done binding with CPP GIC
Server
Aug 25 21:43:56.444 mfwd_ipv4_hw/init 0/4/CPU0 t1 Successfully binded with CPP Rx Adjacency
APIs Lib
Aug 25 21:43:56.445 mfwd_ipv4_hw/init 0/4/CPU0 t1 Successfully binded with CPP Tx Adjacency
APIs Lib
Aug 25 21:43:56.445 mfwd_ipv4_hw/init 0/4/CPU0 t1 Successfully binded with CPP Tx Adjacency
APIs Lib
Aug 25 21:43:56.445 mfwd_ipv4_hw/init 0/4/CPU0 t1 Initialized interface lib
Aug 25 21:43:56.464 mfwd_ipv4_hw/init 0/4/CPU0 t1 Initialized EDM backend
Aug 25 21:43:56.466 mfwd_ipv4_hw/init 0/4/CPU0 t1 Initialized utilities lib
Aug 25 21:43:56.471 mfwd_ipv4_hw/init 0/4/CPU0 t1 MFWD: Platform lib initialization completed
Aug 25 21:43:58.412 mfwd_ipv4_hw/event 0/4/CPU0 t1 CPP Modify adj cpp 1 adj handle 0xa73e907c
ifh 91 link 1 enctype 0 flags 1 hw addr 0x8c580000
Aug 25 21:43:58.412 mfwd_ipv4_hw/event 0/4/CPU0 t1 CPP Modify adj cpp 1 adj handle 0xa73e90c0
ifh 98 link 1 enctype 0 flags 1 hw addr 0x8c58010
Aug 26 22:25:50.253 mfwd_ipv4_hw/error 0/4/CPU0 t1 --> Proc started jid=227, pid=163930
Aug 26 22:25:50.253 mfwd_ipv4_hw/netio 0/4/CPU0 t1 --> Proc started jid=227, pid=163930
Aug 26 22:25:50.253 mfwd_ipv4_hw/event 0/4/CPU0 t1 --> Proc started jid=227, pid=163930
Aug 26 22:25:50.253 mfwd_ipv4_hw/event 0/4/CPU0 t1 --> Proc started jid=227, pid=163930
show mfib hardware resource-counters

To display the allocated and freed hardware resources for the Multicast Forwarding Information Base (MFIB) process, use the `show mfib hardware resource-counters` command in EXEC mode.

```
show mfib [vrf vrf-name] [(ipv4|ipv6)] hardware resource-counters location node-id
```

**Syntax Description**
- **vrf vrf-name** (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- **ipv4** (Optional) Specifies IPv4 address prefixes.
- **ipv6** (Optional) Specifies IPv6 address prefixes.
- **location node-id** Specifies an MFIB-designated node.

**Command Default**
IPv4 addressing is the default.

**Command Modes**
EXEC

**Command History**
- **Release 3.7.2** This command was introduced.

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `show mfib hardware resource-counters` command to understand the table lookup unit (TLU) resource usage by MFIB.

- Usage for each channel
- Storing of specific data
- Allocation counts for metro statistics
- Failure counts for metro statistics

**Note**
Use the location option in the `show mfib hardware resource-counters` command to indicate for which linecard you need information. The command will not display any useful output if only RSP is specified or if no location is specified.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>
The following is a sample output from the `show mfib hardware resource-counters` command on the Cisco ASR 9000 Series SIP-700 line card:

```
RP/0/RSP0/CPU0:router# show mfib hardware resource-counters location 0/4/CPU0

LC Type: A9K-SIP-700

PD Memory Alloc/Free/In Use Stats:

<table>
<thead>
<tr>
<th>Type</th>
<th>Allocated</th>
<th>Freed</th>
<th>In Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>global</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>table extension</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>route extension</td>
<td>18</td>
<td>11</td>
<td>7</td>
</tr>
<tr>
<td>interface extension</td>
<td>18</td>
<td>10</td>
<td>8</td>
</tr>
<tr>
<td>idb extension</td>
<td>3</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>EDM bag data</td>
<td>26</td>
<td>24</td>
<td>2</td>
</tr>
<tr>
<td>vpn extension</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>mdt ea extension</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Ingress Hardware Resource Counters:

<table>
<thead>
<tr>
<th>Type</th>
<th>Allocated</th>
<th>Freed</th>
<th>In Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix stats resource</td>
<td>18</td>
<td>11</td>
<td>7</td>
</tr>
<tr>
<td>PLU prefix resource</td>
<td>18</td>
<td>11</td>
<td>7</td>
</tr>
<tr>
<td>prefix replica resource</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Egress Hardware Resource Counters:

<table>
<thead>
<tr>
<th>Type</th>
<th>Allocated</th>
<th>Freed</th>
<th>In Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>prefix stats resource</td>
<td>18</td>
<td>11</td>
<td>7</td>
</tr>
<tr>
<td>PLU prefix resource</td>
<td>18</td>
<td>11</td>
<td>7</td>
</tr>
<tr>
<td>prefix replica resource</td>
<td>21</td>
<td>12</td>
<td>9</td>
</tr>
</tbody>
</table>

Ingress Hardware Global Multicast Statistics:

<table>
<thead>
<tr>
<th>Type</th>
<th>Allocated</th>
<th>Freed</th>
<th>In Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Punt Packets</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Punt Drop Packets</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inject Packets</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inject Drop Packets</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drop Packets/Bytes</td>
<td>0/0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Egress Hardware Global Multicast Statistics:

<table>
<thead>
<tr>
<th>Type</th>
<th>Allocated</th>
<th>Freed</th>
<th>In Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>Punt Packets</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Punt Drop Packets</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inject Packets</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Inject Drop Packets</td>
<td>0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Drop Packets/Bytes</td>
<td>0/0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```

The following is a sample output of the `show mfib hardware resource-counters` command:

```
RP/0/RSP0/CPU0:router# show mfib hardware resource-counters location 0/0/CPU0
```
LC Type: Trident
prm_stat success calls: ingress: 4250,4092 egress: 0,0
prm_stat failure calls: ingress: 0,0 egress: 0,0

Memory alloc stats

<table>
<thead>
<tr>
<th>Type</th>
<th>Allocated</th>
<th>Freed</th>
<th>Delta</th>
</tr>
</thead>
<tbody>
<tr>
<td>global</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>table extension</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>route extension</td>
<td>187</td>
<td>180</td>
<td>7</td>
</tr>
<tr>
<td>interface extension</td>
<td>221</td>
<td>215</td>
<td>6</td>
</tr>
<tr>
<td>idb extension</td>
<td>52</td>
<td>47</td>
<td>5</td>
</tr>
<tr>
<td>kmrs</td>
<td>159</td>
<td>159</td>
<td>0</td>
</tr>
<tr>
<td>kmrs key</td>
<td>652</td>
<td>652</td>
<td>0</td>
</tr>
<tr>
<td>kmrs result</td>
<td>488</td>
<td>488</td>
<td>0</td>
</tr>
<tr>
<td>uidb data</td>
<td>437</td>
<td>437</td>
<td>0</td>
</tr>
<tr>
<td>EDM bag data</td>
<td>5</td>
<td>3</td>
<td>2</td>
</tr>
</tbody>
</table>

This table describes the significant fields shown in the display.

**Table 17: show mfb hardware resource counters Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>prm_stat success calls</td>
<td>The number of successful calls to allocate and free statistics blocks, for ingress and egress statistics.</td>
</tr>
<tr>
<td>prm_stat failure calls</td>
<td>The number of failed calls to allocate and free statistics blocks, for ingress and egress statistics.</td>
</tr>
<tr>
<td>Type</td>
<td>Describes the structure type.</td>
</tr>
<tr>
<td>Allocated</td>
<td>The number of blocks allocated per structure type.</td>
</tr>
<tr>
<td>Freed</td>
<td>The number of blocks freed per structure type.</td>
</tr>
<tr>
<td>Delta</td>
<td>The difference between allocated and freed blocks per structure type.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mfb interface, on page 200</td>
<td>Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.</td>
</tr>
</tbody>
</table>
show mfib hardware route accept-bitmap

To display platform-specific Multicast Forwarding Information Base (MFIB) information for the interface list that accepts bidirectional routes, use the `show mfib hardware route accept-bitmap` command in EXEC mode.

```
show mfib [vrf vrf-name] ([ipv4|ipv6]) hardware route accept-bitmap [*] [group-address [/prefix-length]] [detail] [location node-id]
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `ipv6` (Optional) Specifies IPv6 address prefixes.
- `*` (Optional) Displays shared tree entry.
- `source-address` (Optional) IP address or hostname of the multicast route source.
- `group-address` (Optional) IP address or hostname of the multicast group.
- `prefix-length` (Optional) Prefix length of the multicast group. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash must precede the decimal value.
- `detail` (Optional) Detailed list of the routing database.
- `location node-id` (Optional) Specifies an MFIB-designated node.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Note**

The command does not display any useful output if only RSP is specified or if no location is specified.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>
The following is sample output from the `show mfib hardware route accept-bitmap` command:

```
RP/0RSP0/CPU0:RTP-VIKING-MCAST-04#show mfib hardware route accept-bitmap detail 227.0.0.0/8 location 0/2/cPU0
LC Type: Typhoon A9K-MOD80-SE
Source: * Group: 227.0.0.0 Mask: 8 RPF Int: None
Accept bitmap summary (HW)
-----------------------------------------------
NP IIF Count Row Count
-----------------------------------------------
 0  2  1
 1  2  1
-----------------------------------------------
IIFs in Accept bitmap (HW)
-----------------------------------------------
NP: 0
-----------------------------------------------
Interface Ifhandle uIDB
-----------------------------------------------
GigabitEthernet0/2/0/16 0x080004c0 17
GigabitEthernet0/2/0/17 0x08000500 18
-----------------------------------------------
NP: 1
-----------------------------------------------
Interface Ifhandle uIDB
-----------------------------------------------
GigabitEthernet0/2/0/16 0x080004c0 17
GigabitEthernet0/2/0/17 0x08000500 18
-----------------------------------------------
Raw Accept bitmap (HW)
-----------------------------------------------
NP: 0 [Parent MLI: 305]
-----------------------------------------------
Key Bits 0 4 8 12
0x0000 2 00000600 00000000 00000000 00000000
-----------------------------------------------
NP: 1 [Parent MLI: 305]
-----------------------------------------------
Key Bits 0 4 8 12
0x0000 2 00000600 00000000 00000000 00000000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mfib interface</code>, on page 200</td>
<td>Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.</td>
</tr>
</tbody>
</table>
show mfib hardware route logical

To display the route internal structures for the platform-specific Multicast Forwarding Information Base (MFIB) in the hardware, use the **show mfib hardware route logical** command in EXEC mode.

```
show mfib [vrf vrf-name] [{ipv4|ipv6}] hardware route logical [*] [source-address] [group-address [[/prefix-length]]] [detail] [location node-id]
```

**Syntax Description**

- *****: (Optional) Displays shared tree entries.
- **A.B.C.D**: (Optional) Source IP address or hostname of the MFIB route.
- **A.B.C.D/length**: (Optional) Group IP address or hostname of the MFIB route and the prefix length. Prefix length of the MFIB group address is a decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash must precede the decimal value.
- **detail**: (Optional) Details of each route (requires 140 columns).
- **location node-id**: (Optional) Specifies the MFIB location.
- **ipv4**: (Optional) Specifies IPv4 address prefixes.
- **ipv6**: (Optional) Specifies IPv6 address prefixes.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.1</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.0</td>
<td>This command was changed from show mfib hardware route internal to show mfib hardware route logical.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Note**

The command does not display any useful output if only RSP is specified or if no location is specified.
### Examples

The following example shows a sample output of the `show mfib hardware route internal show mfib hardware route logical` command:

```
RP/0/RSP0/CPU0:RTP-VIKING-MCAST-04#show mfib hardware route logical detail location 0/2/cPU0

LC Type: Typhoon A9K-MOD80-SE

Legend:

<table>
<thead>
<tr>
<th>Route Information</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NP: NP ID</td>
<td>B: BACL check</td>
<td></td>
<td></td>
</tr>
<tr>
<td>S: RPF Interface signal</td>
<td>DC: Directly connected</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PL: Punt to LC CPU</td>
<td>PR: Punt to RP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>PF: Punt if forwarded</td>
<td>DR: Drop all</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RI: RPF interface</td>
<td>T: Table ID for lookup</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OC: Count of OLIST members</td>
<td>MF: MoFRR enabled</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TR: Tunnel Route</td>
<td>TE: Tunnel Encap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TD: Tunnel Decap</td>
<td>CD: Conditional Decap</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MI: MVET index</td>
<td>Base: Base of the statistics pointer</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NI: Not Installed</td>
<td>BD: Bidir</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MVPN Information</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MLI: MVPN table index</td>
<td>VTID: VRF Table ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RPFID: RPF Identifier</td>
<td>TUS: Tunnel uIDB set</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MVD: MVET entry dirty</td>
<td>NP: NP ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TStat: Tunnel stat pointer</td>
<td>TUIDB: Tunnel uIDB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TIFH: Tunnel Interface handle</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MoFRR Information</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MLI: Multicast leaf index</td>
<td>A: Active RPF interface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>RI: RPF interface (or RPF ID)</td>
<td>WDI: Watchdog counter index</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source: *</th>
<th>Group: 224.0.0.0</th>
<th>Mask: 24</th>
<th>RPF Int: None</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGID: 17161</td>
<td>MLI: 288</td>
<td>Fabric Slotmask: 0x0</td>
<td>FGID: 0x0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Route Information</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NP</td>
<td>B</td>
<td>S</td>
<td>DC</td>
<td>PL</td>
<td>PR</td>
<td>PF</td>
</tr>
<tr>
<td>0</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>0x0</td>
<td>0x0</td>
<td>0x5302e3</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Software MGID Information</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>MGID: 17161</td>
<td>Mask: 0x0</td>
<td>Old MGID: 0</td>
<td>Old Mask: 0x0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Source: *</th>
<th>Group: 224.0.1.39</th>
<th>Mask: 32</th>
<th>RPF Int: None</th>
</tr>
</thead>
<tbody>
<tr>
<td>MGID: 17159</td>
<td>MLI: 286</td>
<td>Fabric Slotmask: 0x0</td>
<td>FGID: 0x0</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Route Information</th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>NP</td>
<td>B</td>
<td>S</td>
<td>DC</td>
<td>PL</td>
<td>PR</td>
<td>PF</td>
</tr>
<tr>
<td>0</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0x0</td>
</tr>
<tr>
<td>0x0</td>
<td>0x0</td>
<td>0x5302d9</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
```
### Multicast Routing and Forwarding Commands

#### show mfib hardware route logical

<table>
<thead>
<tr>
<th>NP</th>
<th>B</th>
<th>S</th>
<th>DC</th>
<th>PL</th>
<th>PR</th>
<th>PF</th>
<th>DR</th>
<th>BD</th>
<th>RI</th>
<th>T</th>
<th>OC</th>
<th>MF</th>
<th>TR</th>
<th>TE</th>
<th>TD</th>
<th>CD</th>
<th>MI</th>
<th>Base</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0x0</td>
<td>0</td>
<td>0</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0x0</td>
<td>0x5300f2</td>
</tr>
<tr>
<td>1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0x0</td>
<td>0</td>
<td>0</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0x0</td>
</tr>
<tr>
<td>0</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0x0</td>
<td>0</td>
<td>0</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0x0</td>
<td>0x530106</td>
</tr>
</tbody>
</table>

---

### Software MGID Information

**MGID:** 17159 **Mask:** 0x0 **Old MGID:** 0 **Old Mask:** 0x0

**Source:***

| Group: 224.0.1.40 | Mask: 32 | RPF Int: None |

**MGID:** 17160 **MLI:** 287 **Fabric Slotmask:** 0x0 **FGID:** 0x0

### Route Information

<table>
<thead>
<tr>
<th>NP</th>
<th>B</th>
<th>S</th>
<th>DC</th>
<th>PL</th>
<th>PR</th>
<th>PF</th>
<th>DR</th>
<th>BD</th>
<th>RI</th>
<th>T</th>
<th>OC</th>
<th>MF</th>
<th>TR</th>
<th>TE</th>
<th>TD</th>
<th>CD</th>
<th>MI</th>
<th>Base</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0x0</td>
<td>0</td>
<td>0</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0x0</td>
</tr>
<tr>
<td>1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0x0</td>
<td>0</td>
<td>0</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0x0</td>
</tr>
</tbody>
</table>

---

### Software MGID Information

**MGID:** 17160 **Mask:** 0x0 **Old MGID:** 0 **Old Mask:** 0x0

**Source:***

| Group: 227.0.0.0 | Mask: 8 | RPF Int: None |

**MGID:** 17178 **MLI:** 305 **Fabric Slotmask:** 0x10 **FGID:** 0x10

**Parent MLI:** 305 **IIF Count:** 2 **AB Rows:** 1

### Route Information

<table>
<thead>
<tr>
<th>NP</th>
<th>B</th>
<th>S</th>
<th>DC</th>
<th>PL</th>
<th>PR</th>
<th>PF</th>
<th>DR</th>
<th>BD</th>
<th>RI</th>
<th>T</th>
<th>OC</th>
<th>MF</th>
<th>TR</th>
<th>TE</th>
<th>TD</th>
<th>CD</th>
<th>MI</th>
<th>Base</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0x0</td>
<td>1</td>
<td>1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0x0</td>
<td>0x5302ed</td>
</tr>
<tr>
<td>1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0x0</td>
<td>0</td>
<td>0</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0x0</td>
<td>0x530106</td>
</tr>
</tbody>
</table>

---

### Software MGID Information

**MGID:** 17178 **Mask:** 0x1 **Old MGID:** 0 **Old Mask:** 0x1

**Source:***

| Group: 232.0.0.0 | Mask: 8 | RPF Int: None |

**MGID:** 17162 **MLI:** 289 **Fabric Slotmask:** 0x0 **FGID:** 0x0

### Route Information

<table>
<thead>
<tr>
<th>NP</th>
<th>B</th>
<th>S</th>
<th>DC</th>
<th>PL</th>
<th>PR</th>
<th>PF</th>
<th>DR</th>
<th>BD</th>
<th>RI</th>
<th>T</th>
<th>OC</th>
<th>MF</th>
<th>TR</th>
<th>TE</th>
<th>TD</th>
<th>CD</th>
<th>MI</th>
<th>Base</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0x0</td>
</tr>
<tr>
<td>1</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0x0</td>
</tr>
</tbody>
</table>

---

### Software MGID Information

**MGID:** 17162 **Mask:** 0x0 **Old MGID:** 0 **Old Mask:** 0x0

---

**RP/0/RSP0/CPUD:RTP-VIKING-MCAST-04#**
show mfib hardware route location

To display the platform-specific Multicast Forwarding Information Base (MFIB)-enabled location in the hardware, use the **show mfib hardware route location** command in EXEC mode.

```
show mfib [vrf vrf-name] [ipv4|ipv6] [*] [source-address] [group-address [/prefix-length]] location node-id
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `ipv6` (Optional) Specifies IPv6 address prefixes.
- `source-address` (Optional) IP address or hostname of the multicast route source.
- `group-address` (Optional) IP address or hostname of the multicast group.
- `/prefix-length` (Optional) Prefix length of the multicast group. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash must precede the decimal value.
- `node-id` Node ID for an MFIB-designated node.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

- The command does not display any useful output if only RSP is specified or if no location is specified.

**Task ID**

- Task ID: multicast
- Operations: read
Examples

The following is sample output from the `show mfib hardware route location` command:

```
RP/0/RSP0CPU0:RTP-VIKING-MCAST-04#show mfib hardware route detail 227.0.0.0/8 location 0/2/cPU0

LC Type: Typhoon A9K-MOD80-SE
--------------------------------------------------------------------------
Legend:
Route Information
NP: NP ID               B: BAcl check
S: RPF Interface signal  DC: Directly connected
PL: Punt to LC CPU      PR: Punt to RP
PF: Punt if forwarded   DR: Drop all
RI: RPF interface      T:  Table ID for lookup
OC: Count of OLIST members MF: MoFRR enabled
TR: Tunnel Route       TE: Tunnel Encap
TD: Tunnel Decap       CD: Conditional Decap
MI: MVET index        Base: Base of the statistics pointer
NI: Not Installed      BD: Bidir
--------------------------------------------------------------------------
MVPN Information
MLI: MVPN table index  VTID: VRF Table ID
RPFID: RPF Identifier  TUS: Tunnel uIDB set
MVD: MVET entry dirty  NP: NP ID
TStat: Tunnel stat pointer TUIDB: Tunnel uIDB
TIFH: Tunnel Interface handle
--------------------------------------------------------------------------
MoFRR Information
MLI: Multicast leaf index A: Active RPF interface
RI: RPF interface (or RPF ID) WDI: Watchdog counter index
--------------------------------------------------------------------------
Source: *  Group: 227.0.0.0  Mask: 8  RPF Int: None
MGID: 17178  MLI: 305  Fabric Slotmask: 0x10  FGID: 0x10
Parent MLI: 305  IIF Count: 2  AB Rows: 1
Route Information
--------------------------------------------------------------------------
NP B S DC PL PR PF DR BD RI T OC MF TR TE TD CD MI Base
--------------------------------------------------------------------------
0 F F F F F F F T 0x0 0 1 F F F F F 0x0 0x5302ed
1 F F F F F F F T 0x0 0 0 F F F F F 0x0 0x530106
--------------------------------------------------------------------------
Software MGID Information
MGID: 17178  Mask: 0x1  Old MGID: 0  Old Mask: 0x1
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mfib route</code>, on page 204</td>
<td>Displays route entries in the Multicast Forwarding Information Base (MFIB).</td>
</tr>
</tbody>
</table>
show mfib hardware route mofrr

To display the platform-specific Multicast Forwarding Information Base (MFIB) information for the MoFRR (multicast only fast reroute)- enabled list stored in the hardware, use the `show mfib hardware route mofrr` command in EXEC mode.

```
show mfib hardware route mofrr {[*] [source-address] [group-address [/prefix-length]] [detail]} [location node-id]
```

**Syntax Description**

- `*` (Optional) Displays all the MoFRR routes configured in the platform.
- `source-address` (Optional) IP address or hostname of the multicast route source.
- `group-address` (Optional) IP address or hostname of the multicast group.
- `detail` (Optional) Displays a detailed list of the MoFRR routing database.
- `location node-id` Specifies the Node ID for an MFIB-designated node.

**Command Default**
IPv4 addressing is the default. Currently, MoFRR supports only IPv4 routes.

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

MoFRR is a mechanism in which two copies of the same multicast stream flow through disjoint paths in the network. At the point in the network (usually the PE closer to the receivers) where the two streams merge, one of the streams is accepted and forwarded on the downstream links, while the other stream is discarded. When a failure is detected in the primary stream due to a link or node failure in the network, MoFRR instructs the forwarding plane to start accepting packets from the backup stream (which now becomes the primary stream).

MoFRR is triggered when the hardware detects traffic loss on the primary path of a given flow or route. Traffic loss is defined as no data packet having been received for 30 ms. When MoFRR is triggered, the primary and secondary reverse-path forwarding (RPF) interfaces are exposed to the forwarding plane and switchover occurs entirely at the hardware level.

The `show mfib hardware route mofrr` command displays the output MoFRR route list of the platform. If there is no MoFRR route enabled in the platform, then the output result is “There are no MoFRR routes configured”.

The command does not display any useful output if only RSP is specified or if no location is specified.
The following is a sample output from the `show mfib hardware route mofrr` command:

```
RP/0/RSP0/CPU0# show mfib hardware route mofrr location 0/0/cpu0

LC Type: Trident
-----------------------------------------------
Legend:
Route MoFRR Information
A: Active RPF interface, MS: Monitoring State,
WDI: Watchdog Count Index, NP: Network Processor,
-----------------------------------------------
Source: 20.20.20.1 Group: 225.0.0.1 Mask length: 64 RPF Int: Gi0/0/0/8
-----------------------------------------------
RPFS Interface A MS WDI
-----------------------------------------------
Primary: Gi0/0/0/8 T 2 1846768
Backup: Gi0/0/0/18 F 0 1846769
-----------------------------------------------
OIFS
-----------
NP Intf
-----------
1 Gi0/0/0/28
-----------
Sequence num: 1 Num of switchovers: 0
WatchDog Counters:
-----------------------------------------------
NP Profile Valid Current-Cnt Last-cnt
-----------------------------------------------
Prim WDC 0 0 0 3848 12
Prim WDC 1 0 0 3848 12
Prim WDC 2 0 0 3848 12
Prim WDC 3 1 1 3848 12
Back WDC 0 0 0 3848 12
Back WDC 1 0 0 3848 12
Back WDC 2 0 0 3848 12
Back WDC 3 0 0 3848 12
-----------------------------------------------
MoFRR Statistics:
-----------------------------------------------
NP Prim pkt rx Back pkt rx Interrupts Punts
-----------------------------------------------
0 0 0 0 0
1 0 0 0 0
2 0 0 0 0
3 406213 0 1 1
-----------------------------------------------
Source: 20.20.20.1 Group: 225.0.0.2 Mask length: 64 RPF Int: Gi0/0/0/8
-----------------------------------------------
RPFS Interface A MS WDI
```

Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference, Release 5.3.x
The following is sample output from the show mfib hardware route MoFRR command with only one multicast group:

```
RP/0/RSP0/CPU0:router# show mfib hardware route mofrr 225.0.0.1 location 0/0/CPU0
LC Type: Trident

Legend:
Route MoFRR Information
A: Active RPF interface, MS: Monitoring State,
WDI: Watchdog Count Index, NP: Network Processor,

Source: 20.20.20.1 Group: 225.0.0.1 Mask length: 64 RPF Int: Gi0/0/0/8

Primary: Gi0/0/0/8 T 2 1846772
Backup: Gi0/0/0/18 F 0 1846773

OIFS
---------------
NP Intf
---------------
1 Gi0/0/0/28

Sequence num: 1 Num of switchovers: 0

WatchDog Counters:

NP Profile Valid Current-Cnt Last-cnt
--------------------------
Prim WDC 0 0 0 3848 12
Prim WDC 1 0 0 3848 12
Prim WDC 2 0 0 3848 12
Prim WDC 3 1 1 3848 12
Back WDC 0 0 0 3848 12
Back WDC 1 0 0 3848 12
Back WDC 2 0 0 3848 12
Back WDC 3 0 0 3848 12

MoFRR Statistics:

NP Prim pkt rx Back pkt rx Interrupts Punts
--------------------------
0 0 0 0 0
1 0 0 0 0
2 0 0 0 0
3 406212 0 1 1

The following is sample output from the show mfib hardware route MoFRR command with only one multicast group:
The following is sample output from the show mfib hardware route MoFRR command with only one multicast source:

```
RP/0/RSP0/CPU0:router# show mfib hardware route mofrr 20.20.20.1 location 0/0/CPU0

LC Type: Trident
Legend:
Route MoFRR Information
A: Active RPF interface, MS: Monitoring State, WDI: Watchdog Count Index, NP: Network Processor,
Source: 20.20.20.1 Group: 225.0.0.1 Mask length: 64 RPF Int: Gi0/0/0/8
```

```
RPFS Interface A MS WDI
Primary: Gi0/0/0/8 T 2 1846772
Backup: Gi0/0/0/18 F 0 1846773
```

```
OIFS
------------------
NP Intf
1 Gi0/0/0/28
```

```
Sequence num: 1 Num of switchovers: 0
WatchDog Counters:
```
-----------------------------
NP Profile Valid Current-Cnt Last-cnt
-----------------------------
Prim WDC 0 0 0 3848 12
Prim WDC 1 0 0 3848 12
Prim WDC 2 0 0 3848 12
Prim WDC 3 1 1 3848 12
Back WDC 0 0 0 3848 12
Back WDC 1 0 0 3848 12
Back WDC 2 0 0 3848 12
Back WDC 3 0 0 3848 12
-----------------------------
```

```
MoFRR Statistics:
-----------------------------
NP Prim pkt rx Back pkt rx Interrupts Punts
-----------------------------
0 0 0 0 0
1 0 0 0 0
2 0 0 0 0
3 400465 0 1 1
-----------------------------
```

```
```
MoFRR Statistics:

<table>
<thead>
<tr>
<th>NP</th>
<th>Prim pkt rx</th>
<th>Back pkt rx</th>
<th>Interrupts</th>
<th>Punts</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

Source: 20.20.20.1  Group: 225.0.0.2  Mask length: 64  RPF Int: Gi0/0/0/8

RPFs Interface A MS WDI

Primary: Gi0/0/0/8  T 2 1846774
Backup: Gi0/0/0/18  F 0 1846775

OIFS

NP Intf

1  Gi0/0/0/28

Sequence num: 1  Num of switchovers: 0

WatchDog Counters:

<table>
<thead>
<tr>
<th>NP</th>
<th>Profile</th>
<th>Valid</th>
<th>Current-Cnt</th>
<th>Last-cnt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prim WDC 0</td>
<td>0</td>
<td>0</td>
<td>3848</td>
<td>12</td>
</tr>
<tr>
<td>Prim WDC 1</td>
<td>0</td>
<td>0</td>
<td>3848</td>
<td>12</td>
</tr>
<tr>
<td>Prim WDC 2</td>
<td>0</td>
<td>0</td>
<td>3848</td>
<td>12</td>
</tr>
<tr>
<td>Prim WDC 3</td>
<td>1</td>
<td>1</td>
<td>3848</td>
<td>12</td>
</tr>
<tr>
<td>Back WDC 0</td>
<td>0</td>
<td>0</td>
<td>3848</td>
<td>12</td>
</tr>
<tr>
<td>Back WDC 1</td>
<td>0</td>
<td>0</td>
<td>3848</td>
<td>12</td>
</tr>
<tr>
<td>Back WDC 2</td>
<td>0</td>
<td>0</td>
<td>3848</td>
<td>12</td>
</tr>
<tr>
<td>Back WDC 3</td>
<td>0</td>
<td>0</td>
<td>3848</td>
<td>12</td>
</tr>
</tbody>
</table>

MoFRR Statistics:

<table>
<thead>
<tr>
<th>NP</th>
<th>Prim pkt rx</th>
<th>Back pkt rx</th>
<th>Interrupts</th>
<th>Punts</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>
This table describes the significant fields shown in the display.

**Table 18: show mfib hardware route mofrr Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPFS</td>
<td>Primary and backup RPF of the route.</td>
</tr>
<tr>
<td>A</td>
<td>Currently active RPF for forwarding the traffic to the egress (OLIST). T: means true, F: means false.</td>
</tr>
<tr>
<td>MS</td>
<td>Monitoring state. It has three states. MS=0, indicates that the monitoring state disabled. MS=1, indicates that active RPF is monitoring traffic activity. MS=2, indicates that active RPF is monitoring traffic loss.</td>
</tr>
<tr>
<td>WDI</td>
<td>Watchdog Count Index. Each MoFRR route has two Line card specific watchdog indexes, associated with primary and backup RPF, respectively.</td>
</tr>
<tr>
<td>OIFS</td>
<td>Output Interfaces in the local line card.</td>
</tr>
<tr>
<td>Sequence num</td>
<td>MoFRR specific route sequence number.</td>
</tr>
<tr>
<td>Num of switchovers</td>
<td>Total number of switchovers triggered by traffic loss detection in the data plane.</td>
</tr>
<tr>
<td>Watchdog Counters</td>
<td>Internal Hardware watchdog counters</td>
</tr>
<tr>
<td>MoFRR Statistics</td>
<td>Internal software watchdog counters</td>
</tr>
</tbody>
</table>

If there is no MoFRR route enabled in the platform, the output result will be as follows:

```
RP/0/RSP0/CPU0:router# show mfib hardware route mofrr location 0/0/CPU0

LC Type: Trident
No matching routes in MFIB
There are no MoFRR routes configured.
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mfib hardware route olist, on page 180</td>
<td>Displays platform-specific Multicast Forwarding Information Base (MFIB) information in the output interface list (olist) stored in the hardware.</td>
</tr>
<tr>
<td>show mfib hardware route statistics, on page 191</td>
<td>Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the packet and byte counters for each route.</td>
</tr>
<tr>
<td>show mfib hardware route summary, on page 195</td>
<td>Displays summary platform-specific Multicast Forwarding Information Base (MFIB) hardware information for each route entry.</td>
</tr>
<tr>
<td>show mfib route, on page 204</td>
<td>Displays route entries in the Multicast Forwarding Information Base (MFIB).</td>
</tr>
<tr>
<td>show mrib route, on page 222</td>
<td>Displays all entries in the Multicast Routing Information Base (MRIB).</td>
</tr>
</tbody>
</table>
show mfib hardware route olist

To display platform-specific Multicast Forwarding Information Base (MFIB) information in the output interface list (olist) stored in the hardware, use the **show mfib hardware route olist** command in the appropriate mode.

```
show mfib [vrf vrf-name] [{ipv4|ipv6}] hardware route olist {[*]|{source-address} [group-address [/ prefix-length]}} {location node-id}
```

**Syntax Description**

- **vrf vrf-name**  (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- **ipv4**          (Optional) Specifies IPv4 address prefixes.
- **ipv6**          (Optional) Specifies IPv6 address prefixes.
- **source-address**  (Optional) IP address or hostname of the multicast route source.
- **group-address**  (Optional) IP address or hostname of the multicast group.
- **prefix-length**  (Optional) Prefix length of the multicast group. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash must precede the decimal value.
- **location node-id**  Specifies an MFIB-designated node.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **show mfib hardware route olist** command displays the output interface list (olist) for each route. The Multicast Forwarding (MFWD) process stores olist interfaces in a table lookup unit (TLU) block (in groups of three). As such, the command displays each route three times. The command does not display any useful output if only RSP is specified or if no location is specified.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast read</td>
</tr>
</tbody>
</table>
**Examples**

The following is sample output from the `show mfib hardware route olist` command. (The output fields are described in the header.)

```
RP/0/RSP0/CPU0# show mfib hardware route olist location 0/0/CPU0

LC Type: Trident

Legend:
Route Information - (Ingress)
C: Chip ID, IC: BACL check, IP: Punt this packet to LC CPU,
ID: Directly connected, IS: RPF interface signal, IU: Punt copy to RP,
IF: Punt to LC CPU if forwarded, IM: Result match, IV: Valid entry,
IR: RPF IF, IA: Fabric slotmask, IG: Multicast group ID

Route Information - (Egress)
ET: Table ID to be used for OLIST lookup, EO: OLIST count bit,
ER: Route MGID to be used for OLIST/NRPF lookup, EM: Result match,
EV: Valid entry, EC: Count of OLIST members on this chip,
BS: Base of the statistics pointer

Hardware Information
C: Chip ID; T: Table ID; M: Member ID; Intf: Interface, U: uIDB index,
I: HW IC flag, B: HW BACL bit, Base: Base of statistics pointer

Source: * Group: 224.0.0.0 Mask length: 24

<table>
<thead>
<tr>
<th>C</th>
<th>IC</th>
<th>IP</th>
<th>ID</th>
<th>IS</th>
<th>IU</th>
<th>IF</th>
<th>IM</th>
<th>IV</th>
<th>IR</th>
<th>IA</th>
<th>IG</th>
<th>ET</th>
<th>EO</th>
<th>ER</th>
<th>EM</th>
<th>EV</th>
<th>EC</th>
<th>BS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8002</td>
<td>0</td>
<td>F</td>
<td>2</td>
<td>T</td>
<td>T</td>
<td>0</td>
<td>0x5516c</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8002</td>
<td>0</td>
<td>F</td>
<td>2</td>
<td>T</td>
<td>T</td>
<td>0</td>
<td>0x5516c</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8002</td>
<td>0</td>
<td>F</td>
<td>2</td>
<td>T</td>
<td>T</td>
<td>0</td>
<td>0x5516c</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8002</td>
<td>0</td>
<td>F</td>
<td>2</td>
<td>T</td>
<td>T</td>
<td>0</td>
<td>0x555a4</td>
<td></td>
</tr>
</tbody>
</table>

Source: * Group: 224.0.1.39 Mask length: 32

<table>
<thead>
<tr>
<th>C</th>
<th>IC</th>
<th>IP</th>
<th>ID</th>
<th>IS</th>
<th>IU</th>
<th>IF</th>
<th>IM</th>
<th>IV</th>
<th>IR</th>
<th>IA</th>
<th>IG</th>
<th>ET</th>
<th>EO</th>
<th>ER</th>
<th>EM</th>
<th>EV</th>
<th>EC</th>
<th>BS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8000</td>
<td>0</td>
<td>F</td>
<td>0</td>
<td>T</td>
<td>T</td>
<td>0</td>
<td>0x55162</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8000</td>
<td>0</td>
<td>F</td>
<td>0</td>
<td>T</td>
<td>T</td>
<td>0</td>
<td>0x55162</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8000</td>
<td>0</td>
<td>F</td>
<td>0</td>
<td>T</td>
<td>T</td>
<td>0</td>
<td>0x55162</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8000</td>
<td>0</td>
<td>F</td>
<td>0</td>
<td>T</td>
<td>T</td>
<td>0</td>
<td>0x5559a</td>
<td></td>
</tr>
</tbody>
</table>

Source: * Group: 224.0.1.40 Mask length: 32

<table>
<thead>
<tr>
<th>C</th>
<th>IC</th>
<th>IP</th>
<th>ID</th>
<th>IS</th>
<th>IU</th>
<th>IF</th>
<th>IM</th>
<th>IV</th>
<th>IR</th>
<th>IA</th>
<th>IG</th>
<th>ET</th>
<th>EO</th>
<th>ER</th>
<th>EM</th>
<th>EV</th>
<th>EC</th>
<th>BS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8001</td>
<td>0</td>
<td>F</td>
<td>1</td>
<td>T</td>
<td>T</td>
<td>0</td>
<td>0x55167</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8001</td>
<td>0</td>
<td>F</td>
<td>1</td>
<td>T</td>
<td>T</td>
<td>0</td>
<td>0x55167</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8001</td>
<td>0</td>
<td>F</td>
<td>1</td>
<td>T</td>
<td>T</td>
<td>0</td>
<td>0x55167</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8001</td>
<td>0</td>
<td>F</td>
<td>1</td>
<td>T</td>
<td>T</td>
<td>0</td>
<td>0x5559f</td>
<td></td>
</tr>
</tbody>
</table>

Source: * Group: 227.0.0.0 Mask length: 16

<table>
<thead>
<tr>
<th>C</th>
<th>IC</th>
<th>IP</th>
<th>ID</th>
<th>IS</th>
<th>IU</th>
<th>IF</th>
<th>IM</th>
<th>IV</th>
<th>IR</th>
<th>IA</th>
<th>IG</th>
<th>ET</th>
<th>EO</th>
<th>ER</th>
<th>EM</th>
<th>EV</th>
<th>EC</th>
<th>BS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8001</td>
<td>0</td>
<td>F</td>
<td>1</td>
<td>T</td>
<td>T</td>
<td>0</td>
<td>0x55167</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8001</td>
<td>0</td>
<td>F</td>
<td>1</td>
<td>T</td>
<td>T</td>
<td>0</td>
<td>0x55167</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8001</td>
<td>0</td>
<td>F</td>
<td>1</td>
<td>T</td>
<td>T</td>
<td>0</td>
<td>0x55167</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>F</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8001</td>
<td>0</td>
<td>F</td>
<td>1</td>
<td>T</td>
<td>T</td>
<td>0</td>
<td>0x5559f</td>
<td></td>
</tr>
</tbody>
</table>
```

**Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference, Release 5.3.x**

181
show mfb hardware route olist

<table>
<thead>
<tr>
<th>C</th>
<th>IC</th>
<th>IP ID</th>
<th>IS</th>
<th>IU</th>
<th>IF</th>
<th>IM</th>
<th>IV</th>
<th>IR</th>
<th>IA</th>
<th>IG</th>
<th>ET</th>
<th>EO</th>
<th>ER</th>
<th>EM</th>
<th>EV</th>
<th>EC</th>
<th>BS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x280</td>
<td>0x0</td>
<td>0x8009</td>
<td>0</td>
<td>F</td>
<td>6</td>
<td>T</td>
<td>T</td>
</tr>
<tr>
<td>1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x280</td>
<td>0x0</td>
<td>0x8009</td>
<td>0</td>
<td>F</td>
<td>6</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x280</td>
<td>0x0</td>
<td>0x8009</td>
<td>0</td>
<td>F</td>
<td>6</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x280</td>
<td>0x0</td>
<td>0x8009</td>
<td>0</td>
<td>F</td>
<td>6</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
</tbody>
</table>

Source: * Group: 227.0.0.1 Mask length: 32

Route Information

<table>
<thead>
<tr>
<th>C</th>
<th>IC</th>
<th>IP ID</th>
<th>IS</th>
<th>IU</th>
<th>IF</th>
<th>IM</th>
<th>IV</th>
<th>IR</th>
<th>IA</th>
<th>IG</th>
<th>ET</th>
<th>EO</th>
<th>ER</th>
<th>EM</th>
<th>EV</th>
<th>EC</th>
<th>BS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x1</td>
<td>0x8004</td>
<td>0</td>
<td>F</td>
<td>5</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x1</td>
<td>0x8004</td>
<td>0</td>
<td>F</td>
<td>5</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x1</td>
<td>0x8004</td>
<td>0</td>
<td>F</td>
<td>5</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x1</td>
<td>0x8004</td>
<td>1</td>
<td>T</td>
<td>5</td>
<td>T</td>
<td>T</td>
<td>3</td>
</tr>
</tbody>
</table>

Interface Information

<table>
<thead>
<tr>
<th>C</th>
<th>T</th>
<th>M</th>
<th>Intf</th>
<th>U</th>
<th>I</th>
<th>B</th>
<th>Base</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>0</td>
<td>G10/0/0/8</td>
<td>9</td>
<td>F</td>
<td>F</td>
<td>0x5540c</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
<td>G10/0/0/4</td>
<td>5</td>
<td>F</td>
<td>F</td>
<td>0x5540f</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>2</td>
<td>G10/0/0/6</td>
<td>7</td>
<td>F</td>
<td>F</td>
<td>0x55412</td>
</tr>
</tbody>
</table>

Source: * Group: 230.0.0.0 Mask length: 8

Route Information

<table>
<thead>
<tr>
<th>C</th>
<th>IC</th>
<th>IP ID</th>
<th>IS</th>
<th>IU</th>
<th>IF</th>
<th>IM</th>
<th>IV</th>
<th>IR</th>
<th>IA</th>
<th>IG</th>
<th>ET</th>
<th>EO</th>
<th>ER</th>
<th>EM</th>
<th>EV</th>
<th>EC</th>
<th>BS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8005</td>
<td>0</td>
<td>F</td>
<td>4</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8005</td>
<td>0</td>
<td>F</td>
<td>4</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8005</td>
<td>0</td>
<td>F</td>
<td>4</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8005</td>
<td>0</td>
<td>F</td>
<td>4</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
</tbody>
</table>

Source: * Group: 232.0.0.0 Mask length: 8

Route Information

<table>
<thead>
<tr>
<th>C</th>
<th>IC</th>
<th>IP ID</th>
<th>IS</th>
<th>IU</th>
<th>IF</th>
<th>IM</th>
<th>IV</th>
<th>IR</th>
<th>IA</th>
<th>IG</th>
<th>ET</th>
<th>EO</th>
<th>ER</th>
<th>EM</th>
<th>EV</th>
<th>EC</th>
<th>BS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8003</td>
<td>0</td>
<td>F</td>
<td>3</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8003</td>
<td>0</td>
<td>F</td>
<td>3</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8003</td>
<td>0</td>
<td>F</td>
<td>3</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x0</td>
<td>0x8003</td>
<td>0</td>
<td>F</td>
<td>3</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
</tbody>
</table>

Source: * Group: 233.1.0.0 Mask length: 16

Route Information

<table>
<thead>
<tr>
<th>C</th>
<th>IC</th>
<th>IP ID</th>
<th>IS</th>
<th>IU</th>
<th>IF</th>
<th>IM</th>
<th>IV</th>
<th>IR</th>
<th>IA</th>
<th>IG</th>
<th>ET</th>
<th>EO</th>
<th>ER</th>
<th>EM</th>
<th>EV</th>
<th>EC</th>
<th>BS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x180</td>
<td>0x0</td>
<td>0x8007</td>
<td>0</td>
<td>F</td>
<td>7</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x180</td>
<td>0x0</td>
<td>0x8007</td>
<td>0</td>
<td>F</td>
<td>7</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x180</td>
<td>0x0</td>
<td>0x8007</td>
<td>0</td>
<td>F</td>
<td>7</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x180</td>
<td>0x0</td>
<td>0x8007</td>
<td>0</td>
<td>F</td>
<td>7</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
</tbody>
</table>
show mfib hardware route olist location 0/4/CPU0

LC Type: A9K-SIP-700

Header : Hardware Route Information
Source : Source address
Group : Group Address
M : Mask Length
C : Directly connected check flag
RPF : Accepting interface for non-bidir entries
S : Signal if packet arrived on RPF interface
IC : Aggregated Internal copy flag
PR : Punt to RP flag for Internal copy in the Loopback interface
PK : PEEK flag
FGID : Fabric Group ID
MGID : Multicast Group ID
PAL Olist : PAL Olist handle
CPP Olist : CPP Olist handle
Num OCE : Number of OCE entries

Header : Route OCE Entry Information
Interface : Interface name
Handle : Interface handle
IC : Internal copy flag
Accept : Accept flag
NS : Negate Signal flag
F/EG : Forwarding flag

Ingress CPP Prefix Information

--- QFP Multicast prefix info ---
Root: a60394c4, Flags: 2 First leaf: 0
Number of nodes: 0x000001, leaves: 00000000  RPF i/f: 00000000
RPF Fast Convergence flags: 00000000 Secondary RPF: 00000000
RPF Fast Convergence timer: 0 ext_leaf: 0x8b900100

Egress CPP Prefix Information

--- QFP Multicast prefix info ---
Root: a60394c4, Flags: 2 First leaf: 0
Number of nodes: 0x000001, leaves: 00000000  RPF i/f: 00000000
show mib hardware route olist

RPF Fast Convergence flags: 00000000 Secondary RPF: 00000000
RPF Fast Convergence timer: 0 ext_leaf: 0x8ce80100

Route OCE Entry Information
Route OLIST Information

TREE .. : root : a60394c4 num_nodes 1 num_leaves 0
(in cp) Node: a60394c4 num_child:0 cum[wt:0 free:7]
(in cpp) Node : 0x8d080060 flags : 0x4
    child[0]: [NULL]
    child[1]: [NULL]
    child[2]: [NULL]
    child[3]: [NULL]
    child[4]: [NULL]
    child[5]: [NULL]
    child[6]: [NULL]

Route Rx Adjacency Information

OCE RX Adj Data for 0x8bb00000:
    base: 39(CPP HW RX ADJ IPV4 MCAST)    adj_flags: 0x0
    pd_16: 0x0    pd_32: 0x4244
    output_uidb: 0x1fab    counters_ptr: 0x893f5c30
    byte count: 0    packet count: 0

Hardware Route Information

Source |Group |M |C|RPF |S|IC|PR|PK|FGID |MGID |PAL Olist Handle|CPP OLIST |Num OCE|
--------------------------------------------
* |224.0.0.0 |24 |F|Null |F| F| F|F |0 |16962|0x9e07d2e4 |0x9dc86924 |0|

Ingress CPP Prefix Information

--- QFP Multicast prefix info ---
Root: 9e07d270, flags: 0 First leaf: 0
Number of nodes: 0x000000, leaves: 00000000 RPF i/f: 00000000
RPF Fast Convergence flags: 00000000 Secondary RPF: 00000000
RPF Fast Convergence timer: 0 ext_leaf: 0x8be90180

Egress CPP Prefix Information

--- QFP Multicast prefix info ---
Root: 9e07d270, flags: 0 First leaf: 0
Number of nodes: 0x000000, leaves: 00000000 RPF i/f: 00000000
RPF Fast Convergence flags: 00000000 Secondary RPF: 00000000
RPF Fast Convergence timer: 0 ext_leaf: 0x8ce80180
### Route Rx Adjacency Information

```
OCE RX Adj Data for 0x8bb00120:
base: 39(CPP HW RX ADJ IPV4 MCAST)  adj_flags: 0x0
pd_16: 0x0  pd_32: 0x4242
output_uidb: 0x1fab  counters_ptr: 0x893f5c10
byte count: 0  packet count: 0
```

### Hardware Route Information

```
<table>
<thead>
<tr>
<th>Source</th>
<th>Group</th>
<th>M</th>
<th>C</th>
<th>RPF</th>
<th>S</th>
<th>IC</th>
<th>PR</th>
<th>PK</th>
<th>FGID</th>
<th>MGID</th>
<th>PAL Olist Handle</th>
<th>CPP OLIST Num OCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>224.0.1.39</td>
<td>32</td>
<td>F</td>
<td>Null</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0</td>
<td>16960</td>
<td>0x9e07d678</td>
<td>0x9dc86970</td>
</tr>
</tbody>
</table>
```

### Ingress CPP Prefix Information

```
--- QFP Multicast prefix info ---
Root: 9e07d604, Flags: 1 First leaf: 0
Number of nodes: 00000001, leaves: 00000000  RPF i/f: 00000000
RPF Fast Convergence flags: 00000000 Secondary RPF: 00000000
RPF Fast Convergence timer: 0 ext_leaf: 0x8b9001c0
```

### Egress CPP Prefix Information

```
--- QFP Multicast prefix info ---
Root: 9e07d604, Flags: 1 First leaf: 0
Number of nodes: 00000001, leaves: 00000000  RPF i/f: 00000000
RPF Fast Convergence flags: 00000000 Secondary RPF: 00000000
RPF Fast Convergence timer: 0 ext_leaf: 0x8ce801c0
```

### Route OCE Entry Information

```
```

### Route OLIST Information

```
```

### Route Rx Adjacency Information

```
OCE RX Adj Data for 0x8bb000f0:
base: 39(CPP HW RX ADJ IPV4 MCAST)  adj_flags: 0x0
pd_16: 0x0  pd_32: 0x4240
output_uidb: 0x1fab  counters_ptr: 0x893f5c10
byte count: 0  packet count: 0
```

--- Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference, Release 5.3.x ---

Page 185
Hardware Route Information
----------------------------------------------------------
Source |Group |M |C|RPF |S|IC|PR|PK|FGID |MGID |PAL Olist Handle|CPP OLIST Handle|Num OCE|
----------------------------------------------------------
* |224.0.1.40|32 |F|Null |T| F| F|F |0 |16961|0x9dcbdab4 |0x9dc869bc
Ingress CPP Prefix Information
----------------------------------------------------------
--- QFP Multicast prefix info ---
Root: 9dcbda40, Flags: 1 First leaf: 0
Number of nodes: 0x000001, leaves: 00000000 RPF i/f: 00000000
RPF Fast Convergence flags: 00000000 Secondary RPF: 00000000
RPF Fast Convergence timer: 0 ext_leaf: 0x8b9000c0
Egress CPP Prefix Information
----------------------------------------------------------
--- QFP Multicast prefix info ---
Root: 9dcbda40, Flags: 1 First leaf: 0
Number of nodes: 0x000001, leaves: 00000000 RPF i/f: 00000000
RPF Fast Convergence flags: 00000000 Secondary RPF: 00000000
RPF Fast Convergence timer: 0 ext_leaf: 0x8ce800c0
Route OCE Entry Information
Route OLIST Information
----------------------------------------------------------
TREE .. : root : 9dcbda40 num_nodes 1 num_leaves 0
(in cp) Node: 9dcbda40 num_child:0 cum[wt:0 free:7]
(in cpp) Node : 0x8d0800c0 flags : 0x4
  child[0]: [NULL]
  child[1]: [NULL]
  child[2]: [NULL]
  child[3]: [NULL]
  child[4]: [NULL]
  child[5]: [NULL]
  child[6]: [NULL]
Route Rx Adjacency Information
----------------------------------------------------------
OCE RX Adj Data for 0x8bb00040:
  base: 39(CPP HW RX ADJ IPV4 MCAST) adj_flags: 0x0
  pd_16: 0x0  pd_32: 0x4241
  output_uidb: 0x1fab counters_ptr: 0x893f5c40
  byte count: 0 packet count: 0
Hardware Route Information
----------------------------------------------------------
Source |Group |M |C|RPF |S|IC|PR|PK|FGID |MGID |PAL Olist Handle|CPP OLIST Handle|Num OCE|
----------------------------------------------------------
* |225.0.0.0 |32 |T|Se0/4/0/0/1|F| F| F|F |64 |17013|0x9dcbda5a4 |0x9dc86a08
Ingress CPP Prefix Information
----------------------------------------------------------
--- QFP Multicast prefix info ---
Root: 9dcbd530, Flags: 2 First leaf: 9dcbd9bc
Number of nodes: 0x000001, leaves: 0x000001
RPF i/f: 0x007fff
RPF Fast Convergence flags: 00000000 Secondary RPF: 00000000
RPF Fast Convergence timer: 0 ext_leaf: 0x000001

Egress CPP Prefix Information
----------------------------------------------------------
--- QFP Multicast prefix info ---
Root: 9dcbd530, Flags: 2 First leaf: 9dcbd9bc
Number of nodes: 0x000001, leaves: 0x000001
RPF i/f: 0x007fff
RPF Fast Convergence flags: 00000000 Secondary RPF: 00000000
RPF Fast Convergence timer: 0 ext_leaf: 0x000001

Route OCE Entry Information
----------------------------------------------------------
Interface Handle IC Accept NS F/EG
----------------------------------------------------------
Se0/4/0/0/1 0xc000ec0 F T T F

**** Leaf Info (in cp) : [9dcbd9bc]
oce flags = 0x6 next obj type : 11 next obj handle : a73e9104

**** Leaf Info (in cpp): [0]
leaf_flags= 0x1 oce_flags: 0 oce_ptr: 0x8c5800c0
----------------------------------------------------------
Interface Handle IC Accept NS F/EG
----------------------------------------------------------
G10/4/3/0 0xc000080 F F T T

**** Leaf Info (in cp) : [9dcbd450]
oce flags = 0x5 next obj type : 11 next obj handle : a73e907c

**** Leaf Info (in cpp): [0x08c58900f0]
leaf_flags= 0x1 oce_flags: 0x2 oce_ptr: 0x8c580000

Route OLIX Information
----------------------------------------------------------
TREE .. : root : 9dcbd530 num_nodes 1 num_leaves 1
(in cpp) Node : 0x8d080080 flags : 0x4
child[0]: [Leaf] in cp : 9dcbd450 in cpp : 0x08c58000f0
child[1]: [NULL]
child[2]: [NULL]
child[3]: [NULL]
child[4]: [NULL]
child[5]: [NULL]
child[6]: [NULL]

Route Rx Adjacency Information
----------------------------------------------------------
OCE RX Adj Data for 0x8bb00160:
base: 39(CPP HW RX ADJ IPV4 MCAST) adj_flags: 0x0
pd_16: 0x40 pd_32: 0x427f
output_uidb: 0x1fab counters_ptr: 0x893f5c50
byte count: 9800 packet count: 196

Hardware Route Information
----------------------------------------------------------
Source |Group |M |C|RPF |S|IC|PR|PK|FGID |MGID |PAL Olist Handle|CPP OLIST Handle|Num OCE|
Ingress CPP Prefix Information

--- QFP Multicast prefix info ---
Root: 9dcbcfb0, Flags: 0 First leaf: 9dcbbccfc
Number of nodes: 0x000001, leaves: 0x000001
RPF Fast Convergence flags: 00000000 Secondary RPF: 00000000
RPF Fast Convergence timer: 0 ext_leaf: 0x8b900200

Egress CPP Prefix Information

--- QFP Multicast prefix info ---
Root: 9dcbcfb0, Flags: 0 First leaf: 9dcbbccfc
Number of nodes: 0x000001, leaves: 0x000001
RPF Fast Convergence flags: 00000000 Secondary RPF: 00000000
RPF Fast Convergence timer: 0 ext_leaf: 0x8ce80200

Route OCE Entry Information

Interface Handle IC Accept NS F/EG
Se0/4/0/0/1 0xc000ec0 F T F F

**** Leaf Info (in cp) : [9dcbbccfc]
oce flags = 0x2 next obj type : 11 next obj handle : a73e9104

**** Leaf Info (in cpp): [0]
leaf_flags= 0x1 oce_flags: 0 oce_ptr: 0x8c5800c0

Interface Handle IC Accept NS F/EG
Gi0/4/3/0 0xc0000080 F F T T

**** Leaf Info (in cp) : [9dcbbddc]
oce flags = 0x5 next obj type : 11 next obj handle : a73e907c

**** Leaf Info (in cpp): [0x8c5800d0]
leaf_flags= 0x1 oce_flags: 0x2 oce_ptr: 0x8c580000

Route OLIST Information

TREE .: root : 9dcbcfb0 num_nodes 1 num_leaves 1
(in cp) Node: 9dcbcfb0 num_child:1 cum[wt:1 free:6]
(in cpp) Node : 0x8d080000 flags : 0x4
child[0]: [Leaf] in cp : 9dcbbddc in cpp : 0x8c5800d0
child[1]: [NULL]
child[2]: [NULL]
child[3]: [NULL]
child[4]: [NULL]
child[5]: [NULL]
child[6]: [NULL]

Route Rx Adjacency Information

OCE RX Adj Data for 0x8bb00050:
base: 39(CPP NW RX ADJ IPV4 MCAST) adj_flags: 0x0
pd_16: 0x40 pd_32: 0x4280
output_uidb: 0x1fab counters_ptr: 0x893f5c60
### Hardware Route Information

<table>
<thead>
<tr>
<th>Source</th>
<th>Group</th>
<th>M</th>
<th>C</th>
<th>RPF</th>
<th>S</th>
<th>IC</th>
<th>PR</th>
<th>PK</th>
<th>FGID</th>
<th>MGID</th>
<th>PAL Olist Handle</th>
<th>CPP OLISAT</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>232.0.0.0</td>
<td>8</td>
<td>F</td>
<td>Null</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>0</td>
<td>16963</td>
<td></td>
<td>9e07d110</td>
</tr>
<tr>
<td></td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Ingress CPP Prefix Information

--- QFP Multicast prefix info ---
Root: 9e07d110, Flags: 0 First leaf: 0
Number of nodes: 000001, leaves: 00000000 RPF i/f: 00000000
RPF Fast Convergence flags: 00000000 Secondary RPF: 00000000
RPF Fast Convergence timer: 0 ext_leaf: 0x8b900140

### Egress CPP Prefix Information

--- QFP Multicast prefix info ---
Root: 9e07d110, Flags: 0 First leaf: 0
Number of nodes: 000001, leaves: 00000000 RPF i/f: 00000000
RPF Fast Convergence flags: 00000000 Secondary RPF: 00000000
RPF Fast Convergence timer: 0 ext_leaf: 0x8ce80140

### Route OCE Entry Information

```
TREE .. : root : 9e07d110 num_nodes 1 num_leaves 0
(in cp) Node: 9e07d110 num_child:0 cum[wt:0 free:7]
(in cpp) Node : 0x8d0800e0 flags : 0x4
child[0]: [NULL]
child[1]: [NULL]
child[2]: [NULL]
child[3]: [NULL]
child[4]: [NULL]
child[5]: [NULL]
child[6]: [NULL]
```

### Route Rx Adjacency Information

```
OCE RX Adj Data for 0x8bb00080:
base: 39(CPP HW RX ADJ IPV4 MCAST) adj_flags: 0x0
pd_16: 0x0 pd_32: 0x4243
output_uidb: 0x1fab counters_ptr: 0x893f5c20
byte count: 0 packet count: 0
```

The following is sample output from the `show mfib hardware route olist` command with only one multicast group:

```
RP/0/RSP0/CPU0:router# show mfib hardware route olist 227.0.0.1 location 0/0/CPU0
Legend:
Route Information - (Ingress)
C: Chip ID, IC: BACL check, IP: Punt this packet to LC CPU,
ID: Directly connected, IS: RPF interface signal, IU: Punt copy to RP,
IF: Punt to LC CPU if forwarded, IM: Result match, IV: Valid entry,
```
IR: RPF IF, IA: Fabric slotmask, IG: Multicast group ID
Route Information - (Egress)
  ET: Table ID to be used for OLIST lookup, EO: OLIST count bit,
  ER: Route MSID to be used for OLIST/NRPF lookup, EM: Result match,
  EV: Valid entry, EC: Count of OLIST members on this chip,
  BS: Base of the statistics pointer
Hardware Information
  C: Chip ID; T: Table ID; M: Member ID; Intf: Interface, U: uIDB index,
  I: HW IC flag, B: HW BACL bit, Base: Base of statistics pointer

Source: * Group: 227.0.0.1 Mask length: 32

<table>
<thead>
<tr>
<th>C</th>
<th>IC</th>
<th>IP ID</th>
<th>IS</th>
<th>IU</th>
<th>IF</th>
<th>IM</th>
<th>IV</th>
<th>IR</th>
<th>IA</th>
<th>IG</th>
<th>ET</th>
<th>EO</th>
<th>ER</th>
<th>EM</th>
<th>EV</th>
<th>EC</th>
<th>BS</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x1</td>
<td>0x8004</td>
<td>0</td>
<td>F</td>
<td>5</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x1</td>
<td>0x8004</td>
<td>0</td>
<td>F</td>
<td>5</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x1</td>
<td>0x8004</td>
<td>0</td>
<td>F</td>
<td>5</td>
<td>T</td>
<td>T</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>T</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>F</td>
<td>T</td>
<td>T</td>
<td>0x0</td>
<td>0x1</td>
<td>0x8004</td>
<td>1</td>
<td>T</td>
<td>5</td>
<td>T</td>
<td>T</td>
<td>3</td>
</tr>
</tbody>
</table>

Interface Information

<table>
<thead>
<tr>
<th>C</th>
<th>T</th>
<th>M</th>
<th>Intf</th>
<th>U</th>
<th>I</th>
<th>B</th>
<th>Base</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1</td>
<td>0</td>
<td>Gi0/0/0/8</td>
<td>9</td>
<td>F</td>
<td>F</td>
<td>0x5540c</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>1</td>
<td>Gi0/0/0/4</td>
<td>5</td>
<td>F</td>
<td>F</td>
<td>0x5540f</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
<td>2</td>
<td>Gi0/0/0/6</td>
<td>7</td>
<td>F</td>
<td>F</td>
<td>0x55412</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mfib hardware route accept-bitmap, on page 167</td>
<td>Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the interface list that accepts bidirectional routes.</td>
</tr>
<tr>
<td>show mfib hardware route statistics, on page 191</td>
<td>Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the packet and byte counters for each route.</td>
</tr>
<tr>
<td>show mfib hardware route summary, on page 195</td>
<td>Displays summary platform-specific Multicast Forwarding Information Base (MFIB) hardware information for each route entry.</td>
</tr>
<tr>
<td>show mfib route, on page 204</td>
<td>Displays route entries in the Multicast Forwarding Information Base (MFIB).</td>
</tr>
</tbody>
</table>
# show mfib hardware route statistics

The `show mfib hardware route statistics` command in EXEC mode is used to display platform-specific Multicast Forwarding Information Base (MFIB) information for the packet and byte counters for each route. The syntax of the command is as follows:

```
show mfib [vrf vrf-name] [ipv4|ipv6] hardware route statistics [detail] [*] [source-address] [group-address [/prefix-length]] [location node-id]
```

### Syntax Description

- **vrf vrf-name** (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- **ipv4** (Optional) Specifies IPv4 address prefixes.
- **ipv6** (Optional) Specifies IPv6 address prefixes.
- ***** (Optional) Displays shared tree entries.
- **source-address** (Optional) IP address or hostname of the multicast route source.
- **group-address** (Optional) IP address or hostname of the multicast group.
- **/prefix-length** (Optional) Prefix length of the multicast group. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash must precede the decimal value.
- **detail** (Optional) Displays a detailed list of the routing database.
- **location node-id** (Optional) Specifies an MFIB-designated node.

### Command Default

IPv4 addressing is the default.

### Command Modes

EXEC

### Command History

**Release 3.7.2**  This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `show mfib hardware route statistics` command to display the hardware packet and byte counter for a route. Route counters are kept for (S, G) routes only. A single set of counters is provided for all (*, G) routes.

This command displays the hardware packet and bytes count on a per-route basis. Per-route hardware counters are kept for (S, G) routes only. However, counters are managed dynamically and allocated on a priority basis and may not be available for each (S, G) route. There is a single set of counters for all (*, G) routes. For example, interface counters and access list counters have higher priority than route counters.
Route counters are local to each line card.

### Examples

The following is sample output from the `show mfib hardware route statistics` command.

```
RP/0/RSP0/CPU0:router# show mfib hardware route statistics location 0/4/CPU0

LC Type: A9K-SIP-700
Hardware Prefix Statistics

<table>
<thead>
<tr>
<th>(s, g) RX/TX: Pkt/Byte: Forward(Pkt/Byte) Punt(Pkt/Byte) RPF Fail(Pkt/Byte) Drop(Pkt/Byte)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(* , 224.0.0.0 ) RX: 0/0 0/0 0/0 0/0</td>
</tr>
<tr>
<td>(* , 224.0.0.0 ) TX: 0/0 0/0 0/0 0/0</td>
</tr>
<tr>
<td>(* , 224.0.0.0 ) RX: 0/0 0/0 0/0 0/0</td>
</tr>
<tr>
<td>(* , 224.0.0.0 ) TX: 0/0 0/0 0/0 0/0</td>
</tr>
<tr>
<td>(* , 224.0.0.0 ) RX: 0/0 0/0 0/0 0/0</td>
</tr>
<tr>
<td>(* , 224.0.1.39) RX: 0/0 0/0 0/0 0/0</td>
</tr>
<tr>
<td>(* , 224.0.1.39) TX: 0/0 0/0 0/0 0/0</td>
</tr>
<tr>
<td>(* , 224.0.1.40) RX: 0/0 0/0 0/0 0/0</td>
</tr>
<tr>
<td>(* , 224.0.1.40) TX: 0/0 0/0 0/0 0/0</td>
</tr>
<tr>
<td>(* , 225.0.0.0 ) RX: 196/9016 1/138 0/0 0/0</td>
</tr>
<tr>
<td>(* , 225.0.0.0 ) TX: 196/9016 0/0 0/0 0/0</td>
</tr>
<tr>
<td>(* , 225.0.0.0 ) RX: 196/9016 1/138 0/0 0/0</td>
</tr>
<tr>
<td>(* , 225.0.0.0 ) TX: 196/9016 0/0 0/0 0/0</td>
</tr>
<tr>
<td>(12.12.12.2, 225.0.0.0 ) RX: 7931284/364839064 3/138 0/0</td>
</tr>
<tr>
<td>(12.12.12.2, 225.0.0.0 ) TX: 7931288/364839248 0/0 0/0</td>
</tr>
<tr>
<td>(* , 232.0.0.0 ) RX: 0/0 0/0 0/0 0/0</td>
</tr>
<tr>
<td>(* , 232.0.0.0 ) TX: 0/0 0/0 0/0 0/0</td>
</tr>
</tbody>
</table>

RP/0/RSP0/CPU0:router# show mfib hardware route statistics location 0/0/CPU0

LC Type: Trident
Legend:
S: Source, G: Group, Pr: Prefix Length, C: Chip ID, R: Received, P: Punted to CPU, F: Forwarded, ID: Ingress Drop, ED: Egress Drop

S: *  G: 224.0.0.0  Pr:24
C  R(packets:bytes)/F(packets:bytes)/P(packets)/ID(packets)/ED(packets)
-----------------------------------------------------------------------
| 0 0:0 / 0:0 / 0 / 0 / 0 |
| 1 0:0 / 0:0 / 0 / 0 / 0 |
```
No OLIST interfaces found for this route

S:  * G: 224.0.1.39  Pr:32

C                  R(packets:bytes)/F(packets:bytes)/P(packets)/ID(packets)/ED(packets)
------------------- -----------------------------------------------
0  0:0 / 0:0 / 0 / 0 / 0
1  0:0 / 0:0 / 0 / 0 / 0
2  0:0 / 0:0 / 0 / 0 / 0
3  0:0 / 0:0 / 0 / 0 / 0

No OLIST interfaces found for this route

S:  * G: 224.0.1.40  Pr:32

C                  R(packets:bytes)/F(packets:bytes)/P(packets)/ID(packets)/ED(packets)
------------------- -----------------------------------------------
0  0:0 / 0:0 / 0 / 0 / 0
1  0:0 / 0:0 / 0 / 0 / 0
2  0:0 / 0:0 / 0 / 0 / 0
3  0:0 / 0:0 / 0 / 0 / 0

No OLIST interfaces found for this route

S:  * G: 227.0.0.1  Pr:32

C                  R(packets:bytes)/F(packets:bytes)/P(packets)/ID(packets)/ED(packets)
------------------- -----------------------------------------------
0  0:0 / 0:0 / 0 / 0 / 0
1  0:0 / 0:0 / 0 / 0 / 0
2  0:0 / 0:0 / 0 / 0 / 0
3  504844:30290640 / 504843:23222778 / 504856 / 0 / 0

Interface Statistics:

<table>
<thead>
<tr>
<th>Interface</th>
<th>F/P/D (packets:bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/0/0/8</td>
<td>504843:23222778 / 0:0 / 0:0</td>
</tr>
<tr>
<td>Gi0/0/0/4</td>
<td>0:0 / 0:0 / 0:0</td>
</tr>
<tr>
<td>Gi0/0/0/6</td>
<td>504843:23222778 / 0:0 / 0:0</td>
</tr>
</tbody>
</table>

S:  4.0.0.2   G: 227.0.0.1  Pr:64

C                  R(packets:bytes)/F(packets:bytes)/P(packets)/ID(packets)/ED(packets)
------------------- -----------------------------------------------
0  0:0 / 0:0 / 0 / 0 / 0
1  0:0 / 0:0 / 0 / 0 / 0
2  0:0 / 0:0 / 0 / 0 / 0
3  3869:232140 / 3869:177974 / 0 / 0 / 0

Interface Statistics:

<table>
<thead>
<tr>
<th>Interface</th>
<th>F/P/D (packets:bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gi0/0/0/4</td>
<td>3869:177974 / 0:0 / 0:0</td>
</tr>
<tr>
<td>Gi0/0/0/8</td>
<td>3869:177974 / 0:0 / 0:0</td>
</tr>
</tbody>
</table>

S:  * G: 230.0.0.0  Pr:8
Show mfb hardware route statistics

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress Counter</td>
<td>Unique identifier of the ingress counter.</td>
</tr>
<tr>
<td>Egress Counter</td>
<td>Unique identifier of the egress counter.</td>
</tr>
<tr>
<td>Forward</td>
<td>Number of forwarded packets and bytes.</td>
</tr>
<tr>
<td>Punt</td>
<td>Number of bytes punted from the line card CPU.</td>
</tr>
<tr>
<td>Drop</td>
<td>Number of dropped bytes.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mfb hardware route accept-bitmap, on page 167</td>
<td>Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the interface list that accepts bidirectional routes.</td>
</tr>
<tr>
<td>show mfb hardware route olist, on page 180</td>
<td>Displays platform-specific Multicast Forwarding Information Base (MFIB) information in the output interface list (olist) stored in the hardware.</td>
</tr>
<tr>
<td>show mfb hardware route summary, on page 195</td>
<td>Displays summary platform-specific Multicast Forwarding Information Base (MFIB) hardware information for each route entry.</td>
</tr>
<tr>
<td>show mfb route, on page 204</td>
<td>Displays route entries in the Multicast Forwarding Information Base (MFIB).</td>
</tr>
</tbody>
</table>
show mfib hardware route summary

To display summary platform-specific Multicast Forwarding Information Base (MFIB) hardware information for each route entry, use the show mfib hardware route summary command in EXEC mode.

```
show mfib [vrf vrf-name] [ipv4|ipv6] hardware route summary location node-id
```

**Syntax Description**
- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `ipv6` (Optional) Specifies IPv6 address prefixes.
- `location node-id` (Optional) Specifies an MFIB-designated node.

**Command Default**
IPv4 addressing is the default.

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the show mfib hardware summary command to display hardware information for the route of the node.

The hardware information of MoFRR (multicast only fast reroute) enabled routes are also displayed. In IOS XR Software Release 3.9.0, the maximum platform supported MoFRR routes are 1024.

The longest-prefix match route is displayed depending on the provided source and group addresses. The command does not display any useful output if only RSP is specified or if no location is specified.

**Task ID**

**Operations**
- multicast read

**Examples**
The following is sample output from the show mfib hardware route summary command:

```
RP/0/RSP0/CPU0:router# show mfib hardware route summary location 0/1/cpu0

LC Type: Trident
H/W IP Multicast Forwarding Information Base Summary
   No. of (*,G) routes = 5
   No. of (S,G) routes = 10

RP/0/RSP0/CPU0:router# show mfib hardware route summary location 0/0/CPU0
```
LC Type: Trident
H/W IP Multicast Forwarding Information Base Summary
   No. of (*,G) routes = 6
   No. of (S,G) routes = 5
   No. of (S,G) MoFRR routes = 0, Maximum supported MoFRR routes = 1024

RP/0/RSP0/CPU0:router# show mfib hardware route summary location 0/4/cPU0

LC Type: A9K-SIP-700
Hardware IP Multicast Forwarding Information Base Route Summary
   Number of hardware (*, G) routes = 6
   Number of hardware (S, G) routes = 1
   Number of hardware route-interfaces = 4
   Number of hardware Rx adjacencies = 7
   Number of hardware Tx adjacencies = 3
   Number of ref to decap adjacency = 0
   Mvpn master LC status = False

If there is no MoFRR configured in the platform:

RP/0/RSP0/CPU0:router# show mfib hardware route summary location 0/0/cPU0

LC Type: Trident
H/W IP Multicast Forwarding Information Base Summary
   No. of (*,G) routes = 6
   No. of (S,G) routes = 5
   No. of (S,G) MoFRR routes = 0, Maximum supported MoFRR routes = 1024

This table describes the significant fields shown in the display.

Table 20: show mfib hardware route summary Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of (*,G) routes</td>
<td>Number of (*,G) routes installed in hardware.</td>
</tr>
<tr>
<td>No. of (S,G) routes</td>
<td>Number of (S,G) routes installed in hardware.</td>
</tr>
<tr>
<td>No. of (S,G) MoFRR routes</td>
<td>Number of MoFRR (S,G) routes installed in hardware.</td>
</tr>
<tr>
<td>Maximum supported MoFRR routes</td>
<td>Maximum number of MoFRR routes supported in hardware.</td>
</tr>
</tbody>
</table>

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mfib hardware route accept-bitmap, on page 167</td>
<td>Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the interface list that accepts bidirectional routes.</td>
</tr>
<tr>
<td>show mfib hardware route mofrr, on page 174</td>
<td>Displays the platform-specific Multicast Forwarding Information Base (MFIB) information for the MoFRR (multicast only fast reroute)-enabled list stored in the hardware.</td>
</tr>
<tr>
<td>show mfib hardware route olist, on page 180</td>
<td>Displays platform-specific Multicast Forwarding Information Base (MFIB) information in the output interface list (olist) stored in the hardware.</td>
</tr>
<tr>
<td>show mfib hardware route statistics, on page 191</td>
<td>Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the packet and byte counters for each route.</td>
</tr>
</tbody>
</table>
### Command | Description
--- | ---
`show mfib route, on page 204` | Displays route entries in the Multicast Forwarding Information Base (MFIB).
show mfib hardware table

To display the platform-specific multicast table information for the Multicast Forwarding Information Base (MFIB) in the hardware, use the `show mfib hardware table` command in EXEC mode.

```
show mfib [vrf vrf-name] [ipv4|ipv6] hardware table [detail] [location node-id]
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `ipv6` (Optional) Specifies IPv6 address prefixes.
- `detail` (Optional) Displays detailed platform-specific multicast table information.
- `location node-id` (Optional) Specifies the MFIB location.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| 3.9.1    | This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Note**

The command does not display any useful output if only RSP is specified or if no location is specified.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows a sample output of the `show mfib hardware table` command:

```
RP/0/RSP0/CPU0:router# show mfib hardware table detail location 0/1/CPU0
LC Type: Trident
```

Legend:
NP: Network Processor, MNP: Master NP, SW OC: Software OLIST Count
TID: Table ID, MLC: Master Linecard (PD Flag)
MNP Id: Master NP ID, C_NP_MASK: Composite NP Mask
This table describes the significant fields shown in the display.

*Table 21: show mfib hardware table Field Descriptions*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NP</td>
<td>Specifies the network processor.</td>
</tr>
<tr>
<td>MNP</td>
<td>Specifies the master network processor.</td>
</tr>
<tr>
<td>SW OC</td>
<td>Specifies the software OLIST count.</td>
</tr>
<tr>
<td>TID</td>
<td>Specifies the Table ID.</td>
</tr>
</tbody>
</table>
show mfib interface

To display interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process, use the `show mfib interface` command in EXEC mode.

```
show mfib [vrf vrf-name] ipv4 interface [type interface-path-id] [{detail|route}] [location node-id]
```

### Syntax Description

- **vrf vrf-name** (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- **ipv4** (Optional) Specifies IPv4 address prefixes.
- **type** (Optional) Interface type. For more information, use the question mark (?) online help function.
- **interface-path-id** (Optional) Physical interface or virtual interface.
  - **Note** Use the `show interfaces` command in EXEC mode to see a list of all interfaces currently configured on the router.
  - For more information about the syntax for the router, use the question mark (?) online help function.
- **detail** (Optional) Specifies detailed information for packet statistics on interfaces.
- **route** (Optional) Specifies a list of routes associated with the interface. This option is available if an interface `type` and `instance` are specified.
- **location node-id** (Optional) Specifies packet statistics associated with an interface of the designated node.

### Command Default

IPv4 addressing is the default.

### Command Modes

EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `show mfib interface` command displays counters for the number of packets and bytes that are handled by software switching. Counters for packets processed by hardware are displayed by the appropriate `show mfib hardware` command.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>
Examples

The following is sample output from the `show mfib interface` command for the multicast route on node 0/2/CPU0 that is associated with the Gigabit Ethernet interface 0/2/0/2:

```
RP/0/RSP0/CPU0:router# show mfib interface GigE 0/2/0/2 location 0/2/CPU0

Interface : GigE0/2/0/2 (Enabled)
Mcast pkts in : 5839, Mcast pkts out : 0 TTL Threshold : 0 Ref Count : 18
```

The following is sample output from the `show mfib interface` command with the `detail` and `location` keywords specified:

```
RP/0/RSP0/CPU0:router# show mfib interface detail location 0/2/CPU0

Interface : FINT0/2/CPU0 [0x3000000] (Disabled) PHYSICAL Create Unknown Mcast pkts in: 0,
Mcast pkts out: 0 TTL Threshold : 0, VRF ID: 0x60000000, Multicast Adjacency Ref Count: 2,
Route Count: 0, Handle: 0x3000000 Primary address : 0.0.0.0/32 Secondary address : 0.0.0.0/32

Interface : GigE0/2/0/2 [0x3000900] (Enabled) PHYSICAL Create Rcvd Mcast pkts in: 5844,
Mcast pkts out: 0 TTL Threshold : 0, VRF ID: 0x60000000, Multicast Adjacency Ref Count: 18,
Route Count: 15, Handle: 0x3000900 Primary address : 112.112.112.203/24 Secondary address
: 0.0.0.0/32
```

This table describes the significant fields shown in the display.

**Table 22: show mfib interface Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface name. Enabled if the interface is configured for multicast routing. The word “PHYSICAL” is displayed if the interface is a nonvirtual interface.</td>
</tr>
<tr>
<td>Mcast pkts in</td>
<td>Number of incoming multicast packets entering the interface during software switching.</td>
</tr>
<tr>
<td>Mcast pkts out</td>
<td>Number of outgoing multicast packets exiting the interface during software switching.</td>
</tr>
<tr>
<td>TTL Threshold</td>
<td>Number of multicast packets that reach the configured multicast time-to-live threshold.</td>
</tr>
<tr>
<td>VRF ID</td>
<td>VPN Routing and Forwarding instance ID.</td>
</tr>
<tr>
<td>Ref Count</td>
<td>Number of references to this interface structure in the MFIB process.</td>
</tr>
<tr>
<td>Primary address</td>
<td>Primary IP address of the interface.</td>
</tr>
<tr>
<td>Secondary address</td>
<td>Secondary IP address of the interface.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mfib hardware interface</code>, on page 155</td>
<td>Displays hardware switching interface information for the Multicast Forwarding Information Base (MFIB) process.</td>
</tr>
</tbody>
</table>
show mfib nsf

To display the state of a nonstop forwarding (NSF) operation for the Multicast Forwarding Information Base (MFIB) line cards, use the `show mfib nsf` command in EXEC mode.

```
show mfib [{ipv4}] nsf [location node-id]
```

**Syntax Description**

- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `location node-id` (Optional) Specifies the MFIB NSF designated node.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `show mfib nsf` command displays the current multicast NSF state for the MFIB process contained on all line cards and route processors (RPs) in the router.

For multicast NSF, the state may be one of the following:

- **Normal**—Normal operation: The MFIBs in the card contain only up-to-date MFIB entries.
- **Boot Card Booting**—Card is initializing and has not yet determined its NSF state.
- **Not Forwarding**—Multicast Forwarding Disabled: Multicast routing failed to recover from a failure-induced NSF state prior to the MFIB NSF timeout.
- **Non-stop Forwarding Activated**—Multicast NSF active: The router is operating in NSF mode while attempting to recover from a control-plane failure. In this mode, data is forwarded based on MFIB entries that were either updated by the recovered Multicast Routing Information Base (MRIB), or MFIB entries that were marked stale when NSF mode began. The times remaining until multicast NSF and multicast-unicast NSF expiration are displayed.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show mfib nsf` command:

```
RP/0/RSP0/CPU0:router# show mfib nsf

IP MFWD Non-Stop Forwarding Status:
    NSF Lifetime: 00:15:00
```
On node 0/1/CPU0:
Multicast routing state: Non-Stop Forwarding is activated
NSF Time Remaining: 00:14:54

On node 0/3/CPU0:
Multicast routing state: Non-Stop Forwarding is activated
NSF Time Remaining: 00:14:54

On node 0/4/CPU0:
Multicast routing state: Non-Stop Forwarding is activated
NSF Time Remaining: 00:14:53

On node 0/6/CPU0:
Multicast routing state: Non-Stop Forwarding is activated
NSF Time Remaining: 00:14:53

This table describes the significant fields shown in the display.

Table 23: show mfib nsf Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP MFWD Non-Stop Forwarding Status</td>
<td>MFIB NSF status of each node in the system: booting, normal, not forwarding, or activated.</td>
</tr>
<tr>
<td>NSF Time Remaining</td>
<td>If MSB NSF is activated, the time remaining until NSF fails and all routes are deleted displays. Before timeout, MRIB signals that NSF (in the control plane) is finished and new, updated routes are populated in the MFIB (which makes the transition to Normal status).</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>nsf lifetime (IGMP)</code></td>
<td>Configures the maximum time for the NSF timeout value under IGMP.</td>
</tr>
<tr>
<td><code>nsf (multicast)</code>, on page 143</td>
<td>Configures the NSF capability for the multicast routing system.</td>
</tr>
<tr>
<td><code>nsf lifetime (PIM)</code></td>
<td>Configures the NSF timeout value for the PIM process.</td>
</tr>
<tr>
<td><code>show igmp nsf</code></td>
<td>Displays the state of NSF operation in IGMP.</td>
</tr>
<tr>
<td><code>show mrib nsf</code>, on page 216</td>
<td>Displays the state of NSF operation in the MRIB.</td>
</tr>
<tr>
<td><code>show pim nsf</code></td>
<td>Displays the state of NSF operation for PIM.</td>
</tr>
</tbody>
</table>
show mfib route

To display route entries in the Multicast Forwarding Information Base (MFIB), use the **show mfib route** command in EXEC mode.

**show mfib [vrf vrf-name] ipv4 route**

[ *rate*source-IP-address|group-IP-address/ prefix-length|detail|summary|location node-id ]

**Syntax Description**

* (Optional) Display shared tree entries.

source-IP-address (Optional) IP address or hostname of the multicast route source. Format is: A.B.C.D

group-IP-address (Optional) IP address or hostname of the multicast group. Format is: A.B.C.D

/prefix-length (Optional) Group IP prefix length of the multicast group. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). Format is: A.B.C.D/length

vrf vrf-name (Optional) Specifies a VPN routing and forwarding (VRF) instance.

ipv4 (Optional) Specifies IPv4 address prefixes.

ipv6 (Optional) Specifies IPv6 address prefixes.

detail (Optional) Specifies detailed route information.

location node-id (Optional) Specifies an MFIB-designated node.

rate (Optional) Displays individual (S, G) rates.

sources-only (Optional) Restricts display of any shared-tree entries.

summary (Optional) Displays a brief list of the routing database.

tech-support (Optional) Displays technical support information.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
All entries in the MFIB table are derived from the Multicast Routing Information Base (MRIB). The flags have the same connotation as in the MRIB. The flags determine the forwarding and signaling behavior according to a set of forwarding rules for multicast packets. In addition to the list of interfaces and flags, each route entry shows various counters. Byte count is the number of total bytes forwarded. Packet count is the number of packets received for this entry.

The `show mfib counter` command displays global counters independent of the routes.

This command displays counters for the number of packets and bytes that are handled by software switching. Counters for packets processed by hardware are displayed by the appropriate `show mfib hardware` command.

The command displays the cumulative rates per route for all line cards in the Multicast Forwarding Information Base (MFIB) table when the `rate` keyword is used with the source and group IP addresses.

The show mfib route rate command is not supported on interfaces such as bundle virtual interfaces and Bridge Group virtual interfaces (BVIs).

The command displays the rate per route for one line card in Multicast Forwarding Information Base (MFIB) table when the `statistics` keyword is used.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>multicast read</td>
</tr>
</tbody>
</table>

### Examples

The following is sample output from the `show mfib route` command with the `location` keyword specified (the output fields are described in the header):

```
RP/0/RSP0/CPU0:router# show mfib route location 0/1/CPU0

IP Multicast Forwarding Information Base
Entry flags: C - Directly-Connected Check, S - Signal, D - Drop,
             IA - Inherit Accept, IF - Inherit From, MA - MDT Address,
             ME - MDT Encap, MD - MDT Decap, MT - MDT Threshold Crossed,
             MH - MDT interface handle, CD - Conditional Decap,
             DT - MDT Decap True
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
                NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
                EG - Egress, EI - Encapsulation Interface, MI - MDT Interface
Forwarding Counts: Packets in/Packets out/Bytes out
Failure Counts: RPF / TTL / Empty Olist / Encap RL / Other

(*,224.0.0.0/24), Flags: D
  Up: 02:16:52
  Last Used: never
  SW Forwarding Counts: 0/0/0
  SW Failure Counts: 0/0/0/0/0

(*,224.0.1.39), Flags: S
  Up: 02:16:52
  Last Used: never
  SW Forwarding Counts: 0/0/0
  SW Failure Counts: 0/0/0/0/0

(*,224.0.1.40), Flags: S
  Up: 02:16:52
  Last Used: never
  SW Forwarding Counts: 0/0/0
  SW Failure Counts: 0/0/0/0/0
```
The following is sample output from the `show mfib route` command with the `summary` and `location` keywords specified:

```
RP/0/RSP0/CPU0:router# show mfib route summary location 0/0/CPU0
IP Multicast Forwarding Information Base Summary for VRF default
 No. of (*,G) routes = 5
 No. of (S,G) routes = 1

The following is sample output from the `show mfib route` command with the `statistics` and `location` keywords specified. If the hardware counters show N/A, it means no hardware statistic blocks were assigned to the route. However, routes may show that both hardware and software statistic blocks are assigned. The output fields are described in the header.

RP/0/RSP0/CPU0:router# show mfib route statistics location 0/0/CPU0
IP Multicast Forwarding Information Base
Entry flags: C - Directly-Connected Check, S - Signal, D - Drop,
 IA - Inherit Accept, IF - Inherit From, MA - MDT Address,
 ME - MDT Encap, MD - MDT Decap, MT - MDT Threshold Crossed,
 MH - MDT interface handle, CD - Conditional Decap,
 DT - MDT Decap True
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
 NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
 EG - Egress, EI - Encapsulation Interface, MI - MDT Interface
SW/HW Forwarding Counts: Packets in/Packets out/Bytes out
SW Failure Counts: RPF / TTL / Empty Olist / Encap RL / Other
HW Drop Counts: Ingress / Egress
HW Forwarding Rates: bps In/pps In/bps Out/pps Out
```

```
(*,227.0.0.1),  Flags:  C
 Up: 02:16:51
 Last Used: 02:16:50
 SW Forwarding Counts: 282/0/0
 SW Failure Counts: 205/0/0/0
 GigabitEthernet0/0/0/4 Flags:  NS EG, Up:02:16:46
 GigabitEthernet0/0/0/8 Flags:  NS EG, Up:02:16:50
 GigabitEthernet0/0/0/6 Flags:  NS EG, Up:02:16:50

(4.0.0.2,227.0.0.1),  Flags:  
 Up: 02:16:50
 Last Used: 00:00:12
 SW Forwarding Counts: 125/0/0
 SW Failure Counts: 0/0/0/0/0
 GigabitEthernet0/0/0/8 Flags:  NS EG, Up:02:16:50
 GigabitEthernet0/0/0/6 Flags:  NS EG, Up:02:16:50
 GigabitEthernet0/0/0/4 Flags:  A EG, Up:02:16:50

(*,232.0.0.0/8),  Flags:  D
 Up: 02:16:52
 Last Used: never
 SW Forwarding Counts: 0/0/0
 SW Failure Counts: 0/0/0/0/0
 HW Forwarding Counts: 0/0/0
 HW Drop Counts: 0/0
 HW Forwarding Rates: N/A /N/A /N/A /N/A

(*,224.0.0.0/24),  Flags:  D
 Up: 02:16:52
 Last Used: never
 SW Forwarding Counts: 0/0/0
 SW Failure Counts: 0/0/0/0
 HW Forwarding Counts: 0/0/0
 HW Drop Counts: 0/0
 HW Forwarding Rates: N/A /N/A /N/A /N/A

(*,224.0.1.39),  Flags:  S
```
The following is a sample output for MoFRR enabled route without and with the detail keyword:

```
RP/0/RSP0/CPU0:router# show mfib route
```

```
IP Multicast Forwarding Information Base

Entry flags: C - Directly-Connected Check, S - Signal, D - Drop,
   IA - Inherit Accept, IF - Inherit From, MA - MDT Address,
   ME - MDT Encap, MD - MDT Decap, MT - MDT Threshold Crossed,
   MI - MDT interface handle, CD - Conditional Decap,
   DT - MDT Decap True, EX - Extranet
   MoFE - MoFRR Enabled, MoFS - MoFRR State

Interface flags: F - Forward, A - Accept, IC - Internal Copy,
   NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
   EG - Egress, EI - Encapsulation Interface, MI - MDT Interface
```

EX - Extranet, A2 - Secondary Accept
Forwarding/Replication Counts: Packets in/Packets out/Bytes out
Failure Counts: RPF / TTL / Empty Olist / Encap RL / Other

(20.20.20.1,225.0.0.1), Flags: MoFE MoFS
Up: 03:22:30
Last Used: never
SW Forwarding Counts: 0/0/0
SW Replication Counts: 0/0/0
SW Failure Counts: 0/0/0/0/0
GigabitEthernet0/0/0/8 Flags: A, Up:03:22:30
GigabitEthernet0/0/0/18 Flags: A2, Up:03:22:30
GigabitEthernet0/0/0/28 Flags: NS, Up:03:22:30

(20.20.20.1,225.0.0.2), Flags: MoFE MoFS
Up: 03:22:30
Last Used: never
SW Forwarding Counts: 0/0/0
SW Replication Counts: 0/0/0
SW Failure Counts: 0/0/0/0/0
GigabitEthernet0/0/0/8 Flags: A, Up:03:22:30
GigabitEthernet0/0/0/18 Flags: A2, Up:03:22:30
GigabitEthernet0/0/0/28 Flags: NS, Up:03:22:30

In the above command, A flag represents the primary RPF of the MoFRR route, and A2 flag represents the backup RPF of the MoFRR route.

RP/0/RSP0/CPU0:router# show mfib route detail

IP Multicast Forwarding Information Base
Entry flags: C - Directly-Connected Check, S - Signal, D - Drop,
IA - Inherit Accept, IF - Inherit From, MA - MDT Address,
ME - MDT Encap, MD - MDT Decap, MT - MDT Threshold Crossed,
MH - MDT Interface handle, CD - Conditional Decap,
DT - MDT Decap True, EX - Extranet
MoFE - MoFRR Enabled, MoFS - MoFRR State
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
EG - Egress, EI - Encapsulation Interface, MI - MDT Interface,
EX - Extranet, A2 - Secondary Accept
Forwarding/Replication Counts: Packets in/Packets out/Bytes out
Failure Counts: RPF / TTL / Empty Olist / Encap RL / Other

(20.20.20.1,225.0.0.1), Flags: MoFE MoFS
Up: 03:25:31
Last Used: never
SW Forwarding Counts: 0/0/0
SW Replication Counts: 0/0/0
SW Failure Counts: 0/0/0/0/0
Route ver: 0x4a13
MVPN Info :

<table>
<thead>
<tr>
<th>MDT Handle</th>
<th>MDT Probe: N</th>
<th>Rate: N</th>
<th>Acc: N</th>
</tr>
</thead>
</table>

MOPRR State: Inactive Sequence No 1
GigabitEthernet0/0/0/8 Flags: A, Up:03:25:31
GigabitEthernet0/0/0/18 Flags: A2, Up:03:25:31
GigabitEthernet0/0/0/28 Flags: NS, Up:03:25:31

(20.20.20.1,225.0.0.2), Flags: MoFE MoFS
Up: 03:25:31
Last Used: never
SW Forwarding Counts: 0/0/0
SW Replication Counts: 0/0/0
SW Failure Counts: 0/0/0/0/0
Route ver: 0x443e
MVPN Info :-
The detail option illustrates the MoFRR state of each MoFRR route. At any moment, only one RPF forwards the traffic to the egress. The inactive state means the primary RPF forwards the traffic to the egress. The active state means that the backup RPF forwards the traffic to the egress. The sequence number reflects the number of switchovers of the MoFRR route.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mfib counter, on page 151</td>
<td>Displays Multicast Forwarding Information Base (MFIB) counter statistics for packets that have dropped.</td>
</tr>
<tr>
<td>show mfib hardware route accept-bitmap, on page 167</td>
<td>Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the interface list that accepts bidirectional routes.</td>
</tr>
<tr>
<td>show mfib hardware route olist, on page 180</td>
<td>Displays platform-specific Multicast Forwarding Information Base (MFIB) information in the output interface list (olist) stored in the hardware.</td>
</tr>
<tr>
<td>show mfib hardware route statistics, on page 191</td>
<td>Displays platform-specific Multicast Forwarding Information Base (MFIB) information for the packet and byte counters for each route.</td>
</tr>
<tr>
<td>show mfib interface, on page 200</td>
<td>Displays interface-related information used during software multicast switching in the Multicast Forwarding Information Base (MFIB) process.</td>
</tr>
<tr>
<td>show mrrib route, on page 222</td>
<td>Displays all entries in the Multicast Routing Information Base (MRIB).</td>
</tr>
</tbody>
</table>
show mfib table-info

To display Multicast Forwarding Information Base (MFIB) table information, use the `show mfib table-info` command in EXEC mode.

```
show mfib [{ipv4|ipv6}] table-info {table-id|vrf-name} [local|remote] [location node-id]
```

**Syntax Description**
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `ipv6` (Optional) Specifies IPv6 address prefixes.
- `table-id` Specifies the table identifier. Range is 0 to 4294967295.
- `vrf-name` Specifies the VRF name.
- `local` Specifies local tables only.
- `remote` Specifies remote tables only.
- `location node-id` (Optional) Specifies MFIB connections associated with an interface of the designated node.

**Command Default**
IPv4 addressing is the default.

**Command Modes**
EXEC

**Command History**
Release 3.7.2  This command was introduced.

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**
- `multicast read`

**Examples**
The following is sample output from the `show mfib table-info` command:

```
RP/0/RSP0/CPU0:router# show mfib table-info table-id 0/0/CPU0 location

Table Name : default
VRid/TID/VID : 0x0 / 0xe0000000 / 0x60000000
Table type : TBL_TYPE_TID
Active/Linked : Y / Y
Prev Table ID : 0x0
Location : Local
Local ifcount : 16
Default MDT Encap : (*. *,/32)
```
MDT Master LC : N
Loopback (Encap Src) : 0x0 (Ha0x0)
Local EG intf cnt : 6
Data MDT : Acl - (-), All vrf routes N, 0 Kbps

RP/0/RSP0/CPU0:router# show mfib table-info vrf 101

Table Name : vrf15
VRid/TID/VID : 0x0 / 0xe000000f / 0x6000000f
Table type : TBL_TYPE_NAME_VID
Active/Linked : Y / Y
Prev Table ID : 0x0
Location : Local
Local ifcount : 2
Child routes : (5.5.5.5, 225.101.1.15/32)
Default MDT Handle : 0x0 (Ha0x0)

MDT Master LC : Y
Loopback (Encap Src) : 0x9000180 (Loopback0)
Local EG intf cnt : 508
Data MDT : Acl - (-), All vrf routes N, 0 Kbps

This table describes the significant fields shown in the display.

Table 24: show mfib table-info Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table Name</td>
<td>Name of the MFIB table.</td>
</tr>
<tr>
<td>VRid/TID/VID</td>
<td>Table identifiers.</td>
</tr>
<tr>
<td>Table type</td>
<td>Type of MFIB table.</td>
</tr>
<tr>
<td>Active/Linked</td>
<td>Table is active and linked.</td>
</tr>
<tr>
<td>Location</td>
<td>Location of the MFIB table.</td>
</tr>
<tr>
<td>Local ifcount</td>
<td>Local interface count.</td>
</tr>
<tr>
<td>Child routes</td>
<td>Child routes shows the number of extranet routes in receiver VRFs that reference this source VRF.</td>
</tr>
<tr>
<td>Default MDT Encap</td>
<td>Default MDT encapsulation.</td>
</tr>
<tr>
<td>Default MDT Handle</td>
<td>Default MDT interface handle for this VRF.</td>
</tr>
<tr>
<td>MDT Master LC</td>
<td>Field contains &quot;Y&quot; if this line card is a master line card for this VRF.</td>
</tr>
<tr>
<td>Loopback (Encap Src)</td>
<td>Loopback (encapsulation source).</td>
</tr>
<tr>
<td>Local EG intf cnt</td>
<td>Shows the number of local egress interfaces for this VRF and location.</td>
</tr>
<tr>
<td>Data MDT</td>
<td>Routes for which multicast data for a multicast distribution tree (MDT) was triggered.</td>
</tr>
</tbody>
</table>
**show mrib client**

To display the state of the Multicast Routing Information Base (MRIB) client connections, use the `show mrib client` command in the appropriate mode.

```
show mrib [vrf vrf-name] ipv4 client [filter] [client-name]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a VPN routing and forwarding (VRF) instance.</td>
</tr>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IPv4 address prefixes.</td>
</tr>
<tr>
<td>ipv6</td>
<td>(Optional) Specifies IPv6 address prefixes.</td>
</tr>
<tr>
<td>filter</td>
<td>(Optional) Displays route and interface level flag changes that various MRIB clients have registered and shows what flags are owned by the MRIB clients.</td>
</tr>
<tr>
<td>client-name</td>
<td>(Optional) Name of a multicast routing protocol that acts as a client of MRIB, such as Protocol Independent Multicast (PIM) or Internet Group Management Protocol (IGMP).</td>
</tr>
</tbody>
</table>

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show mrib client` command using the `filter` option:

```
RP/0/RSP0/CPU0:router# show mrib client filter
IP MRIB client-connections
igmp:417957 (connection id 0)
  ownership filter:
  interface attributes: II ID LI LD
  groups:
    include 0.0.0.0/0
  interfaces:
    include All
pim:417959 (connection id 1)
  interest filter:
    entry attributes: E
```
interface attributes: SP II ID LI LD
  groups:
    include 0.0.0.0/0
  interfaces:
    include All
ownership filter:
  entry attributes: L S C IA IF D
  interface attributes: F A IC NS DP DI EI
  groups:
    include 0.0.0.0/0
  interfaces:
    include All
bcdl_agent:1 (connection id 2)
interest filter:
  entry attributes: S C IA IF D
  interface attributes: F A IC NS DP EI
  groups:
    include 0.0.0.0/0
  interfaces:
    include All
ownership filter:
  groups:
    include 0.0.0.0/0
  interfaces:
    include All

This table describes the significant fields shown in the display.

Table 25: show mrib client Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp</td>
<td>Name of the client.</td>
</tr>
<tr>
<td>417957</td>
<td>Personal identifier (PID) or a unique ID assigned by MRIB.</td>
</tr>
<tr>
<td>(connection id 0)</td>
<td>Unique client connection identifier.</td>
</tr>
<tr>
<td>ownership filter:</td>
<td>Specifies all the route entry and interface-level flags that are owned by the client. As the owner of the flag, only the client can add or remove the flag. For example, only the Internet Group Management Protocol (IGMP) client can add the II flag on an interface. MRIB does not allow a non-owner to register or modify the same flag.</td>
</tr>
<tr>
<td>groups: include 0.0.0.0/0/interfaces: include All</td>
<td>Groups and interfaces registered by the clients consisting of two lists. One is an include list (items for which the client requests to be notified.) The use of “All” implies all interfaces and 0.0.0.0/0 to indicate all groups. Not shown in this example is the exclude list. This list contains items for which the client requests not to be notified when modifications occur.</td>
</tr>
<tr>
<td>interface attributes: II ID LI LD</td>
<td>Interface-level flags set on the interface belong to a route.</td>
</tr>
<tr>
<td>interest filter:</td>
<td>Specifies all the flags, groups, and interfaces from which the client requests information. When a flag of interest for a client is modified, the client is notified.</td>
</tr>
</tbody>
</table>
show mrib client

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>entry attributes:</td>
<td>Entry-level flags that are set on the route.</td>
</tr>
<tr>
<td>S C I A I F D</td>
<td></td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mfib nsf, on page 202</td>
<td>Displays the state of a nonstop forwarding (NSF) operation for the Multicast Forwarding Information Base (MFIB) line cards.</td>
</tr>
<tr>
<td>show mfib route, on page 204</td>
<td>Displays route entries in the Multicast Forwarding Information Base (MFIB).</td>
</tr>
<tr>
<td>show mrib nsf, on page 216</td>
<td>Displays the state of nonstop forwarding (NSF) operation in the Multicast Routing Information Base (MRIB).</td>
</tr>
</tbody>
</table>
**show mrib bvi**

To display the Bridge Virtual Interface (BVI) details in the Multicast Routing Information Base (MRIB), use the `show mrib bvi` command EXEC mode.

```
show mrib bvi [interface | route] bvi/bvi_number
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>interface</code></td>
<td>MRIB BVI interface.</td>
</tr>
<tr>
<td><code>route</code></td>
<td>BVI route entry.</td>
</tr>
<tr>
<td><code>bvi_number</code></td>
<td>BVI interface number. Range is from 1 to 65535.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

```
Task ID  Operation
multicast  read
```

**Example**

This example shows how to run the `show mrib bvi` command:

```
RP/0/RSP0/CPU0:router # show mrib bvi route bvi 200
```
show mrib nsf

To display the state of nonstop forwarding (NSF) operation in the Multicast Routing Information Base (MRIB), use the `show mrib nsf` command in the appropriate mode.

```
show mrib ipv4 nsf
```

**Syntax Description**

```
ipv4  (Optional) Specifies IPv4 address prefixes.
```

**Command Default**

IPV4 addressing is the default.

**Command Modes**

EXEC

**Command History**

```
Release Modification
3.7.2  This command was introduced.
```

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `show mrib nsf` command displays the current multicast NSF state for the MRIB. The state may be normal or activated for NSF. The activated state indicates that recovery is in progress due to a failure in MRIB or Protocol Independent Multicast (PIM). The total NSF timeout and time remaining are displayed until NSF expiration.

**Examples**

The following is sample output from the `show mrib nsf` command:

```
RP/0/RSP0/CPU0:router# show mrib nsf

IP MRIB Non-Stop Forwarding Status:
Multicast routing state: Non-Stop Forwarding Activated
NSF Lifetime: 00:03:00
NSF Time Remaining: 00:01:40
```

This table describes the significant fields shown in the display.

**Table 26: show mrib nsf Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast routing state</td>
<td>Multicast NSF status of the MRIB (Normal or NSF Activated).</td>
</tr>
<tr>
<td>NSF Lifetime</td>
<td>Timeout for MRIB NSF, computed as the maximum of the PIM and Internet Group Management Protocol (IGMP) NSF lifetimes, plus 60 seconds.</td>
</tr>
</tbody>
</table>
If MRIB NSF state is activated, the time remaining until MRIB reverts to Normal mode displays. Before this timeout, MRIB receives notifications from IGMP and PIM, triggering a successful end of NSF and causing the transition to normal state. If notifications are not received, the timer triggers a transition back to normal mode, causing new routes to download to MFIB and old routes to be deleted.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSF Time Remaining</td>
<td>If MRIB NSF state is activated, the time remaining until MRIB reverts to Normal mode displays. Before this timeout, MRIB receives notifications from IGMP and PIM, triggering a successful end of NSF and cause the transition to normal state. If notifications are not received, the timer triggers a transition back to normal mode, causing new routes to download to MFIB and old routes to be deleted.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>nsf (multicast)</code></td>
<td>Configures the NSF capability for the multicast routing system.</td>
</tr>
<tr>
<td><code>nsf lifetime (IGMP)</code></td>
<td>Configures the maximum time for the NSF timeout value under IGMP.</td>
</tr>
<tr>
<td><code>nsf lifetime (PIM)</code></td>
<td>Configures the NSF timeout value for the PIM process.</td>
</tr>
<tr>
<td><code>show igmp nsf</code></td>
<td>Displays the state of NSF operation in IGMP.</td>
</tr>
<tr>
<td><code>show mfib nsf</code></td>
<td>Displays the state of NSF operation in the MFIB line cards.</td>
</tr>
<tr>
<td><code>show pim nsf</code></td>
<td>Displays the state of NSF operation for PIM.</td>
</tr>
</tbody>
</table>
**show mrib nsr end**

To display nonstop routing (NSR) operation in the Multicast Routing Information Base (MRIB), use the `show mrib nsr end` command in the appropriate mode.

```
show mrib ipv4|ipv6 nsr end
```

**Syntax Description**
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `ipv6` (Optional) Specifies IPv6 address prefixes.

**Command Default**
IPv4 addressing is the default.

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 5.2.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command after an NSR event (for example, RPFO or a process restart) to determine when each of the MRIB or MRIB6's NSR clients finished re-downloading the information to the MRIB and if any previously downloaded information was purged in the process.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show mrib nsr end` command:

```
RP/0/RSP0/CPU0:router# show mrib nsr end
Time                              Client  Idx  Change
Oct 17 18:43:36  Membership       1     N
Oct 17 18:43:40  Routing           2     Y
```

This table describes the significant fields shown in the display.

**Table 27: show mrib nsr end Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time</td>
<td>The time at which the client finished downloading information back to MRIB or MRIB6 after the NSR event.</td>
</tr>
<tr>
<td>Client</td>
<td>Client type (Membership - IGMP/MLD, Routing - PIM/PIM6)</td>
</tr>
</tbody>
</table>
### Field Description

| Change | Was there an route or interface attribute purge Y - yes, N - no |

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show msdp nsr</td>
<td>Displays the state of NSR operation for MSDP.</td>
</tr>
<tr>
<td>show igmp nsr</td>
<td>Displays the state of NSR operation for IGMP.</td>
</tr>
<tr>
<td>show pim nsr</td>
<td>Displays the state of NSR operation for PIM.</td>
</tr>
</tbody>
</table>
show mrib platform trace location standby

To display platform-specific data for the Multicast Routing Information Base (MRIB) on a standby RP, use the `show mrib platform trace location standby` command in EXEC mode.

```
show mrib [vrf vrf-name] ipv4 platform trace
[\{file\hexdump\last\reverse\stats\tailf\unique\verbose\wrapping\}] location standby[\{allnode-id\}]
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `file` (Optional) Specifies the filename.
- `hexdump` (Optional) Displays the traces in hexadecimal form.
- `last` (Optional) Displays the last `n` entries.
- `reverse` (Optional) Displays the traces in reverse order.
- `stats` (Optional) Displays statistics.
- `tailf` (Optional) Displays new traces as they are added.
- `unique` (Optional) Displays unique entries with counts.
- `verbose` (Optional) Displays internal debugging information.
- `wrapping` (Optional) Displays wrapping entries.
- `location standby node-id` (Optional) Specifies the location of the trace.
- `location standby all` (Optional) Specifies that the trace be performed for all locations.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

Examples

The following example shows a sample output of `show mrib platform trace location standby` command:

RP/0/RSP0/CPU0:router#show mrib platform trace location standby

2 wrapping entries (512 possible, 0 filtered, 2 total)
show mrib route

To display all entries in the Multicast Routing Information Base (MRIB), use the `show mrib route` command in the appropriate mode.

```
show mrib [vrf vrf-name] [ipv4|ipv6] [old-output] route
  [summary|outgoing-interface[{*source-address}] [group-address [/prefix-length]]]
  [detail]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>vrf vrf-name</strong></td>
</tr>
<tr>
<td><strong>ipv4</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>source-address</strong></td>
</tr>
<tr>
<td><strong>group-address</strong></td>
</tr>
<tr>
<td><strong>/prefix-length</strong></td>
</tr>
<tr>
<td><strong>outgoing-interface</strong></td>
</tr>
<tr>
<td><strong>summary</strong></td>
</tr>
<tr>
<td><strong>detail</strong></td>
</tr>
</tbody>
</table>

**Command Default**
IPv4 addressing is the default.

**Command Modes**
EXEC

**Command History**
Release 3.7.2 This command was introduced.

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Each line card has an individual Multicast Forwarding Information Base (MFIB) table. The MFIB table maintains a subset of entries and flags updated from MRIB. The flags determine the forwarding and signaling behavior according to a set of forwarding rules for multicast packets. In addition to the list of interfaces and flags, each route entry shows various counters. Byte count is the number of total bytes forwarded. Packet count is the number of packets received for this entry.

The `show mfib counter, on page 151` command displays global counters independent of the routes.
## Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>multicast  read</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show mfib counter, on page 151</code></td>
<td>Displays MFIB counter statistics for packets that have dropped.</td>
</tr>
<tr>
<td><code>show mrib route-collapse, on page 224</code></td>
<td>Displays the contents of the MRIB route collapse database.</td>
</tr>
<tr>
<td><code>show mfib route, on page 204</code></td>
<td>Displays all entries in the MFIB table.</td>
</tr>
</tbody>
</table>
show mrib route-collapse

To display the contents of the Multicast Routing Information Base (MRIB) route-collapse database, use the `show mrib route-collapse` command in the appropriate mode.

```
show mrib [vrf vrf-name] ipv4 route-collapse [core-tree]
```

### Syntax Description

- **vrf vrf-name** (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- **ipv4** (Optional) Specifies IPv4 address prefixes.
- **core-tree** (Optional) IPv4 Multicast Distribution Tree (MDT) group address.

### Command Default

IPv4 addressing is the default.

### Command Modes

EXEC

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

#### Task ID

**Task ID**

- multicast
- read

#### Examples

The following is sample output from the `show mrib route-collapse` command:

```
RP/0/RSP0/CPU0:router# show mrib route-collapse

226.1.1.1  TID: 0xe0000038  TLC TID: 0xe0000038
  Customer route database count: 5
    (192.168.5.204,224.0.1.40/32)
    (*,226.226.226.226/32)
    (*,228.228.228.228/32)
    (192.168.113.17,228.228.228.228/32)
    (*,229.229.229.229/32)
  Core route database count: 4
    (*,226.1.1.1/32)
    (192.168.5.201,226.1.1.1/32)
    (192.168.5.202,226.1.1.1/32)
    (192.168.5.204,226.1.1.1/32)
  Core egress node database count: 1
    nodeid  slot  refcount
    0x20 0/2/CPU0 1

192.168.27.1  TID: 0xe0000039  TLC TID: 0xe0000039
  Customer route database count: 1
```
(192.168.113.33, 227.227.227.227/32)
Core route database count: 3
(*, 227.27.27.1/32)
(192.168.5.201, 227.27.27.1/32)
(192.168.5.202, 227.27.27.1/32)
Core egress node database count: 1
<table>
<thead>
<tr>
<th>nodeid</th>
<th>slot</th>
<th>refcount</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x20</td>
<td>0/2/CPU0</td>
<td>1</td>
</tr>
</tbody>
</table>

192.168.28.1  TID: 0xe000003a  TLC TID: 0xe000003a
Customer route database count: 2
(192.168.5.204, 224.0.1.40/32)
(192.168.113.49, 229.229.229.229/32)
Core route database count: 3
(192.168.5.201, 228.28.28.1/32)
(192.168.5.202, 228.28.28.1/32)
(192.168.5.204, 228.28.28.1/32)
Core egress node database count: 1
<table>
<thead>
<tr>
<th>nodeid</th>
<th>slot</th>
<th>refcount</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x20</td>
<td>0/2/CPU0</td>
<td>1</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mrib route, on page 222</td>
<td>Displays all entries in the Multicast Routing Information Base (MRIB).</td>
</tr>
</tbody>
</table>
show mrib route outgoing-interface

To display the outgoing-interface information on the Multicast Routing Information Base (MRIB), use the **show mrib route outgoing-interface** command in the appropriate mode.

**show mrib route outgoing-interface** [\{\*source-address]\} [group-address \[/prefix-length\]]

**Syntax Description**

<table>
<thead>
<tr>
<th><strong>Syntax</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>(Optional) Displays shared tree entries.</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>(Optional) Source IP address or hostname of the MRIB route. Format is: A.B.C.D</td>
</tr>
<tr>
<td>A.B.C.D</td>
<td>(Optional) Group IP address or hostname of the MRIB route and the prefix length.</td>
</tr>
<tr>
<td>/prefix-length</td>
<td>(Optional) Prefix length of the MRIB group address. A decimal value that indicates how many of the high-order contiguous bits of the address compose the prefix (the network portion of the address). A slash must precede the decimal value. Format is: A.B.C.D</td>
</tr>
</tbody>
</table>

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th><strong>Release</strong></th>
<th><strong>Modification</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th><strong>Task ID</strong></th>
<th><strong>Operations</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the **show mrib route outgoing-interface** command:

```
RP/0/RSP0/CPU0:router# show mrib route outgoing-interface

IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
C - Directly-Connected Check, S - Signal, IA - Inherit Accept,
IF - Inherit From, D - Drop, MA - MDT Address, ME - MDT Encap,
MD - MDT Decap, MT - MDT Threshold Crossed, MH - MDT interface handle
CD - Conditional Decap, MPLS - MPLS Decap, MF - MPLS Encap, EX - Extranet
MoFE - MoFRR Enabled, MoFS - MoFRR State

(*,224.0.0.0/4), Up:6d10h, OIF count:0, flags: C
(*,224.0.0.0/24), Up:6d10h, OIF count:0, flags: D
```
Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mrib route, on page 222</td>
<td>Displays all entries in the Multicast Routing Information Base (MRIB).</td>
</tr>
</tbody>
</table>
show mrib table-info

To display Multicast Routing Information Base (MRIB) table information, use the `show mrib table-info` command in the appropriate mode.

```plaintext
show mrib [vrf vrf-name] ipv4 table-info
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show mrib table-info` command:

```
RP/0/RSP0/CPU0:router# show mrib vrf vrf101 table-info

VRF: default [tid 0xe0000000]
Registered Client:
  igmp [ccbid: 0 cltid: 4485366]
  pim [ccbid: 1 cltid: 4485368]
  bcdl_agent [ccbid: 2 cltid: 1]
  m NDP [ccbid: 3 cltid: 8827135]
```

**Table 28: show mrib table-info Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF</td>
<td>Default VRF or a VRF configured for the purpose of an override in MVPN.</td>
</tr>
<tr>
<td>cltid</td>
<td>Client ID.</td>
</tr>
<tr>
<td>bcdl_agent</td>
<td>A process like igmp and pim, which is used to download routes to line card.</td>
</tr>
<tr>
<td>MDT handle</td>
<td>MDT interface handle for this VRF.</td>
</tr>
</tbody>
</table>
### Field | Description
--- | ---
MDT group | Default MDT group associated with this VRF.
MDT source | Per-VRF MDT source information.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mrib tlc, on page 230</td>
<td>Displays the contents of the Multicast Routing Information Base (MRIB) table-line card (TLC) database.</td>
</tr>
</tbody>
</table>
show mrib tlc

To display the contents of the Multicast Routing Information Base (MRIB) table-line card (TLC) database, use the `show mrib tlc` command in the appropriate mode.

```
show mrib [vrf vrf-name] ipv4 tlc
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show mrib tlc` command:

```
RP/0/RSP0/CPU0:router# show mrib tlc
VRF: default [tid 0xe0000000]
Master LC slot: Not selected
Associated MDT group: 0
Forwarding LC node: 0
```

This table describes the significant fields shown in the display.

**Table 29: show msdp peer Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Associated MDT group</td>
<td>IP address of the MSDP peer.</td>
</tr>
<tr>
<td>Master LC slot</td>
<td>Indicates whether the master LC slot has been selected.</td>
</tr>
<tr>
<td>Forwarding LC node</td>
<td>Autonomous system to which the peer belongs.</td>
</tr>
<tr>
<td>Associated MDT group</td>
<td>Indicates the number of associated MDT groups.</td>
</tr>
</tbody>
</table>
static-rpf

To configure a static Reverse Path Forwarding (RPF) rule for a specified prefix mask, use the `static-rpf` command in an appropriate configuration mode. To return to the default behavior, use the `no` form of this command.

```
static-rpf prefix-address prefix-mask type path-id next-hop-address
no static-rpf
```

**Syntax Description**

- `prefix-address` IP address of a prefix for an address range.
- `prefix-mask` Prefix mask for an address range. Range is 0 to 32 for IPv4.
- `type` Interface type. For more information, use the question mark (?) online help function.
- `interface-path-id` Physical interface or virtual interface.

**Note** Use the `show interfaces` command in EXEC mode to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark ( ? ) online help function.

- `next-hop-address` IP address for an RPF neighbor.

**Command Default**

A static RPF rule for a specified prefix mask is not configured.

**Command Modes**

- Multicast routing address family ipv4 and ipv6 configuration
- Multicast VRF configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `static-rpf` command is used to configure incompatible topologies for unicast and multicast traffic.

Use the `static-rpf` command to configure a static route to be used for RPF checking in Protocol Independent Multicast (PIM) instead of using the unicast routing table.

**Task ID**

- `multicast` read, write

**Examples**

The following example configures the static RPF rule for IP address 10.0.0.1:
RP/0/RSP0/CPU0:router(config)# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# vrf green
RP/0/RSP0/CPU0:router(config-mcast)# static-rpf 10.0.0.1 32 GigE 0/0/5/0 10.1.1.1

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show pim context</td>
<td>Displays reverse path forwarding (RPF) table information configured for a VRF context.</td>
</tr>
</tbody>
</table>
source-tree-prune-delay

To set the delay-time for the (S,G) prune of the ingress-PE (provider edge), use the `source-tree-prune-delay` command in the appropriate mode. To remove the set delay, use the `no` form of the command.

```
source-tree-prune-delay  time
nosource-tree-prune-delay  time
```

**Syntax Description**

| time | Delay in seconds. Range is 0 to 300. |

**Command Default**

60 seconds

**Command Modes**

C-multicast-routing configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command is used to delay (S,G) Prune on the Ingress-PE, when the last Type-7 route is withdrawn.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to use the `source-tree-prune-delay` command:

```
RP/0/RSP0/CPU0:router (config-pim-vl-ipv4-mdt-cmcast) # source-tree-prune-delay 100
```
**suppress-pim-data-signaling**

To suppress PIM data signaling, use the `suppress-pim-data-signaling` command in the appropriate mode. To remove the suppressed condition, use the `no` form of the command.

`suppress-pim-data-signaling`  
`nosuppress-pim-data-signaling`

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

None

**Command Modes**

PIM C-multicast routing configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command supports c-anycast RP and can be used only under the PIM c-multicast routing mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to use the `suppress-pim-data-signaling` command:

```
RP/0/RSP0/CPU0:router (config-pim-v1-ipv4-mdt-cmcast) # suppress-pim-data-signaling
```
suppress-shared-tree-join

To suppress shared tree joins and support the SPT-only mode, use the `suppress-shared-tree-join` command in the appropriate mode.

To remove the suppress condition, use the `no` form of the command.

```
suppress-shared-tree-join
no suppress-shared-tree-join
```

### Syntax Description

This command has no keywords or arguments.

### Command Default

None

### Command Modes

C-multicast-routing configuration mode

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command enables the SPT-only (Shortest Path Tree) mode.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Example

This command shows how to use the `suppress-shared-tree-join` command:

```
RP/0/RSP0/CPU0:router(config-pim-v1-ipv4-mdt-cmcast) # suppress-shared-tree-join
```
To configure the time-to-live (TTL) threshold for packets being forwarded out an interface, use the `ttl-threshold` command in the appropriate configuration mode. To return to the default behavior, use the `no` form of this command.

```
ttl-threshold ttl
no ttl-threshold ttl
```

### Syntax Description
- `ttl`: Time to live value. Range is 1 to 255.

### Command Default
- `ttl`: 0

### Command Modes
- Multicast routing interface configuration
- Multicast routing VRF interface configuration

### Command History
- **Release** 3.7.2 This command was introduced.

### Usage Guidelines
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Only multicast packets with a TTL value greater than the threshold are forwarded out of the interface. The TTL threshold is compared to the TTL of the packet after it has been decremented by one and before being forwarded.

Configure the TTL threshold only on border routers.

### Note
Do not confuse this command with the `ttl-threshold (MSDP)` command in router MSDP configuration mode that is used to confine the multicast data packet TTL to be sent by an Multicast Source Discovery Protocol (MSDP) Source-Active (SA) message.

### Task ID
- **Task ID** Operations
  - `multicast`: read, write

### Examples
The following example shows how to configure the TTL threshold to 23, which means that a multicast packet is dropped and not forwarded out of the GigE 0/1/0/0 interface:

```
RP/0/RSP0/CPU0:router(config)# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# interface GigE 0/1/0/CPU0
RP/0/RSP0/CPU0:router(config-mcast-default-ipv4-if)# ttl-threshold 23
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ttl-threshold (MSDP)</td>
<td>Limits which multicast data packets are sent in SA messages to an MSDP peer.</td>
</tr>
</tbody>
</table>
**unicast-reachability**

To disable VPN-IP attributes, use the `unicast-reachability` command in the appropriate mode. To restore the attributes, use the `no` form of the command.

```
unicast-reachability [ connector-disable | source-as-disable | vrf-route-import-disable ]
```

**nounicast-reachability [ connector-disable | source-as-disable | vrf-route-import-disable ]**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>connector-disable</th>
<th>source-as-disable</th>
<th>vrf-route-import-disable</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Disables connector addition.</td>
<td>Disables source AS extended community addition.</td>
<td>Disables VRF route import extended community addition.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

C-multicast routing configuration mode

**Command History**

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command controls addition of extended communities to unicast VPN-IP routes. These attributes have specific purposes in PIM and BGP C-multicast Routing.

**Task ID**

```
Task ID | Operation
-------|-----------
multicast | read, write
```

**Example**

This example shows how to use the `unicast-reachability` command:

```
RP/0/RSP0/CPU0:router (config-pim-v1-ipv4-mdt-cmsgcast) # unicast-reachability connector-disable
```
vrf (multicast)

To configure a virtual routing and forwarding (VRF) instance for a VPN table, use the `vrf` command in multicast routing configuration mode. To remove the VRF instance from the configuration file and restore the system to its default condition, use the `no` form of this command.

```
vrf vrf-name ipv4
no vrf vrf-name ipv4
```

**Syntax Description**
- **vrf-name**: Name of the VRF instance. The following names cannot be used: all, default, and global.
- **ipv4**: (Optional) Configures IPv4 address prefixes.

**Command Default**
No default behavior or values.

**Command Modes**
Multicast routing configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

A VRF instance is a collection of VPN routing and forwarding tables maintained at the provider edge (PE) router.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to configure a VRF instance and enter VRF configuration mode:

```
RP/0/RSP0/CPU0:router(config)# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# vrf vrf_1
RP/0/RSP0/CPU0:router(config-mcast-vrf_1-ipv4)# mdt ?
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>boundary, on page 112</td>
<td>Configures a boundary to keep multicast packets from being forwarded.</td>
</tr>
<tr>
<td>accounting per-prefix, on page 105</td>
<td>Enables per-prefix counters only in hardware.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>interface (multicast), on page 123</td>
<td>Configures multicast interface properties.</td>
</tr>
<tr>
<td>log-traps, on page 129</td>
<td>Enables logging of trap events.</td>
</tr>
<tr>
<td>multipath, on page 142</td>
<td>Enables Protocol Independent Multicast (PIM) to divide the multicast load among several equal-cost paths.</td>
</tr>
<tr>
<td>rate-per-route, on page 146</td>
<td>Enables individual (source, group [S, G]) rate calculations.</td>
</tr>
<tr>
<td>ssm</td>
<td>Defines the Protocol Independent Multicast (PIM)-Source Specific Multicast (SSM) range of IP multicast addresses.</td>
</tr>
<tr>
<td>static-rpf, on page 231</td>
<td>Configures a static Reverse Path Forwarding (RPF) rule for a specified prefix mask.</td>
</tr>
</tbody>
</table>
To configure the frr-holdtime of MLDP LSPs in a scale setup (with more than 500 LSPs configured), use the cef platform lsm frr-holdtime command in global configuration mode.

**cef platform lsm frr-holdtime**

**Syntax Description**

```
cef platform lsm frr-holdtime seconds
```

- **seconds**  The number of seconds to set the frr-holdtime. Default value is 2 seconds.
- **Note**  The range of the frr-holdtime (in seconds) is 3 to 180 seconds.

**Command Default**  None

**Command Modes**

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.2</td>
<td>This command is introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**  No specific guidelines impact the use of this command.

**Example**

The following example shows how to set the frr-holdtime value to 45 seconds.

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# cef platform lsm frr-holdtime 45
```
cef platform ism frr-holdtime
IGMP and MLD Snooping Commands on Cisco ASR 9000 Series Routers

This chapter describes the commands used to configure and monitor IGMP and MLD snooping on Cisco ASR 9000 Series Router.

For detailed information about IGMP snooping concepts, configuration tasks, and examples, refer to the Implementing Layer 2 Multicast Using IGMP / MLD Snooping on Cisco ASR 9000 Series Routers module in the Multicast Configuration Guide for Cisco ASR 9000 Series Routers.

- access-group (snooping profile), on page 245
- clear igmp snooping bridge-domain, on page 246
- clear igmp snooping group, on page 248
- clear igmp snooping port, on page 250
- clear igmp snooping summary, on page 252
- clear l2vpn forwarding bridge-domain mroute, on page 253
- group limit, on page 254
- group policy, on page 256
- igmp snooping profile, on page 258
- immediate-leave, on page 261
- internal-querier, on page 263
- internal-querier (MLD), on page 265
- internal-querier max-response-time, on page 266
- internal-querier query-interval, on page 268
- internal-querier robustness-variable, on page 270
- internal-querier tcn query count, on page 272
- internal-querier tcn query interval, on page 274
- internal-querier timer expiry, on page 276
- internal-querier version, on page 278
- last-member-query count, on page 280
- last-member-query count (MLD), on page 282
- last-member-query interval, on page 283
- last-member-query interval (MLD), on page 285
- minimum-version, on page 286
- minimum version (MLD), on page 288
- mld snooping profile, on page 289
• mrouter, on page 290
• nv satellite offload ipv4 multicast enable, on page 292
• querier query-interval, on page 293
• querier robustness-variable, on page 295
• redundancy iccp-group report-standby-state disable, on page 297
• report-suppression disable, on page 299
• report-suppression disable(MLD), on page 301
• router-alert-check disable, on page 302
• router-guard, on page 304
• show igmp snooping bridge-domain, on page 306
• show igmp snooping group, on page 313
• show igmp snooping port, on page 321
• show igmp snooping profile, on page 327
• show igmp snooping redundancy, on page 332
• show igmp snooping summary, on page 335
• show igmp snooping trace, on page 340
• show 12vpn forwarding bridge-domain mroute, on page 342
• show 12vpn forwarding bridge-domain mroute detail, on page 344
• show 12vpn forwarding bridge-domain mroute hardware ingress detail, on page 346
• show mld snooping bridge-domain, on page 353
• show mld snooping group, on page 359
• show mld snooping port, on page 363
• show mld snooping profile, on page 367
• show mld snooping summary, on page 372
• show mld snooping trace, on page 376
• startup query count, on page 378
• startup query iccp-group, on page 379
• startup query interval, on page 381
• startup query max-response-time, on page 382
• startup query port-up disable, on page 383
• startup query process start, on page 384
• startup query topology-change, on page 385
• static group, on page 386
• system-ip-address, on page 388
• tcn flood disable, on page 390
• tcn flood query count, on page 392
• tcn flood query count (MLD), on page 394
• tcn query solicit, on page 396
• tcn query solicit (MLD), on page 398
• ttl-check disable, on page 399
• unsolicited-report-interval, on page 401
access-group (snooping profile)

To instruct IGMP/MLD snooping to apply the specified access list filter to received membership reports, use the `access-group` command in the appropriate snooping profile configuration mode. To discontinue membership report filtering, use the `no` form of this command.

```
access-group acl-name
no access-group
```

**Syntax Description**

- `acl-name` Name of the ACL filter.

**Command Default**

Membership reports are not filtered by default.

**Command Modes**

- IGMP snooping profile configuration
- MLD snooping profile configuration

**Command History**

- **Release** Modification
- Release 3.9.0 This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following examples show how to configure an ACL to filter membership reports:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# access-group acl-name

RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# access-group acl-name
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group limit, on page 254</td>
<td>Specifies the group limit of the port.</td>
</tr>
<tr>
<td>group policy, on page 256</td>
<td>Instructs IGMP snooping to use the specified route policy to determine the weight contributed by a new <code>&lt;*,G&gt;</code> or <code>&lt;S,G&gt;</code> membership request.</td>
</tr>
<tr>
<td>show igmp snooping profile, on page 327</td>
<td>Displays the contents of profiles and to see associations of profiles with bridge-domains and ports, including access group, group limit, and TCN flood parameters.</td>
</tr>
</tbody>
</table>
clear igmp snooping bridge-domain

To clear IGMP snooping information at the bridge domain level, use the clear igmp snooping bridge-domain command in EXEC mode.

clear igmp snooping bridge-domain [bridge-domain-name] statistics [include-ports]

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bridge-domain-name</td>
<td>(Optional) Clears information for the named bridge domain.</td>
</tr>
<tr>
<td>statistics</td>
<td>Clears counters and other statistics. In Release 3.7.2, this is the only keyword available and it is required.</td>
</tr>
<tr>
<td>include-ports</td>
<td>(Optional) Clears port-level counters and statistics in addition to the bridge domain level.</td>
</tr>
</tbody>
</table>

Command Default

None

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 3.9.0</td>
<td>This command was modified to clear new statistical information added in the current release to support multicast admission control.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

In Release 3.7.2, the only items available for clearing are counters and statistics. You have the option to clear statistics for one or all bridge domains. You also have the option to clear only bridge domain statistics, or bridge domain statistics plus all statistics for all ports under the cleared bridge domains.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>12vpn</td>
<td>execute</td>
</tr>
</tbody>
</table>

Examples

The following example clears IGMP snooping statistics for all bridge domains on the router:

```
RP/0/RSP0/CPU0:router# clear igmp snooping bridge-domain statistics
```

The following example clears IGMP snooping statistics for one bridge domain and all ports under it:

```
RP/0/RSP0/CPU0:router# clear igmp snooping bridge-domain bd-1 statistics include-ports
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show igmp snooping bridge-domain</code>, on page 306</td>
<td>Displays IGMP snooping configuration information and statistics for bridge domains.</td>
</tr>
</tbody>
</table>
clear igmp snooping group

To clear IGMP snooping group states, use the `clear igmp snooping group` command in EXEC mode.

`clear igmp snooping group [group-address] [{port {interface-name|neighbor ipaddr pw-id id}|bridge-domain bridge-domain}]`

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>group-address</code></td>
<td>(Optional) Clears the specified group from the forwarding tables.</td>
</tr>
<tr>
<td><code>port interface-name</code></td>
<td>(Optional) Clears groups for the named interface from the forwarding tables.</td>
</tr>
<tr>
<td><code>port neighbor ipaddr pw-id id</code></td>
<td>(Optional) Clears groups for the named pseudowire (PW) from the forwarding tables.</td>
</tr>
<tr>
<td><code>bridge-domain bridge-domain</code></td>
<td>(Optional) Clears groups for the named bridge domain from the forwarding tables.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

IGMP snooping propagates the request to clear group information through the L2FIB to the forwarding plane. After this command is issued, IGMP snooping relearns group information by snooping packets as they are received from the network.

Use the `address` keyword to clear one group, identified by address. Otherwise, all groups are cleared. You can clear the named group from all ports or bridges, or from a specifically identified port or bridge.

Use the `bridge-domain` keyword to clear groups only for a named bridge domain. Use the `port` keyword to clear groups for a named port. A port can be an access interface or a pseudowire. The `bridge-domain` and `port` keywords are mutually exclusive.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>12vpn</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

The following example clears all group membership information from the forwarding tables:
RP/0/RSP0/CPU0:router# clear igmp snooping group

The following example clears one group from the forwarding table for one identified access circuit:

RP/0/RSP0/CPU0:router# clear igmp snooping group port
GigabitEthernet 0/1/1/1

The following example clears all group membership information from the forwarding table for one identified pseudowire:

RP/0/RSP0/CPU0:router# clear igmp snooping group port
neighbor 10.5.5.5 pw-id 5

The following example clears one group from the forwarding table for one identified pseudowire:

RP/0/RSP0/CPU0:router# clear igmp snooping group 10.10.10.1 port
neighbor 10.5.5.5 pw-id 5

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show igmp snooping group, on page 313</td>
<td>Displays IGMP snooping configuration information and statistics by group address.</td>
<td></td>
</tr>
</tbody>
</table>
clear igmp snooping port

To clear IGMP snooping port information, use the clear igmp snooping port command in EXEC mode.

clear igmp snooping port [{interface-name|neighbor ipaddr pw-id id|bridge-domain bridge-domain-name}] statistics

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-name</td>
<td>(Optional) Clears information for the named interface from the forwarding tables.</td>
</tr>
<tr>
<td>neighbor ipaddr pw-id id</td>
<td>(Optional) Clears information for the named PW from the forwarding tables.</td>
</tr>
<tr>
<td>bridge-domain bridge-domain-name</td>
<td>(Optional) Clears information for all ports under the named bridge domain.</td>
</tr>
<tr>
<td>statistics</td>
<td>Clears counters and other statistics. In Release 3.7.2, this keyword is required.</td>
</tr>
</tbody>
</table>

Command Default
None

Command Modes
EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 3.9.0</td>
<td>This command was modified to clear new statistical information added in the current release to support multicast admission control.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You can use this command to clear IGMP snooping information at the port level for:

- All ports on the router
- A specific port, using its interface name
- A specific PW, using the neighbor keyword
- All ports under a named bridge domain, using the bridge-domain keyword. In this case, only the port-level information is cleared under the bridge-domain. Use the clear igmp snooping bridge-domain command to clear statistics at the bridge-domain level.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>12vpn</td>
<td>execute</td>
</tr>
</tbody>
</table>
Examples

The following example clears IGMP snooping port-level counters for all ports on the router.

```
RP/0/RSP0/CPU0:router# clear igmp snooping port statistics
```

The following example clears IGMP snooping counters for one AC.

```
RP/0/RSP0/CPU0:router# clear igmp snooping port GigabitEthernet 0/1/1/1 statistics
```

The following example clears IGMP snooping counters for one PW.

```
RP/0/RSP0/CPU0:router# clear igmp snooping port neighbor 10.5.5.5 pw-id 5 statistics
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear igmp snooping bridge-domain, on page 246</td>
<td>Clears IGMP snooping information at the bridge level.</td>
</tr>
<tr>
<td>show igmp snooping port, on page 321</td>
<td>Displays IGMP snooping configuration information and statistics by port.</td>
</tr>
</tbody>
</table>
clear igmp snooping summary

To clear IGMP snooping summary counters, use the `clear igmp snooping summary` command in EXEC mode.

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Command Default</th>
<th>Command Modes</th>
<th>Command History</th>
<th>Usage Guidelines</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>statistics</strong></td>
<td>None</td>
<td>EXEC</td>
<td>Release 3.7.2</td>
<td>To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Release 3.9.0</td>
<td>This command clears summary level statistics about IGMP snooping. This command does not affect statistics at the bridge domain level or the port level.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Command Default</strong></td>
<td></td>
<td></td>
<td>Release 3.7.2</td>
<td></td>
</tr>
<tr>
<td><strong>Command Modes</strong></td>
<td>EXEC</td>
<td></td>
<td>Release 3.9.0</td>
<td></td>
</tr>
<tr>
<td><strong>Command History</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Usage Guidelines</strong></td>
<td></td>
<td></td>
<td>Release 3.9.0</td>
<td></td>
</tr>
</tbody>
</table>

### Examples

The following example clears all IGMP snooping statistics.

```
RP/0/RSP0/CPU0:router# clear igmp snooping summary statistics
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show igmp snooping summary, on page 335</code></td>
<td>Displays IGMP snooping configuration and traffic statistics at a summary level for the router.</td>
</tr>
</tbody>
</table>
clear l2vpn forwarding bridge-domain mroute

To clear multicast routes from the Layer-2 forwarding tables, use the `clear l2vpn forwarding bridge-domain mroute` command in EXEC mode.

```
clear l2vpn forwarding bridge-domain [bg:bd] mroute [{ipv4|ipv6}] [location node-id ]
```

**Syntax Description**

- `[bg:bd]` (Optional) Clears Layer-2 multicast routes only for the specified bridge group and bridge domain.
- `ipv4` (Optional) Specifies the IPv4 addressing scheme.
- `location node-id` (Optional) Clears Layer-2 multicast routes only for the specified node ID.

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command removes multicast routes in the Layer-2 forwarding information base (l2fib) tables. If you issue the command without a specific bridge group and bridge domain, information for all bridge groups and domains is cleared.

This command does not remove the state from the control plane. So, multicast routes will not be recreated.

You can use the `clear igmp snooping group` command which not only clears state from the control plane but also clears the state from the forwarding plane.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

The following example clears all multicast routes across all bridge domains on one module.

```
RP/0/RSP0/CPU0:router# clear l2vpn forwarding mroute location 0/5/CPU0
```
To specify the maximum number of groups or source-groups that may be joined on a port, use the `group limit` command in the appropriate snooping profile configuration mode. By default, each group or source-group contributes a weight of 1 towards this limit. To remove the group limit, use the `no` form of this command.

```
group limit group-limit-value
no group limit group-limit-value
```

**Syntax Description**
- Group-limit-value: Limit value for the port. Range is from 0-65535.

**Command Default**
No group limit

**Command Modes**
- IGMP snooping profile configuration
- MLD snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

No new group or source group will be accepted if its contributed weight would cause this limit to be exceeded.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to set the group limit of a port for weighting:

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)#igmp snooping profile
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# group limit 699
```

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)#mld snooping profile
RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# group limit 699
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-group (snooping profile), on page 245</td>
<td>Instructs IGMP snooping to apply the specified access list filter to received membership reports</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>group policy, on page 256</td>
<td>Instructs IGMP snooping to use the specified route policy to determine the weight contributed by a new &lt;*,G&gt; or &lt;S,G&gt; membership request.</td>
</tr>
<tr>
<td>show igmp snooping profile, on page 327</td>
<td>Displays the contents of profiles and to see associations of profiles with bridge-domains and ports, including access group, group limit, and TCN flood parameters.</td>
</tr>
<tr>
<td>show igmp snooping group, on page 313</td>
<td>Displays a summary of IGMP group information by group.</td>
</tr>
<tr>
<td>show igmp snooping group detail</td>
<td>Displays detailed IGMP group information in a multiline display per group.</td>
</tr>
<tr>
<td>show igmp snooping port, on page 321</td>
<td>Displays IGMP snooping configuration information and traffic counters by router interface port.</td>
</tr>
<tr>
<td>show igmp snooping port detail</td>
<td>Displays IGMP snooping configuration information and traffic counters by router interface port. You can use this command to see groups admitted against the configured limit.</td>
</tr>
<tr>
<td>show igmp snooping port group detail</td>
<td>Displays detailed IGMP membership information by port. You can use this command to see how group limits are assigned to groups on a port.</td>
</tr>
</tbody>
</table>
**group policy**

To instruct IGMP / MLD snooping to use the specified route policy to determine the weight contributed by a new <*,G> or <S,G> membership request, use the `group policy` command in the appropriate snooping profile configuration mode. To remove the group weight route policy from the profile and use the default group weight of 1 for all groups, use the `no` form of this command.

```
group policy policy-name
no group policy
```

**Syntax Description**

`policy-name` Name of the route policy that should determine the weight contributed by a new <*,G> or <S,G> membership request.

**Command Default**

Default weight for all groups is 1. By default, no route policy is configured to determine the weight of new <*,G> or <S,G> membership requests.

**Command Modes**

IGMP snooping profile configuration

MLD snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

To limit the number of IGMP v2/v3 groups, in which the maximum number of concurrently allowed multicast channels must be configurable on a per EFP-basis and per PW-basis, configure group weighting.

IGMP snooping limits the membership on a bridge port to a configured maximum limit. This feature also supports IGMPv3 source groups and allows different weights to be assigned to individual groups or source groups. This enables the IPTV provider, for example, to associate standard and high-definition IPTV streams, as appropriate, to specific subscribers.

This feature does not limit the actual multicast bandwidth that may be transmitted on a port. Rather, it limits the number of IGMP groups and source-groups, of which a port can be a member. It is the responsibility of the IPTV operator to configure subscriber membership requests to the appropriate multicast flows.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>12vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure a group route policy for weighting new <*,G> or <S,G>-membership requests:
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# igmp snooping profile
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# group policy
   policy name

RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# mld snooping profile
RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# group policy
   policy name

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-group (snooping profile), on page 245</td>
<td>Instructs IGMP snooping to apply the specified access list filter to received membership reports</td>
</tr>
<tr>
<td>group limit, on page 254</td>
<td>Specifies the group limit of a port for weighting purposes.</td>
</tr>
<tr>
<td>show run route-policy</td>
<td>Displays the route policy information.</td>
</tr>
</tbody>
</table>
igmp snooping profile

To create or change an IGMP snooping profile, or to attach an IGMP snooping profile to a bridge or a port, use the `igmp snooping profile` command in the appropriate configuration mode. To detach a profile from a bridge domain or port, use the `no` form of this command. To delete a profile from the database, use the `no` form of this command in global configuration mode.

`igmp snooping profile profile-name`
`no igmp snooping`

**Syntax Description**

`profile-name` Name that uniquely identifies the IGMP snooping profile.

**Command Default**

IGMP snooping is inactive on a bridge domain until a profile is attached to the bridge domain.

**Command Modes**

Global configuration

L2 VPN bridge group bridge domain configuration

L2 VPN bridge group bridge domain interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command accomplishes different tasks depending on the configuration mode you are in when you issue it.

- In global configuration mode, this command creates and changes profiles.
- In L2 VPN bridge group bridge domain configuration mode, this command attaches profiles to bridge domains.
- In L2 VPN bridge group bridge domain interface configuration mode, this command attaches profiles to ports.

Use the `igmp snooping profile` command in global configuration mode to create a new IGMP snooping profile or to change an existing profile. The command enters you into IGMP snooping profile configuration mode, from which you can issue commands that configure IGMP snooping.

The minimum configuration is an empty profile. An empty profile enables IGMP snooping with a default configuration.

To enable IGMP snooping on a bridge domain, you must attach a profile to the bridge domain. To disable IGMP snooping on a bridge domain, detach the profile from the bridge domain.

To attach a profile to a bridge domain, use the `igmp snooping profile` command in Layer-2 VPN bridge group bridge domain configuration mode. At the bridge domain level, only one IGMP snooping profile can be attached to a bridge.
If a profile attached to a bridge domain contains port-specific configuration options, the values apply to all of the ports under the bridge, unless a port-specific profile is attached to one of the ports. In that case, the port with the attached profile is configured using only the commands in the port profile, and any port configurations in the bridge profile are ignored.

Optionally, profiles can be attached to specific ports under a bridge domain. To attach a profile to a port, use the `igmp snooping profile` command in Layer-2 VPN bridge group bridge domain interface configuration mode. Each port can have only one port-specific profile attached to it.

IGMP snooping must be enabled on the bridge domain for any port-specific configurations to take effect. When a profile is attached to a port, IGMP snooping reconfigures that port, disregarding any port configurations that may exist in the bridge-level profile.

To detach a profile from a bridge domain, use the `no` form of this command in Layer-2 VPN bridge group bridge domain configuration mode. To detach a profile from a port, use the `no` form of this command in the interface configuration mode under the bridge domain.

When you detach a profile from a bridge domain or a port, the profile still exists and is available for use at a later time.

Detaching a profile has the following results:

- If you detach a profile from a bridge domain, IGMP snooping is deactivated in the bridge domain.
- If you detach a profile from a port, IGMP snooping configuration values for the port are instantiated from the bridge domain profile.

An active profile is one that is currently attached.

If you need to change an active profile, you must detach it from all bridges or ports, change it, and reattach it. An alternate procedure is to create a new profile incorporating the desired changes, detach the existing one, and immediately attach the new one.

To access an existing profile, use the `igmp snooping profile` command with the existing `profile-name` in global configuration mode. The command enters you into IGMP snooping profile configuration mode, from which you can issue commands to add to the current configuration or enter the `no` form of existing commands to delete them from the configuration.

To delete a profile from the router database, use the `no` form of this command in global configuration mode.

---

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read,</td>
<td>write</td>
</tr>
</tbody>
</table>

---

**Examples**

The following example shows how to create a new IGMP snooping profile or edit an existing profile:

```
router(config)# igmp snooping profile Profile-1
router(config-igmp-snooping-profile)#
```

The following example attaches a profile to the bridge domain ISP1:

```
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-12vpn)# bridge group GRP1
RP/0/RSP0/CPU0:router(config-12vpn-bg)# bridge-domain ISP1
RP/0/RSP0/CPU0:router(config-12vpn-bg-bd)# igmp snooping profile profile-1
```
The following example attaches a profile to the GigabitEthernet 0/1/1 port:

```
RP/0/RSP0/CPU0:router(config)# l2vpn
RP/0/RSP0/CPU0:router(config-l2vpn)# bridge group GRP1
RP/0/RSP0/CPU0:router(config-l2vpn-bg)# bridge-domain ISP1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd)# interface GigabitEthernet 0/1/1
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-if)# igmp snooping profile mrouter-port-profile
RP/0/RSP0/CPU0:router(config-l2vpn-bg-bd-if)# commit
```
**immediate-leave**

To configure fast leave processing on a port for IGMPv2 / MLDv1 queriers, use the `immediate-leave` command in the appropriate snooping profile configuration mode. To remove the functionality, use the `no` form of this command.

```
immediate-leave
no immediate-leave
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
Disabled

**Command Modes**
IGMP snooping profile configuration
MLD snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Immediate leave is an optional port-level configuration parameter. Immediate leave processing causes IGMP snooping to remove a Layer-2 interface from the forwarding table entry immediately, without first sending IGMP group-specific queries to the interface. Upon receiving an IGMP leave message, IGMP snooping immediately removes the interface from the Layer-2 forwarding table entry for that multicast group, unless a multicast router was learned on the port.

Immediate leave processing improves leave latency but is appropriate only when one receiver is configured on a port. For example, immediate leave is appropriate in the following situations:

- Point-to-point configurations, such as an IPTV channel receiver.
- Downstream DSLAMs with proxy reporting.

**Caution**
Do not use immediate leave on a port when the possibility exists for more than one receiver per port. Doing so could prevent an interested receiver from receiving traffic. For example, immediate leave is not appropriate in a LAN.

Immediate leave processing is a port-level option. You can configure this option explicitly per port in port profiles or in the bridge domain profile, in which case it applies to all ports under the bridge.

For MLD snooping - Immediate-leave should only be configured if there is a single MLD host on the port. Immediate-leave is implicitly enabled for MLDv2, if explicit-tracking is enabled.
The following example shows how to add immediate leave to a profile:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# immediate-leave

RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# immediate-leave
```

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
<td></td>
</tr>
</tbody>
</table>
**internal-querier**

To configure an internal IGMP /MLD querier on a bridge domain, use the **internal-querier** command in the appropriate snooping profile configuration mode. To disable the internal querier, use the **no** form of this command.

```
internal-querier
no internal-querier
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The internal querier is disabled by default.

**Command Modes**

IGMP snooping profile configuration
MLD snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command to configure an IGMP querier in a bridge domain where no external querier exists. An internal querier injects query packets into the bridge domain.

In a network where IP multicast routing is configured, the IP multicast router acts as the IGMP querier. In situations when no mrouter port exists in the bridge domain (because the multicast traffic does not need to be routed), but local multicast sources exist, you must configure an internal querier to implement IGMP snooping. The internal querier solicits membership reports from hosts in the bridge domain so that IGMP snooping can build constrained multicast forwarding tables for the multicast traffic within the bridge domain.

An internal querier might also be useful when there are interoperability issues that prevent IGMP snooping from working correctly with an external querier. In this case, you can:

1. Prevent the uncooperative external querier from being discovered by placing the **router-guard** command on that port.
2. Configure an internal querier to learn group membership interests from the ports in the bridge domain.
3. Configure static mrouter ports to receive multicast traffic.

The minimum configuration for an internal querier is as follows. Both of the following commands are required.

- Add the **internal-querier** command to a profile attached to the bridge domain. This command configures the internal querier with the default configuration.
- Add the **system-ip-address** command to a profile attached to the bridge domain to configure an address other than the default 0.0.0.0.

You can disable the internal querier (using the **no** form of the **internal-querier** command) without removing any other internal querier commands. The additional internal querier commands are ignored in that case.
The scope for the **internal-querier** command is per bridge domain. If the command appears in profiles attached to ports, it has no effect.

The local IGMP snooping process responds to the internal querier's general queries. In particular, the IGMPv3 proxy (if enabled) generates a current-state report and forwards it to all mrouters. For IGMPv2 or when the IGMPv3 proxy is disabled, IGMP snooping generates current-state reports for static group state only.

### Task ID

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example activates an internal querier with default configuration values:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# system-ip-address 10.1.1.1
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# internal-querier

RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# internal-querier
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
<tr>
<td>internal-querier max-response-time</td>
<td>Configures the maximum response time advertised by the internal querier.</td>
</tr>
<tr>
<td>internal-querier query-interval</td>
<td>Configures the time between general queries issued by the internal querier.</td>
</tr>
<tr>
<td>internal-querier robustness-variable</td>
<td>Configures the robustness variable for the internal querier.</td>
</tr>
<tr>
<td>internal-querier tcn query count</td>
<td>Configures the number of queries the internal querier sends after receiving a group leave from IGMP snooping.</td>
</tr>
<tr>
<td>internal-querier tcn query interval</td>
<td>Configures the time between queries that the internal querier sends after receiving a group leave from IGMP snooping.</td>
</tr>
<tr>
<td>internal-querier timer expiry</td>
<td>Configure the time IGMP snooping waits to receive messages from an external querier before making the internal querier the active querier.</td>
</tr>
<tr>
<td>internal-querier version</td>
<td>Configures the IGMP version that the internal querier runs.</td>
</tr>
<tr>
<td>mrouter</td>
<td>Sets a port to receive query packets.</td>
</tr>
<tr>
<td>router-guard</td>
<td>Sets a port to block query packets.</td>
</tr>
<tr>
<td>system-ip-address</td>
<td>Configures an IP address for IGMP snooping use.</td>
</tr>
</tbody>
</table>
**internal-querier** (MLD)

To configure an internal MLD querier on a bridge domain, use the `internal querier` command in the MLD snooping profile configuration mode. To disable the internal querier, use the `no` form of the command.

```plaintext
internal-querier

no internal-querier
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

The internal querier is disabled by default.

**Command Modes**

MLD snooping profile configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The internal-querier is disabled by default. However, if PIMv6 snooping is active in the domain, then the internal-querier is active. If queries are received from another querier in the domain, MLD querier election is performed (where the lowest ip-address wins). If the internal-querier is the election-loser, then a timer (the other-querier-present-timer) is run for the timer expiry interval. If this timer expires before another query is received from the election-winner, then the internal-querier becomes the querier.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

The following example shows how to use the internal-querier command:

```plaintext
RP/0/RSP0/CPU0:router(config-mld-snooping-profile) # internal-querier
```
**internal-querier max-response-time**

To configure the maximum response time advertised by the internal querier, use the `internal-querier max-response-time` command in the appropriate snooping profile configuration mode. To return to the default value, use the `no` form of this command.

```plaintext
internal-querier max-response-time seconds
no internal-querier max-response-time
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>seconds</code></td>
<td>Configures the maximum response time included in queries from the internal querier. Valid values are from 1 to 25 (seconds).</td>
</tr>
</tbody>
</table>

| Command Default    | 10 (seconds) |

| Command Modes      | IGMP snooping profile configuration<br>MLD snooping profile configuration |

<table>
<thead>
<tr>
<th>Command History</th>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
<td></td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The maximum response time (MRT) is the amount of time during which receivers are required to report their membership state.

In addition, the maximum response time is used in the calculation of the Group Management Interval (GMI). GMI controls when IGMP snooping expires stale group membership states. See the “Implementing IGMP Snooping on Cisco ASR 9000 Series Router” module in the *Cisco ASR 9000 Series Routers Multicast Configuration Guide* for more information about the GMI.

The maximum response time is advertised in general queries issued by the internal querier.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
<td></td>
</tr>
</tbody>
</table>

**Examples**

The following example configures a maximum response time for the internal querier, overriding the default value:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# internal-querier max-response-time 5

RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# internal-querier max-response-time 5
```
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
<tr>
<td>internal-querier, on page 263</td>
<td>Enables an internal querier in the bridge domain.</td>
</tr>
</tbody>
</table>
internal-querier query-interval

To configure the time between general queries issued by the internal querier, use the `internal-querier query-interval` command in the appropriate snooping profile configuration mode. To return to the default value, use the `no` form of this command.

```
internal-querier query-interval seconds
no internal-querier query-interval
```

**Syntax Description**
- `seconds`: Configures the number of seconds between general queries for membership reports issued by the internal querier. Valid values are from 1 to 18000 (seconds).

**Command Default**
60 (seconds). This is a nonstandard default value.

**Command Modes**
- IGMP snooping profile configuration
- MLD snooping profile configuration

**Command History**
```
Release       Modification
3.7.2          This command was introduced.
```

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

When the internal querier is the active querier in the domain, it solicits membership reports by sending IGMP general queries at the interval specified by this command on every active port in the bridge domain.

**Note**
Cisco IOS and Cisco IOS XR software use the non-standard default value of 60 for query interval.

**Task ID**
- Task ID: `l2vpn`
  - Operations: `read, write`

**Examples**
The following example sets a query interval for the internal querier, overriding the default value:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# internal-querier query-interval 125

RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# internal-querier query-interval 125
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
<tr>
<td>internal-querier, on page 263</td>
<td>Enables an internal querier in the bridge domain.</td>
</tr>
</tbody>
</table>
**internal-querier robustness-variable**

To configure the robustness variable for the internal querier, use the `internal-querier robustness-variable` command in the appropriate snooping profile configuration mode. To return to the default value, use the `no internal-querier robustness-variable` command.

```
internal-querier robustness-variable number
no internal-querier robustness-variable
```

**Syntax Description**

- `number` Valid values are from 1 to 7 (for IGMP snooping). For MLD snooping, range is from 1 to 3.

**Command Default**

2

**Command Modes**

- IGMP snooping profile configuration
- MLD snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command to set the internal querier’s robustness variable to a value other than the default configuration value. If the internal querier is running IGMPv3, it advertises the robustness variable in its general queries.

In addition, the robustness variable is used in the calculation of the Group Management Interval (GMI). GMI controls when IGMP snooping expires stale group membership states. See the “Implementing IGMP Snooping on Cisco ASR 9000 Series Routers” module in the *Cisco ASR 9000 Series Routers Multicast Configuration Guide* for more information about GMI.

**Task ID**

- **Operations**
  - Read, write

**Examples**

The following example configures the robustness variable for an internal querier, overriding the default value:

```
RP/0/RSP0/CPU0:router (config-igmp-snooping-profile)# internal-querier robustness-variable 3
```

```
RP/0/RSP0/CPU0:router (config-mld-snooping-profile)# internal-querier robustness-variable 3
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
<tr>
<td>internal-querier, on page 263</td>
<td>Enables an internal querier in the bridge domain.</td>
</tr>
</tbody>
</table>
**internal-querier tcn query count**

To configure the number of queries the internal querier sends after receiving a group leave from the snooping process, use the **internal-querier tcn query count** command in the appropriate snooping profile configuration mode. To return to the default value, use the **no** form of this command.

```
internal-querier tcn query count number
no internal-querier tcn query count
```

**Syntax Description**

- **number**: Configures the number of queries the internal querier sends after receiving a group leave from IGMP snooping. Valid values are from 0 to 3. The time between queries is controlled by the **internal-querier tcn query interval** command.

**Command Default**

2

**Command Modes**

- IGMP snooping profile configuration
- MLD snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Snooping reacts to Spanning Tree Protocol (STP) topology change notifications (TCNs) by flooding all multicast traffic and sending group leaves to expedite relearning. When the internal querier receives a group leave, it sends queries to solicit membership reports. This command configures the number of queries to send. The time between queries is controlled by the **internal-querier tcn query interval** command.

If you set **internal-querier tcn query count** to 0, the internal querier does not respond to group leaves.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>12vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example configures the tcn query count for an internal querier, overriding the default value:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# internal-querier tcn query count 3
RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# internal-querier tcn query count 3
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>igmp snooping profile, on page 258</code></td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
<tr>
<td><code>internal-querier, on page 263</code></td>
<td>Enables an internal querier in the bridge domain.</td>
</tr>
<tr>
<td><code>internal-querier tcn query interval, on page 274</code></td>
<td>Configures the interval between queries the internal querier sends after receiving a group leave from IGMP snooping.</td>
</tr>
</tbody>
</table>
**internal-querier tcn query interval**

To configure the time between queries that the internal querier sends after receiving a group leave from IGMP / MLD snooping, use the `internal-querier tcn query interval` command in the appropriate snooping profile configuration mode. To return to the default value, use the `no` form of this command.

```
internal-querier tcn query interval seconds
no internal-querier tcn query interval
```

**Syntax Description**
- `seconds` Configures the time between queries. Valid values are from 1 to 18000.

**Command Default**
- 10

**Command Modes**
- IGMP snooping profile configuration
- MLD snooping configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Snooping reacts to STP topology change notifications by flooding all multicast traffic and sending group leaves to expedite relearning. When the internal querier receives the group leave, it sends queries to solicit membership reports. This command configures the time between queries.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example configures the tcn query interval for an internal querier, overriding the default value:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# internal-querier tcn query interval 100
```

```
RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# internal-querier tcn query interval 100
```
<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
<tr>
<td>internal-querier, on page 263</td>
<td>Enables an internal querier in the bridge domain.</td>
</tr>
<tr>
<td>internal-querier tcn query count, on page 272</td>
<td>Configures the number of queries the internal querier sends after receiving a group leave from IGMP snooping.</td>
</tr>
</tbody>
</table>
**internal-querier timer expiry**

To configure the time IGMP/MLD snooping waits to receive messages from an external querier before making the internal querier the active querier, use the `internal-querier timer expiry` command in the appropriate snooping profile configuration mode. To return to the default value, use the `no` form of this command.

`internal-querier timer expiry` *seconds*

`no internal-querier timer expiry`

**Syntax Description**

`seconds`  The time IGMP snooping waits to receive messages from an external querier before making the internal querier the active querier. Valid values are from 60 to 300 (seconds).

**Command Default**

125 (seconds), as defined in RFC-3376, Section 8.5:

\[(\text{robustness-variable} \times \text{query-interval}) + \frac{1}{2}(\text{max-response-time})\]

Using the default values for all components:

\[(2 \times 60) + \frac{1}{2}(10) = 125\]

**Command Modes**

IGMP snooping profile configuration

MLD snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

A bridge domain can have only one active querier at a time. If the internal querier receives queries from another querier in a bridge domain, it performs querier election. The lowest IP address wins. If the internal querier is the election loser, the snooping technique sets a timer to the `internal-querier timer expiry` value. If this timer expires before another query is received from the election winner, the internal querier becomes the active querier.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example configures the timer expiry value for an internal querier, overriding the default value:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# internal-querier timer expiry 100
```
RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# internal-querier timer expiry 100

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
<tr>
<td></td>
<td>internal-querier, on page 263</td>
<td>Enables an internal querier in the bridge domain.</td>
</tr>
</tbody>
</table>
internal-querier version

To configure the version for the internal querier, use the **internal-querier version** command in the appropriate snooping profile configuration mode. To return to the default value, use the **no** form of this command.

**syntax**

```
internal-querier version  version
no internal-querier version
```

**Syntax Description**

- **version**: Controls the version of the internal querier. Valid values are 2 or 3 (for IGMP) and 1 or 2 (for MLD).

**Command Default**

3

**Command Modes**

- IGMP snooping profile configuration
- MLD snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The internal querier sends IGMP queries on the bridge domain. This command sets the internal querier to run as either an IGMPv2 or IGMPv3 querier.

This command sets the internal querier to run as either a MLDv1 or MLDv2 querier.

**Task ID**

```
<table>
<thead>
<tr>
<th>Task ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
</tr>
</tbody>
</table>
```

**Operations**

- read,
- write

**Examples**

The following example configures the internal querier to send version2 queries, overriding the default value:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# internal-querier version 2
RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# internal-querier version 2
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>internal-querier, on page 263</td>
<td>Enables an internal querier in the bridge domain.</td>
</tr>
</tbody>
</table>
**last-member-query count**

To configure the number of group-specific queries IGMP snooping sends in response to a leave message, use the `last-member-query count` command in IGMP snooping profile configuration mode. To return to the default value, use the `no` form of this command.

```
last-member-query count number
no last-member-query count
```

**Syntax Description**

| `number` | Specifies the number of queries IGMP snooping sends in response to a leave message. Valid values are from 1 to 7. |

**Command Default**

2

**Command Modes**

IGMP snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Last member query is the default group leave processing method used by IGMP snooping. With last member query processing, IGMP snooping processes leave messages as follows:

- IGMP snooping sends group-specific queries on the port that receives the leave message to determine if any other devices connected to that interface are interested in traffic for the specified multicast group. Using the following two configuration commands, you can control the latency between the request for a leave and the actual leave:
  - `last-member-query-count` command—Controls the number of group-specific queries IGMP snooping sends in response to a leave message.
  - `last-member-query-interval` command—Controls the amount of time between group-specific queries.

- If IGMP snooping does not receive an IGMP Join message in response to group-specific queries, it assumes that no other devices connected to the port are interested in receiving traffic for this multicast group, and it removes the port from its Layer-2 forwarding table entry for that multicast group.
- If the leave message was from the only remaining port, IGMP snooping removes the group entry and generates an IGMP leave to the multicast routers.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>12vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>
Examples

The following example configures the number of queries that IGMP snooping sends in response to a leave, overriding the default value:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# last-member-query count 1
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile and attaches a profile to a bridge domain or port.</td>
</tr>
<tr>
<td>last-member-query interval, on page 283</td>
<td>Configures the time between queries sent in response to an IGMP leave.</td>
</tr>
</tbody>
</table>
last-member-query count (MLD)

To configure the number of group-specific queries MLD snooping sends in response to a leave message, use the last-member-query count command in MLD snooping profile configuration mode. To return to the default value, use the no form of this command.

last-member-query count number
no last-member-query count number

Syntax Description

number Specifies the number of queries MLD snooping sends in response to a leave message. Range is from 1 to 7.

Command Default
The default count is 2.

Command Modes
MLD snooping profile configuration mode.

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Last member query is the default group leave processing method used by MLD snooping. MLD snooping sends group-specific queries on the port that receives the leave message to determine if any other devices connected to that interface are interested in traffic for the specified multicast group. Using the following two configuration commands, you can control the latency between the request for a leave and the actual leave: last-member-query count and last-member-query interval.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
<td></td>
</tr>
</tbody>
</table>

Example

The following example shows how to set the last member query count to 5:

RP/0/RSP0/CPU0:router (config-mld-snooping-profile) # last-member-query count 5
last-member-query interval

To configure the amount of time between group-specific queries, use the `last-member-query interval` command in IGMP snooping profile configuration mode. To return to the default value, use the `no` form of this command.

```
last-member-query interval milliseconds
no last-member-query interval
```

**Syntax Description**

`milliseconds` Specifies the time between queries that IGMP snooping sends in response to a leave message. Valid values are from 100 to 5000 (milliseconds).

**Command Default**

1000 (milliseconds)

**Command Modes**

IGMP snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Last member query is the default group leave processing method used by IGMP snooping. With last member query processing, IGMP snooping processes leave messages as follows:

- IGMP snooping sends group-specific queries on the port that receives the leave message to determine if any other devices connected to that interface are interested in traffic for the specified multicast group. Using the following two configuration commands, you can control the latency between the request for a leave and the actual leave:
  - `last-member-query-count` command—Controls the number of group-specific queries IGMP snooping sends in response to a leave message.
  - `last-member-query-interval` command—Controls the amount of time between group-specific queries.

- If IGMP snooping does not receive an IGMP Join message in response to group-specific queries, it assumes that no other devices connected to the port are interested in receiving traffic for this multicast group, and it removes the port from its Layer-2 forwarding table entry for that multicast group.
- If the leave message was from the only remaining port, IGMP snooping removes the group entry and generates an IGMP leave to the multicast routers.

**Task ID**

```
Task ID      Operations
l2vpn        read, write
```
Examples

The following example configures the interval between queries that IGMP snooping sends in response to a leave, overriding the default value:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# last-member-query interval 2000
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
<tr>
<td>last-member-query count, on page 280</td>
<td>Configures the number of queries sent in response to an IGMP leave.</td>
</tr>
</tbody>
</table>
last-member-query interval (MLD)

To configure the amount of time between group-specific queries, use the last-member-query interval command in MLD snooping profile configuration mode. To return to the default value, use the no form of this command.

`last-member-query interval milliseconds`
`no last-member-query interval milliseconds`

**Syntax Description**

`milliseconds` Specifies the time between queries that MLD snooping sends in response to a leave message. Valid values are from 100 to 5000 (milliseconds).

**Command Default**

1000 milliseconds

**Command Modes**

MLD snooping profile

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

The following example shows how to set the last member query interval to 2000 ms:

```
RP/0/RSP0/CPU0:router(config-mld-snooping-profile) # last-member-query interval 2000
```
minimum-version

To change the IGMP versions supported by IGMP snooping, use the minimum-version command in IGMP snooping profile configuration mode. To return to the default value, use the no form of this command.

```
minimum-version number
no minimum-version
```

**Syntax Description**

<table>
<thead>
<tr>
<th>number</th>
<th>Specifies the minimum IGMP version supported by IGMP snooping. Supported values are:</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Snoops messages from IGMPv2 and IGMPv3.</td>
</tr>
<tr>
<td>3</td>
<td>Only IGMPv3 messages are snooped. All IGMPv2 messages are ignored by IGMP snooping.</td>
</tr>
</tbody>
</table>

**Command Default**

2 (supporting IGMPv2 and IGMPv3)

**Command Modes**

IGMP snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The minimum-version command controls which IGMP versions are supported by IGMP snooping in the bridge domain.

- When minimum-version is 2, IGMP snooping intercepts IGMPv2 and IGMPv3 messages. This is the default value.
- When minimum-version is 3, IGMP snooping intercepts only IGMPv3 messages and drops all IGMPv2 messages.

The scope for this configuration option is per bridge domain. If the command appears in profiles attached to ports, it has no effect.

**Examples**

The following example configures IGMP snooping to support only IGMPv3 and to ignore IGMPv2 reports and queries:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# minimum-version 3
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
</tbody>
</table>
To enable MLD snooping to filter out all packets of MLD versions, less than the minimum-version, use the `minimum-version` command in the MLD snooping profile configuration mode. To disable minimum version, use the `no` form of the command.

```
minimum-version number
nomimum-version number
```

**Syntax Description**

- `number`: Specifies the MLD version supported by MLD snooping. The available values are -1 and 2.

**Command Default**

By default, MLD snooping supports minimum-version 1.

**Command Modes**

MLD snooping profile configuration mode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If minimum version is set to 2, all MLD packets set to (minimum version) 1, are dropped.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to use the `minimum-version` command:

```
RP/0/RSP0/CPU0:router (config-mld-snooping-profile) # minimum-version 2
```
mld snooping profile

To enter Multicast Listener Discovery (MLD) snooping profile configuration mode, use the `mld snooping profile` command in configuration mode. To exit from the MLD snooping profile configuration mode, use the `no` form of the command.

```
mld snooping profile profile-name
nomld snooping profile profile-name
```

**Syntax Description**

| `profile-name` | Name that uniquely identifies the MLD snooping profile. |

**Command Default**

No default behavior or values.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to use the `mld snooping profile` command:

```
RP/0/RSP0/CPU0:router(config) #mld snooping profile p1
```
**mrouter**

To statically configure a port to receive query packets, use the `mrouter` command in the appropriate snooping profile configuration mode. To remove the configuration, use the `no` form of this command.

```
  mrouter
  no mrouter
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

No default behavior or values

**Command Modes**

IGMP snooping profile configuration
MLD snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

You can statically configure a port as an mrouter port with the `mrouter` command.

You can use the `router-guard` and the `mrouter` commands on the same port to configure a guarded port as a static mrouter. For example:

- In situations where there are a large number of downstream host ports, you may want to block dynamic mrouter discovery and configure static mrouters. In this case, configure the router guard feature at the domain level. By default, it will be applied to all ports, including the (typically) large number of downstream host ports. Then use another profile without router guard configured for the relatively few upstream ports on which you want to permit dynamic mrouter discovery or configure static mrouters.
- In situations when incompatibilities with non-Cisco equipment prevents correct dynamic discovery, you can disable all attempts for dynamic discovery using the router guard feature, and statically configure the mrouter.

If you are using the router guard feature because there is an incompatible IGMP router on the port, you should also configure the `mrouter` command on the port to ensure that the router receives snooping reports and multicast flows.

The scope of this command is port level. If you use this command in a profile attached to a bridge domain, you are configuring all ports as mrouter ports.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>
The following example shows how to add static mrouter configuration to a profile:

RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# mrouter

RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# mrouter

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
<tr>
<td>internal-querier, on page 263</td>
<td>Sets a port to send query packets to bridge domain ports.</td>
</tr>
<tr>
<td>router-guard, on page 304</td>
<td>Blocks query packets on the port.</td>
</tr>
</tbody>
</table>
nv satellite offload ipv4 multicast enable

To enable the IPv4 Multicast Satellite Offloading, use the `nv satellite offload ipv4 multicast enable` command in L2vpn bridge domain, nv satellite configuration sub mode.

**Command Default**
By default, the configuration command is disabled.

**Command Modes**
L2vpn bridge domain nv satellite configuration sub mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use this command only when you want to enable replication of IPv4 multicast on the satellite nodes. When set, the replication will be offloaded to the satellite devices that have offload eligible ports configured under this bridge-domain.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to enable the IPv4 Multicast Offload feature on the Satellite nV System:

```
RP/0/0/CPU0:ios(config)#l2vpn
RP/0/0/CPU0:ios(config-l2vpn)#bridge group <bg>
RP/0/0/CPU0:ios(config-l2vpn-bg)#bridge-domain <bd>
RP/0/0/CPU0:ios(config-l2vpn-bg-bd)#nv
RP/0/0/CPU0:ios(config-l2vpn-bg-bd-nv)#nv satellite offload ipv4 multicast enable
```
querier query-interval

To configure the query interval for processing IGMPv2 membership states, use the `querier query-interval` command in IGMP snooping profile configuration mode. To return to the default setting, use the `no` form of this command.

```
querier query-interval seconds
no querier query-interval
```

**Syntax Description**

- **seconds** Specifies the integer to use as the query interval in calculations performed by IGMP snooping when processing IGMPv2 messages.

**Note**

IGMPv3 messages convey the query interval from the querier.

Valid values are integers from 1 to 18000 (seconds). The default is 60.

**Command Default**

60 (seconds). This is a nonstandard default value.

**Command Modes**

IGMP snooping profile configuration

**Command History**

Release 3.7.2 This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Query interval is the interval between general queries and is used in the calculated group management interval (GMI). GMI controls when IGMP snooping expires stale group membership states. For more information about GMI, see the “Implementing IGMP Snooping on Cisco ASR 9000 Series Routers” module in the *Cisco ASR 9000 Series Routers Multicast Configuration Guide*.

If the querier is running IGMPv2, IGMP snooping uses the IGMP snooping configured values for robustness variable and query interval. These parameter values must match the configured values for the querier. In most cases, if you are interacting with other Cisco routers, you should not need to explicitly configure these values—the default values for IGMP snooping should match the default values of the querier. If they do not, use the `querier robustness-variable` and `querier query-interval` commands to configure matching values.

**Note**

Cisco IOS and Cisco IOS XR software use the nonstandard default value of 60 for query interval.

**Note**

IGMPv3 general queries convey values for robustness variable and query interval (QRV and QOI, respectively). IGMP snooping uses the values from the query, making the IGMP snooping GMI exactly match that of the querier.
The scope for this command is per bridge domain. If the command appears in profiles attached to ports, it has no effect.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to add the command to a profile that configures the query interval:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# querier query-interval 1500
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
<tr>
<td>internal-querier robustness-variable, on page 270</td>
<td>Configures a robustness variable for an internal querier.</td>
</tr>
<tr>
<td>internal-querier query-interval, on page 268</td>
<td>Configures the query interval for an internal querier.</td>
</tr>
<tr>
<td>querier robustness-variable, on page 295</td>
<td>Configures the robustness variable required for processing IGMPv2 membership reports.</td>
</tr>
</tbody>
</table>
**querier robustness-variable**

To configure the robustness variable for processing IGMPv2 membership states, use the `querier robustness-variable` command in IGMP snooping profile configuration mode. To return to the default setting, use the `no` form of this command.

```plaintext
querier robustness-variable  robustness-number
no querier robustness-variable
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Specification</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>robustness-number</code></td>
<td>Specifies the integer to use as the robustness variable in calculations performed by IGMP snooping when processing IGMPv2 messages.</td>
<td></td>
</tr>
<tr>
<td><code>Note</code></td>
<td>IGMPv3 messages convey the robustness variable from the querier.</td>
<td></td>
</tr>
<tr>
<td><code>Valid values are integers from 1 to 7. The default is 2.</code></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

2

**Command Modes**

IGMP snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Robustness variable is an integer used to influence the calculated GMI. GMI controls when IGMP snooping expires stale group membership states. For more information about GMI, see the “Implementing IGMP Snooping on Cisco ASR 9000 Series Routers” module in the *Cisco ASR 9000 Series Routers Multicast Configuration Guide*.

If the querier is running IGMPv2, IGMP snooping uses the IGMP snooping configured values for robustness variable and query interval. These parameter values must match the configured values for the querier. In most cases, if you are interacting with other Cisco routers, you should not need to explicitly configure these values—the default values for IGMP snooping should match the default values of the querier. If they do not, use the `querier robustness-variable` and `querier query-interval` commands to configure matching values.

**Note**

IGMPv3 general queries convey values for robustness variable and query interval (QRV and QOI, respectively). IGMP snooping uses the values from the query, making the IGMP snooping GMI exactly match that of the querier.

The scope for this command is per bridge domain. If the command appears in profiles attached to ports, it has no effect.
### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to add the command to a profile that configures the robustness variable:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# querier robustness-variable 1
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>igmp snooping profile, on page 258</code></td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
<tr>
<td><code>internal-querier robustness-variable, on page 270</code></td>
<td>Configures a robustness variable for an internal querier.</td>
</tr>
<tr>
<td><code>internal-querier query-interval, on page 268</code></td>
<td>Configures the query interval for an internal querier.</td>
</tr>
<tr>
<td><code>querier query-interval, on page 293</code></td>
<td>Configures the query interval required for processing IGMPv2 membership reports.</td>
</tr>
</tbody>
</table>
redundancy iccp-group report-standby-state disable

To enable IGMP Snooping for generating unsolicited state-change reports only when the port transitions from standby to active, use the `redundancy iccp-group report-standby-state disable` command in IGMP snooping profile configuration mode. To use the default behavior, use the `no` form of this command.

```
redundancy iccp-group report-standby-state disable
no redundancy iccp-group report-standby-state disable
```

**Note**
By default, IGMP Snooping generates state-change and current-state reports to all multicast routers to reflect state that exists on standby MC-LAG ports only. This causes the upstream sources to forward multicast streams to the router, where they will be dropped (on egress side).

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
None

**Command Modes**
IGMP snooping profile configuration (config-igmp-snooping-profile)

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Note**
This command is applicable only when MC-LAG is configured.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
This example shows how to use the `redundancy iccp-group report-standby-state disable` command:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# redundancy iccp-group report-standby-state disable
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
</tbody>
</table>
report-suppression disable

To disable IGMPv2 report suppression or IGMPv3 proxy reporting, use the report-suppression disable command in IGMP snooping profile configuration mode. To enable report suppression or proxy reporting functionality, use the no form of this command.

```plaintext
report-suppression disable
no report-suppression disable
```

### Syntax Description

This command has no arguments or keywords.

### Command Default

Report suppression and proxy reporting, whichever is appropriate, are enabled by default.

### Command Modes

IGMP snooping profile configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command to disable report suppression for IGMPv2 queriers and proxy reporting for IGMPv3 queriers. Both features are enabled by default, with the following results:

- **IGMPv2 report suppression**—For IGMPv2 bridge domain queriers, IGMP snooping suppresses reports from a host if the report was previously forwarded from another host. IGMP snooping sends only the first join and last leave to mrouter ports.
- **IGMPv3 proxy reporting**—For IGMPv3 bridge domain queriers, IGMP snooping acts as a proxy, generating state change reports from a proxy reporting IP address. You can configure that IP address using the `system-ip-address` command. The default is 0.0.0.0.

These features are enabled and disabled per bridge domain. This command is ignored if it appears in a profile attached to a port.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to add the command to a profile to turn off report suppression and proxy reporting:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# report-suppression disable
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
<tr>
<td>system-ip-address, on page 388</td>
<td>Configures an IP address used by IGMP snooping.</td>
</tr>
</tbody>
</table>
**report-suppression disable(MLD)**

To minimize the number of MLD reports sent to the mrouters, use the `report-suppression disable` command in the MLD snooping profile configuration mode.

```
report-suppression disable
noreport-suppression disable
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

By default, report suppression is enabled.

**Command Modes**

MLD snooping profile configuration mode.

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The report suppression command instructs MLD Snooping to suppress the forwarding of reports from individual hosts and instead to send the first-join and last-leave reports to the mrouters.

If the querier in the BD is running at MLD version 1, then report-suppression is performed and the snooper suppresses reports from a host if it has already forwarded the same report from another host. If the querier is on version 2, then proxy-reporting is performed. In this mode, the snooper acts as a proxy, generating reports from the proxy reporting IP address.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to use the report suppression disable command:

```
RP/0/RSP0/CPU0:router (config-mld-snooping-profile) # report suppression disable
```
**router-alert-check disable**

To disable the IGMP snooping check for the presence of the router alert option in the IP packet header, use the `router-alert-check disable` command in IGMP snooping profile configuration mode. To enable this functionality after a disable, use the `no` form of this command.

```
router-alert-check disable
no router-alert-check disable
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

The router alert check feature is enabled by default.

**Command Modes**

IGMP snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

By default, IGMP snooping checks for the presence of the router alert option in the IP packet header of the IGMP message and drops packets that do not include this option. If your network performs this validation elsewhere, you can disable this IGMP snooping validation.

You can disable this check using the `router-alert-check disable` command, in which case IGMP snooping does perform the validation before processing the message.

The scope for this configuration option is per bridge domain. If the command appears in profiles attached to ports, it has no effect.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to add the command to a profile that turns off the router alert check:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# router-alert-check disable
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
</tbody>
</table>
router-guard

To block a port from receiving query packets, use the **router-guard** command in the appropriate snooping profile configuration mode. To remove the restriction, use the **no** form of this command.

```
router-guard
no router-guard
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

None

**Command Modes**

IGMP snooping profile configuration

MLD snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Router guard is a security feature that prevents malicious users from making a host port into an mrouter port. (This undesirable behavior is known as spoofing.) When a port is protected with the **router-guard** command, it cannot be dynamically discovered as an mrouter. When router guard is on a port, IGMP snooping filters protocol packets sent to the port and discards any that are multicast router control packets.

---

**Caution**

If you add the **router-guard** command in a bridge domain profile, you disable dynamic discovery of all mrouters in that bridge domain.

You can use the **router-guard** and the **mrouter** commands on the same port to configure a guarded port as a static mrouter. For example:

- In situations where there are a large number of downstream host ports, you may want to block dynamic mrouter discovery and configure static mrouters. In this case, configure the router guard feature at the domain level. By default, it will be applied to all ports, including the (typically) large number of downstream host ports. Then use another profile without router guard configured for the relatively few upstream ports on which you want to permit dynamic mrouter discovery or configure static mrouters.

- In situations when incompatibilities with non-Cisco equipment prevents correct dynamic discovery, you can disable all attempts for dynamic discovery using the router guard feature, and statically configure the mrouter.

If you are using the router guard feature because there is an incompatible IGMP router on the port, you should also configure the **mrouter** command on the port to ensure that the router receives reports and multicast flows.
**Examples**

The following example shows how to add the command to a profile that prevents a port from being dynamically discovered as an mrouter:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# router-guard
```

```
RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# router-guard
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
<tr>
<td>internal-querier, on page 263</td>
<td>Sets a port to send query packets to bridge domain ports.</td>
</tr>
<tr>
<td>mrouter, on page 290</td>
<td>Sets a port to receive query packets.</td>
</tr>
</tbody>
</table>
show igmp snooping bridge-domain

To display IGMP snooping configuration information and traffic statistics for bridge domains, use the `show igmp snooping bridge-domain` command in EXEC mode.

```
show igmp snooping bridge-domain [bridge-domain-name] [detail [statistics [include-zeroes]]]
```

**Syntax Description**
- `bridge-domain-name` (Optional) Displays information only for the specified bridge domain.
- `detail` (Optional) Includes more details, including configuration information about the bridge domain querier.
- `statistics` (Optional) Includes traffic counters and statistics.
- `include-zeroes` (Optional) Includes all statistics, even if they are zero. Without this keyword, many statistics are omitted from the display when their values are zero.

**Command Default**
None

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 3.9.0</td>
<td>Bridge domain counters for access group permits, access group denials, and group limits exceeded fields were added to the detail statistics display output.</td>
</tr>
<tr>
<td>Release 5.2.2</td>
<td>The command output was enhanced to include the Multicast Offload information.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command displays IGMP snooping information by bridge domain. Use the command without any keywords to display summary information about all bridge domains, in a single line per bridge domain.

Use optional keywords to request additional details and traffic statistics per bridge domain. You can also limit the display to a single bridge domain.

The `statistics` keyword displays IGMP traffic information, including IGMP queries, reports, and leaves. The three columns in the statistics section of the display are:

- Received—Number of packets received.
- Rejected—Number of packets received, processed, and re-injected back into the forwarding path.
- Generated—Number of packets generated by the IGMP snooping application and injected into the forwarding path.
Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>12vpn</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows the basic command without any keywords.

```
RP/0/RSP0/CPU0:router# show igmp snooping bridge-domain
```

<table>
<thead>
<tr>
<th>Bridge Domain</th>
<th>Profile</th>
<th>Act</th>
<th>Ver</th>
<th>#Ports</th>
<th>Mrtrs</th>
<th>#Grps</th>
<th>#SGs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group1:BD-1</td>
<td>profile1</td>
<td>Y v2</td>
<td>8</td>
<td>2</td>
<td>5</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Group1:BD-2</td>
<td></td>
<td>N</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Group1:BD-3</td>
<td>profile1</td>
<td>Y v3</td>
<td>6</td>
<td>3</td>
<td>2</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Group1:BD-4</td>
<td></td>
<td>N</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Group1:BD-5</td>
<td>profile1</td>
<td>Y v3</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

The following example shows the summary line for a named bridge domain.

```
RP/0/RSP0/CPU0:router# show igmp snooping bridge-domain Group1:BD-1
```

<table>
<thead>
<tr>
<th>Bridge Domain</th>
<th>Profile</th>
<th>Act</th>
<th>Ver</th>
<th>#Ports</th>
<th>Mrtrs</th>
<th>#Grps</th>
<th>#SGs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group1:BD-1</td>
<td>profile1</td>
<td>Y v2</td>
<td>8</td>
<td>2</td>
<td>5</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

The following example shows detailed information about all bridge domains:

```
RP/0/RSP0/CPU0:router# show igmp snooping bridge-domain detail
```

<table>
<thead>
<tr>
<th>Bridge Domain</th>
<th>Profile</th>
<th>Act</th>
<th>Ver</th>
<th>#Ports</th>
<th>Mrtrs</th>
<th>#Grps</th>
<th>#SGs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1</td>
<td>1</td>
<td>Y v3</td>
<td>3</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

**Profile Configured Attributes:**
- System IP Address: 10.1.1.1
- Minimum Version: 2
- Report Suppression: Enabled
- Unsolicited Report Interval: 1000 (milliseconds)
- TCN Query Solicit: Disabled
- TCN Membership Sync: Disabled
- TCN Flood: Enabled
- TCN Flood Query Count: 2
- Router Alert Check: Enabled
- TTL Check: Enabled
- nV Mcast Offload: Enabled
- Internal Querier Support: Enabled
- Internal Querier Version: 3
- Internal Querier Timeout: 0 (seconds)
- Internal Querier Interval: 60 (seconds)
- Internal Querier Max Response Time: 10.0 (seconds)
- Internal Querier Robustness: 2
- Internal Querier TCN Query Interval: 10 (seconds)
- Internal Querier TCN Query Count: 2
- Internal Querier TCN Query MRT: 0 (seconds)
- Querier Query Interval: 60 (seconds)
- Querier LMQ Interval: 1000 (milliseconds)
- Querier LMQ Count: 2
- Querier Robustness: 2
- Startup Query Interval: 15 seconds
- Startup Query Count: 2
The following example displays traffic statistics with detailed information. The display omits many statistics whose values are zero.

```
RP/0/RSP0/CPU0:router# show igmp snooping bridge-domain Group1:BD-1 detail statistics
```

<table>
<thead>
<tr>
<th>Bridge Domain</th>
<th>Profile</th>
<th>Act</th>
<th>Ver</th>
<th>#Ports</th>
<th>#Mrtrs</th>
<th>#Grps</th>
<th>#SGs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group1:BD-1</td>
<td>profile1</td>
<td>Y</td>
<td>v2</td>
<td>8</td>
<td>2</td>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>

Profile Configured Attributes:
- System IP Address: 0.0.0.0
- Minimum Version: 2
- Report Suppression: Enabled
- TCN Query Solicit: Disabled
- TCN Flood: Enabled
- TCN Flood Query Count: 2
- TCN Membership Sync: Disabled
- ICCP Group Report Standby State: Disabled
- Router Alert Check: Enabled
- TTL Check: Enabled
- Unsolicted Report Interval: 1000 (milliseconds)
- Internal Querier Support: Disabled
- Querier Query Interval: 60 (seconds)
- Querier LMQ Interval: 1000 (milliseconds)
- Querier LMQ Count: 2
- Querier Robustness: 2
- Startup Query Interval: 15 seconds
- Startup Query Count: 2
- Startup Query Max Response Time: 10.0 seconds

Querier:
- IP Address: 192.1.1.10
- Port: GigabitEthernet0/2/0/10.1
- Version: v2
- Query Interval: 60 seconds
- Robustness: 2
- Max Resp Time: 1.0 seconds
- Time since last G-Query: 3 seconds
- Mrouter Ports: 2
- Dynamic: GigabitEthernet0/2/0/10.1
- Static: GigabitEthernet0/2/0/10.2
- STP Forwarding Ports: 0
Groups: 5
Member Ports: 9
V3 Source Groups: 0
Static/Include/Exclude: 0/0/0
Member Ports (Include/Exclude): 0/0
Traffic Statistics (elapsed time since last cleared 00:32:04):

<table>
<thead>
<tr>
<th>Received</th>
<th>Reinjected</th>
<th>Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages: 473</td>
<td>236</td>
<td>236</td>
</tr>
<tr>
<td>IGMP General Queries: 237</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IGMP Group Specific Queries: 0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IGMP G&amp;S Specific Queries: 0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IGMP V2 Reports: 236</td>
<td>236</td>
<td>236</td>
</tr>
<tr>
<td>IGMP V3 Reports: 0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IGMP V2 Leaves: 0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IGMP Global Leaves: 0</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>PIM Hellos: 0</td>
<td>0</td>
<td>-</td>
</tr>
</tbody>
</table>

Rx Packet Treatment:
- Packets Flooded: 0
- Packets Forwarded To Members: 0
- Packets Forwarded To Mrouters: 236
- Packets Consumed: 237

Rx Errors:
- None

Tx Errors:
- None

Startup Query Sync Statistics:
- None

ICCP Group Port Statistics (elapsed time since last cleared 01:21:27):
- Port Created Standby: 6
- Port Created Active: 1
- Port Goes Standby: 6
- Port Goes Active: 7

ICCP Traffic Statistics (elapsed time since last cleared 01:21:27):

Rx Messages:
- App State TLVs: 24006
- App State start of sync: 6
- App State end of sync: 6
- Request Sync TLVs: 2
- Port Membership TLVs: 24002
- Port Membership adds: 23966
- Port Membership removes: 8000
- Querier Info TLVs: 2

Rx Errors:
- App State sync TLVs ignored: 2

Tx Messages:
- App State replay attempts: 2
- Request Sync TLVs: 6
- Port Membership TLVs: 16651
- Port Membership adds: 16123
- Port Membership removes: 5543

Tx Errors:
- None

The following example shows details for all statistics regardless of whether their values are zero.

RP/0/RSP0/CP00:router# show igmp snooping bridge-domain Group1:BD-1 detail statistics include-zeroes

<table>
<thead>
<tr>
<th>Bridge Domain</th>
<th>Profile</th>
<th>Act</th>
<th>Ver</th>
<th>#Ports</th>
<th>#Mrtrs</th>
<th>#Grs</th>
<th>#SGs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group1:BD-1</td>
<td>profile1</td>
<td>Y</td>
<td>v2</td>
<td>8</td>
<td>2</td>
<td>5</td>
<td>0</td>
</tr>
</tbody>
</table>

Profile Configured Attributes:
<table>
<thead>
<tr>
<th>Configuration Item</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>System IP Address</td>
<td>0.0.0.0</td>
</tr>
<tr>
<td>Minimum Version</td>
<td>2</td>
</tr>
<tr>
<td>Report Suppression</td>
<td>Enabled</td>
</tr>
<tr>
<td>TCN Query Solicit</td>
<td>Disabled</td>
</tr>
<tr>
<td>TCN Flood</td>
<td>Enabled</td>
</tr>
<tr>
<td>TCN Flood Query Count</td>
<td>2</td>
</tr>
<tr>
<td>TCN Membership Sync</td>
<td>Disabled</td>
</tr>
<tr>
<td>ICCP Group Report Standby State</td>
<td>Disabled</td>
</tr>
<tr>
<td>Router Alert Check</td>
<td>Enabled</td>
</tr>
<tr>
<td>TTL Check</td>
<td>Enabled</td>
</tr>
<tr>
<td>Internal Querier Support</td>
<td>Disabled</td>
</tr>
<tr>
<td>Querier Query Interval</td>
<td>60 (seconds)</td>
</tr>
<tr>
<td>Querier LMQ Interval</td>
<td>1000 (milliseconds)</td>
</tr>
<tr>
<td>Querier LMQ Count</td>
<td>2</td>
</tr>
<tr>
<td>Querier Robustness</td>
<td>2</td>
</tr>
<tr>
<td>Querier:</td>
<td></td>
</tr>
<tr>
<td>IP Address</td>
<td>192.1.1.10</td>
</tr>
<tr>
<td>Port</td>
<td>GigabitEthernet0/2/0/10.1</td>
</tr>
<tr>
<td>Version</td>
<td>v2</td>
</tr>
<tr>
<td>Query Interval</td>
<td>60 seconds</td>
</tr>
<tr>
<td>Robustness</td>
<td>2</td>
</tr>
<tr>
<td>Max Resp Time</td>
<td>1.0 seconds</td>
</tr>
<tr>
<td>Time since last G-Query</td>
<td>3 seconds</td>
</tr>
<tr>
<td>Mrouter Ports</td>
<td>2</td>
</tr>
<tr>
<td>Dynamic</td>
<td>GigabitEthernet0/2/0/10.1</td>
</tr>
<tr>
<td>Static</td>
<td>GigabitEthernet0/2/0/10.2</td>
</tr>
<tr>
<td>STP Forwarding Ports</td>
<td>0</td>
</tr>
<tr>
<td>Groups</td>
<td>5</td>
</tr>
<tr>
<td>Member Ports</td>
<td>9</td>
</tr>
<tr>
<td>V3 Source Groups</td>
<td>0</td>
</tr>
<tr>
<td>Static/Include/Exclude</td>
<td>0/0/0</td>
</tr>
<tr>
<td>Member Ports (Include/Exclude)</td>
<td>0/0</td>
</tr>
<tr>
<td>Traffic Statistics (elapsed time since last cleared 00:32:52):</td>
<td></td>
</tr>
<tr>
<td>Messages</td>
<td></td>
</tr>
<tr>
<td>IGMP General Queries</td>
<td>243</td>
</tr>
<tr>
<td>IGMP Group Specific Queries</td>
<td>0</td>
</tr>
<tr>
<td>IGMP G&amp;S Specific Queries</td>
<td>0</td>
</tr>
<tr>
<td>IGMP V2 Reports</td>
<td>243</td>
</tr>
<tr>
<td>IGMP V3 Reports</td>
<td>0</td>
</tr>
<tr>
<td>IGMP V2 Leaves</td>
<td>0</td>
</tr>
<tr>
<td>IGMP Global Leaves</td>
<td>0</td>
</tr>
<tr>
<td>PIM Hellos</td>
<td>0</td>
</tr>
<tr>
<td>Rx Packet Treatment</td>
<td></td>
</tr>
<tr>
<td>Packets Flooded</td>
<td>0</td>
</tr>
<tr>
<td>Packets Forwarded To Members</td>
<td>0</td>
</tr>
<tr>
<td>Packets Forwarded To Mrouters</td>
<td>243</td>
</tr>
<tr>
<td>Packets Consumed</td>
<td>243</td>
</tr>
<tr>
<td>Reports Suppressed</td>
<td>0</td>
</tr>
<tr>
<td>IGMP Blocks Ignored in V2 Compat Mode</td>
<td>0</td>
</tr>
<tr>
<td>IGMP EX S-lists Ignored in V2 Compat Mode</td>
<td>0</td>
</tr>
<tr>
<td>Rx Errors</td>
<td></td>
</tr>
<tr>
<td>Packets On Inactive Bridge Domain</td>
<td>0</td>
</tr>
<tr>
<td>Packets On Inactive Port</td>
<td>0</td>
</tr>
<tr>
<td>Packets Martian</td>
<td>0</td>
</tr>
<tr>
<td>Packets Bad Protocol</td>
<td>0</td>
</tr>
<tr>
<td>Packets DA Not Multicast</td>
<td>0</td>
</tr>
<tr>
<td>Packets Missing Router Alert</td>
<td>0</td>
</tr>
<tr>
<td>Packets Missing Router Alert Drop</td>
<td>0</td>
</tr>
<tr>
<td>Packets Bad IGMP Checksum</td>
<td>0</td>
</tr>
<tr>
<td>Packets TTL Not One</td>
<td>0</td>
</tr>
<tr>
<td>Packets TTL Not One Drop</td>
<td>0</td>
</tr>
<tr>
<td>Queries Too Short</td>
<td>0</td>
</tr>
<tr>
<td>V1 Reports Too Short</td>
<td>0</td>
</tr>
</tbody>
</table>
The detail statistics display shows the following new bridge-domain counters:
show igmp snooping bridge-domain

RP/0/RSP0/CPU0:router#  show igmp snooping bridge-domain Group1:BD-1 detail statistics
#Access Group Permits
#Access Group Denials
#Group Limits Exceeded

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>clear igmp snooping bridge-domain, on page 246</td>
<td>Clears traffic counters at the bridge domain level.</td>
</tr>
</tbody>
</table>
show igmp snooping group

To display IGMP group membership information, use the `show igmp snooping group` command in EXEC mode.

```
/show igmp snooping group [summary [group-address] [{bridge-domain bridge-domain-name|port {interface-name|neighbor ipaddr pw-id id}]}][{group-address} [{bridge-domain bridge-domain-name|port {interface-name|neighbor ipaddr pw-id id}]}] [source source-address] [detail]]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>(Optional) Provides per group summary information.</td>
</tr>
<tr>
<td>group-address</td>
<td>(Optional) Provides IP group address information for the specified group in <code>A.B.C.D</code> format.</td>
</tr>
<tr>
<td>bridge-domain bridge-domain-name</td>
<td>(Optional) Provides group membership information for the specified bridge domain.</td>
</tr>
<tr>
<td>port interface-name</td>
<td>(Optional) Provides group membership information for the specified AC port.</td>
</tr>
<tr>
<td>port neighbor ipaddr pw-id id</td>
<td>(Optional) Provides group membership information for the specified PW port.</td>
</tr>
<tr>
<td>source source-address</td>
<td>(Optional) Provides group membership information for groups indicating interest in a specified source address.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Provides detailed information in a multiline display per group.</td>
</tr>
</tbody>
</table>

**Command Default**
None

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 5.2.2</td>
<td>The Bidirectional IGMP Snoop Sync feature enhancement enables the command to be run on both active and standby nodes.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command to display information about group membership in the Layer-2 forwarding tables. The display includes indicators identifying whether the group information was obtained dynamically (for example, snooped) or statically configured.

The command offers the following levels of detail:
- The basic command with no keywords displays group membership information as one line per port within group.
- The `summary` keyword summarizes the port statistics into one line per group. The `summary` keyword is mutually exclusive with the `port-view`, `source`, and `detail` keywords.
- The `detail` keyword includes traffic statistics and counters.

### Examples

The following example shows group membership information by groups within bridge domains.

```
RP/0/RSP0/CPU0:router# show igmp snooping group

Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, E=Explicit Tracking, R=Replicated

<table>
<thead>
<tr>
<th>Bridge Domain Group1:BD-1</th>
<th>Group</th>
<th>Ver</th>
<th>GM</th>
<th>Source</th>
<th>PM</th>
<th>Port</th>
<th>Exp</th>
<th>Flg</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>225.1.1.1</td>
<td>V2</td>
<td>-</td>
<td>-</td>
<td>GigabitEthernet0/2/0/10.1</td>
<td>-</td>
<td>never</td>
<td>S</td>
</tr>
<tr>
<td></td>
<td>238.1.1.1</td>
<td>V2</td>
<td>-</td>
<td>-</td>
<td>GigabitEthernet0/2/0/10.1</td>
<td>71</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>238.1.1.2</td>
<td>V2</td>
<td>-</td>
<td>-</td>
<td>GigabitEthernet0/2/0/10.5</td>
<td>103</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>238.1.1.2</td>
<td>V2</td>
<td>-</td>
<td>-</td>
<td>GigabitEthernet0/2/0/10.2</td>
<td>79</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>238.1.1.3</td>
<td>V2</td>
<td>-</td>
<td>-</td>
<td>GigabitEthernet0/2/0/10.6</td>
<td>111</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>238.1.1.3</td>
<td>V2</td>
<td>-</td>
<td>-</td>
<td>GigabitEthernet0/2/0/10.3</td>
<td>87</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>238.1.1.4</td>
<td>V2</td>
<td>-</td>
<td>-</td>
<td>GigabitEthernet0/2/0/10.8</td>
<td>63</td>
<td>D</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bridge Domain Group1:BD-3</th>
<th>Group</th>
<th>Ver</th>
<th>GM</th>
<th>Source</th>
<th>PM</th>
<th>Port</th>
<th>Exp</th>
<th>Flg</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>227.1.1.1</td>
<td>V3</td>
<td>EX</td>
<td>10.1.1.1</td>
<td>GigabitEthernet0/2/0/10.10</td>
<td>-</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>227.1.1.1</td>
<td>V3</td>
<td>EX</td>
<td>10.1.1.1</td>
<td>GigabitEthernet0/2/0/10.11</td>
<td>-</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>227.1.1.1</td>
<td>V3</td>
<td>EX</td>
<td>10.1.1.1</td>
<td>GigabitEthernet0/2/0/10.12</td>
<td>-</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>227.1.1.1</td>
<td>V3</td>
<td>EX</td>
<td>10.1.1.1</td>
<td>GigabitEthernet0/2/0/10.13</td>
<td>-</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>227.1.1.1</td>
<td>V3</td>
<td>EX</td>
<td>10.1.1.1</td>
<td>GigabitEthernet0/2/0/10.14</td>
<td>-</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>227.1.1.1</td>
<td>V3</td>
<td>EX</td>
<td>*</td>
<td>GigabitEthernet0/2/0/10.10</td>
<td>123</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>227.1.1.1</td>
<td>V3</td>
<td>EX</td>
<td>*</td>
<td>GigabitEthernet0/2/0/10.11</td>
<td>83</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>227.1.1.1</td>
<td>V3</td>
<td>EX</td>
<td>*</td>
<td>GigabitEthernet0/2/0/10.12</td>
<td>91</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>227.1.1.1</td>
<td>V3</td>
<td>EX</td>
<td>*</td>
<td>GigabitEthernet0/2/0/10.13</td>
<td>99</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>227.1.1.1</td>
<td>V3</td>
<td>EX</td>
<td>*</td>
<td>GigabitEthernet0/2/0/10.14</td>
<td>107</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>227.1.1.1</td>
<td>V3</td>
<td>EX</td>
<td>*</td>
<td>GigabitEthernet0/2/0/10.9</td>
<td>115</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>227.1.1.2</td>
<td>V3</td>
<td>EX</td>
<td>10.2.3.4</td>
<td>GigabitEthernet0/2/0/10.10</td>
<td>121</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>227.1.1.2</td>
<td>V3</td>
<td>EX</td>
<td>10.2.3.4</td>
<td>GigabitEthernet0/2/0/10.11</td>
<td>129</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>227.1.1.2</td>
<td>V3</td>
<td>EX</td>
<td>10.2.3.4</td>
<td>GigabitEthernet0/2/0/10.12</td>
<td>89</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>227.1.1.2</td>
<td>V3</td>
<td>EX</td>
<td>10.2.3.4</td>
<td>GigabitEthernet0/2/0/10.13</td>
<td>97</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>227.1.1.2</td>
<td>V3</td>
<td>EX</td>
<td>10.2.3.4</td>
<td>GigabitEthernet0/2/0/10.14</td>
<td>105</td>
<td>D</td>
<td></td>
</tr>
<tr>
<td></td>
<td>227.1.1.2</td>
<td>V3</td>
<td>EX</td>
<td>*</td>
<td>GigabitEthernet0/2/0/10.9</td>
<td>124</td>
<td>D</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Bridge Domain Group1:BD-5</th>
<th>Group</th>
<th>Ver</th>
<th>GM</th>
<th>Source</th>
<th>PM</th>
<th>Port</th>
<th>Exp</th>
<th>Flg</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>------</td>
<td>---</td>
<td>---</td>
<td>------</td>
<td>--</td>
<td>----</td>
<td>----</td>
<td>------</td>
</tr>
</tbody>
</table>
```
```
227.1.1.1  V3  EX  *  
EX  GigabitEthernet0/2/0/10.15  114  D
227.1.1.1  V3  EX  *  
EX  GigabitEthernet0/2/0/10.16  122  D

RP/0/RSP0/CPU0:router#  show igmp snooping group

Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, E=Explicit Tracking, R=Replicated

### Bridge Domain satellite:10

<table>
<thead>
<tr>
<th>Group</th>
<th>Ver</th>
<th>GM Source</th>
<th>Port</th>
<th>Exp</th>
<th>Flgs</th>
</tr>
</thead>
<tbody>
<tr>
<td>232.0.0.1</td>
<td>V3</td>
<td>IN 192.10.1.2</td>
<td>IN Gi100/0/0/22</td>
<td>129</td>
<td>D</td>
</tr>
<tr>
<td>232.0.0.1</td>
<td>V3</td>
<td>IN 192.10.1.2</td>
<td>IN Gi100/0/0/32</td>
<td>129</td>
<td>D</td>
</tr>
<tr>
<td>232.0.0.1</td>
<td>V3</td>
<td>IN 192.10.1.2</td>
<td>IN Gi200/0/0/34</td>
<td>129</td>
<td>D</td>
</tr>
</tbody>
</table>

### Bridge Domain satellite:20

<table>
<thead>
<tr>
<th>Group</th>
<th>Ver</th>
<th>GM Source</th>
<th>Port</th>
<th>Exp</th>
<th>Flgs</th>
</tr>
</thead>
<tbody>
<tr>
<td>232.0.0.1</td>
<td>V3</td>
<td>IN 192.10.1.2</td>
<td>IN Gi1200/0/0/23</td>
<td>129</td>
<td>D</td>
</tr>
<tr>
<td>232.0.0.1</td>
<td>V3</td>
<td>IN 192.10.1.2</td>
<td>IN Gi1200/0/0/25</td>
<td>129</td>
<td>D</td>
</tr>
<tr>
<td>232.0.0.1</td>
<td>V3</td>
<td>IN 192.10.1.2</td>
<td>IN Gi1300/0/0/34</td>
<td>129</td>
<td>D</td>
</tr>
</tbody>
</table>

For an active node:

```
RP/0/RSP0/CPU0:router#  show igmp snooping group debug
Fri Oct 10 08:41:45.968 UTC

Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, E=Explicit Tracking, R=Replicated

### Bridge Domain native:native

<table>
<thead>
<tr>
<th>Group</th>
<th>Ver</th>
<th>GM Source</th>
<th>Port</th>
<th>Exp</th>
<th>Flgs</th>
</tr>
</thead>
<tbody>
<tr>
<td>229.107.0.1</td>
<td>V3</td>
<td>IN 5.1.25.2</td>
<td>IN Gi100/0/0/10.7</td>
<td>79</td>
<td>D</td>
</tr>
<tr>
<td>229.107.0.1</td>
<td>V3</td>
<td>IN 5.1.25.2</td>
<td>IN Gi200/0/0/6.7</td>
<td>79</td>
<td>D</td>
</tr>
<tr>
<td>232.107.0.1</td>
<td>V3</td>
<td>IN 5.1.25.2</td>
<td>IN Gi100/0/0/10.7</td>
<td>79</td>
<td>D</td>
</tr>
<tr>
<td>232.107.0.1</td>
<td>V3</td>
<td>IN 5.1.25.2</td>
<td>IN Gi200/0/0/6.7</td>
<td>79</td>
<td>D</td>
</tr>
</tbody>
</table>

For a standby node:

```
RP/0/RSP0/CPU0:router#  show igmp snooping group debug
Fri Oct 10 09:36:55.146 UTC

Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, E=Explicit Tracking, R=Replicated

### Bridge Domain native:native

<table>
<thead>
<tr>
<th>Group</th>
<th>Ver</th>
<th>GM Source</th>
<th>Port</th>
<th>Exp</th>
<th>Flgs</th>
</tr>
</thead>
<tbody>
<tr>
<td>229.107.0.1</td>
<td>V3</td>
<td>IN 5.1.25.2</td>
<td>IN Gi100/0/0/10.7</td>
<td>11</td>
<td>DR</td>
</tr>
<tr>
<td>229.107.0.1</td>
<td>V3</td>
<td>IN 5.1.25.2</td>
<td>IN Gi200/0/0/6.7</td>
<td>11</td>
<td>DR</td>
</tr>
<tr>
<td>232.107.0.1</td>
<td>V3</td>
<td>IN 5.1.25.2</td>
<td>IN Gi100/0/0/10.7</td>
<td>11</td>
<td>DR</td>
</tr>
<tr>
<td>232.107.0.1</td>
<td>V3</td>
<td>IN 5.1.25.2</td>
<td>IN Gi200/0/0/6.7</td>
<td>11</td>
<td>DR</td>
</tr>
</tbody>
</table>

The following example shows group membership information by group within a specific bridge domain.

```
RP/0/RSP0/CPU0:router#  show igmp snooping group bridge-domain Group1:BD-1
```
Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, E=Explicit Tracking, R=Replicated

Bridge Domain Group1:BD-1

<table>
<thead>
<tr>
<th>Group</th>
<th>Ver</th>
<th>GM Source</th>
<th>PM Port</th>
<th>Exp</th>
<th>Flg</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.1.1.1</td>
<td>V2</td>
<td>-</td>
<td>GigabitEthernet0/2/0/10.1</td>
<td>never</td>
<td>S</td>
</tr>
<tr>
<td>238.1.1.1</td>
<td>V2</td>
<td>-</td>
<td>GigabitEthernet0/2/0/10.1</td>
<td>84 D</td>
<td></td>
</tr>
<tr>
<td>238.1.1.1</td>
<td>V2</td>
<td>-</td>
<td>GigabitEthernet0/2/0/10.5</td>
<td>116 D</td>
<td></td>
</tr>
<tr>
<td>238.1.1.2</td>
<td>V2</td>
<td>-</td>
<td>GigabitEthernet0/2/0/10.2</td>
<td>92 D</td>
<td></td>
</tr>
<tr>
<td>238.1.1.2</td>
<td>V2</td>
<td>-</td>
<td>GigabitEthernet0/2/0/10.6</td>
<td>60 D</td>
<td></td>
</tr>
<tr>
<td>238.1.1.3</td>
<td>V2</td>
<td>-</td>
<td>GigabitEthernet0/2/0/10.7</td>
<td>88 D</td>
<td></td>
</tr>
<tr>
<td>238.1.1.4</td>
<td>V2</td>
<td>-</td>
<td>GigabitEthernet0/2/0/10.4</td>
<td>76 D</td>
<td></td>
</tr>
<tr>
<td>238.1.1.4</td>
<td>V2</td>
<td>-</td>
<td>GigabitEthernet0/2/0/10.8</td>
<td>76 D</td>
<td></td>
</tr>
</tbody>
</table>

The following example shows group membership information by groups within a specific port.

RP/0/RSP0/CPU0:router# show igmp snooping group port GigabitEthernet 0/2/0/10.10

Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, E=Explicit Tracking, R=Replicated

Bridge Domain Group1:BD-3

<table>
<thead>
<tr>
<th>Group</th>
<th>Ver</th>
<th>GM Source</th>
<th>PM Port</th>
<th>Exp</th>
<th>Flg</th>
</tr>
</thead>
<tbody>
<tr>
<td>227.1.1.1</td>
<td>V3</td>
<td>EX 10.1.1.1</td>
<td>EX GigabitEthernet0/2/0/10.10</td>
<td>-</td>
<td>D</td>
</tr>
<tr>
<td>227.1.1.1</td>
<td>V3</td>
<td>*</td>
<td>EX GigabitEthernet0/2/0/10.10</td>
<td>111 D</td>
<td></td>
</tr>
<tr>
<td>227.1.1.2</td>
<td>V3</td>
<td>EX 10.2.3.4</td>
<td>IN GigabitEthernet0/2/0/10.10</td>
<td>109 D</td>
<td></td>
</tr>
</tbody>
</table>

The following example summarizes each group's membership information into a single line.

RP/0/RSP0/CPU0:router# show igmp snooping group summary

Bridge Domain Group1:BD-1

<table>
<thead>
<tr>
<th>Group</th>
<th>Source</th>
<th>#Mem</th>
<th>#Inc</th>
<th>#Exc</th>
</tr>
</thead>
<tbody>
<tr>
<td>225.1.1.1</td>
<td>-</td>
<td>1</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>238.1.1.1</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>238.1.1.2</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>238.1.1.3</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>238.1.1.4</td>
<td>-</td>
<td>2</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Bridge Domain Group1:BD-3

<table>
<thead>
<tr>
<th>Group</th>
<th>Source</th>
<th>#Mem</th>
<th>#Inc</th>
<th>#Exc</th>
</tr>
</thead>
<tbody>
<tr>
<td>227.1.1.1</td>
<td>10.1.1.1</td>
<td>0</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>227.1.1.1</td>
<td>*</td>
<td>6</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>227.1.1.2</td>
<td>10.2.3.4</td>
<td>5</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>227.1.1.2</td>
<td>*</td>
<td>1</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>227.1.1.2</td>
<td>*</td>
<td>1</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Bridge Domain Group1:BD-5

<table>
<thead>
<tr>
<th>Group</th>
<th>Source</th>
<th>#Mem</th>
<th>#Inc</th>
<th>#Exc</th>
</tr>
</thead>
</table>
The following example shows detail information about each group.

```
RP/0/RSP0/CPU0# router# show igmp snooping group detail
Bridge Domain Group1:BD-1

Group Address: 225.1.1.1
Version: V2
Uptime: 00:42:13
Port Count: 1
  GigabitEthernet0/2/0/10.1:
    Uptime: 00:42:13
    Persistence: static
    Expires: never

Group Address: 238.1.1.1
Version: V2
Uptime: 00:41:38
Port Count: 2
  GigabitEthernet0/2/0/10.1:
    Uptime: 00:41:38
    Persistence: dynamic
    Expires: 119
  GigabitEthernet0/2/0/10.5:
    Uptime: 00:41:06
    Persistence: dynamic
    Expires: 87

Group Address: 238.1.1.2
Version: V2
Uptime: 00:41:30
Port Count: 2
  GigabitEthernet0/2/0/10.2:
    Uptime: 00:41:30
    Persistence: dynamic
    Expires: 63
  GigabitEthernet0/2/0/10.6:
    Uptime: 00:40:58
    Persistence: dynamic
    Expires: 95

Group Address: 238.1.1.3
Version: V2
Uptime: 00:41:22
Port Count: 2
  GigabitEthernet0/2/0/10.3:
    Uptime: 00:41:22
    Persistence: dynamic
    Expires: 71
  GigabitEthernet0/2/0/10.7:
    Uptime: 00:40:50
    Persistence: dynamic
    Expires: 103

Group Address: 238.1.1.4
Version: V2
Uptime: 00:41:14
Port Count: 2
  GigabitEthernet0/2/0/10.4:
    Uptime: 00:41:14
    Persistence: dynamic
    Expires: 79
  GigabitEthernet0/2/0/10.8:
    Uptime: 00:40:42
```
show igmp snooping group

Persistence: dynamic
Expires: 111

Bridge Domain bg1:bg1_bd1

Group Address: 225.0.0.1
Version: V3
Uptime: 01:47:00
Group Filter Mode: Exclude
Source: (
Exclude Port Count: 1

Bundle-Ether10
ICCP Group: 1
Redundancy State: Active
Uptime: 01:47:00
Persistence: dynamic
Expires: 197

Bridge Domain Group1:BD-3

Group Address: 227.1.1.1
Version: V3
Uptime: 00:41:35
Group Filter Mode: Exclude
Source Count: 1
Static/Include/Exclude Source Count: 0/0/1
Source: 10.1.1.1
Static/Include/Exclude Port Count: 0/0/6
Exclude Port Count: 6

GigabitEthernet0/2/0/10.10:
Uptime: 00:41:27
Persistence: dynamic
Expires: -

GigabitEthernet0/2/0/10.11:
Uptime: 00:41:19
Persistence: dynamic
Expires: -

GigabitEthernet0/2/0/10.12:
Uptime: 00:41:11
Persistence: dynamic
Expires: -

GigabitEthernet0/2/0/10.13:
Uptime: 00:41:03
Persistence: dynamic
Expires: -

GigabitEthernet0/2/0/10.14:
Uptime: 00:40:55
Persistence: dynamic
Expires: -

GigabitEthernet0/2/0/10.9:
Uptime: 00:41:35
Persistence: dynamic
Expires: -
Source: *
Exclude Port Count: 6

GigabitEthernet0/2/0/10.10
Uptime: 00:41:27
Persistence: dynamic
Expires: 91

GigabitEthernet0/2/0/10.11
Uptime: 00:41:19
Persistence: dynamic
Expires: 99

GigabitEthernet0/2/0/10.12
Uptime: 00:41:11
show igmp snooping group

Persistence: dynamic
Expires: 107
GigabitEthernet0/2/0/10.13
Uptime: 00:41:03
Persistence: dynamic
Expires: 115
GigabitEthernet0/2/0/10.14
Uptime: 00:40:55
Persistence: dynamic
Expires: 123
GigabitEthernet0/2/0/10.9
Uptime: 00:41:35
Persistence: dynamic
Expires: 83
Group Address: 227.1.1.2
Version: V3
Uptime: 00:41:37
Group Filter Mode: Exclude
Source Count: 1
Static/Include/Exclude Source Count: 0/1/0
Source: 10.2.3.4
Static/Include/Exclude Port Count: 0/5/0
Include Port Count: 5
GigabitEthernet0/2/0/10.10
Uptime: 00:41:29
Persistence: dynamic
Expires: 89
GigabitEthernet0/2/0/10.11
Uptime: 00:41:21
Persistence: dynamic
Expires: 97
GigabitEthernet0/2/0/10.12
Uptime: 00:41:13
Persistence: dynamic
Expires: 105
GigabitEthernet0/2/0/10.13
Uptime: 00:41:05
Persistence: dynamic
Expires: 113
GigabitEthernet0/2/0/10.14
Uptime: 00:40:57
Persistence: dynamic
Expires: 121
Source: *
Exclude Port Count: 1
GigabitEthernet0/2/0/10.9
Uptime: 00:41:34
Persistence: dynamic
Expires: 124

Bridge Domain Group1:BD-5

Group Address: 227.1.1.1
Version: V3
Uptime: 00:41:36
Group Filter Mode: Exclude
Source: *
Exclude Port Count: 2
GigabitEthernet0/2/0/10.15
Uptime: 00:41:36
Persistence: dynamic
Expires: 114
GigabitEthernet0/2/0/10.16
Uptime: 00:41:28
Persistence: dynamic
Expires: 122

If a group limit is configured on an output port, the detail display shows the group weight value associated with each group or source group on that port:

RP/0/RSP0/CPU0:router1# show igmp snooping port group detail

Bridge Domain bg1:bg1_bd1

Group Address: 225.0.0.1
Version: V3
Uptime: 01:43:25
Group Filter Mode: Exclude
Source:
Exclude Port Count: 1
Bundle-Ether10
ICCP Group: 1
Redundancy State: Active
Uptime: 01:43:25
Persistences: dynamic
Expires: 249

RP/0/RSP0/CPU0:router2# show igmp snooping group detail

Bridge Domain bg1:bg1_bd1

Group Address: 225.0.0.1
Version: V3
Uptime: 01:43:25
Group Filter Mode: Exclude
Source:
Exclude Port Count: 1
Bundle-Ether10
ICCP Group: 1
Redundancy State: Standby
Uptime: 01:43:25
Persistences: dynamic
Expires: 249

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear igmp snooping group, on page 248</td>
<td>Clears group states.</td>
</tr>
</tbody>
</table>
show igmp snooping port

To display IGMP snooping configuration information and traffic counters by router interface port, use the **show igmp snooping port** command in EXEC mode.

```
show igmp snooping port
interface-name [neighbor ipaddr] [pw-id] id [bridge-domain] [bridge-domain-name]
detail [statistics [include-zeroes]]
group [group-address] [source source-address] [detail]
```

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface-name</td>
<td>(Optional) Displays information only for the specified AC port.</td>
</tr>
<tr>
<td>neighbor ipaddr pw-id id</td>
<td>(Optional) Displays information only for the specified PW port.</td>
</tr>
<tr>
<td>bridge-domain bridge-domain-name</td>
<td>(Optional) Displays information for ports in the specified bridge domain.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Includes port details, rather than a single line summary.</td>
</tr>
<tr>
<td>statistics</td>
<td>(Optional) Includes IGMP traffic counters and statistics in the detail display.</td>
</tr>
<tr>
<td>include-zeroes</td>
<td>(Optional) Includes all statistics, even if they are zero. Without this keyword, many statistics are omitted from the display when their values are zero.</td>
</tr>
<tr>
<td>group</td>
<td>(Optional) Provides group membership information in its entirety as received at each port. The display is organized by port, showing groups within ports.</td>
</tr>
<tr>
<td>group-address</td>
<td>(Optional) Displays information only for the specified group address, organized by port.</td>
</tr>
<tr>
<td>source source-address</td>
<td>(Optional) Displays information only for the specified source address, organized by port.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Includes group details.</td>
</tr>
</tbody>
</table>

### Command Default

None

### Command Modes

EXEC

### Command History

**Release** | **Modification**
---|---
Release 3.7.2 | This command was introduced.
Release 3.9.0 | The total group weight accumulated by all groups and source groups on the port, the configured limit, access group permits, access group denials, and group limits exceeded fields were added to the detail display output.
Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command displays IGMP snooping information organized by IGMP snooping port. Use the command without any keywords to display summary information about all ports, in a single line per port.

Use optional arguments and keywords to request the following:

- Limit the display to a specified port.
- Limit the display to ports under a specified bridge.
- Request details and traffic statistics per port.

Note

The statistics keyword cannot be used in the same command with the group keyword.

- Organize the display by group within ports. Use the group keyword with or without a specified interface or bridge domain.
- Limit the group information to specific groups or source addresses.

The statistics keyword displays IGMP traffic information, including IGMP queries, reports, and leaves. The three columns in the statistics section of the display are:

- Received—Number of packets received.
- Reinjected—Number of packets received, processed, and reinjected back into the forwarding path.
- Generated—Number of packets generated by the IGMP snooping application and injected into the forwarding path.

Examples

The following example shows summary information per port:

```
RP/0/RSP0/CPU0:router# show igmp snooping port

Bridge Domain bg1:bd1

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Oper</th>
<th>STP</th>
<th>Red</th>
<th>#Grps</th>
<th>#SGs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bundle-Ether10</td>
<td></td>
<td>Up</td>
<td>S</td>
<td>1</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>Neighbor 40.40.40.40</td>
<td>Up</td>
<td>-</td>
<td>-</td>
<td>4</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>
```

The following example shows summary information for a specific port.

```
RP/0/RSP0/CPU0:router# show igmp snooping port GigabitEthernet 0/1/0/3.215

Bridge Domain 215:215

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Oper</th>
<th>STP</th>
<th>Red</th>
<th>#Grps</th>
<th>#SGs</th>
</tr>
</thead>
</table>
```
The following example shows detail information about a specified port.

```
RP/0/RSP0/CPU0:router# show igmp snooping port Bundle-Ether10 detail

Bundle-Ether10 is Up
Bridge Domain: bg1:bg1_bd1
ICCP Group: 1
Redundancy State: Active since Thu Aug 26 12:52:37 2010
IGMP Snoo Profile: profile2
 Dynamic Mrouter Port: Querier(192.1.1.10)
 Expires: 116 seconds
IGMP Groups: 2
 Static/Dynamic: 1/1
IGMP Source Groups: 0
 Static/Include/Exclude: 0/0/0
Admitted Weight: 1/(no limit)
```

The following example shows detail information that includes the total group weight accumulated by all groups and source groups on the port and the configured limit—Admitted Weight: 12/16:

```
RP/0/RSP0/CPU0:router# show igmp snooping port gigabitEthernet 0/2/0/10.2 detail

GigabitEthernet0/2/0/10.2 is Up
Bridge Domain: bg1:bd1
IGMP Groups: 4
Static/Dynamic: 0/4
IGMP Source Groups: 0
Static/Include/Exclude: 0/0/0
Admitted Weight: 33/36
```

The following example shows detail, including statistics, for a specified port.

```
RP/0/RSP0/CPU0:router# show igmp snooping port GigabitEthernet 0/2/0/10.1 detail statistics

GigabitEthernet0/2/0/10.1 is Up
Bridge Domain: Group1:BD-1
IGMP Snoo Profile: profile2
 Dynamic Mrouter Port: Querier(192.1.1.10)
 Expires: 117 seconds
IGMP Groups: 2
 Static/Dynamic: 1/1
IGMP Source Groups: 0
 Static/Include/Exclude: 0/0/0
Access Group Permits
Access Group Denials
Group Limits Exceeded

Traffic Statistics (elapsed time since last cleared 01:19:32):
Received 668 75 0
```

---

GigabitEthernet0/1/0/3.215

Up - - 1 0
The following example shows all statistics, even those with zero values, for a specified port.

```
RP/0/RSP0/CPU0:router# show igmp snooping port GigabitEthernet 0/2/0/10.1 detail statistics include-zeroes
```

GigabitEthernet0/2/0/10.1 is Up
Bridge Domain: Group1:BD-1
IGMP Snoop Profile: profile2
Dynamic Mrouter Port: Querier(192.1.1.10)
Expires: 120 seconds
IGMP Groups: 2
Static/Dynamic: 1/1
IGMP Source Groups: 0
Static/Include/Exclude: 0/0/0
Traffic Statistics (elapsed time since last cleared 01:20:42):

<table>
<thead>
<tr>
<th></th>
<th>Received</th>
<th>Rejected</th>
<th>Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>IGMP General Queries</td>
<td>602</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IGMP Group Specific Queries</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IGMP G&amp;S Specific Queries</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IGMP V2 Reports</td>
<td>76</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IGMP V3 Reports</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IGMP V2 Leaves</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IGMP Global Leaves</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PIM Hellos</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
</tbody>
</table>

Rx Packet Treatment:
- Packets Flooded: 0
- Packets Forwarded To Members: 0
- Packets Forwarded To Mrouters: 76
- Packets Consumed: 602

Reports Suppressed: 0
IGMP Blocks Ignored in V2 Compat Mode: 0
IGMP EX S-lists Ignored in V2 Compat Mode: 0

Rx Errors:
- Packets On Inactive Bridge Domain: 0
- Packets On Inactive Port: 0
- Packets Martian: 0
- Packets Bad Protocol: 0
- Packets DA Not Multicast: 0
- Packets Missing Router Alert: 0
- Packets Missing Router Alert Drop: 0
- Packets Bad IGMP Checksum: 0
- Packets TTL Not One: 0
- Packets TTL Not One Drop: 0
- Queries Too Short: 0
- V1 Reports Too Short: 0
The following information shows summary information for all port groups under a specific bridge domain.

```
show igmp snooping port bridge-domain Group1:BD-1 group
```

Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, E=Explicit Tracking, R=Replicated

<table>
<thead>
<tr>
<th>Port</th>
<th>PM Group</th>
<th>Ver GM</th>
<th>Source</th>
<th>Exp</th>
<th>Flg</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/2/0/10.1</td>
<td>225.1.1.1</td>
<td>V2</td>
<td>-</td>
<td>never</td>
<td>S</td>
</tr>
<tr>
<td>GigabitEthernet0/2/0/10.1</td>
<td>238.1.1.1</td>
<td>V2</td>
<td>-</td>
<td>77</td>
<td>D</td>
</tr>
<tr>
<td>GigabitEthernet0/2/0/10.2</td>
<td>238.1.1.2</td>
<td>V2</td>
<td>-</td>
<td>85</td>
<td>D</td>
</tr>
<tr>
<td>GigabitEthernet0/2/0/10.3</td>
<td>238.1.1.3</td>
<td>V2</td>
<td>-</td>
<td>93</td>
<td>D</td>
</tr>
<tr>
<td>GigabitEthernet0/2/0/10.4</td>
<td>238.1.1.4</td>
<td>V2</td>
<td>-</td>
<td>101</td>
<td>D</td>
</tr>
<tr>
<td>GigabitEthernet0/2/0/10.5</td>
<td>238.1.1.1</td>
<td>V2</td>
<td>-</td>
<td>109</td>
<td>D</td>
</tr>
<tr>
<td>GigabitEthernet0/2/0/10.6</td>
<td>238.1.1.2</td>
<td>V2</td>
<td>-</td>
<td>117</td>
<td>D</td>
</tr>
<tr>
<td>GigabitEthernet0/2/0/10.7</td>
<td>238.1.1.3</td>
<td>V2</td>
<td>-</td>
<td>61</td>
<td>D</td>
</tr>
<tr>
<td>GigabitEthernet0/2/0/10.8</td>
<td>238.1.1.4</td>
<td>V2</td>
<td>-</td>
<td>69</td>
<td>D</td>
</tr>
</tbody>
</table>

The following information shows detail information for all port groups under a specific bridge domain.

```
show igmp snooping port bridge-domain Group1:BD-1 group detail
```

Bridge Domain Group1:BD-1

```
<table>
<thead>
<tr>
<th>Port</th>
<th>PM Group</th>
<th>Ver GM</th>
<th>Source</th>
<th>Exp</th>
<th>Flg</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/2/0/10.1</td>
<td>225.1.1.1</td>
<td>V2</td>
<td>-</td>
<td>never</td>
<td>S</td>
</tr>
<tr>
<td>GigabitEthernet0/2/0/10.1</td>
<td>238.1.1.1</td>
<td>V2</td>
<td>-</td>
<td>77</td>
<td>D</td>
</tr>
<tr>
<td>GigabitEthernet0/2/0/10.2</td>
<td>238.1.1.2</td>
<td>V2</td>
<td>-</td>
<td>85</td>
<td>D</td>
</tr>
<tr>
<td>GigabitEthernet0/2/0/10.3</td>
<td>238.1.1.3</td>
<td>V2</td>
<td>-</td>
<td>93</td>
<td>D</td>
</tr>
<tr>
<td>GigabitEthernet0/2/0/10.4</td>
<td>238.1.1.4</td>
<td>V2</td>
<td>-</td>
<td>101</td>
<td>D</td>
</tr>
<tr>
<td>GigabitEthernet0/2/0/10.5</td>
<td>238.1.1.1</td>
<td>V2</td>
<td>-</td>
<td>109</td>
<td>D</td>
</tr>
<tr>
<td>GigabitEthernet0/2/0/10.6</td>
<td>238.1.1.2</td>
<td>V2</td>
<td>-</td>
<td>117</td>
<td>D</td>
</tr>
<tr>
<td>GigabitEthernet0/2/0/10.7</td>
<td>238.1.1.3</td>
<td>V2</td>
<td>-</td>
<td>61</td>
<td>D</td>
</tr>
<tr>
<td>GigabitEthernet0/2/0/10.8</td>
<td>238.1.1.4</td>
<td>V2</td>
<td>-</td>
<td>69</td>
<td>D</td>
</tr>
</tbody>
</table>
```
Port: GigabitEthernet0/2/0/10.1
  Group Address: 225.1.1.1
  Version: V2
  Uptime: 01:27:20
  Persistence: static
  Expires: never
Port: GigabitEthernet0/2/0/10.2
  Group Address: 238.1.1.2
  Version: V2
  Uptime: 01:26:45
  Persistence: dynamic
  Expires: 100
Port: GigabitEthernet0/2/0/10.3
  Group Address: 238.1.1.3
  Version: V2
  Uptime: 01:26:37
  Persistence: dynamic
  Expires: 108
Port: GigabitEthernet0/2/0/10.4
  Group Address: 238.1.1.4
  Version: V2
  Uptime: 01:26:21
  Persistence: dynamic
  Expires: 116
Port: GigabitEthernet0/2/0/10.5
  Group Address: 238.1.1.1
  Version: V2
  Uptime: 01:26:13
  Persistence: dynamic
  Expires: 60
Port: GigabitEthernet0/2/0/10.6
  Group Address: 238.1.1.2
  Version: V2
  Uptime: 01:26:05
  Persistence: dynamic
  Expires: 68
Port: GigabitEthernet0/2/0/10.7
  Group Address: 238.1.1.3
  Version: V2
  Uptime: 01:25:57
  Persistence: dynamic
  Expires: 84
Port: GigabitEthernet0/2/0/10.8
  Group Address: 238.1.1.4
  Version: V2
  Uptime: 01:25:49
  Persistence: dynamic
  Expires: 92

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear igmp snooping port, on page 250</td>
<td>Clears traffic counters at the port level.</td>
</tr>
</tbody>
</table>
show igmp snooping profile

To display IGMP snooping profile information, use the `show igmp snooping profile` command in EXEC mode.

```
show igmp snooping profile [summary][[profile-name] [detail [include-defaults]] [references [bridge-domain [bridge-domain-name]]] port [interface-name] [neighbor ipaddr pw-id id]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>(Optional) Displays a summary of profile instances, bridge domain references, and port references.</td>
</tr>
<tr>
<td>profile-name</td>
<td>(Optional) Displays information only for the named profile.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays the contents of profiles.</td>
</tr>
<tr>
<td>include-defaults</td>
<td>(Optional) Displays all default configurations with the profile contents. Without this keyword, only configured profile information is displayed.</td>
</tr>
<tr>
<td>references</td>
<td>(Optional) Shows which bridge domains and bridge ports reference each profile.</td>
</tr>
<tr>
<td>bridge-domain</td>
<td>(Optional) Provides a bridge domain filter for the references keyword. Without bridge-domain-name, the display shows profiles attached to all bridge domains. With bridge-domain-name, the display shows only the profile attached to the specified bridge domain.</td>
</tr>
<tr>
<td>port</td>
<td>(Optional) Provides a port filter for the references keyword.</td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>port</td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 3.9.0</td>
<td>New fields were added to the detail display to show access-group, group limit, and TCN flood parameters.</td>
</tr>
<tr>
<td>Release 4.0.0</td>
<td>New fields were added to the detail display to show ICCP Group statistics, and Startup Query parameters.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to display the contents of profiles and to see associations of profiles with bridge-domains and ports.
The `summary` keyword lists profile names and summarizes their usage on bridge domains and ports. No other keywords can be used with `summary`.

Use the `details` keyword with a profile name to show the contents of a specific profile. Without a profile name, the `detail` keyword shows the contents of all profiles.

Use the `references` keyword to list the relationships between profiles and bridge domains or profiles and ports. You have the following options:

- Use the `references` keyword without any other keywords to show all profiles and the ports and bridge domains they are attached to.
- Use the `references` keyword with the `name` keyword to show a specific profile and where it is attached.
- Use the `port` keyword to list all ports and the profiles attached to them.
- Use the `port` keyword with a specific AC interface or PW to see the profile attached to the named port.
- Use the `bridge-domain` keyword to list all bridge domains and the profiles attached to them.
- Use the `bridge-domain` keyword with a specific bridge domain name to see the profile attached to a specific bridge domain.

### Examples

The following example lists profile names and shows summary level profile usage.

```
RP/0/RSP0/CPU0:router# show igmp snooping profile

<table>
<thead>
<tr>
<th>Profile</th>
<th>Bridge Domain</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile1</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>profile2</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>profile3</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
```

The following example shows summary level profile usage for a named profile.

```
RP/0/RSP0/CPU0:router# show igmp snooping profile profile1

<table>
<thead>
<tr>
<th>Profile</th>
<th>Bridge Domain</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile1</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>
```

The following example shows the contents of each profile.

```
RP/0/RSP0/CPU0:router# show igmp snooping profile detail

IGMP Snoop Profile profile1:

  Bridge Domain References: 3
  Port References: 0

IGMP Snoop Profile profile2:

  Static Groups: 225.1.1.1
  Bridge Domain References: 0
  Port References: 1
```
IGMP Snoop Profile profile3:

Static Mrouter: Enabled

Bridge Domain References: 0
Port References: 1

The following example shows output reflecting the access-group, group limit, and tcn flood disable parameters:

RP/0/RSP0/CPU0:router# show igmp snooping profile detail

IGMP Snoop Profile profile:

Querier LMQ Count: 2

Access Group ACL: iptv-white-list
Group Policy: iptv-group-weights
Group Limit: 16
Immediate Leave: Enabled
TCN Flood: Disabled

Bridge Domain References: 1
Port References: 0

The following example shows the contents of a named profile. In this example, the profile is empty.

RP/0/RSP0/CPU0:router# show igmp snooping profile profile1 detail

IGMP Snoop Profile profile1:

Bridge Domain References: 3
Port References: 0

The following example shows the contents of a named profile and the implied default configurations:

RP/0/RSP0/CPU0:router# show igmp snooping profile profile1 detail include-defaults

IGMP Snoop Profile profile p1:

System IP Address: 10.144.144.144
Minimum Version: 2
Report Suppression: Enabled
Unsolicited Report Interval: 1000 (milliseconds)
TCN Query Solicit: Enabled
TCN Membership Sync: Disabled
TCN Flood: Enabled
TCN Flood Query Count: 2
Router Alert Check: Disabled
TTL Check: Disabled

Internal Querier Support: Enabled
Internal Querier Version: 3
Internal Querier Timeout: 0 (seconds)
Internal Querier Interval: 60 (seconds)
Internal Querier Max Response Time: 10 (seconds)
Internal Querier TCN Query Interval: 10 (seconds)
Internal Querier TCN Query Count: 2
Internal Querier TCN Query MRT: 0
Internal Querier Robustness: 2
show igmp snooping profile

Querier Query Interval: 60 (seconds)
Querier LMQ Interval: 1000 (milliseconds)
Querier LMQ Count: 2
Querier Robustness: 2
Immediate Leave: Disabled
Explicit Tracking: Disabled
Static Mrouter: Disabled
Router Guard: Disabled
Access Group ACL: (empty)
Group Policy:
  Group Limit: -1
ICCP Group Report Standby State: Enabled
Startup Query Interval: 15 (seconds)
Startup Query Count: 2
Startup Query Max Response Time: 10 (seconds)
Startup Query on Port Up: Enabled
Startup Query on IG Port Active: Disabled
Startup Query on Topology Change: Disabled
Startup Query on Process Start: Disabled
Bridge Domain References: 1
Port References: 0

The following command shows a summary of profile usage, by profile name.

RP/0/RSP0/CPU0:router# show igmp snooping profile summary
  Number of profiles: 3
  Number of bridge domain references: 3
  Number of port references: 2

The following command lists all IGMP snooping profiles and shows which bridge domains and ports are configured to use each profile.

RP/0/RSP0/CPU0:router# show igmp snooping profile references

Profile: profile1
  Bridge Domains:
    Group1:BD-5
    Group1:BD-3
    Group1:BD-1
  No Port References

Profile: profile2
  No Bridge Domain References
  Ports: GigabitEthernet0/2/0/10.1

Profile: profile3
  No Bridge Domain References
  Ports: GigabitEthernet0/2/0/10.2

The following command lists all bridges or ports that are configured to use the profile named profile1.

RP/0/RSP0/CPU0:router# show igmp snooping profile profile1 references

Profile: profile1
  Bridge Domains: None
The following example shows the profile attached to a specific bridge domain.

```
RP/0/RSP0/CPU0:router# show igmp snooping profile references bridge-domain Group1:BD-1
Profile:   profile1
Bridge Domains: Group1:BD-1
```

The following example shows the profile attached to a specific port.

```
RP/0/RSP0/CPU0:router# show igmp snooping profile references port GigabitEthernet 0/2/0/10.1
Profile:   profile2
Ports:      GigabitEthernet0/2/0/10.1
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile.</td>
</tr>
<tr>
<td>show l2vpn forwarding bridge-domain mroute, on page 342</td>
<td>Shows profile names associated with the bridge domain and its ports.</td>
</tr>
</tbody>
</table>
**show igmp snooping redundancy**

To display IGMP snooping redundancy information, use the `show igmp snooping redundancy` command in EXEC mode.

```
{show igmp snooping redundancy iccp[profile-name] [detail [include-defaults]] [references [bridge-domain [bridge-domain-name]]] [port [interface-name|neighbor ipaddr pw-id id]]}
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>iccp</td>
<td>Displays ICCP redundancy information.</td>
</tr>
<tr>
<td>profile-name</td>
<td>(Optional) Displays information only for the named profile.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays the contents of profiles.</td>
</tr>
<tr>
<td>include-defaults</td>
<td>(Optional) Displays all default configurations with the profile contents. Without this keyword, only configured profile information is displayed.</td>
</tr>
<tr>
<td>references</td>
<td>(Optional) Shows which bridge domains and bridge ports reference each profile.</td>
</tr>
<tr>
<td>bridge-domain</td>
<td>(Optional) Provides a bridge domain filter for the references keyword. Without <code>bridge-domain-name</code>, the display shows profiles attached to all bridge domains. With <code>bridge-domain-name</code>, the display shows only the profile attached to the specified bridge domain.</td>
</tr>
<tr>
<td>[bridge-domain-name]</td>
<td></td>
</tr>
<tr>
<td>port</td>
<td>(Optional) Provides a port filter for the references keyword.</td>
</tr>
<tr>
<td>[interface-name]</td>
<td></td>
</tr>
<tr>
<td>or</td>
<td></td>
</tr>
<tr>
<td>port [neighbor ipaddr pw-id id]</td>
<td></td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.0.0</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>5.2.2</td>
<td>The Bidirectional IGMP SnooP Sync feature enhancement enables the command to be run on both active and standby hosts.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command to display the contents of profiles and to see associations of profiles with bridge-domains and ports.
The **summary** keyword lists profile names and summarizes their usage on bridge domains and ports. No other keywords can be used with **summary**.

Use the **details** keyword with a profile name to show the contents of a specific profile. Without a profile name, the **detail** keyword shows the contents of all profiles.

Use the **references** keyword to list the relationships between profiles and bridge domains or profiles and ports. You have the following options:

- Use the **references** keyword without any other keywords to show all profiles and the ports and bridge domains they are attached to.
- Use the **references** keyword with the **name** keyword to show a specific profile and where it is attached.
- Use the **port** keyword to list all ports and the profiles attached to them.
- Use the **port** keyword with a specific AC interface or PW to see the profile attached to the named port.
- Use the **bridge-domain** keyword to list all bridge domains and the profiles attached to them.
- Use the **bridge-domain** keyword with a specific bridge domain name to see the profile attached to a specific bridge domain.

### Examples

The following example lists profile names and shows summary level profile usage.

```
RP/0/RSP0/CPU0:router# show igmp snooping redundancy
Profile          Bridge Domain  Port
-------          ------------- ----
profile1         3              0
profile2         0              1
profile3         0              1
```

From an active host:

```
RP/0/RSP0/CPU0:router# show igmp snooping redundancy iccp group 1
Fri Oct 10 08:40:26.231 UTC

ICCP Group Id  #Peers  Active Standby Down  ICCP Group State
------------------------  ------  ------  ------  -------
     1           1       15      0      0  Connected Peer Present
```

From a standby host:

```
RP/0/RSP0/CPU0:router# show igmp snooping redundancy iccp group 1
Fri Oct 10 09:35:19.273 UTC

ICCP Group Id  #Peers  Active Standby Down  ICCP Group State
------------------------  ------  ------  ------  -------
     1           1        0      15      0  Connected Peer Present
```
show igmp snooping redundancy

RP/0/RSP0/CPU0>P1#
show igmp snooping summary

To display summary information about IGMP snooping configuration and traffic statistics for the router, use the `show igmp snooping summary` command in EXEC mode.

```
show igmp snooping summary [statistics [include-zeroes]]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>statistics</code></td>
<td>(Optional) Displays IGMP traffic counters and statistics.</td>
</tr>
<tr>
<td><code>include-zeroes</code></td>
<td>(Optional) Displays all statistics, even if they are zero. Without this keyword, many statistics are omitted from the display when their values are zero.</td>
</tr>
</tbody>
</table>

**Command Default**: None

**Command Modes**: EXEC

**Command History**

- **Release 3.7.2**: This command was introduced.
- **Release 3.9.0**: Three new fields were added to the output for the statistics display.

**Usage Guidelines**: To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command summarizes the number of bridge domains, mrouter ports, host ports, groups, and sources configured on the router.

The `statistics` keyword displays IGMP traffic information, including IGMP queries, reports, and leaves. The three columns in the statistics section of the display are:

- Received—Number of packets received.
- Reinjected—Number of packets received, processed, and reinjected back into the forwarding path.
- Generated—Number of packets generated by the IGMP snooping application and injected into the forwarding path.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following example summarizes IGMP snooping configuration on the router:

```
RP/0/RSP0/CPU0:router# show igmp snooping summary
Bridge Domains:      5
  IGMP Snooping Bridge Domains: 3
Ports:               16
  IGMP Snooping Ports: 16
Mrouters:            6
```
The following example summarizes IGMP snooping configuration on the router and includes non-zero traffic statistics:

```
RP/0/RSP0/CPU0# show igmp snooping summary statistics
Bridge Domains: 5
IGMP Snooping Bridge Domains: 3
Ports: 16
IGMP Snooping Ports: 16
Mrouters: 6
STP Forwarding Ports: 0
ICCP Group Ports: 2
IGMP Groups: 8
   Member Ports: 18
   IGMP Source Groups: 2
   Static/Include/Exclude: 0/1/1
   Member Ports (Include/Exclude): 5/6
```

Traffic Statistics (elapsed time since last cleared 02:08:21):

```
Messages: 7150 894 2381
  IGMP General Queries: 2682 0 0
  IGMP Group Specific Queries: 0 0 0
  IGMP G&S Specific Queries: 0 0 0
  IGMP V2 Reports: 1787 894 893
  IGMP V3 Reports: 2681 0 1488
  IGMP V2 Leaves: 0 0 0
  IGMP Global Leaves: 0 - 0
  PIM Hellos: 0 0 -

Rx Packet Treatment:
  Packets Flooded: 0
  Packets Forwarded To Members: 0
  Packets Forwarded To Mrouters: 894
  Packets Consumed: 6256

Rx Errors:
  None

Tx Errors:
  None

Startup Query Sync Statistics:
  Stale Port Groups deleted: 1
  Stale Port SGs deleted: 1

ICCP Statistics:
  ICCP Up 1
  ICCP Down 1
  Congestion Detected 1
  Congestion Cleared 1
  Peer Up 1
  Peer Down 1
```
ICCP Group Port Statistics:
Port Goes Active: 1
Port Goes Standby: 1

ICCP Traffic Statistics (elapsed time since last cleared 01:01:01):
RX Messages:
  App Data messages: 1
  App Data NAKs: 1
  App Data TLVs: 1
  App State TLVs: 1
  Request Sync TLVs: 1
  Port Membership TLVs: 1
  Querier Info TLVs: 1
  Dynamic Mrouter TLVs: 1
RX Errors:
  None

TX Messages:
  Request Sync TLVs: 1
  Port Membership TLVs: 1
  Querier Info TLVs: 1
  Dynamic Mrouter TLVs: 1
TX Errors:
  None

The following example shows all summary statistics, including those whose value is zero.

```
RP/0/RSP0/CPU0:router# show igmp snooping summary statistics include-zeroes
```

Bridge Domains: 5
IGMP Snooping Bridge Domains: 3
Ports: 16
IGMP Snooping Ports: 16
Mrouters: 6
STP Forwarding Ports: 0
IGMP Groups: 8
Member Ports: 18
IGMP Source Groups:
  Static/Include/Exclude: 0/1/1
  Member Ports (Include/Exclude): 5/6
Traffic Statistics (elapsed time since last cleared 02:08:56):

<table>
<thead>
<tr>
<th></th>
<th>Received</th>
<th>Rejected</th>
<th>Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages:</td>
<td>7185</td>
<td>898</td>
<td>2395</td>
</tr>
<tr>
<td>IGMP General Queries:</td>
<td>2695</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IGMP Group Specific Queries:</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IGMP G&amp;S Specific Queries:</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IGMP V2 Reports:</td>
<td>1796</td>
<td>898</td>
<td>898</td>
</tr>
<tr>
<td>IGMP V3 Reports:</td>
<td>2694</td>
<td>0</td>
<td>1497</td>
</tr>
<tr>
<td>IGMP V2 Leaves:</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>IGMP Global Leaves:</td>
<td>0</td>
<td>-</td>
<td>0</td>
</tr>
<tr>
<td>PIM Hellos:</td>
<td>0</td>
<td>0</td>
<td>-</td>
</tr>
</tbody>
</table>

Rx Packet Treatment:
- Packets Flooded: 0
- Packets Forwarded To Members: 0
- Packets Forwarded To Mrouters: 898
- Packets Consumed: 6287
- Reports Suppressed: 0
- IGMP Blocks Ignored in V2 Compat Mode: 0
- IGMP EX S-lists Ignored in V2 Compat Mode: 0

Rx Errors:
- Packets On Inactive Bridge Domain: 0
- Packets On Inactive Port: 0
- Packets Martian: 0
- Packets Bad Protocol: 0
Packets DA Not Multicast: 0
Packets Missing Router Alert: 0
Packets Missing Router Alert Drop: 0
Packets Bad IGMP Checksum: 0
Packets TTL Not One: 0
Packets TTL Not One Drop: 0
Queries Too Short: 0
V1 Reports Too Short: 0
V2 Reports Too Short: 0
V3 Reports Too Short: 0
V2 Leaves Too Short: 0
IGMP Messages Unknown: 0
IGMP Messages GT Max Ver: 0
IGMP Messages LT Min Ver: 0
Queries Bad Source: 0
Queries Dropped by S/W Router Guard: 0
General Queries DA Not All Nodes: 0
GS-Queries Invalid Group: 0
GS-Queries DA Not Group: 0
GS-Queries Not From Querier: 0
GS-Queries Unknown Group: 0
Reports Invalid Group: 0
Reports Link-Local Group: 0
Reports DA Not Group: 0
Reports No Querier: 0
Leaves Invalid Group: 0
Leaves DA Not All Routers: 0
Leaves No Querier: 0
Leaves Non-Member: 0
Leaves Non-Dynamic Member: 0
Leaves Non-V2 Member: 0
V3 Reports Invalid Group: 0
V3 Reports Link-Local Group: 0
V3 Reports DA Not All V3 Routers: 0
V3 Reports No Querier: 0
V3 Reports Older Version Querier: 0
V3 Reports Invalid Group Record Type: 0
V3 Reports No Sources: 0
V3 Leaves Non-Member: 0
PIM Mgs Dropped by S/W Router Guard: 0
TxErrors:
V3 Sources Not Reported: 0
ICCP Statistics (elapsed time since last cleared 10:56:58):
ICCP Up: 3
ICCP Down: 3
Congestion Detected: 0
Congestion Cleared: 0
Peer Up: 5
Peer Down: 1
ICCP Group Connect attempts: 4
ICCP Group Connect failures: 0
ICCP Group Disconnect attempts: 3
ICCP Group Disconnect failures: 0
ICCP Group Port Statistics (elapsed time since last cleared 10:56:58):
Port Created Down: 0
Port Created Standby: 4
Port Created Active: 0
Port Goes Down: 0
Port Goes Standby: 1
Port Goes Active: 2
ICCP Traffic Statistics (elapsed time since last cleared 10:56:58):
Rx Messages:
App Data messages: 21
App Data NAKs: 3
App Data TLVs: 21
App State TLVs: 20
App State start of sync: 6
App State end of sync: 6
Global Request Sync TLVs: 0
Request Sync TLVs: 1
Port Membership TLVs: 16
Port Membership adds: 10
Port Membership removes: 2
Querier Info TLVs: 0
Querier Info delete TLVs: 0
Dynamic Mrouter TLVs: 0
Dynamic Mrouter delete TLVs: 0
Rx Errors:
  App State sync TLVs ignored: 4
  App State TLVs ignored: 0
  App Data unknown ICCP Group: 0
  App Data unknown ICCP Group Port: 0
  App Data wrong ICCP Group: 0
  App Data BD inactive: 0
  App Data BD port inactive: 0
  App Data ICCP Group port not standby: 0
  App Data ICCP Group port not active: 0
  App Data unsupported global TLV type: 0
  App Data truncated: 0
  App Data length error: 0
  App Data unsupported TLV type: 0
  Port Membership TLV ignored, No Querier: 0
  Port Membership TLV error: 0
  Port Membership TLV too long: 0
  Querier Info TLV error: 0
  Dynamic Mrouter TLV error: 0
  ICCP Rx buffer parse failures: 0
Tx Messages:
  ICCP Tx buffer send count: 11
  App State replay attempts: 2
  Request Sync TLVs: 7
  Port Membership TLVs: 4
  Port Membership adds: 4
  Port Membership removes: 2
  Querier Info TLVs: 0
  Querier Info delete TLVs: 0
  Dynamic Mrouter TLVs: 0
  Dynamic Mrouter delete TLVs: 0
Tx Errors:
  Request to send App State refused: 0
  App State replay failures: 0
  Request Sync TLV Tx failures: 0
  Port Membership TLV Tx failures: 0
  Querier Info TLV Tx failures: 0
  Querier Info delete TLV Tx failures: 0
  Dynamic Mrouter TLV Tx failures: 0
  Dynamic Mrouter delete TLV Tx failures: 0
  ICCP Get Tx buffer parse failures: 0
  ICCP Get Tx buffer send failures: 0
show igmp snooping trace

To display IGMP snooping process activity, use the `show igmp snooping trace` command in EXEC mode.

```
show igmp snooping trace [{all|error|packet-error}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>(Optional) Displays all IGMP snooping process activity.</td>
</tr>
<tr>
<td>error</td>
<td>(Optional) Displays all IGMP snooping process activity.</td>
</tr>
<tr>
<td>packet-error</td>
<td>(Optional) Displays packet error tracepoints.</td>
</tr>
</tbody>
</table>

**Command Default**
The `all` keyword is the default when no keywords are used.

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command to research IGMP snooping process activity.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>12vpn</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows IGMP snooping process status during a restart and a new profile configuration.

```
RP/0/RSP0/CPU0:router# show igmp snooping summary trace all
51 wrapping entries (1024 possible, 0 filtered, 51 total)
Feb 2 14:30:24.902 igmpsn/all 0/5/CPU0 t1 TP001:             0/5/CPU0 t1 TP001: IGMP SNOOP PROCESS RESTART
Feb 2 14:30:24.902 igmpsn/all 0/5/CPU0 t1 TP002: ******** IGMP SNOOP PROCESS RESTART
Feb 2 14:30:24.902 igmpsn/all 0/5/CPU0 t1 TP286: initialize profile wavl tree
Feb 2 14:30:24.902 igmpsn/all 0/5/CPU0 t1 TP185: initialize bd wavl tree
Feb 2 14:30:24.902 igmpsn/all 0/5/CPU0 t1 TP230: initialize port wavl tree
Feb 2 14:30:24.902 igmpsn/all 0/5/CPU0 t1 TP019: entered init_chkpt
Feb 2 14:30:24.902 igmpsn/all 0/5/CPU0 t1 TP165: igmpsn_init_l2fib entered
Feb 2 14:30:24.902 igmpsn/all 0/5/CPU0 t1 TP611: l2fib_restart_timer_init
Feb 2 14:30:24.902 igmpsn/all 0/5/CPU0 t1 TP680: igmpsn_pd_mgid_api_init entered
Feb 2 14:30:24.902 igmpsn/all 0/5/CPU0 t1 TP681: failed to open
libl2mc_snoop_mgid_client_pd.dll
Feb 2 14:30:24.902 igmpsn/all 0/5/CPU0 t1 TP683: 12mc_snoop_pd_mgid funcs are stubbed
```
Feb 2 14:30:25.037 igmpsn/all 0/5/CPU0 t1 TP080: socket open succeeded
Feb 2 14:30:25.037 igmpsn/all 0/5/CPU0 t1 TP031: connection open for socket
Feb 2 14:30:25.037 igmpsn/all 0/5/CPU0 t1 TP614: igmpsn_l2fib_restart_timer_start, 300 secs
Feb 2 14:30:25.038 igmpsn/all 0/5/CPU0 t1 TP555: IGMP SNOOP PROCESS READY
Feb 2 14:30:25.038 igmpsn/all 0/5/CPU0 t1 TP017: entered event loop
Feb 2 14:30:25.038 igmpsn/all 0/5/CPU0 t1 TP112: sysdb register verification
Feb 2 14:30:25.038 igmpsn/all 0/5/CPU0 t1 TP286: initialize profile wavl tree
Feb 2 14:30:25.040 igmpsn/all 0/5/CPU0 t1 TP110: sysdb event verify func (CREATE & SET, profile/profile1/enter)
Feb 2 14:30:25.040 igmpsn/all 0/5/CPU0 t1 TP287: create profile profile1
Feb 2 14:30:25.040 igmpsn/all 0/5/CPU0 t1 TP534: profile profile1 (0x4826b838): initialized static_group tree
(... missing lines)
show l2vpn forwarding bridge-domain mroute

To display multicast routes in the forwarding tables, use the `show l2vpn forwarding bridge-domain mroute` command in EXEC mode.

```
show l2vpn forwarding bridge-domain [bridge-group-name : bridge-domain-name] mroute [ipv4]
location rack/slot/module
```

**Syntax Description**
- `bridge-group-name bridge-domain-name` (Optional) Displays information for a specific bridge domain. The colon that separates the two arguments is required.
- `ipv4` This keyword is required.
- `location rack/slot/module` Displays route information for a specific rack/slot/module.

**Command Default**
None

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 5.2.2</td>
<td>The show output command was enhanced to include the satellite multicast offload information.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command displays multicast routes as they are converted into the forwarding plane forwarding tables. The source for the conversion is the multicast routes configured in the control plane with IGMP snooping configuration commands. If the routes displayed by this command are not as expected, check the control plane configuration and correct the corresponding IGMP snooping profiles.

Use optional arguments to limit the display to a specific bridge domain.

**Examples**
This example displays high-level statistics about routes for one bridge domain:

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain mroute ipv4 location 0/5/cPU0
mroute ipv4 location 0/5/cPU0
Bridge-Domain Name: nv-mcast:nv-mcast-1
Prefix: (0.0.0.0,224.0.0.0/4) P2MP enabled: N
IRB platform data: {0x84a0000, 0x0, 0x4a00008d, 0x123bb4e0}, len: 16
Ingress
```
IGMP and MLD Snooping Commands on Cisco ASR 9000 Series Routers

show 12vpn forwarding bridge-domain mroute

Forwarded (Packets/Bytes): 0/0
Received (Packets/Bytes): 0/0
Punted (Packets/Bytes): 0/0
Dropped (Packets/Bytes): 0/0
show l2vpn forwarding bridge-domain mroute detail

To display multicast routes in the forwarding tables, use the `show l2vpn forwarding bridge-domain mroute detail` command in EXEC mode.

```
show l2vpn forwarding bridge-domain [bridge-group-name : bridge-domain-name] mroute [ipv4] detail location rack/slot/module
```

**Syntax Description**

- `bridge-group-name bridge-domain-name` (Optional) Displays information for a specific bridge domain. The colon that separates the two arguments is required.
- `ipv4` This keyword is required.
- `location rack/slot/module` Displays route information for a specific rack/slot/module.

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 5.2.2</td>
<td>The show output command was enhanced to include the satellite multicast offload information.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command displays multicast routes as they are converted into the forwarding plane forwarding tables. The source for the conversion is the multicast routes configured in the control plane with IGMP snooping configuration commands. If the routes displayed by this command are not as expected, check the control plane configuration and correct the corresponding IGMP snooping profiles.

Use optional arguments to limit the display to a specific bridge domain.

**Examples**

This example displays satellite multicast offload information for one bridge domain.

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain mroute ipv4 detail location 0/1/cPU0
Bridge-Domain: nv-mcast:nv-mcast-1, ID: 2122
Prefix: (0.0.0.0,224.31.0.1/32) P2MP enabled: N
IRB platform data: {0x84a0001, 0x0, 0x4a000093, 0x115444e0}, len: 16
Ingress
```
Forwarded (Packets/Bytes): 9278034/7220724021
Received (Packets/Bytes): 0/0
Core Received (Packets/Bytes): 0/0
Core Forwarded (Packets/Bytes): 0/0
Punted (Packets/Bytes): 0/0
Dropped (Packets/Bytes): 0/0
Bridge Port:
GigabitEthernet301/0/0/4, Xconnect id: 0x3880015 SatId: 301, Isid: 0x3fd, Ver: 0x1, Ring Id: 0xe000600, oleIsOffLoaded
Forwarded (Packets/Bytes): 9278034/7220724021
Punted (Packets/Bytes): 0/0
Dropped (Packets/Bytes): 0/0
**show l2vpn forwarding bridge-domain mroute hardware ingress detail**

To display multicast routes in the forwarding tables, use the `show l2vpn forwarding bridge-domain mroute hardware ingress detail` command in EXEC mode.

```
show l2vpn forwarding bridge-domain [bridge-group-name : bridge-domain-name] mroute [ipv4] hardware ingress detail location rack/slot/module
```

**Syntax Description**
- `bridge-group-name bridge-domain-name` (Optional) Displays information for a specific bridge domain. The colon that separates the two arguments is required.
- `ipv4` This keyword is required.
- `location rack/slot/module` Displays route information for a specific rack/slot/module.

**Command Default**
None

**Command Modes**
EXEC

**Command History**
- Release 3.7.2 This command was introduced.
- Release 5.2.2 The show output command was enhanced to include the satellite multicast offload information.

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command displays multicast routes as they are converted into the forwarding plane forwarding tables. The source for the conversion is the multicast routes configured in the control plane with IGMP snooping configuration commands. If the routes displayed by this command are not as expected, check the control plane configuration and correct the corresponding IGMP snooping profiles.

Use optional arguments to limit the display to a specific bridge domain.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

This example displays satellite multicast offload information for one bridge domain. The text in bold indicates the hardware ingress detail information.

```
RP/0/RSP0/CPU0:router# show l2vpn forwarding bridge-domain mroute ipv4 hardware ingress detail location 0/1/CPU0
```
Bridge-Domain: satellite:10, ID: 0
Prefix: (0.0.0.0,224.0.0.0/4) P2MP enabled: N
IRB platform data: (0x0, 0x0, 0x8a, 0x939070e0), len: 16
Ingress
  Forwarded (Packets/Bytes): 0/0
  Received (Packets/Bytes): 0/0
  Core Received (Packets/Bytes): 0/0
  Core Forwarded (Packets/Bytes): 0/0
  Punted (Packets/Bytes): 0/0
  Dropped (Packets/Bytes): 0/0
Platform multicast leaf context:

Legend:
Route information - (Ingress)
C: NP ID, IR: MGID Mask
IS: Single SHG0 on LC, IX: Single SHG0 XID
IA0: FGID_SHG0, IA1: FGID_SHG1, IA2: FGID_SHG2
IG: Multicast group ID, IB: Base statistics pointer
Route information - (Egress)
ET: Table ID for OLIST lookup, EO: OLIST count bit, ER: MLI
EC1: SHG1 OLIST members count on this chip,
EC2: SHG2 OLIST members count on this chip,
EC: Total count of OLIST members on this chip,
SD: Single OLIST member Optimization,
Hardware Information
C: NP ID; T: Table ID; M: Member ID; I: IRB OLE; U: XID-ID,
RF0: R_FGID_SHG0, RF1: R_FGID_SHG1, RF2: R_FGID_SHG2, O: Offloaded
Statistics Information
S: Source, G: Group, Pr: Prefix Length, C: NP ID, R: Received,
FF: Forwarded to fabric, P: Punted to CPU, D: Dropped,
F: Forwarded, CR: Core Received, CF: Core Forwarded

Source: * Group: 224.0.0.0 Mask length: 4

IRB Route Notification Information

Bridge_ID:0x0 NP_Mask:0x0 Rack0 Slot_Mask:0x0 Rack1 Slot_Mask:0x0

VPLS LSM Inclusive Tree Local Rack Information

Route_LSM_Flag: F Latest Update from Bud Label MGID: 0
Head Label NP Mask:[old:0x0, new:0x0] All Route OLE NP Mask: 0x1

VPLS LSM Inclusive Tree Remote Rack Information

Head Label Slot Mask:[old:0x0, new:0x0] Aggregated Bud Label Slot Mask:[old:0x0, new:0x0]
Route Information

<table>
<thead>
<tr>
<th>C</th>
<th>IR</th>
<th>IS</th>
<th>IX</th>
<th>IA0</th>
<th>IA1</th>
<th>IA2</th>
<th>IG</th>
<th>IB</th>
<th>ET</th>
<th>EO</th>
<th>ER</th>
<th>EC1</th>
<th>EC2</th>
<th>EC</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0x0</td>
<td>F</td>
<td>0x0</td>
<td>0x0</td>
<td>0x0</td>
<td>0x0</td>
<td>0x4233</td>
<td>0xS3017c</td>
<td>0</td>
<td>F</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>0x0</td>
<td>F</td>
<td>0x0</td>
<td>0x0</td>
<td>0x0</td>
<td>0x0</td>
<td>0x4233</td>
<td>0xS3031c</td>
<td>0</td>
<td>F</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Statistics Information: S: * G: 224.0.0.0 Pr: 4

<table>
<thead>
<tr>
<th>C</th>
<th>R(packets:bytes)/FF(packets:bytes)/P(packets)/D(packets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0:0 / 0:0 / 0 / 0</td>
</tr>
<tr>
<td>1</td>
<td>0:0 / 0:0 / 0 / 0</td>
</tr>
</tbody>
</table>

Bridge-Domain: satellite:10, ID: 0
Prefix: (192.10.1.2,232.0.0.1/64) P2MP enabled: N
IRB platform data: (0x1, 0x0, 0x8b, 0x92203ce8), len: 16
Ingress
- Forwarded (Packets/Bytes): 886211028/239276977560
- Received (Packets/Bytes): 0/0
- Core Received (Packets/Bytes): 0/0
- Core Forwarded (Packets/Bytes): 0/0
- Punted (Packets/Bytes): 0/0
- Dropped (Packets/Bytes): 0/0

Bridge Port:
- GigabitEthernet100/0/0/22, Xconnect id: 0x1880010 SatId: 100, Isid: 0x3f2, Ver: 0x1,
  Ring Id: 0x60000c0, oleIsOffLoaded
  - Forwarded (Packets/Bytes): 0/0
  - Punted (Packets/Bytes): 0/0
  - Dropped (Packets/Bytes): 0/0
- GigabitEthernet100/0/0/32, Xconnect id: 0x1880011 SatId: 100, Isid: 0x3f2, Ver: 0x1,
  Ring Id: 0x60000c0, oleIsOffLoaded
  - Forwarded (Packets/Bytes): 0/0
  - Punted (Packets/Bytes): 0/0
  - Dropped (Packets/Bytes): 0/0
- GigabitEthernet200/0/0/34, Xconnect id: 0x1880013 SatId: 200, Isid: 0x3f2, Ver: 0x1,
  Ring Id: 0x60000c0, oleIsOffLoaded
  - Forwarded (Packets/Bytes): 886236660/239283898200
  - Punted (Packets/Bytes): 0/0
  - Dropped (Packets/Bytes): 0/0

Platform multicast leaf context:Source: 192.10.1.2 Group: 232.0.0.1 Mask length: 64
IRB Route Notification Information

| Bridge_ID:0x0 | NP_Mask:0x1 | Rack0 Slot_Mask:0x8 | Rack1 Slot_Mask:0x0 |
Master_Slot:0x0

VPLS LSM Inclusive Tree Local Rack Information

<table>
<thead>
<tr>
<th>Route_LSM_Flag: F</th>
<th>Head Label NP Mask: [old:0x0, new:0x0]</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latest Update from Bud Label MGID: 0</td>
<td>All Route OLE NP Mask: 0x1</td>
</tr>
</tbody>
</table>

VPLS LSM Inclusive Tree Remote Rack Information

<table>
<thead>
<tr>
<th>Head Label Slot Mask: [old:0x0, new:0x0]</th>
<th>Aggregated Bud Label Slot Mask: [old:0x0, new:0x0]</th>
</tr>
</thead>
</table>

Route Information

<table>
<thead>
<tr>
<th>C</th>
<th>IR</th>
<th>IS</th>
<th>IX</th>
<th>IA0</th>
<th>IA1</th>
<th>IA2</th>
<th>IG</th>
<th>IB</th>
<th>ET</th>
<th>EO</th>
<th>ER</th>
<th>EC1</th>
<th>EC2</th>
</tr>
</thead>
<tbody>
<tr>
<td>EC</td>
<td>SD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0x1</td>
<td>T</td>
<td>0x6300013</td>
<td>0x0</td>
<td>0x8</td>
<td>0x8</td>
<td>0x4234</td>
<td>0x530f98</td>
<td>1</td>
<td>T</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0x1</td>
<td>T</td>
<td>0x6300013</td>
<td>0x0</td>
<td>0x8</td>
<td>0x8</td>
<td>0x4234</td>
<td>0x530390</td>
<td>1</td>
<td>F</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Hardware Information

<table>
<thead>
<tr>
<th>C</th>
<th>T</th>
<th>M</th>
<th>I</th>
<th>U</th>
<th>RF0</th>
<th>RF1</th>
<th>RF2</th>
<th>O</th>
<th>ISID</th>
<th>VER</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>0</td>
<td>F</td>
<td>0x13</td>
<td>0x0</td>
<td>0x0</td>
<td>0x0</td>
<td>T</td>
<td>0x3f2</td>
<td>0x1</td>
</tr>
</tbody>
</table>

Statistics Information:  S: 192.10.1.2   G: 232.0.0.1   Pr: 64

<table>
<thead>
<tr>
<th>C</th>
<th>R (packets:bytes) / FF (packets:bytes) / F (packets) / D (packets)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0:0 / 886721677:239414852790 / 0 / 0</td>
</tr>
<tr>
<td>1</td>
<td>0:0 / 0:0 / 0 / 0</td>
</tr>
</tbody>
</table>

XID Statistics:

<table>
<thead>
<tr>
<th>C</th>
<th>XID-ID</th>
<th>Stats_Ptr</th>
<th>F/P/D (packets:bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0x13</td>
<td>0x530fa4</td>
<td>886211028:239276977560 / 0:0 / 0:0</td>
</tr>
</tbody>
</table>

Offloaded XID Information
show l2vpn forwarding bridge-domain mroute hardware ingress detail

<table>
<thead>
<tr>
<th>XID-ID</th>
<th>IFHandle</th>
<th>Ring</th>
<th>CSFL</th>
<th>ISID</th>
<th>VER</th>
<th>O:M</th>
<th>SAT-ID</th>
<th>F/P/D (packets:bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x10</td>
<td>0x6009600</td>
<td>0</td>
<td>0x60000c0</td>
<td>0x3f2</td>
<td>0x1</td>
<td>1:0</td>
<td>100</td>
<td>0:0 0:0 0:0</td>
</tr>
<tr>
<td>0x11</td>
<td>0x6009880</td>
<td>0</td>
<td>0x60000c0</td>
<td>0x3f2</td>
<td>0x1</td>
<td>1:0</td>
<td>100</td>
<td>0:0 0:0 0:0</td>
</tr>
<tr>
<td>0x13</td>
<td>0x600a400</td>
<td>0</td>
<td>0x60000c0</td>
<td>0x3f2</td>
<td>0x1</td>
<td>1:1</td>
<td>200</td>
<td>0:0 0:0 0:0</td>
</tr>
</tbody>
</table>

Bridge-Domain: satellite:20, ID: 1
Prefix: (0.0.0.0, 224.0.0.0/4) F2MP enabled: N
IRB platform data: (0x10000, 0x0, 0x100008a, 0x939ea8e0), len: 16
Ingress
  Forwarded (Packets/Bytes): 0/0
  Received (Packets/Bytes): 0/0
  Core Received (Packets/Bytes): 0/0
  Core Forwarded (Packets/Bytes): 0/0
  Punted (Packets/Bytes): 0/0
  Dropped (Packets/Bytes): 0/0

Platform multicast leaf context: Source: * Group: 224.0.0.0 Mask length: 4

IRB Route Notification Information

<table>
<thead>
<tr>
<th>Bridge_ID</th>
<th>NP_Mask</th>
<th>Rack0 Slot_Mask</th>
<th>Rack1 Slot_Mask</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x1</td>
<td>0x0</td>
<td>0x0</td>
<td>0x0</td>
</tr>
</tbody>
</table>

VPLS LSM Inclusive Tree Local Rack Information

<table>
<thead>
<tr>
<th>Route_LSM_Flag</th>
<th>Head Label NP Mask: [old:0x0, new:0x0]</th>
</tr>
</thead>
<tbody>
<tr>
<td>F</td>
<td>All Route OLE NP Mask: 0x1</td>
</tr>
</tbody>
</table>

VPLS LSM Inclusive Tree Remote Rack Information

| Head Label Slot Mask: [old:0x0, new:0x0] | Aggregated Bud Label Slot Mask: [old:0x0, new:0x0] |

Route Information

<table>
<thead>
<tr>
<th>C</th>
<th>IR</th>
<th>IS</th>
<th>IX</th>
<th>IA0</th>
<th>IA1</th>
<th>IA2</th>
<th>IG</th>
<th>IB</th>
<th>ET</th>
<th>EC</th>
<th>EC1</th>
<th>EC2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>0x0</td>
<td>F</td>
<td>0x0</td>
<td>0x0</td>
<td>0x0</td>
<td>0x0</td>
<td>0x0</td>
<td>0x4232</td>
<td>0x530178</td>
<td>0</td>
<td>F</td>
<td>1</td>
</tr>
</tbody>
</table>
Statistics Information:  S: *  G: 224.0.0.0  Pr: 4

C  R(packets:bytes)/FF(packets:bytes)/P(packets)/D(packets)

Bridge-Domain: satellite:20, ID: 1
 Prefix: (192.10.1.2,232.0.0.1/64)  P2MP enabled: N
 IRB platform data: \{0x10001, 0x0, 0x100008b, 0x920484e8\}, len: 16
 Ingress
   Forwarded (Packets/Bytes): 886199961/239273989470
   Received (Packets/Bytes): 0/0
 Core Received (Packets/Bytes): 0/0
 Core Forwarded (Packets/Bytes): 0/0
 Punted (Packets/Bytes): 0/0
 Dropped (Packets/Bytes): 0/0

Bridge Port:
 GigabitEthernet200/0/0/23, Xconnect id: 0x1880012 SatId: 200, Isid: 0x3f3, Ver: 0x1
 Ring Id: 0x60000c0, oleIsOffLoaded
   Forwarded (Packets/Bytes): 0/0
   Punted (Packets/Bytes): 0/0
   Dropped (Packets/Bytes): 0/0

 GigabitEthernet300/0/0/25, Xconnect id: 0x1880014 SatId: 300, Isid: 0x3f3, Ver: 0x1
 Ring Id: 0x60000c0, oleIsOffLoaded
   Forwarded (Packets/Bytes): 0/0
   Punted (Packets/Bytes): 0/0
   Dropped (Packets/Bytes): 0/0

 GigabitEthernet300/0/0/34, Xconnect id: 0x1880015 SatId: 300, Isid: 0x3f3, Ver: 0x1
 Ring Id: 0x60000c0, oleIsOffLoaded
   Forwarded (Packets/Bytes): 886308945/239303415150
   Punted (Packets/Bytes): 0/0
   Dropped (Packets/Bytes): 0/0

Platform multicast leaf context:Source: 192.10.1.2  Group: 232.0.0.1  Mask length: 64

IRB Route Notification Information

VPLS LSM Inclusive Tree Local Rack Information
### VPLS LSM Inclusive Tree Remote Rack Information

- **Head Label Slot Mask:** [old: 0x0, new: 0x0]
- **Aggregated Bud Label Slot Mask:** [old: 0x0, new: 0x0]

### Route Information

<table>
<thead>
<tr>
<th>C</th>
<th>IR</th>
<th>IS</th>
<th>IX</th>
<th>IA0</th>
<th>IA1</th>
<th>IA2</th>
<th>IG</th>
<th>IB</th>
<th>ET</th>
<th>EO</th>
<th>ER</th>
<th>EC1</th>
<th>EC2</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0x1</td>
<td>T</td>
<td>0x6300015</td>
<td>0x0</td>
<td>0x8</td>
<td>0x8</td>
<td>0x4236</td>
<td>0x530f9c</td>
<td>0</td>
<td>T</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
<td>0x1</td>
<td>T</td>
<td>0x6300015</td>
<td>0x0</td>
<td>0x8</td>
<td>0x8</td>
<td>0x4236</td>
<td>0x530394</td>
<td>0</td>
<td>F</td>
<td>4</td>
</tr>
</tbody>
</table>

### Hardware Information

<table>
<thead>
<tr>
<th>C</th>
<th>T</th>
<th>M</th>
<th>I</th>
<th>U</th>
<th>RF0</th>
<th>RF1</th>
<th>RP2</th>
<th>O</th>
<th>ISID</th>
<th>VER</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>F</td>
<td>0x15</td>
<td>0x0</td>
<td>0x0</td>
<td>0x0</td>
<td>T</td>
<td>0x3f3</td>
<td>0x1</td>
</tr>
</tbody>
</table>

### Statistics Information:

<table>
<thead>
<tr>
<th>S: 192.10.1.2</th>
<th>G: 232.0.0.1</th>
<th>Pr: 64</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>R(packets:bytes)/FF(packets:bytes)/P(packets)/D(packets)</td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>0:0 / 886721671:239414851170 / 0 / 0</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>0:0 / 0:0 / 0:0 / 0:0</td>
<td></td>
</tr>
</tbody>
</table>

### XID Statistics:

<table>
<thead>
<tr>
<th>C</th>
<th>XID-ID Stats Ptr F/P/D (packets:bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0x15 0x530fac 886199961:239273989470 / 0:0 / 0:0</td>
</tr>
</tbody>
</table>

### Offloaded XID Information

<table>
<thead>
<tr>
<th>XID-ID</th>
<th>IFHandle</th>
<th>Ring</th>
<th>CSFL</th>
<th>ISID</th>
<th>VER</th>
<th>O:M</th>
<th>SAT-ID</th>
<th>F/P/D (packets:bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x12</td>
<td>0x600a140</td>
<td>0</td>
<td>0x600000c0</td>
<td>0x3f3</td>
<td>0x1</td>
<td>1:0</td>
<td>200</td>
<td>0:0 0:0 0:0</td>
</tr>
<tr>
<td>0x14</td>
<td>0x600acc0</td>
<td>0</td>
<td>0x600000c0</td>
<td>0x3f3</td>
<td>0x1</td>
<td>1:0</td>
<td>300</td>
<td>0:0 0:0 0:0</td>
</tr>
<tr>
<td>0x15</td>
<td>0x600af00</td>
<td>0</td>
<td>0x600000c0</td>
<td>0x3f3</td>
<td>0x1</td>
<td>1:1</td>
<td>300</td>
<td>0:0 0:0 0:0</td>
</tr>
</tbody>
</table>
show mld snooping bridge-domain

To display MLD snooping configuration information and traffic statistics for bridge domains, use the `show mld snooping bridge-domain` command in EXEC mode.

```
show mld snooping bridge-domain [bridge-domain-name] [detail [statistics [include-zeroes]]]
```

**Syntax Description**

- **bridge-domain-name** (Optional) Displays information only for the specified bridge domain.
- **detail** (Optional) Includes more details, including configuration information about the bridge domain querier.
- **statistics** (Optional) Includes traffic counters and statistics.
- **include-zeroes** (Optional) Includes all statistics, even if they are zero. Without this keyword, many statistics are omitted from the display when their values are zero.

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command displays mld snooping information by bridge domain. Use the command without any keywords to display summary information about all bridge domains, in a single line per bridge domain.

Use optional keywords to request additional details and traffic statistics per bridge domain. You can also limit the display to a single bridge domain.

The **statistics** keyword displays mld traffic information, including mld queries, reports, and leaves. The three columns in the statistics section of the display are:

- **Received**—Number of packets received.
- **Reinjected**—Number of packets received, processed, and reinjected back into the forwarding path.
- **Generated**—Number of packets generated by the mld snooping application and injected into the forwarding path.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read</td>
</tr>
</tbody>
</table>
**Examples**

The following example shows the basic command without any keywords.

```
RP/0/RSP0/CPU0:router# show mld snooping bridge-domain
```

<table>
<thead>
<tr>
<th>Bridge Domain</th>
<th>Profile</th>
<th>Act Ver</th>
<th>#Ports</th>
<th>#Mtrs</th>
<th>#Grps</th>
<th>#Srcs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain1:BD-1</td>
<td>profile1</td>
<td>Y V2</td>
<td>8195</td>
<td>0</td>
<td>4096</td>
<td>0</td>
</tr>
<tr>
<td>Domain1:BD-4</td>
<td>profile1</td>
<td>Y V2</td>
<td>100</td>
<td>2</td>
<td>512</td>
<td>0</td>
</tr>
<tr>
<td>Domain1:BD-7</td>
<td>profile1</td>
<td>Y V2</td>
<td>55</td>
<td>0</td>
<td>44</td>
<td>0</td>
</tr>
</tbody>
</table>

The following example shows the summary line for a named bridge domain.

```
RP/0/RSP0/CPU0:router# show mld snooping bridge-domain Group1:BD-1
```

<table>
<thead>
<tr>
<th>Bridge Domain</th>
<th>Profile</th>
<th>Act Ver</th>
<th>#Ports</th>
<th>#Mtrs</th>
<th>#Grps</th>
<th>#Srcs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain1:BD-1</td>
<td>profile1</td>
<td>Y V2</td>
<td>8195</td>
<td>0</td>
<td>4096</td>
<td>0</td>
</tr>
</tbody>
</table>

The following example shows detailed information about all bridge domains:

```
RP/0/RSP0/CPU0:router# show mld snooping bridge-domain detail
```

| Bridge Domains: | 5 |
| MLD Snooping Bridge Domains: | 3 |

<table>
<thead>
<tr>
<th>Bridge Domain</th>
<th>Profile</th>
<th>Act Ver</th>
<th>#Ports</th>
<th>#Mtrs</th>
<th>#Grps</th>
<th>#Srcs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain1:BD-1</td>
<td>profile1</td>
<td>Y V2</td>
<td>8195</td>
<td>0</td>
<td>4096</td>
<td>0</td>
</tr>
</tbody>
</table>

Profile Configured Attributes:
- System IP Address: fe80::1aef:63ff:fee2:5fc6
- Minimum Version: 1
- Report Suppression: Enabled
- Unsolicited Report Interval: 1000 (milliseconds)
- TCN Query Solicit: Disabled
- TCN Membership Sync: Disabled
- TCN Flood: Enabled
- TCN Flood Query Count: 2
- Router Alert Check: Enabled
- TTL Check: Enabled
- Internal Querier Support: Disabled
- Querier Query Interval: 125 (seconds)
- Querier LMQ Interval: 1000 (milliseconds)
- Querier LMQ Count: 2
- Querier Robustness: 2
- Startup Query Interval: 0 seconds
- Startup Query Count: 0
- Startup Query Max Response Time: 0.0 seconds
- Mrouter Forwarding: Enabled
- Querier: Not Present
- Mrouter Ports: 0
- STP Forwarding Ports: 0
- ICCP Group Ports: 0
- Groups: 0
- Member Ports: 0
- V2 Source Groups: 0
- Static/Include/Exclude: 0/0/0
- Member Ports (Include/Exclude): 0/0
The following example displays traffic statistics with detailed information. The display omits many statistics whose values are zero.

```
RP/0/RSP0/CPU0:router# show mld snooping bridge-domain Group1:BD-1 detail statistics
```

```
Bridge Domain Profile Act Ver #Ports #Mrtrs #Grps #Srcs
------------- ------ ------ ------ ------ ------ ------ ----
Domain1:BD-1 profile1 Y V2 8195 0 4096 0 4096 0
```

Profile Configured Attributes:
- System IP Address: fe80::1aef:63ff:fe2:5fc6
- Minimum Version: 1
- Report Suppression: Enabled
- Unsolicited Report Interval: 1000 (milliseconds)
- TCN Query Solicit: Disabled
- TCN Membership Sync: Disabled
- TCN Flood: Enabled
- TCN Flood Query Count: 2
- Router Alert Check: Enabled
- TTL Check: Enabled
- Internal Querier Support: Disabled
- Querier Query Interval: 125 (seconds)
- Querier LMQ Interval: 1000 (milliseconds)
- Querier LMQ Count: 2
- Querier Robustness: 2
- Startup Query Interval: 0 seconds
- Startup Query Count: 0
- Startup Query Max Response Time: 0.0 seconds
- Mrouter Forwarding: Enabled
- Querier: Not Present
- Mrouter Ports: 0
- STP Forwarding Ports: 0
- ICCP Group Ports: 0
- Groups: 0
- Member Ports: 0
- V2 Source Groups: 0
- Static/Include/Exclude: 0/0/0
- Member Ports (Include/Exclude): 0/0

The following example displays traffic statistics with detailed information. The display omits many statistics whose values are zero.

```
RP/0/RSP0/CPU0:router# show mld snooping bridge-domain Group1:BD-1 detail statistics
```

```
Bridge Domain Profile Act Ver #Ports #Mrtrs #Grps #Srcs
------------- ------ ------ ------ ------ ------ ------ ----
Domain1:BD-1 profile1 Y V2 8195 0 4096 0 4096 0
```

Profile Configured Attributes:
- System IP Address: fe80::1aef:63ff:fe2:5fc6
- Minimum Version: 1
- Report Suppression: Enabled
- Unsolicited Report Interval: 1000 (milliseconds)
- TCN Query Solicit: Disabled
- TCN Membership Sync: Disabled
- TCN Flood: Enabled
- TCN Flood Query Count: 2
- Router Alert Check: Enabled
- TTL Check: Enabled
- Internal Querier Support: Disabled
- Querier Query Interval: 125 (seconds)
- Querier LMQ Interval: 1000 (milliseconds)
- Querier LMQ Count: 2
- Querier Robustness: 2
- Startup Query Interval: 0 seconds
- Startup Query Count: 0
- Startup Query Max Response Time: 0.0 seconds

```

Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference, Release 5.3.x

355
show mld snooping bridge-domain

Mrouter Forwarding: Enabled
Querier: Not Present
Mrouter Ports: 0
STP Forwarding Ports: 0
ICCP Group Ports: 0
Groups: 0
Member Ports: 0
V2 Source Groups: 0
Static/Include/Exclude: 0/0/0
Member Ports (Include/Exclude): 0/0
Traffic Statistics (elapsed time since last cleared 00:54:30):
Messages: Received Reinjected Generated
MLD General Queries: 0 0 0
MLD Group Specific Queries: 0 0 0
MLD G&S Specific Queries: 0 0 0
MLD V1 Reports: 0 0 0
MLD V2 Reports: 0 0 0
MLD V1 Leaves: 0 0 0
MLD Global Leaves: 0 - 0
PIM Hellos: 0 0 -
Rx Packet Treatment:
Packets Flooded: 0
Packets Forwarded To Members: 0
Packets Forwarded To Mrouters: 0
Packets Consumed: 0
Rx Errors:
Packets DA Not Multicast: 4
Rx Other:
None
Tx Errors:
None
Startup Query Sync Statistics:
None

The following example shows details for all statistics regardless of whether their values are zero.

RP/0/RSP0/CPU0:router# show mld snooping bridge-domain Group1:BD-1 detail statistics include-zeroes

<table>
<thead>
<tr>
<th>Bridge Domain</th>
<th>Profile</th>
<th>Act Ver</th>
<th>#Ports</th>
<th>#Mrtrs</th>
<th>#Grps</th>
<th>#Srcs</th>
</tr>
</thead>
<tbody>
<tr>
<td>BD-1</td>
<td>profile1</td>
<td>Y V2</td>
<td>8195</td>
<td>0</td>
<td>4096</td>
<td>0</td>
</tr>
</tbody>
</table>

Profile Configured Attributes:
System IP Address: fe80::1aef:63ff:fee2:5fc6
Minimum Version: 1
Report Suppression: Enabled
Unsolicited Report Interval: 1000 (milliseconds)
TCN Query Solicit: Disabled
TCN Membership Sync: Disabled
TCN Flood: Enabled
TCN Flood Query Count: 2
Router Alert Check: Enabled
TTL Check: Enabled
Internal Querier Support: Disabled
Querier Query Interval: 125 (seconds)
Querier LMQ Interval: 1000 (milliseconds)
Querier LMQ Count: 2
Querier Robustness: 2
Startup Query Interval: 0 seconds
Startup Query Count: 0
Startup Query Max Response Time: 0.0 seconds
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mrouter Forwarding:</td>
<td>Enabled</td>
</tr>
<tr>
<td>Querier:</td>
<td>Not Present</td>
</tr>
<tr>
<td>Mrouter Ports:</td>
<td>0</td>
</tr>
<tr>
<td>STP Forwarding Ports:</td>
<td>0</td>
</tr>
<tr>
<td>ICCP Group Ports:</td>
<td>0</td>
</tr>
<tr>
<td>Groups:</td>
<td>0</td>
</tr>
<tr>
<td>Member Ports:</td>
<td>0</td>
</tr>
<tr>
<td>V2 Source Groups:</td>
<td>0</td>
</tr>
<tr>
<td>Static/Include/Exclude:</td>
<td>0/0/0</td>
</tr>
<tr>
<td>Traffic Statistics (elapsed time since last cleared 00:55:19):</td>
<td></td>
</tr>
<tr>
<td>Messages:</td>
<td>0/0/0</td>
</tr>
<tr>
<td>MLD General Queries:</td>
<td>0/0/0</td>
</tr>
<tr>
<td>MLD Group Specific Queries:</td>
<td>0/0/0</td>
</tr>
<tr>
<td>MLD G&amp;S Specific Queries:</td>
<td>0/0/0</td>
</tr>
<tr>
<td>MLD V1 Reports:</td>
<td>0/0/0</td>
</tr>
<tr>
<td>MLD V2 Reports:</td>
<td>0/0/0</td>
</tr>
<tr>
<td>MLD V1 Leaves:</td>
<td>0/0/0</td>
</tr>
<tr>
<td>MLD Global Leaves:</td>
<td>0/0/0</td>
</tr>
<tr>
<td>PIM Hellos:</td>
<td>0/0/0</td>
</tr>
<tr>
<td>Rx Packet Treatment:</td>
<td></td>
</tr>
<tr>
<td>Packets Flooded:</td>
<td>0</td>
</tr>
<tr>
<td>Packets Forwarded To Members:</td>
<td>0</td>
</tr>
<tr>
<td>Packets Forwarded To Mrouters:</td>
<td>0</td>
</tr>
<tr>
<td>Packets Consumed:</td>
<td>0</td>
</tr>
<tr>
<td>Reports Suppressed:</td>
<td>0</td>
</tr>
<tr>
<td>Access Group Permits:</td>
<td>0</td>
</tr>
<tr>
<td>Access Group Denials:</td>
<td>0</td>
</tr>
<tr>
<td>Group Limits Exceeded:</td>
<td>0</td>
</tr>
<tr>
<td>MLD Blocks Ignored in V1 Compat Mode:</td>
<td>0</td>
</tr>
<tr>
<td>MLD EX S-lists Ignored in V1 Compat Mode:</td>
<td>0</td>
</tr>
<tr>
<td>Rx MLD V2 Report Group Record Types:</td>
<td></td>
</tr>
<tr>
<td>Is Include:</td>
<td>0</td>
</tr>
<tr>
<td>Change To Include:</td>
<td>0</td>
</tr>
<tr>
<td>Is Exclude:</td>
<td>0</td>
</tr>
<tr>
<td>Change To Exclude:</td>
<td>0</td>
</tr>
<tr>
<td>Allow New Sources:</td>
<td>0</td>
</tr>
<tr>
<td>Block Old Sources:</td>
<td>0</td>
</tr>
<tr>
<td>Rx Errors:</td>
<td></td>
</tr>
<tr>
<td>Packets On Inactive Bridge Domain:</td>
<td>0</td>
</tr>
<tr>
<td>Packets On Inactive Port:</td>
<td>0</td>
</tr>
<tr>
<td>Packets Martian:</td>
<td>0</td>
</tr>
<tr>
<td>Packets Bad Protocol:</td>
<td>0</td>
</tr>
<tr>
<td>Packets DA Not Multicast:</td>
<td>4</td>
</tr>
<tr>
<td>Packets Missing Router Alert:</td>
<td>0</td>
</tr>
<tr>
<td>Packets Missing Router Alert Drop:</td>
<td>0</td>
</tr>
<tr>
<td>Packets Bad mld Checksum:</td>
<td>0</td>
</tr>
<tr>
<td>Packets TTL Not One:</td>
<td>0</td>
</tr>
<tr>
<td>Packets TTL Not One Drop:</td>
<td>0</td>
</tr>
<tr>
<td>Queries Too Short:</td>
<td>0</td>
</tr>
<tr>
<td>V1 Reports Too Short:</td>
<td>0</td>
</tr>
<tr>
<td>V2 Reports Too Short:</td>
<td>0</td>
</tr>
<tr>
<td>V1 Leaves Too Short:</td>
<td>0</td>
</tr>
<tr>
<td>MLD Messages Unknown:</td>
<td>0</td>
</tr>
<tr>
<td>MLD Messages GT Max Ver:</td>
<td>0</td>
</tr>
<tr>
<td>MLD Messages LT Min Ver:</td>
<td>0</td>
</tr>
<tr>
<td>Queries Bad Source:</td>
<td>0</td>
</tr>
<tr>
<td>Queries Dropped by S/W Router Guard:</td>
<td>0</td>
</tr>
<tr>
<td>General Queries DA Not All Nodes:</td>
<td>0</td>
</tr>
<tr>
<td>GS-Queries Invalid Group:</td>
<td>0</td>
</tr>
<tr>
<td>GS-Queries DA Not Group:</td>
<td>0</td>
</tr>
<tr>
<td>GS-Queries Not From Querier:</td>
<td>0</td>
</tr>
<tr>
<td>GS-Queries Unknown Group:</td>
<td>0</td>
</tr>
<tr>
<td>Command</td>
<td>Count</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Reports Invalid Group:</td>
<td>0</td>
</tr>
<tr>
<td>Reports Link-Local Group:</td>
<td>0</td>
</tr>
<tr>
<td>Reports DA Not Group:</td>
<td>0</td>
</tr>
<tr>
<td>Reports No Querier:</td>
<td>0</td>
</tr>
<tr>
<td>Leaves Invalid Group:</td>
<td>0</td>
</tr>
<tr>
<td>Leaves Invalid DA:</td>
<td>0</td>
</tr>
<tr>
<td>Leaves No Querier:</td>
<td>0</td>
</tr>
<tr>
<td>Leaves Non-Member:</td>
<td>0</td>
</tr>
<tr>
<td>Leaves Non-Dynamic Member:</td>
<td>0</td>
</tr>
<tr>
<td>Leaves Non-V1 Member:</td>
<td>0</td>
</tr>
<tr>
<td>V2 Reports Invalid Group:</td>
<td>0</td>
</tr>
<tr>
<td>V2 Reports Link-Local Group:</td>
<td>0</td>
</tr>
<tr>
<td>V2 Reports DA Not All V2 Routers:</td>
<td>0</td>
</tr>
<tr>
<td>V2 Reports No Querier:</td>
<td>0</td>
</tr>
<tr>
<td>V2 Reports Older Version Querier:</td>
<td>0</td>
</tr>
<tr>
<td>V2 Reports Invalid Group Record Type:</td>
<td>0</td>
</tr>
<tr>
<td>V2 Reports No Sources:</td>
<td>0</td>
</tr>
<tr>
<td>V2 Leaves Non-Member:</td>
<td>0</td>
</tr>
<tr>
<td>PIM Msgs Dropped by S/W Router Guard:</td>
<td>0</td>
</tr>
<tr>
<td>Rx Other:</td>
<td></td>
</tr>
<tr>
<td>Proxy General Queries:</td>
<td>0</td>
</tr>
<tr>
<td>Proxy GS-Queries:</td>
<td>0</td>
</tr>
<tr>
<td>Proxy Reports:</td>
<td>0</td>
</tr>
<tr>
<td>Tx Errors:</td>
<td></td>
</tr>
<tr>
<td>V2 Sources Not Reported:</td>
<td>0</td>
</tr>
<tr>
<td>No Querier in BD:</td>
<td>0</td>
</tr>
<tr>
<td>No L2 Info for BD:</td>
<td>0</td>
</tr>
<tr>
<td>Startup Query Sync Statistics:</td>
<td></td>
</tr>
<tr>
<td>Stale Port Groups Deleted:</td>
<td>0</td>
</tr>
<tr>
<td>Stale Port Group Sources Deleted:</td>
<td>0</td>
</tr>
</tbody>
</table>
### show mld snooping group

To display MLD group membership information, use the **show mld snooping group** command in EXEC mode.

```
show mld snooping group [summary [group-address] [{bridge-domain bridge-domain-name|port {interface-name|neighbor ipaddr pw-id id}}][{group-address} [{bridge-domain bridge-domain-name|port {interface-name|neighbor ipaddr pw-id id}}] [source source-address] [detail]]
```

#### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>(Optional) Provides per group summary information.</td>
</tr>
<tr>
<td>group-address</td>
<td>(Optional) Provides IP group address information for the specified group in A.B.C.D format.</td>
</tr>
<tr>
<td>bridge-domain</td>
<td>(Optional) Provides group membership information for the specified bridge domain.</td>
</tr>
<tr>
<td>bridge-domain-name</td>
<td></td>
</tr>
<tr>
<td>port</td>
<td>(Optional) Provides group membership information for the specified AC port.</td>
</tr>
<tr>
<td>port neighbor</td>
<td>(Optional) Provides group membership information for the specified PW port.</td>
</tr>
<tr>
<td>ipaddr pw-id</td>
<td></td>
</tr>
<tr>
<td>id</td>
<td></td>
</tr>
<tr>
<td>source</td>
<td>(Optional) Provides group membership information for groups indicating interest in a specified source address.</td>
</tr>
<tr>
<td>source-address</td>
<td></td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Provides detailed information in a multiline display per group.</td>
</tr>
</tbody>
</table>

#### Command Default

None

#### Command Modes

EXEC

#### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

#### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command to display information about group membership in the Layer-2 forwarding tables. The display includes indicators identifying whether the group information was obtained dynamically (for example, snooped) or statically configured.

The command offers the following levels of detail:

- The basic command with no keywords displays group membership information as one line per port within group.
• The **summary** keyword summarizes the port statistics into one line per group. The **summary** keyword is mutually exclusive with the **port-view**, **source**, and **detail** keywords.
• The **detail** keyword includes traffic statistics and counters.

### Examples

The following example shows group membership information by groups within bridge domains.

```bash
RP/0/RSP0/CPU0:router# show mld snooping group

Flags Key: S=Static, D=Dynamic, E=Explicit Tracking

**Bridge Domain bg1:bd1**

<table>
<thead>
<tr>
<th>Group</th>
<th>Ver GM</th>
<th>Source</th>
<th>PM Port</th>
<th>Exp Flg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ff12:1:1::1 V2 Exc</td>
<td>-</td>
<td>- GigabitEthernet/1/1/0</td>
<td>122</td>
<td>DE</td>
</tr>
<tr>
<td>Ff12:1:1::1 V2 Exc 2002:1:1:1</td>
<td>Inc GigabitEthernet/1/1/1</td>
<td>5</td>
<td>DE</td>
<td></td>
</tr>
<tr>
<td>Ff12:1:1::1 V2 Exc 2002:1:1:1</td>
<td>Inc GigabitEthernet/1/1/2</td>
<td>never S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ff12:1:1::1 V2 Exc 2002:1:1:1</td>
<td>Exc GigabitEthernet/1/1/3</td>
<td>- DE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ff12:1:1::1 V2 Exc 2002:1:1:2</td>
<td>Inc GigabitEthernet/1/1/0</td>
<td>202</td>
<td>DE</td>
<td></td>
</tr>
<tr>
<td>Ff12:1:1::1 V2 Exc 2002:1:1:2</td>
<td>Exc GigabitEthernet/1/1/1</td>
<td>- DE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ff12:1:1::2 V2 Exc 2002:1:1:1</td>
<td>Inc GigabitEthernet/1/1/0</td>
<td>145</td>
<td>DE</td>
<td></td>
</tr>
<tr>
<td>Ff12:1:1::2 V2 Exc 2002:1:1:1</td>
<td>Inc GigabitEthernet/1/1/1</td>
<td>0</td>
<td>DE</td>
<td></td>
</tr>
<tr>
<td>Ff12:1:1::2 V2 Exc 2002:1:1:1</td>
<td>Exc GigabitEthernet/1/1/2</td>
<td>11</td>
<td>DE</td>
<td></td>
</tr>
</tbody>
</table>

**Bridge Domain bg1:bd4**

<table>
<thead>
<tr>
<th>Group</th>
<th>Ver GM</th>
<th>Source</th>
<th>PM Port</th>
<th>Exp Flg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ff24:1:1::2 V1 Exc</td>
<td>-</td>
<td>- GigabitEthernet/1/1/0</td>
<td>122</td>
<td>DE</td>
</tr>
<tr>
<td>Ff28:1:1::1 V1 -</td>
<td>- GigabitEthernet/1/1/1</td>
<td>33</td>
<td>DE</td>
<td></td>
</tr>
<tr>
<td>Ff29:1:2::3 V1 Exc</td>
<td>- GigabitEthernet/1/2/0</td>
<td>122</td>
<td>DE</td>
<td></td>
</tr>
<tr>
<td>Ff32:1:2::3 V2 Exc 2000:1:1:2</td>
<td>Exc GigabitEthernet/1/2/1</td>
<td>5</td>
<td>DE</td>
<td></td>
</tr>
</tbody>
</table>

The following example shows group membership information by group within a specific bridge domain.

```bash
RP/0/RSP0/CPU0:router# show mld snooping group bridge-domain Group1:BD-1

Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, E=Explicit Tracking

**Bridge Domain bg1:bd1**

<table>
<thead>
<tr>
<th>Group</th>
<th>Ver GM</th>
<th>Source</th>
<th>PM Port</th>
<th>Exp Flg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ff12:1:1::1 V2 Exc</td>
<td>-</td>
<td>- GigabitEthernet/1/1/0</td>
<td>122</td>
<td>DE</td>
</tr>
<tr>
<td>Ff12:1:1::1 V2 Exc 2002:1:1:1</td>
<td>Inc GigabitEthernet/1/1/1</td>
<td>5</td>
<td>DE</td>
<td></td>
</tr>
<tr>
<td>Ff12:1:1::1 V2 Exc 2002:1:1:1</td>
<td>Inc GigabitEthernet/1/1/2</td>
<td>never S</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ff12:1:1::1 V2 Exc 2002:1:1:1</td>
<td>Exc GigabitEthernet/1/1/3</td>
<td>- DE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ff12:1:1::1 V2 Exc 2002:1:1:2</td>
<td>Inc GigabitEthernet/1/1/0</td>
<td>202</td>
<td>DE</td>
<td></td>
</tr>
<tr>
<td>Ff12:1:1::1 V2 Exc 2002:1:1:2</td>
<td>Exc GigabitEthernet/1/1/1</td>
<td>- DE</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ff12:1:1::2 V2 Exc 2002:1:1:1</td>
<td>Inc GigabitEthernet/1/1/0</td>
<td>145</td>
<td>DE</td>
<td></td>
</tr>
</tbody>
</table>
```
The following example shows group membership information by groups within a specific port.

```
RP/0/RSP0/CPU0:router# show mld snooping group port GigabitEthernet 0/1/1/1

Key: GM=Group Filter Mode, PM=Port Filter Mode
Flags Key: S=Static, D=Dynamic, E=Explicit Tracking
```

```
Bridge Domain bg1:bd1

<table>
<thead>
<tr>
<th>Group</th>
<th>Ver</th>
<th>GM</th>
<th>Source</th>
<th>PM</th>
<th>Port</th>
<th>Exp</th>
<th>Flg</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ff12:1:1::1</td>
<td>V2</td>
<td>Exc</td>
<td>2002:1::1</td>
<td>Inc GigabitEthernet0/1/1</td>
<td>0</td>
<td>DE</td>
<td></td>
</tr>
<tr>
<td>Ff12:1:1::2</td>
<td>V2</td>
<td>Exc</td>
<td>2002:1::1</td>
<td>Exc GigabitEthernet0/1/1</td>
<td>11</td>
<td>DE</td>
<td></td>
</tr>
<tr>
<td>Ff12:1:1::3</td>
<td>V2</td>
<td>Exc</td>
<td>2002:1::1</td>
<td>Inc GigabitEthernet0/1/1</td>
<td>0</td>
<td>DE</td>
<td></td>
</tr>
</tbody>
</table>
```

The following example summarizes each group's membership information into a single line.

```
RP/0/RSP0/CPU0:router# show mld snooping group summary

Bridge Domain bg1:bd1
```

```
<table>
<thead>
<tr>
<th>Group</th>
<th>Ver</th>
<th>GM</th>
<th>Source</th>
<th>#Ports</th>
<th>#Srcs</th>
<th>#Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ff12:1:1::1</td>
<td>V1</td>
<td>-</td>
<td>-</td>
<td>5</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Ff12:1:1::2</td>
<td>V2</td>
<td>Exc</td>
<td>2002:1:1</td>
<td>22</td>
<td>55</td>
<td>78</td>
</tr>
<tr>
<td>Ff12:1:1::3</td>
<td>V2</td>
<td>Exc</td>
<td>2002:1:1</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Ff12:1:1::4</td>
<td>V2</td>
<td>Inc</td>
<td>2002:1:1</td>
<td>12</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>Ff12:1:1::5</td>
<td>V2</td>
<td>Exc</td>
<td>2002:1:1</td>
<td>22</td>
<td>22</td>
<td>22</td>
</tr>
</tbody>
</table>
```

The following example shows detail information about each group.

```
RP/0/RSP0/CPU0:router# show mld snooping group detail

Flags Key: S=Static, D=Dynamic, E=Explicit Tracking
```

```
Bridge Domain bg1:bd1
```

```
<table>
<thead>
<tr>
<th>Group Address:</th>
<th>ff28:1:2::3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version:</td>
<td>V2</td>
</tr>
<tr>
<td>Uptime:</td>
<td>02:22:22</td>
</tr>
<tr>
<td>Group Filter Mode:</td>
<td>Exclude</td>
</tr>
<tr>
<td>Expires:</td>
<td>158</td>
</tr>
<tr>
<td>Static Port Group Count:</td>
<td>2</td>
</tr>
<tr>
<td>Source Count:</td>
<td>10</td>
</tr>
<tr>
<td>Include Source Count:</td>
<td>6</td>
</tr>
<tr>
<td>Exclude Source Count:</td>
<td>6</td>
</tr>
<tr>
<td>Static Include Source Count:</td>
<td>2</td>
</tr>
<tr>
<td>Source:</td>
<td>star</td>
</tr>
<tr>
<td>Include Port Count:</td>
<td>1</td>
</tr>
<tr>
<td>Exclude Port Count:</td>
<td>1</td>
</tr>
</tbody>
</table>
show mld snooping group

Static Include Port Count: 0
Include Ports:
- GigabitEthernet0/1/1/0 02:02:22 145 D
Exclude Ports:
- GigabitEthernet0/1/1/1 02:02:22 222 DE
Source: 2000:1:2::3
Include Port Count: 4
Exclude Port Count: 3
Static Include Port Count: 3
Include Ports:
- GigabitEthernet0/1/1/0 02:02:22 never S
- GigabitEthernet0/1/1/1 02:02:22 15 DE
- GigabitEthernet0/1/1/2 02:02:22 98 SE
- GigabitEthernet0/1/1/3 02:02:22 never S
Exclude Ports:
- GigabitEthernet0/1/1/4 02:02:22 22 D
- GigabitEthernet0/1/1/5 02:02:22 2 DE
- GigabitEthernet0/1/1/6 02:02:22 0 D
Source: 2000:1:2::4
Include Port Count: 1
Exclude Port Count: 1
Static Include Port Count: 0
Include Ports:
- GigabitEthernet0/1/1/0 02:02:22 34 D
Exclude Ports:
- GigabitEthernet0/1/1/1 02:02:22 34 E
Group Address: ff28:2:2::4
Version: V1
Uptime: 02:22:22
Expires: 115
Port Count: 3
Ports:
- GigabitEthernet0/1/1/0 02:02:22 29 D
- GigabitEthernet0/1/1/1 02:02:22 310 D
- GigabitEthernet0/1/1/2 02:02:22 12 D
show mld snooping port

To display MLD snooping configuration information and traffic counters by router interface port, use the show mld snooping port command in EXEC mode.

```
show mld snooping port
interface-name|neighbor ipaddr pw-id id|bridge-domain bridge-domain-name
detail [statistics [include-zeroes]]
group [ group-address ] [source source-address] [detail]
```

**Syntax Description**

- **interface-name** (Optional) Displays information only for the specified AC port.
- **neighbor ipaddr pw-id id** (Optional) Displays information only for the specified PW port.
- **bridge-domain**
  - **bridge-domain-name** (Optional) Displays information for ports in the specified bridge domain.
- **detail** (Optional) Includes port details, rather than a single line summary.
- **statistics** (Optional) Includes mld traffic counters and statistics in the detail display.
- **include-zeroes** (Optional) Includes all statistics, even if they are zero. Without this keyword, many statistics are omitted from the display when their values are zero.
- **group** (Optional) Provides group membership information in its entirety as received at each port. The display is organized by port, showing groups within ports.
- **group-address** (Optional) Displays information only for the specified group address, organized by port.
- **source source-address** (Optional) Displays information only for the specified source address, organized by port.
- **detail** (Optional) Includes group details.

**Command Default**

None

**Command Modes**

EXEC

**Command History**

- **Release 4.3.0** This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
This command displays mld snooping information organized by mld snooping port. Use the command without any keywords to display summary information about all ports, in a single line per port.

Use optional arguments and keywords to request the following:

- Limit the display to a specified port.
- Limit the display to ports under a specified bridge.
- Request details and traffic statistics per port.

Note: The `statistics` keyword cannot be used in the same command with the `group` keyword.

- Organize the display by group within ports. Use the `group` keyword with or without a specified interface or bridge domain.
- Limit the group information to specific groups or source addresses.

The `statistics` keyword displays mld traffic information, including mld queries, reports, and leaves. The three columns in the statistics section of the display are:

- Received—Number of packets received.
- Rejected—Number of packets received, processed, and rejected back into the forwarding path.
- Generated—Number of packets generated by the mld snooping application and injected into the forwarding path.

### Examples

The following example shows summary information per port:

```
RP/0/RSP0/CPU0:router# show mld snooping port

Bridge Domain Domain1:BD-1

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>#Grps</th>
<th>#Srcs</th>
<th>#Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/1/0/1</td>
<td>Up</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/2</td>
<td>Up</td>
<td>4</td>
<td>22</td>
<td>2</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/3</td>
<td>Up</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/4</td>
<td>Up</td>
<td>4</td>
<td>23</td>
<td>2</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/5</td>
<td>Up</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/6</td>
<td>Up</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/7</td>
<td>Up</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/8</td>
<td>Up</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/9</td>
<td>Up</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/10</td>
<td>Up</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/11</td>
<td>Up</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/12</td>
<td>Up</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

(Bridge Domain Domain1:BD-4)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>#Grps</th>
<th>#Srcs</th>
<th>#Hosts</th>
</tr>
</thead>
</table>
```

The following example shows summary information per port:

```
RP/0/RSP0/CPU0:router# show mld snooping port

Bridge Domain Domain1:BD-1

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>#Grps</th>
<th>#Srcs</th>
<th>#Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>GigabitEthernet0/1/0/1</td>
<td>Up</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/2</td>
<td>Up</td>
<td>4</td>
<td>22</td>
<td>2</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/3</td>
<td>Up</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/4</td>
<td>Up</td>
<td>4</td>
<td>23</td>
<td>2</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/5</td>
<td>Up</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/6</td>
<td>Up</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/7</td>
<td>Up</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/8</td>
<td>Up</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/9</td>
<td>Up</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/10</td>
<td>Up</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/11</td>
<td>Up</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>GigabitEthernet0/1/0/12</td>
<td>Up</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>

(Bridge Domain Domain1:BD-4)

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>#Grps</th>
<th>#Srcs</th>
<th>#Hosts</th>
</tr>
</thead>
</table>
```
The following example shows summary information for a specific port.

```
RP/0/RSP0/CPU0:router# show mld snooping port GigabitEthernet 0/1/0/2  
Bridge Domain Domain1:BD-1
Port  State  #Grps  #Srcs  #Hosts
----  ------  -----  -----  -----  
GigabitEthernet0/1/0/2  Up  4  4  4
```

The following example shows detail information about a specified port.

```
RP/0/RSP0/CPU0:router# show mld snooping port gigabitEthernet0/1/0/2 detail statistics
GigabitEthernet0/1/0/2 is up
Bridge Domain: Domain1:BD-1
MLD Snoop Profile: profile1
Explicit Tracking Enabled
MLD Group Count: 4
Traffic Statistics (elapsed time since last cleared 00:58:04):

  | Received | Reinjected | Generated |
---|----------|------------|-----------|
Valid Packets: | 110869512 | 120327 | 28 |
MLD General Queries: | 4950 | 0 | 28 |
MLD Group Specific Queries: | 0 | 0 | 0 |
MLD V1 Reports: | 0 | - | - |
MLD V2 Reports: | 110864562 | 120327 | 0 |
MLD V3 Reports: | 0 | 0 | - |
MLD V2 Leaves: | 0 | 0 | 0 |
MLD Global Leaves: | 0 | - | 0 |
```
PIM Hellos: 0 0 -  
Rx Packets Flooded: 0  
Rx Packets Forwarded To Members: 0  
Rx Packets Forwarded To Mrouters: 120327  
Rx Packets Consumed: 110749185  
Reports Suppressed: 110749185  
Errors: None  

The following example shows detail, including statistics, for a specified port (with the include zeroes option).

```
RP/0/RSP0/CPU0:router# show mld snooping port GigabitEthernet 0/1/0/2 detail statistics include-zeroes

GigabitEthernet0/1/0/2 is up  
Bridge Domain: Domain1:BD-1  
MLD Snoop Profile: profile1  
Explicit Tracking Enabled  
MLD Group Count: 4  
Traffic Statistics (elapsed time since last cleared 00:58:04):  

<table>
<thead>
<tr>
<th>Valid Packets</th>
<th>Received</th>
<th>Reinjected</th>
<th>Generated</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLD General Queries</td>
<td>110869512</td>
<td>120327</td>
<td>28</td>
</tr>
<tr>
<td>MLD Group Specific Queries</td>
<td>4950</td>
<td>0</td>
<td>28</td>
</tr>
<tr>
<td>MLD V1 Reports</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MLD V2 Reports</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MLD V1 Leaves</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>MLD Global Leaves</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>PIM Hellos</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Packets Flooded</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Packets Forwarded To Members</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Packets Forwarded To Mrouters</td>
<td>120327</td>
<td>120327</td>
<td>0</td>
</tr>
<tr>
<td>Rx Packets Consumed</td>
<td>110749185</td>
<td>110749185</td>
<td>0</td>
</tr>
<tr>
<td>Reports Suppressed</td>
<td>110749185</td>
<td>110749185</td>
<td>0</td>
</tr>
<tr>
<td>Errors:</td>
<td>Rx Packets On Inactive Port</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Packet Martian</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Packet Bad Protocol</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Packet DA Not Multicast</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Packet Missing Router Alert</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Packet Missing Router Alert Drop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Packet Bad MLD Checksum</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Packets TTL Not One</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Packets TTL Not One Drop</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Queries Too Short</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx V1 Reports Too Short</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx V2 Reports Too Short</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx MLD Messages Unknown</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx MLD Messages GT Max Ver</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx MLD Messages LT Min Ver</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Queries Bad Source</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx General Queries DA Not All Nodes</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Reports DA Not Group</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Reports No Querier</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Leaves Invalid Group</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Leaves DA Not All Routers</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Leaves No Querier</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Leaves Unknown Group</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Rx Leaves Non Member</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
show mld snooping profile

To display MLD snooping profile information, use the **show mld snooping profile** command in EXEC mode.

```
show mld snooping profile [summary][profile-name] [detail [include-defaults]] [[references
bridge-domain [bridge-domain-name]]|port [interface-name|neighbor ipaddr pw-id id]]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>(Optional) Displays a summary of profile instances, bridge domain references, and port references.</td>
</tr>
<tr>
<td>profile-name</td>
<td>(Optional) Displays information only for the named profile.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays the contents of profiles.</td>
</tr>
<tr>
<td>include-defaults</td>
<td>(Optional) Displays all default configurations with the profile contents. Without this keyword, only configured profile information is displayed.</td>
</tr>
<tr>
<td>references</td>
<td>(Optional) Shows which bridge domains and bridge ports reference each profile.</td>
</tr>
<tr>
<td>bridge-domain</td>
<td>(Optional) Provides a bridge domain filter for the references keyword. Without bridge-domain-name, the display shows profiles attached to all bridge domains. With bridge-domain-name, the display shows only the profile attached to the specified bridge domain.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Command Default</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Command Modes</td>
<td>EXEC</td>
</tr>
<tr>
<td>Command History</td>
<td>Release 4.3.0  This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

Use this command to display the contents of profiles and to see associations of profiles with bridge-domains and ports.

The **summary** keyword lists profile names and summarizes their usage on bridge domains and ports. No other keywords can be used with summary.

Use the **details** keyword with a profile name to show the contents of a specific profile. Without a profile name, the **detail** keyword shows the contents of all profiles.
Use the **references** keyword to list the relationships between profiles and bridge domains or profiles and ports. You have the following options:

- Use the **references** keyword without any other keywords to show all profiles and the ports and bridge domains they are attached to.
- Use the **references** keyword with the **name** keyword to show a specific profile and where it is attached.
- Use the **port** keyword to list all ports and the profiles attached to them.
- Use the **port** keyword with a specific AC interface or PW to see the profile attached to the named port.
- Use the **bridge-domain** keyword to list all bridge domains and the profiles attached to them.
- Use the **bridge-domain** keyword with a specific bridge domain name to see the profile attached to a specific bridge domain.

**Examples**

The following example lists profile names and shows summary level profile usage.

```plaintext
RP/0/RSP0/CPU0:router# show mld snooping profile

<table>
<thead>
<tr>
<th>Profile</th>
<th>Bridge Domain</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile1</td>
<td>0</td>
<td>8193</td>
</tr>
<tr>
<td>profile2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>profile3</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>profile4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>profile5</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>profile6</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>profile7</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>
```

The following example shows summary level profile usage for a named profile.

```plaintext
RP/0/RSP0/CPU0:router# show mld snooping profile profile1

<table>
<thead>
<tr>
<th>Profile</th>
<th>Bridge Domain</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile1</td>
<td>0</td>
<td>8193</td>
</tr>
</tbody>
</table>
```

The following example shows the contents of each profile.

```plaintext
RP/0/RSP0/CPU0:router# show mld snooping profile detail

mld Snoop Profile profile1:

  Bridge Domain References: 3
  Port References: 0

MLD Snoop Profile profile2:

  Static Groups: ff28:1:1::2
                 ff29:1:1::4    2000:1::2
  Bridge Domain References: 0
  Port References: 1
```
MLD Snoop Profile profile3:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static Mrouter</td>
<td>Enabled</td>
</tr>
<tr>
<td>Bridge Domain References</td>
<td>0</td>
</tr>
<tr>
<td>Port References</td>
<td>1</td>
</tr>
</tbody>
</table>

The following example shows output reflecting the access-group, group limit, and tcn flood disable parameters:

```
RP/0/RSP0/CPU0:router# show mld snooping profile detail
MLD Snoop Profile profile:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Querier LMQ Count</td>
<td>2</td>
</tr>
<tr>
<td>Access Group ACL</td>
<td>iptv-white-list</td>
</tr>
<tr>
<td>Group Policy</td>
<td>iptv-group-weights</td>
</tr>
<tr>
<td>Group Limit</td>
<td>16</td>
</tr>
<tr>
<td>Immediate Leave</td>
<td>Enabled</td>
</tr>
<tr>
<td>TCN Flood</td>
<td>Disabled</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bridge Domain References</td>
<td>1</td>
</tr>
<tr>
<td>Port References</td>
<td>0</td>
</tr>
</tbody>
</table>
```

The following example shows the contents of a named profile and the implied default configurations:

```
RP/0/RSP0/CPU0:router# show mld snooping profile profile1 detail include-defaults
mld Snoop Profile profile p1:

<table>
<thead>
<tr>
<th>Feature</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>System IP Address</td>
<td>fe80::1aef:63ff:fee2:5fc6</td>
</tr>
<tr>
<td>Minimum Version</td>
<td>2</td>
</tr>
<tr>
<td>Report Suppression</td>
<td>Enabled</td>
</tr>
<tr>
<td>Unsolicited Report Interval</td>
<td>1000 (milliseconds)</td>
</tr>
<tr>
<td>TCN Query Solicit</td>
<td>Enabled</td>
</tr>
<tr>
<td>TCN Membership Sync</td>
<td>Disabled</td>
</tr>
<tr>
<td>TCN Flood</td>
<td>Enabled</td>
</tr>
<tr>
<td>TCN Flood Query Count</td>
<td>2</td>
</tr>
<tr>
<td>Router Alert Check</td>
<td>Disabled</td>
</tr>
<tr>
<td>TTL Check</td>
<td>Disabled</td>
</tr>
<tr>
<td>Internal Querier Support</td>
<td>Enabled</td>
</tr>
<tr>
<td>Internal Querier Version</td>
<td>3</td>
</tr>
<tr>
<td>Internal Querier Timeout</td>
<td>0 (seconds)</td>
</tr>
<tr>
<td>Internal Querier Interval</td>
<td>60 (seconds)</td>
</tr>
<tr>
<td>Internal Querier Max Response Time</td>
<td>10 (seconds)</td>
</tr>
<tr>
<td>Internal Querier TCN Query Interval</td>
<td>10 (seconds)</td>
</tr>
<tr>
<td>Internal Querier TCN Query Count</td>
<td>2</td>
</tr>
<tr>
<td>Internal Querier TCN Query MRT</td>
<td>0</td>
</tr>
<tr>
<td>Internal Querier Robustness</td>
<td>2</td>
</tr>
<tr>
<td>Querier Query Interval</td>
<td>60 (seconds)</td>
</tr>
<tr>
<td>Querier LMQ Interval</td>
<td>1000 (milliseconds)</td>
</tr>
<tr>
<td>Querier LMQ Count</td>
<td>2</td>
</tr>
<tr>
<td>Querier Robustness</td>
<td>2</td>
</tr>
<tr>
<td>Immediate Leave</td>
<td>Disabled</td>
</tr>
<tr>
<td>Explicit Tracking</td>
<td>Disabled</td>
</tr>
<tr>
<td>Static Mrouter</td>
<td>Disabled</td>
</tr>
<tr>
<td>Router Guard</td>
<td>Disabled</td>
</tr>
</tbody>
</table>
```
Access Group ACL: (empty)

Group Policy: 
Group Limit: -1

ICCP Group Report Standby State: Enabled

Startup Query Interval: 15 (seconds)
Startup Query Count: 2
Startup Query Max Response Time: 10 (seconds)
Startup Query on Port Up: Enabled
Startup Query on IG Port Active: Disabled
Startup Query on Topology Change: Disabled
Startup Query on Process Start: Disabled

Static Groups: ff28:1:1::2
ff29:1:1::4 2000:1::2

Bridge Domain References: 1
Port References: 0

The following command shows a summary of profile usage, by profile name.

```
RP/0/RSP0/CPU0:router# show mld snooping profile summary
```

Number of profiles: 3
Number of bridge domain references: 3
Number of port references: 8195

The following command lists all MLD snooping profiles and shows which bridge domains and ports are configured to use each profile.

```
RP/0/RSP0/CPU0:router# show mld snooping profile references
```

<table>
<thead>
<tr>
<th>Profile</th>
<th>Bridge Domains</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile1</td>
<td>None</td>
<td>GigabitEthernet0/1/0/0&lt;br&gt;GigabitEthernet0/1/0/1&lt;br&gt;GigabitEthernet0/1/0/2&lt;br&gt;GigabitEthernet0/1/0/3&lt;br&gt;GigabitEthernet0/1/0/4&lt;br&gt;GigabitEthernet0/1/0/5&lt;br&gt;(... missing lines)&lt;br&gt;GigabitEthernet0/3/3/1109&lt;br&gt;GigabitEthernet0/3/3/1110&lt;br&gt;GigabitEthernet0/3/3/1111</td>
</tr>
<tr>
<td>profile2</td>
<td>Domain1:BD-1</td>
<td>None</td>
</tr>
<tr>
<td>profile3</td>
<td>None</td>
<td>Domain1:BD103</td>
</tr>
<tr>
<td>profile4</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>profile5</td>
<td>None</td>
<td>Domain1:BD105</td>
</tr>
</tbody>
</table>

Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference, Release 5.3.x
Profile: profile6
Bridge Domains: None
Ports: None

Profile: profile7
Bridge Domains: Domain1:BD107
Ports: None

The following command lists all bridges or ports that are configured to use the profile named profile1.

RP/0/RSP0/CPU0:router# show mld snooping profile profile1 references

Profile: profile1
Bridge Domains: None
Ports: GigabitEthernet 0/1/0/0
GigabitEthernet 0/1/0/1
GigabitEthernet 0/1/0/2
GigabitEthernet 0/1/0/3
GigabitEthernet 0/1/0/4
GigabitEthernet 0/1/0/5
(... missing lines)
GigabitEthernet 0/3/3/1109
GigabitEthernet 0/3/3/1110
GigabitEthernet 0/3/3/1111

The following example shows the profile attached to a specific bridge domain.

RP/0/RSP0/CPU0:router# show mld snooping profile references bridge-domain Group1:BD-1

Profile: profile1
Bridge Domains: Group1:BD-1

The following example shows the profile attached to a specific port.

RP/0/RSP0/CPU0:router# show mld snooping profile references port GigabitEthernet 0/1/0/2

Profile: profile2
Ports: GigabitEthernet0/1/0/2
show mld snooping summary

To display summary information about MLD snooping configuration and traffic statistics for the router, use the show mld snooping summary command in EXEC mode.

```
show mld snooping summary [statistics [include-zeroes]]
```

**Syntax Description**

- **statistics** (Optional) Displays mld traffic counters and statistics.
- **include-zeroes** (Optional) Displays all statistics, even if they are zero. Without this keyword, many statistics are omitted from the display when their values are zero.

**Command Default**

None

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

This command summarizes the number of bridge domains, mrouter ports, host ports, groups, and sources configured on the router.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read</td>
</tr>
</tbody>
</table>

**Example**

The following example shows the output of the command:

```
Bridge Domains: 1
  MLD Snooping Bridge Domains: 1
  Ports: 3
  MLD Snooping Ports: 3
  Mroute: 0
  STP Forwarding Ports: 0
  ICCP Group Ports: 0
  MLD Groups: 0
  Member Ports: 0
  MLD Source Groups: 0
  Static/Include/Exclude: 0/0/0
  Member Ports (Include/Exclude): 0/0
```

The following example shows the output of the command with the **statistics** keyword:
Bridge Domains: 1
MLD Snooping Bridge Domains: 1
Ports: 3
MLD Snooping Ports: 3
Mrouters: 0
STP Forwarding Ports: 0
ICCP Group Ports: 0
MLD Groups: 0
Member Ports: 0
MLD Source Groups: 0
Static/Include/Exclude: 0/0/0
Member Ports (Include/Exclude): 0/0
Traffic Statistics (elapsed time since last cleared 00:57:52):

Received  Reinjected  Generated
Messages: 0 0 0
MLD General Queries: 0 0 0
MLD Group Specific Queries: 0 0 0
MLD G&S Specific Queries: 0 0 0
MLD V1 Reports: 0 0 0
MLD V2 Reports: 0 0 0
MLD V1 Leaves: 0 0 0
MLD Global Leaves: 0 - 0
PIM Hellos: 0 0 -
Rx Packet Treatment:
Packets Flooded: 0
Packets Forwarded To Members: 0
Packets Forwarded To Mrouters: 0
Packets Consumed: 0
Rx Errors:
Packets DA Not Multicast: 4
Rx Other:
None
Tx Errors:
None
Startup Query Sync Statistics:
None

The following example shows the output of the command with the `include-zeroes` keyword:

Bridge Domains: 1
MLD Snooping Bridge Domains: 1
Ports: 3
MLD Snooping Ports: 3
Mrouters: 0
STP Forwarding Ports: 0
ICCP Group Ports: 0
MLD Groups: 0
Member Ports: 0
MLD Source Groups: 0
Static/Include/Exclude: 0/0/0
Member Ports (Include/Exclude): 0/0
Traffic Statistics (elapsed time since last cleared 00:57:52):

Received  Reinjected  Generated
Messages: 0 0 0
MLD General Queries: 0 0 0
MLD Group Specific Queries: 0 0 0
MLD G&S Specific Queries: 0 0 0
MLD V1 Reports: 0 0 0
MLD V2 Reports: 0 0 0
MLD V1 Leaves: 0 0 0
MLD Global Leaves: 0 - 0
PIM Hellos: 0 0 -
Rx Packet Treatment:
Packets Flooded: 0
Packets Forwarded To Members: 0
show mld snooping summary

Packets Forwarded To Mrouters: 0
Packets Consumed: 0
Reports Suppressed: 0
Access Group Permits: 0
Access Group Denials: 0
Group Limits Exceeded: 0
MLD Blocks Ignored in V1 Compat Mode: 0
MLD EX S-lists Ignored in V1 Compat Mode: 0
Rx MLD V2 Report Group Record Types:
Is Include: 0
Change To Include: 0
Is Exclude: 0
Change To Exclude: 0
Allow New Sources: 0
Block Old Sources: 0
Rx Errors:
Packets On Inactive Bridge Domain: 0
Packets On Inactive Port: 0
Packets Martian: 0
Packets Bad Protocol: 0
Packets DA Not Multicast: 4
Packets Missing Router Alert: 0
Packets Missing Router Alert Drop: 0
Packets Bad mld Checksum: 0
Packets TTL Not One: 0
Packets TTL Not One Drop: 0
Queries Too Short: 0
V1 Reports Too Short: 0
V2 Reports Too Short: 0
V1 Leaves Too Short: 0
V2 Reports Link-Local Group: 0
MLD Messages Unknown: 0
MLD Messages GT Max Ver: 0
MLD Messages LT Min Ver: 0
Queries Bad Source: 0
Queries Dropped by S/W Router Guard: 0
General Queries DA Not All Nodes: 0
GS-Queries Invalid Group: 0
GS-Queries DA Not Group: 0
GS-Queries Not From Querier: 0
GS-Queries Unknown Group: 0
Reports Invalid Group: 0
Reports Link-Local Group: 0
Reports DA Not Group: 0
Reports No Querier: 0
Leaves Invalid Group: 0
Leaves Invalid DA: 0
Leaves No Querier: 0
Leaves Non-Member: 0
Leaves Non-Dynamic Member: 0
Leaves Non-V1 Member: 0
V2 Reports Invalid Group: 0
V2 Reports Link-Local Group: 0
V2 Reports DA Not All V2 Routers: 0
V2 Reports No Querier: 0
V2 Reports Older Version Querier: 0
V2 Reports Invalid Group Record Type: 0
V2 Reports No Sources: 0
V2 Leaves Non-Member: 0
PIM Msgs Dropped by S/W Router Guard: 0
Rx Other:
Proxy General Queries: 0
Proxy GS-Queries: 0
Proxy Reports: 0
Tx Errors:
show mld snooping summary

V2 Sources Not Reported: 0
No Querier in BD: 0
No L2 Info for BD: 0
Startup Query Sync Statistics:
Stale Port Groups Deleted: 0
Stale Port Group Sources Deleted: 0
show mld snooping trace

To display MLD snooping process activity, use the **show mld snooping trace** command in EXEC mode.

```
show mld snooping trace [all|error|packet-error]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>all</th>
<th>(Optional) Displays all mld snooping process activity.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>error</td>
<td>(Optional) Displays only error tracepoints.</td>
</tr>
<tr>
<td></td>
<td>packet-error</td>
<td>(Optional) Displays packet error tracepoints.</td>
</tr>
</tbody>
</table>

**Command Default**

The **all** keyword is the default when no keywords are used.

**Command Modes**

EXEC

**Command History**

- **Release 3.7.2** This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use this command to research mldsnooping process activity.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows MLD snooping process status during a restart and a new profile configuration.

```
RP/0/RSP0/CPU0:router# show mld snooping summary trace all
51 wrapping entries (1024 possible, 0 filtered, 51 total)
Feb 1 14:30:24.902 mldsn/all 0/5/CPU0 t1 TP001:
Feb 2 14:30:24.902 mldsn/all 0/5/CPU0 t1 TP002: ******** mld SNOOP PROCESS RESTART ********
Feb 2 14:30:24.902 mldsn/all 0/5/CPU0 t1 TP001:
Feb 2 14:30:24.902 mldsn/all 0/5/CPU0 t1 TP286: initialize profile wavl tree
Feb 2 14:30:24.902 mldsn/all 0/5/CPU0 t1 TP185: initialize bd wavl tree
Feb 2 14:30:24.902 mldsn/all 0/5/CPU0 t1 TP230: initialize port wavl tree
Feb 2 14:30:24.902 mldsn/all 0/5/CPU0 t1 TP019: entered init_chkpt
Feb 2 14:30:24.902 mldsn/all 0/5/CPU0 t1 TP165: mldsn_init_l2fib entered
Feb 2 14:30:24.934 mldsn/all 0/5/CPU0 t1 TP611: l2fib_restart_timer_init
Feb 2 14:30:24.934 mldsn/all 0/5/CPU0 t1 TP680: mldsn_pd_mgid_api_init entered
Feb 2 14:30:24.937 mldsn/all 0/5/CPU0 t1 TP681: failed to open
libl2mc_snoop_mgid_client_pd.dll
Feb 2 14:30:24.937 mldsn/all 0/5/CPU0 t1 TP683: l2mc_snoop_pd_mgid funcs are stubbed
Feb 2 14:30:25.037 mldsn/all 0/5/CPU0 t1 TP080: socket open succeeded
```
Feb 2 14:30:25.037 mldsn/all 0/5/CPU0 t1 TP031: connection open for socket
Feb 2 14:30:25.037 mldsn/all 0/5/CPU0 t1 TP614: mldsn_l2fib_restart_timer_start, 300 secs
Feb 2 14:30:25.038 mldsn/all 0/5/CPU0 t1 TP555: mld SNOOP PROCESS READY
Feb 2 14:30:25.038 mldsn/all 0/5/CPU0 t1 TP017: entered event loop
Feb 2 14:30:25.038 mldsn/all 0/5/CPU0 t1 TP112: sysdb register verification
Feb 2 14:30:25.038 mldsn/all 0/5/CPU0 t1 TP286: initialize profile wav1 tree
Feb 2 14:30:25.040 mldsn/all 0/5/CPU0 t1 TP110: sysdb event verify func (CREATE & SET, profile/profile1/enter)
Feb 2 14:30:25.040 mldsn/all 0/5/CPU0 t1 TP287: create profile profile1
Feb 2 14:30:25.040 mldsn/all 0/5/CPU0 t1 TP534: profile profile1 (0x4826b838): initialized
static_group tree
(... missing lines)
startup query count

To configure the number of startup G-queries that are to be sent to the recipient routers, use the **startup query count** command in the appropriate snooping profile configuration mode. To restore the default startup query count to be the Querier’s Robustness Value (QRV), use the **no** form of this command.

```
startup query count number
no startup query count
```

**Syntax Description**

`number` Indicates the number of startup queries sent. The range is from 0-7.

**Command Default**

2

**Command Modes**

IGMP snooping profile configuration (config-igmp-snooping-profile) MLD snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following examples show how to configure the startup query count:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# startup query count

RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# startup query count
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
</tbody>
</table>
**startup query iccp-group**

To enable the generation of startup G-query on a port, when an MC-LAG transitions from standby state to active state, use the **startup query iccp-group** command in the appropriate snooping profile configuration mode. The snooping technique performs a mark and sweep synchronization of the snooping state over the startup query period.

To disable the startup query generation on this event, use the **no** form of this command.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port-active</td>
<td>(Optional) Issues startup queries when iccp-group goes active. This parameter is specific to IGMP Snooping over MC-LAG.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

IGMP snooping profile configurationMLD snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If configured in a bridge-domain profile, the **startup query iccp-group** command applies to all ports in that bridge-domain. If configured in a profile attached to a specific port, this command applies to that port only.

**Examples**

The following examples show how to enable the startup G-query configuration:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# startup query iccp-group

RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# startup query iccp-group
```
**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
</tbody>
</table>
startup query interval

To configure the time between successive startup G-queries, use the `startup query interval` command in the appropriate snooping profile configuration mode. To restore the default startup query interval of 1/4 querier's query-interval (up to a max of 32 secs), use the `no` form of this command.

```
startup query interval number
no startup query interval
```

**Syntax Description**

- `number` Interval, in seconds. The range is from 1 to 18000.

**Command Default**

- `15 seconds`

**Command Modes**

- IGMP snooping profile configuration
- MLD snooping profile configuration

**Command History**

- **Release 4.0.0** This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

- **Task ID**
  - `l2vpn` read, write

**Examples**

The following examples show how to configure the startup query interval:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# startup query interval

RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# startup query interval
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
</tbody>
</table>
startup query max-response-time

To configure the maximum response time (MRT) transmitted in the startup G-queries in seconds, use the `startup query max-response-time` command in the appropriate snooping profile configuration mode. To restore the default startup query max-response-time to be the querier's max-response-time (MRT), use the `no` form of this command.

```
startup query max-response-time number
no startup query max-response-time
```

**Syntax Description**

- `number` Enter an interval between 1 to 25 seconds.

**Command Default**

10 seconds

**Command Modes**

- IGMP snooping profile configuration
- MLD snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Examples**

The following examples show how to configure the MRT:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# startup query max-reponse-time
RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# startup query max-reponse-time
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
</tbody>
</table>
startup query port-up disable

To disable the sending of startup G-queries on port-up, use the `startup query port-up disable` command in IGMP snooping profile configuration mode. To restore the default behavior that sends G-queries on port-up, use the `no` form of this command.

```
startup query port-up disable
no startup query port-up disable
```

**Syntax Description**
This command has no arguments or keywords.

**Command Default**
None

**Command Modes**
IGMP snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If configured in a bridge-domain profile, this command applies to all ports in the bridge-domain. If configured in a profile attached to a specific port, this command applies to only the specific port.

**Examples**
The following examples show how to use the `startup query port-up disable` command:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# startup query port-up disable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
</tbody>
</table>
To enable the startup G-query generation on all ports in the bridge domain when the IGMP Snooping (IGMPSN) process restarts, use the `startup query process start` command in IGMP snooping profile configuration mode. To disable the startup query generation of this event, use the `no` form of this command. This command must be included in the bridge-domain profile.

```
startup query process start [sync]
no startup query process start
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>sync</code></td>
<td>(Optional) Removes the unrefreshed membership state. This parameter instructs the IGMPSN to perform a mark and sweep synchronization of the IGMP snooping state over the startup query period.</td>
</tr>
</tbody>
</table>

**Command Default**

None

**Command Modes**

IGMP snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following examples show how to use the `startup query process start` command into an IGMP snooping profile:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# startup query process start
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
</tbody>
</table>
**startup query topology-change**

To enable startup G-query generation on all ports in the bridge domain when a topology change is indicated and the bridge is the root, use the `startup query topology-change` command in IGMP snooping profile configuration mode.

To disable the startup query generation on this event, use the `no` form of this command.

```
startup query topology-change [{sync|always}]
no startup query topology-change
```

**Syntax Description**

- `sync` (Optional) Removes the unrefreshed membership state. Instructs the IGMP Snooping profile to perform a mark and sweep synchronization of the IGMP snooping state over the startup query period.

- `always` (Optional) Instructs the IGMP Snooping profile to generate startup G-queries regardless of whether the bridge is the root.

**Command Default**

None

**Command Modes**

IGMP snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to use the `startup query topology-change` command into an IGMP snooping profile in the Command Line Interface:

```
RP/0/RSP0:CPU0:router(config-igmp-snooping-profile)# startup query topology-change
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
</tbody>
</table>
**static group**

To configure static group membership entries in the Layer-2 forwarding tables, use the `static group` command in IGMP snooping profile configuration mode. To remove a static group entry from the forwarding tables, use the `no` form of this command.

```
static group group-addr [source source-addr]
no static group group-addr [source source-addr]
```

**Syntax Description**

- `group-addr`  
  IP multicast group address.

- `source`  
  (Optional) Statically forwards an (S, G) channel out of the port.

- `source-addr`  
  IP multicast source address.

**Command Default**

None

**Command Modes**

IGMP snooping profile configuration

**Command History**

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

IGMP snooping learns Layer-2 multicast groups dynamically. You can also statically configure Layer-2 multicast groups.

You can use the `static group` command in profiles intended for bridge domains or ports. If you configure this option in a profile attached to a bridge domain, it applies to all ports under the bridge.

A profile can contain multiple static groups. You can define different source addresses for the same group address. Using the `source` keyword, you can configure IGMPv3 source groups.

Static group membership supersedes any dynamic manipulation by IGMP snooping. Multicast group membership lists can contain both static and dynamic group definitions.

When you configure a static group or source group on a port, IGMP snooping adds the port as an outgoing port to the corresponding <S*,G> forwarding entry and sends an IGMPv2 join or IGMPv3 report to all mrouter ports. IGMP snooping continues to send the membership report in response to general queries for as long as the static group remains configured on the port.

The scope of this command can be either bridge domain level or port level. If you use this command in a profile attached to a bridge domain, the static group membership applies to all ports under the bridge. If you use the command in a profile attached to a port, the static group membership applies only to that port.
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task ID Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>12vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following examples show how to add static group membership configuration into an IGMP snooping profile:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# static group 10.1.1.1
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# static group 10.1.1.1 source 10.1.12.0
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
</tbody>
</table>
system-ip-address

To configure an IP address for the internal querier, use the `system-ip-address` command in IGMP snooping profile configuration mode. To return to the default value, use the `no` form of this command.

```
system-ip-address  ip-address
no  system-ip-address
```

**Syntax Description**
- `ip-address` Assigns an IP address for IGMP use.

**Command Default**
- 0.0.0.0

**Command Modes**
- IGMP snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| Release 3.7.2 | This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `system-ip-address` command configures an IP address for IGMP snooping use. If not explicitly configured, the default address is 0.0.0.0. The default is adequate except in the following circumstances:

- If you are configuring an internal querier. The internal querier cannot use 0.0.0.0.
- If the bridge needs to communicate with a non-Cisco IGMP router that does not accept the 0.0.0.0 address.

IGMP snooping uses the value set by the `system-ip-address` command in the following ways:

- The internal-querier sends queries from the system IP address. An address other than the default 0.0.0.0 must be configured.
- IGMPv3 sends proxy reports from the system IP address. The default address 0.0.0.0 is preferred but may not be acceptable to some IGMP routers.
- In response to topology change notifications (TCNs) in the bridge domain, IGMP snooping sends global-leaves from the system IP address. The default address 0.0.0.0 is preferred but may not be acceptable to some IGMP routers.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>12vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example assigns a system IP address, overriding the default value:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# system-ip-address 10.1.1.1
```
## Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
</tbody>
</table>
**tcn flood disable**

To disable Spanning Tree Protocol (STP) port flooding during a topology change, use the `tcn flood disable` command in the appropriate snooping profile configuration mode. To reenable STP port flooding, use the `no` form of this command.

```
tcn flood disable
no tcn flood disable
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

TCN flooding is enabled by default.

**Command Modes**

IGMP snooping profile configuration

MLD snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.9.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Examples**

This example illustrates how to disable TCN flooding:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# tcn flood disable
```

```
RP/0/RSP0/CPU0:router(config-mld-snooping-profile)# tcn flood disable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show igmp snooping profile, on page 327</td>
<td>Displays the contents of profiles and to see associations of profiles with bridge-domains and ports, including access group, group limit, and TCN flood parameters.</td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>tcn flood query count, on page 392</td>
<td>Configures the number of general queries that must be sent before IGMP snooping stops flooding all routes in response to STP topology changes.</td>
</tr>
<tr>
<td>tcn query solicit, on page 396</td>
<td>Enables global leave messaging on non-root bridges in response to STP topology changes.</td>
</tr>
</tbody>
</table>
tcn flood query count

To configure how long IGMP snooping floods all routes in response to topology changes, use the `tcn flood query count` command in IGMP snooping profile configuration mode. To return to the default value, use the `no` form of this command.

```plaintext
tcn flood query count number
no tcn flood query count
```

**Syntax Description**

- `number`: Specifies the number of general queries that must occur after a TCN before IGMP snooping stops multicast flooding to all ports and resumes restricted forwarding.

  Valid values are integers from 1 to 10.

**Command Default**

2

**Command Modes**

IGMP snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

In a Spanning Tree Protocol (STP) topology, a topology change notification (TCN) indicates that an STP topology change has occurred. As a result of a topology change, mrouters and hosts reporting group membership may migrate to other STP ports under the bridge domain. Mrouter and membership states must be relearned after a TCN.

IGMP snooping reacts to TCNs in the following way:

1. IGMP snooping temporarily extends the flood set for all known multicast routes to include all ports participating in STP that are in forwarding state. The short term flooding ensures that multicast delivery continues to all mrouters and all member hosts in the bridge domain while mrouter and membership states are relearned.

2. The STP root bridge issues a global leave (leave for group 0.0.0.0) on all ports. This action triggers mrouters to send general queries, expediting the relearning process.

**Note**

Sending global leaves for query solicitation is a Cisco-specific implementation.

1. When the TCN refresh period ends, IGMP snooping withdraws the non-mrouter and non-member STP ports from the multicast route flood sets. You can control the amount of time that flooding occurs with the `tcn flood query count` command. This command sets the number of IGMP general queries for which the multicast traffic is flooded following a TCN, thus influencing the refresh period.
IGMP snooping default behavior is that the STP root bridge always issues a global leave in response to a TCN, and the non-root bridges do not issue global leaves.

With the `tcn query solicit` command, you can enable a bridge to always issue a global leave in response to TCNs, even when it is not the root bridge. In that case, the root bridge and the non-root bridge would issue the global leave and both would solicit general queries in response to a TCN. Use the `no` form of the command to turn off soliciting when the bridge is not the root.

The root bridge always issues a global leave in response to a TCN. This behavior cannot be disabled.

The internal querier has its own set of configuration options that control its reactions to TCNs.

The scope for this configuration option is per bridge domain. If the command appears in profiles attached to ports, it has no effect.

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Task Operations</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read,</td>
<td>write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the `tcn flood query count` in an IGMP snooping profile, overriding the default:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# tcn flood query count 5
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>igmp snooping profile</code>, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
<tr>
<td><code>tcn query solicit</code>, on page 396</td>
<td>Enables global leave messaging on non-root bridges in response to STP topology changes.</td>
</tr>
</tbody>
</table>
**tcn flood query count (MLD)**

To configure how long MLD snooping floods all routes in response to topology changes, use the `tcn flood query count` command in the MLD snooping profile configuration mode. To return to the default value, use the `no` form of the command.

```
tcn flood query count  number
notcn flood query count  number
```

**Syntax Description**

- `number` Specifies the number of queries. Range is from 1 to 10.

**Command Default**

2

**Command Modes**

MLD snooping profile

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

In a Spanning Tree Protocol (STP) topology, a topology change notification (TCN) indicates that an STP topology change has occurred. As a result of a topology change, mrouter and hosts reporting group membership may migrate to other STP ports under the bridge domain. Mrouter and membership states must be relearned after a TCN.

IGMP snooping reacts to TCNs in the following way:

- MLD snooping temporarily extends the flood set for all known multicast routes to include all ports participating in STP that are in forwarding state. The short term flooding ensures that multicast delivery continues to all mrouter and all member hosts in the bridge domain while mrouter and membership states are relearned.

- The STP root bridge issues a global leave (leave for group 0.0.0.0) on all ports. This action triggers mrouter to send general queries, expediting the relearning process.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

The following example shows how to set the query count to 5:
RP/0/RSP0/CPU0:router(config-mld-snooping-profile) # tcn flood query count 5
tcn query solicit

To enable global leave messaging on non-root bridges in response to STP topology changes, use the **tcn query solicit** command in IGMP snooping profile configuration mode. To disable this functionality (on non-root bridges), use the **no** form of this command.

```
tcn query solicit
no tcn query solicit
```

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

It is disabled by default.

**Command Modes**

IGMP snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

In a Spanning Tree Protocol (STP) topology, a topology change notification (TCN) indicates that an STP topology change has occurred. As a result of a topology change, mrouters and hosts reporting group membership may migrate to other STP ports under the bridge domain. Mrouter and membership states must be relearned after a TCN.

IGMP snooping reacts to TCNs in the following way:

1. IGMP snooping temporarily extends the flood set for all known multicast routes to include all ports participating in STP that are in forwarding state. The short term flooding ensures that multicast delivery continues to all mrouters and all member hosts in the bridge domain while mrouter and membership states are relearned.

2. The STP root bridge issues a global leave (leave for group 0.0.0.0) on all ports. This action triggers mrouters to send general queries, expediting the relearning process.

**Note**

Sending global leaves for query solicitation is a Cisco-specific implementation.

1. When the TCN refresh period ends, IGMP snooping withdraws the non-mrouter and non-member STP ports from the multicast route flood sets. You can control the amount of time that flooding occurs with the **tcn flood query count** command. This command sets the number of IGMP general queries for which the multicast traffic is flooded following a TCN, thus influencing the refresh period.

IGMP snooping default behavior is that the STP root bridge always issues a global leave in response to a TCN, and the non-root bridges do not issue global leaves.
With the `tcn query solicit` command, you can enable a bridge to always issue a global leave in response to TCNs, even when it is not the root bridge. In that case, the root bridge and the non-root bridge would issue the global leave and both would solicit general queries in response to a TCN. Use the `no` form of the command to turn off soliciting when the bridge is not the root.

The root bridge always issues a global leave in response to a TCN. This behavior cannot be disabled.

The internal querier has its own set of configuration options that control its reactions to TCNs.

The scope for this configuration option is per bridge domain. If the command appears in profiles attached to ports, it has no effect.

### Examples

The following example shows how to ensure that a bridge will always issue a global leave in response to a TCN, even when it is not the STP root bridge:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# tcn query solicit
```
tcn query solicit (MLD)

To enable global leave messaging on non-root bridges in response to STP topology changes, use the `tcn query solicit` command in MLD snooping profile configuration mode. To disable this functionality, in non-root bridges, use the `no` form of the command.

```
tcn query solicit

no tcn query solicit
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

Disabled

**Command Modes**

MLD snooping profile

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

With the `tcn query solicit` command, you can enable a bridge to always issue a global leave in response to TCNs, even when it is not the root bridge. In that case, the root bridge and the non-root bridge would issue the global leave and both would solicit general queries in response to a TCN. Use the `no` form of the command to turn off soliciting when the bridge is not the root. The root bridge always issues a global leave in response to a TCN. This behavior cannot be disabled. The internal querier has its own set of configuration options that control its reactions to TCNs. The scope for this configuration option is per bridge domain. If the command appears in profiles attached to ports, it has no effect.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
<th>ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read,</td>
<td>write</td>
</tr>
</tbody>
</table>

**Example**

The following example shows how to ensure that a bridge will always issue a global leave in response to a TCN, even when it is not the STP root-bridge:

```
RP/0/RSP0/CPU0:router (config-mld-snooping-profile) # tcn query solicit
```
ttl-check disable

To disable the IGMP snooping check on the time-to-live (TTL) field in the IGMP header, use the `ttl-check disable` command in IGMP snooping profile configuration mode. To enable this functionality after a disable, use the `no` form of this command.

`ttl-check disable`
`no ttl-check disable`

**Syntax Description**

This command has no arguments or keywords.

**Command Default**

It is enabled by default.

**Command Modes**

IGMP snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

By default, IGMP snooping examines the time-to-live (TTL) field in the IGMP header and processes packets as follows:

- If the TTL field is 1, IGMP snooping processes the packet. The TTL field is always set to 1 in the headers of IGMP reports and queries.
- If the TTL field is not 1, IGMP snooping drops the packet

When the IGMP snooping TTL check feature is disabled, IGMP snooping processes all packets without examining the TTL field in the IGMP header.

The scope for this configuration option is per bridge domain. If the command appears in profiles attached to ports, it has no effect.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>l2vpn</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to turn off the check on the ttl field:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# ttl-check disable
```
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>igmp snooping profile, on page 258</td>
<td>Creates or edits a profile, and attaches a profile to a bridge domain or port.</td>
</tr>
</tbody>
</table>
**unsolicited-report-interval**

To set the length of time that IGMP snooping has to send state change reports for IGMPv3 queriers when proxy reporting is enabled, use the `unsolicited-report-interval` command in IGMP snooping profile configuration mode. To return to the default value, use the `no` form of this command.

```
unsolicited-report-interval  timer-value
no unsolicited-report-interval
```

**Syntax Description**

- `timer-value` Specifies the length of time that IGMP snooping can take to send state change reports for IGMPv3 queriers.

  Valid values are integers from 100 to 5000 (milliseconds).

**Command Default**

1000 (milliseconds)

**Command Modes**

IGMP snooping profile configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If a bridge domain querier is running IGMPv3 and proxy reporting is enabled, IGMP snooping acts as a proxy, generating reports from the proxy reporting address. As insurance against lost reports, IGMP snooping generates and forwards state change reports `robustness-variable` times, where the `robustness-variable` is the QRV value in the querier’s general query. IGMP snooping forwards the reports at random intervals within the timeframe configured with the `unsolicited-report-timer` command.

Proxy reporting is enabled by default. To disable proxy reporting, use the `report-suppression disable` command.

**Task ID**

- **Task ID**: l2vpn
  - **Operations**: read, write

**Examples**

The following example shows how to configure the unsolicited report interval:

```
RP/0/RSP0/CPU0:router(config-igmp-snooping-profile)# unsolicited-report-interval 2000
```
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>report-suppression disable</code>, on page 299</td>
<td>Disables IGMPv2 report suppression and IGMPv3 proxy reporting.</td>
</tr>
<tr>
<td><code>system-ip-address</code>, on page 388</td>
<td>Configures the proxy reporting address.</td>
</tr>
</tbody>
</table>
Multicast PIM Commands

This chapter describes the commands used to configure and monitor Protocol Independent Multicast (PIM).

For detailed information about multicast routing concepts, configuration tasks, and examples, refer to *Multicast Configuration Guide for Cisco ASR 9000 Series Routers*.

- accept-register, on page 405
- auto-rp candidate-rp, on page 406
- bsr candidate-bsr, on page 408
- bsr candidate-rp, on page 410
- clear pim counters, on page 412
- clear pim topology, on page 415
- clone source, on page 417
- dr-priority, on page 418
- global maximum, on page 420
- global maximum bsr crp-cache threshold, on page 421
- global maximum group-mappings bsr threshold, on page 423
- hello-interval (PIM), on page 425
- interface (PIM), on page 427
- join-prune-interval, on page 429
- join-prune-mtu, on page 430
- maximum register-states, on page 431
- maximum route-interfaces, on page 432
- maximum routes, on page 433
- mofr, on page 434
- neighbor-check-on-receive enable, on page 436
- neighbor-check-on-send enable, on page 437
- neighbor-filter, on page 438
- nsf lifetime (PIM), on page 439
- old-register-checksum, on page 440
- router pim, on page 441
- rp-address, on page 443
- rpf topology route-policy, on page 445
- rpf-redirect, on page 446
- rpf-vector, on page 447
- rp-static-deny, on page 448
• show auto-rp candidate-rp, on page 449
• show pim context, on page 451
• show pim context table, on page 454
• show pim global summary, on page 456
• show pim group-map, on page 458
• show pim interface, on page 460
• show pim join-prune statistic, on page 463
• show pim rpf-redraw, on page 465
• show pim rpf-redraw route, on page 466
• show pim mstatic, on page 467
• show pim neighbor, on page 469
• show pim nsf, on page 472
• show pim nsr, on page 474
• show pim range-list, on page 476
• show pim rpf, on page 478
• show pim rpf hash, on page 480
• show pim rpf route-policy statistics, on page 482
• show pim rpf route-policy test, on page 484
• show pim rpf summary, on page 486
• show pim summary, on page 488
• show pim topology, on page 490
• show pim topology detail, on page 496
• show pim topology entry-flag, on page 499
• show pim topology interface-flag, on page 502
• show pim topology summary, on page 505
• show pim traffic, on page 507
• show pim tunnel info, on page 509
• spt-threshold infinity, on page 511
• ssm, on page 512
accept-register

To configure a rendezvous point (RP) router to filter Protocol Independent Multicast (PIM) register messages, use the `accept-register` command in PIM configuration mode. To return to the default behavior, use the `no` form of this command.

```
accept-register access-list-name
no accept-register
```

Syntax Description

| access-list-name | Access list number or name. |

Command Default

No default behavior or values

Command Modes

PIM configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `accept-register` command prevents unauthorized sources from registering with the rendezvous point. If an unauthorized source sends a register message to the rendezvous point, the rendezvous point immediately sends back a register-stop message.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to restrict the rendezvous point. Sources in the Source Specific Multicast (SSM) range of addresses are not allowed to register with the rendezvous point. These statements need to be configured only on the rendezvous point.

```
RP/0/RSP0/CPU0:router(config)# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# accept-register no-ssm-range
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# exit
RP/0/RSP0/CPU0:router(config)# ipv4 access-list no-ssm-range
RP/0/RSP0/CPU0:router(config-ipv4-acl)# deny ipv4 any 232.0.0.0 0.255.255.255
RP/0/RSP0/CPU0:router(config-ipv4-acl)# permit any
```
auto-rp candidate-rp

To configure a router as a Protocol Independent Multicast (PIM) rendezvous point (RP) candidate that sends messages to the well-known CISCO-RP-ANNOUNCE multicast group (224.0.1.39), use the **auto-rp candidate-rp** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

**auto-rp candidate-rp** *type* *interface-path-id* *scope* *ttl-value* [*group-list* *access-list-name*] [*interval seconds*] [*bidir*]

**no auto-rp candidate-rp** *type* *interface-path-id* *scope* *ttl-value* [*group-list* *access-list-name*] [*interval seconds*] [*bidir*]

### Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>type</strong></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><em>interface-path-id</em></td>
<td>Physical interface or virtual interface.</td>
</tr>
<tr>
<td><strong>scope</strong> <em>ttl-value</em></td>
<td>Specifies a time-to-live (TTL) value (in router hops) that limits the scope of the auto-rendezvous point (Auto-RP) announce messages that are sent out of that interface. Range is 1 to 255.</td>
</tr>
<tr>
<td><em>group-list</em> <em>access-list-name</em></td>
<td>(Optional) Specifies an access list that describes the group ranges for which this router is the rendezvous point.</td>
</tr>
<tr>
<td><em>interval</em> <em>seconds</em></td>
<td>(Optional) Specifies the time between rendezvous point announcements. Range is 1 to 600.</td>
</tr>
<tr>
<td><strong>bidir</strong></td>
<td>(Optional) Specifies a bidirectional rendezvous point for PIM.</td>
</tr>
</tbody>
</table>

### Command Default

A router is not configured as a PIM rendezvous point candidate by default.

*seconds* : 60

### Command Modes

PIM configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **auto-rp candidate-rp** command is used by the rendezvous point for a multicast group range. The router sends an Auto-RP announcement message to the well-known group CISCO-RP-ANNOUNCE (224.0.1.39).
This message announces the router as a candidate rendezvous point for the groups in the range described by the access list.

When the `interval` keyword is specified, the interval between Auto-RP announcements is set to number of `seconds` with the total hold time of the announcements automatically set to three times the interval time. The recommended interval time range is from 1 to 180 seconds.

The hold time of the Auto-RP announcement is the time for which the announcement is valid. After the designated hold time, the announcement expires and the entry is purged from the mapping cache until there is another announcement.

If the optional `group-list` keyword is omitted, the group range advertised is 224.0.0.0/4. This range corresponds to all IP multicast group addresses, which indicates that the router is willing to serve as the rendezvous point for all groups.

A router may be configured to serve as a candidate rendezvous point for more than one group range by a carefully crafted access list in the router configuration.

The `auto-rp candidate-rp` command is available for IPv4 address prefixes only.

### Examples

The following example shows how to send rendezvous point announcements from all PIM-enabled interfaces for a maximum of 31 hops. The IP address by which the router wants to be identified as a rendezvous point is the IP address associated with GigabitEthernet interface 0/1/0/1. Access list 5 designates the groups that this router serves as the rendezvous point.

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list 5
RP/0/RSP0/CPU0:router(config-ipv4-acl)# permit ipv4 any 224.0.0.0 15.255.255.255
RP/0/RSP0/CPU0:router(config-ipv4-acl)# exit
RP/0/RSP0/CPU0:router(config)# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# auto-rp candidate-rp GigE 0/1/0/1 scope 31
    group-list 5
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# end
```

The router identified in the following example advertises itself as the candidate rendezvous point and is associated with loopback interface 0 for the group ranges 239.254.0.0 to 239.255.255.255 and 224.0.0.0 to 231.255.255.255:

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list 10
RP/0/RSP0/CPU0:router(config-ipv4-acl)# permit ipv4 any 239.254.0.0 0.0.255.255
RP/0/RSP0/CPU0:router(config-ipv4-acl)# exit
RP/0/RSP0/CPU0:router(config)# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# auto-rp candidate-rp loopback 0 scope 16
    group-list 10
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# end
```
bsr candidate-bsr

To configure the router to announce its candidacy as a bootstrap router (BSR), use the `bsr candidate-bsr` command in PIM configuration mode. To return to the default behavior, use the `no` form of this command.

```plaintext
bsr candidate-bsr ip-address [hash-mask-len length] [priority value]
no bsr candidate-bsr
```

**Syntax Description**

- `ip-address`: IP address of the BSR router for the domain. For IPv4, this is an IP address in four-part dotted-decimal notation. For IPv6, the IP address is specified in hexadecimal format using 16-bit values between colons.

- `hash-mask-len length`: (Optional) Specifies the length of a mask that is to be used in the hash function.
  - All groups with the same seed hash (correspond) to the same rendezvous point (RP). For example, if this value is 24, only the first 24 bits of the group addresses matter. This fact allows you to get one RP for multiple groups.
  - For IPv4 addresses, we recommend a value of 30. The range is 0 to 32.
  - For IPv6 addresses, we recommend a value of 126. The range is 0 to 128.

- `priority value`: (Optional) Specifies the priority of the candidate BSR. Range is 1 to 255. We recommend the BSR with the higher priority. If the priority values are the same, the router with the higher IP address is the BSR.

**Command Default**

- `value`: 1
  - Default C-RP cache state limit in both Candidate BSR and Elected BSR is 100.
  - Configurable maximum C-RP cache in both BSR and Elected BSR is in the range of 1 - 100000.
  - Default RP-group mapping state limit in PIMv2 router is 100.
  - Configurable maximum RP-group mapping state in PIMv2 router is in the range of 1 - 100000.

**Command Modes**

- PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.3</td>
<td>PIM BSR limits were introduced for this command.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `bsr candidate-bsr` command causes the router to send bootstrap messages to all its Protocol Independent Multicast (PIM) neighbors, with the address of the designated interface as the BSR address. Each neighbor compares the BSR address with the address it had from previous bootstrap messages (not necessarily received on the same interface). If the current address is the same or higher address, the PIM neighbor caches the current address and forwards the bootstrap message. Otherwise, the bootstrap message is dropped.
This router continues to be the BSR until it receives a bootstrap message from another candidate BSR saying that it has a higher priority (or if the same priority, a higher IP address).

**Note**
Use the `bsr candidate-bsr` command only in backbone routers with good connectivity to all parts of the PIM domain. A subrouter that relies on an on-demand dial-up link to connect to the rest of the PIM domain is not a good candidate BSR.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to configure the router as a candidate BSR with a hash mask length of 30:

```plaintext
RP/0/RSP0/CPU0:router(config)# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# bsr candidate-bsr 10.0.0.1 hash-mask-len 30
```
**bsr candidate-rp**

To configure the router to advertise itself as a Protocol Independent Multicast (PIM) Version 2 candidate rendezvous point (RP) to the bootstrap router (BSR), use the `bsr candidate-rp` command in PIM configuration mode. To return to the default behavior, use the `no` form of this command.

```
bsr candidate-rp ip-address [group-list access-list] [interval seconds] [priority value][bidir]
no bsr candidate-rp ip-address
```

**Syntax Description**

- **ip-address**: IP address of the router that is advertised as a candidate rendezvous point address.
- **group-list access-list**: (Optional) Specifies the IP access list number or name that defines the group prefixes that are advertised in association with the rendezvous point address. The access list name cannot contain a space or quotation mark, and must begin with an alphabetic character to avoid confusion with numbered access lists.
- **interval seconds**: (Optional) Specifies the candidate rendezvous point advertisement interval in seconds. Range is 30 to 600.
- **priority value**: (Optional) Indicates the rendezvous point priority value. Range is 1 to 255.
- **bidir**: (Optional) Configures a bidirectional (bidir) rendezvous point.

**Command Default**

- **value**: 1
- Default C-RP cache state limit in both Candidate BSR and Elected BSR is 100.
- Configurable maximum C-RP cache in both BSR and Elected BSR is in the range of 1 - 100000.
- Default RP-group mapping state limit in PIMv2 router is 100.
- Configurable maximum RP-group mapping state in PIMv2 router is in the range of 1 - 100000.

**Command Modes**

PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.0.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `bsr candidate-rp` command causes the router to send a PIM Version 2 message advertising itself as a candidate rendezvous point to the BSR. The addresses allowed by the access list, together with the router identified by the IP address, constitute the rendezvous point and its range of addresses for which it is responsible.
Use the `bsr candidate-rp` command only in backbone routers that have good connectivity to all parts of the PIM domain. That is, a stub router that relies on an on-demand dial-up link to connect to the rest of the PIM domain is not a good candidate rendezvous point.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the router to advertise itself as a candidate rendezvous point to the BSR in its PIM domain. Access list number 4 specifies the group prefix associated with the candidate rendezvous point address 172.16.0.0. This rendezvous point is responsible for the groups with the prefix 239.

```
RP/0/RSP0/CPU0:router(config)# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# bsr candidate-rp 172.16.0.0 group-list 4
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# exit
RP/0/RSP0/CPU0:router(config)# ipv4 access-list 4
RP/0/RSP0/CPU0:router(config-ipv4-acl)# permit ipv4 any 239.0.0.0 0.255.255.255
RP/0/RSP0/CPU0:router(config-ipv4-acl)# end
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>bsr candidate-bsr</code>, on page 408</td>
<td>Configures the router to announce its candidacy as a bootstrap router (BSR).</td>
</tr>
</tbody>
</table>
clear pim counters

To clear Protocol Independent Multicast (PIM) counters and statistics, use the `clear pim counters` command in EXEC mode.

```
clear pim [vrf vrf-name] [ipv4] counters
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Specifies a VPN routing and forwarding (VRF) instance.</td>
</tr>
<tr>
<td><code>ipv4</code></td>
<td>(Optional) Specifies IPv4 address prefixes.</td>
</tr>
<tr>
<td><code>ipv6</code></td>
<td>(Optional) Specifies IPv6 address prefixes.</td>
</tr>
</tbody>
</table>

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If you do not explicitly specify a particular VRF, the default VRF is used.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows sample output before and after clearing PIM counters and statistics:

```
RP/0/RSP0/CPU0:router# show pim traffic
PIM Traffic Counters
Elapsed time since counters cleared: 1d01h

           Received             Sent
Valid PIM Packets 15759217 15214426
Hello         9207         12336
Join-Prune   1076805       531981
Data Register 14673205      0
Null Register 73205         0
Register Stop  0       14673205
Assert         0              0
Batched Assert 0              0
Bidir DF Election 0           0
BSR Message   0              0
Candidate-RP Adv. 0            0
```
Join groups sent 0
Prune groups sent 0
Output JP bytes 0
Output hello bytes 4104

Errors:
Malformed Packets 0
Bad Checksums 0
Socket Errors 0
Subnet Errors 0
Packets dropped since send queue was full 0
Packets dropped due to invalid socket 0
Packets which couldn’t be accessed 0
Packets sent on Loopback Errors 6
Packets received on PIM-disabled Interface 0
Packets received with Unknown PIM Version 0

This table describes the significant fields shown in the display.

Table 30: show pim traffic Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elapsed time since counters cleared</td>
<td>Time (in days and hours) that had elapsed since the counters were cleared with the <strong>clear pim counters</strong> command.</td>
</tr>
<tr>
<td>Valid PIM Packets</td>
<td>Total PIM packets that were received and sent.</td>
</tr>
<tr>
<td>HelloJoin-PruneRegisterRegister StopAssertBidir DF Election</td>
<td>Specific type of PIM packets that were received and sent.</td>
</tr>
<tr>
<td>Malformed Packets</td>
<td>Invalid packets due to format errors that were received and sent.</td>
</tr>
<tr>
<td>Bad Checksums</td>
<td>Packets received or sent due to invalid checksums.</td>
</tr>
<tr>
<td>Socket Errors</td>
<td>Packets received or sent due to errors from the router’s IP host stack sockets.</td>
</tr>
<tr>
<td>Packets dropped due to invalid socket</td>
<td>Packets received or sent due to invalid sockets in the router’s IP host stack.</td>
</tr>
<tr>
<td>Packets which couldn’t be accessed</td>
<td>Packets received or sent due to errors when accessing packet memory.</td>
</tr>
<tr>
<td>Packets sent on Loopback Errors</td>
<td>Packets received or sent due to use of loopback interfaces.</td>
</tr>
<tr>
<td>Packets received on PIM-disabled Interface</td>
<td>Packets received or sent due to use of interfaces not enabled for PIM.</td>
</tr>
<tr>
<td>Packets received with Unknown PIM Version</td>
<td>Packets received or sent due to invalid PIM version numbers in the packet header.</td>
</tr>
</tbody>
</table>

RP/0/RSP0/CPU0:router# **clear pim counters**
RP/0/RSP0/CPU0:router# **show pim traffic**

PIM Traffic Counters
Elapsed time since counters cleared: 00:00:04
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show pim traffic, on page 507</td>
<td>Displays Protocol Independent Multicast (PIM) traffic counter information.</td>
</tr>
</tbody>
</table>
clear pim topology

To clear group entries from the Protocol Independent Multicast (PIM) topology table and reset the Multicast Routing Information Base (MRIB) connection, use the `clear pim topology` command in EXEC mode.

`clear pim [vrf vrf-name] [ipv4] topology [ip-address-name reset]`

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `ip-address-name` (Optional) Can be either one of the following:
  - Name of the multicast group, as defined in the Domain Name System (DNS) hosts table or with the `domain IPv4` or `domain IPv6 host` command.
  - IP address of the multicast group, in IPv4 or IPv6 format according to the specified address family.
- `reset` (Optional) Deletes all entries from the topology table and resets the MRIB connection.

**Command Default**

No default behavior or values

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `clear pim topology` command clears existing PIM routes from the PIM topology table. Information obtained from the MRIB table, such as Internet Group Management Protocol (IGMP) local membership, is retained. If a multicast group is specified, only those group entries are cleared.

When the command is used with no arguments, all group entries located in the PIM topology table are cleared of PIM protocol information.

If the `reset` keyword is specified, all information from the topology table is cleared and the MRIB connections are automatically reset. This form of the command can be used to synchronize state between the PIM topology table and the MRIB database. The `reset` keyword should be strictly reserved to force synchronized PIM and MRIB entries when communication between the two components is malfunctioning.

If you do not explicitly specify a particular VRF, the default VRF is used.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>
The following example shows how to clear the PIM topology table:

RP/0/RSP0/CPU0:router# clear pim topology
**clone source**

To clone the S,G traffic as S1, G traffic and S2,G traffic, use the `clone source` command in the mofrr configuration submode.

```
clone source  source S1 source S2 masklen value
```

**Syntax Description**

- `source S`  IP address of the source traffic (S).

**Command Default**

No default behavior or value.

**Command Modes**

MOFRR configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

This example shows how to use the `clone source` command:

```
RP/0/RSP0/CP00:router(config-pim-ipv4-mofrr) # clone source 1.1.1 to 3.3.3.3 and 5.5.5.5 masklen 30
```
**dr-priority**

To configure the designated router (DR) priority on a Protocol Independent Multicast (PIM) router, use the `dr-priority` command in the appropriate configuration mode. To return to the default behavior, use the `no` form of this command.

```
dr-priority value
no dr-priority
```

**Syntax Description**

- `value` An integer value to represent DR priority. Range is from 0 to 4294967295.

**Command Default**

If this command is not specified in interface configuration mode, the interface adopts the DR priority value specified in PIM configuration mode.

If this command is not specified in PIM configuration mode, the DR priority value is 1.

**Command Modes**

- PIM interface configuration

**Command History**

- **Release 3.7.2** This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

If all the routers on the LAN support the DR priority option in the PIM Version 2 (PIMv2) hello message that they send, you can force the DR election by use of the `dr-priority` command so that a specific router on the subnet is elected as DR. The router with the highest DR priority becomes the DR.

When PIMv2 routers receive a hello message without the DR priority option (or when the message has priority of 0), the receiver knows that the sender of the hello message does not support DR priority and that DR election on the LAN segment should be based on IP address alone.

**Note**

If this command is configured in PIM configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces from PIM interface configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read,</td>
</tr>
<tr>
<td></td>
<td>write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the router to use DR priority 4 for Packet-over-SONET/SDH (POS) interface 0/1/0/0, but other interfaces will inherit DR priority 2:

```
RP/0/RSP0/CPU0# router pim
```
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# **dr-priority** 2
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# interface pos 0/1/0/0
RP/0/RSP0/CPU0:router(config-pim-ipv4-if)# **dr-priority** 4
global maximum

To configure the global maximum limit states that are allowed by Protocol Independent Multicast (PIM) for all VRFs, use the `global maximum` command in PIM configuration mode. To return to the default behavior, use the `no` form of this command.

```
global maximum [{register states|route-interfaces|routes number}]
no global maximum [{register states|route-interfaces|routes}]
```

**Syntax Description**

- **register states** (Optional) Specifies the PIM source register states for all VRFs. Range is 0 to 75000.
  
  **Note**  PIM registers throttle at 20000 due to the default global threshold set.

- **route-interfaces** (Optional) Specifies the total number of PIM interfaces on routes for all VRFs. Range is 1 to 600000.

- **routes** (Optional) Specifies the PIM routes for all VRFs. Range is 1 to 200000.

**Command Default**

Default value is 20000.

**Command Modes**

PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| Release 3.9.0 | This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `global maximum` command is used to set an upper limit for register states, route interfaces, and routes on all VRFs. When the limit is reached, PIM discontinues route interface creation for its topology table.

**Note**

After the maximum threshold values for routes or route-interfaces are reached, throttling begins and will remain in effect until the values fall below 95% of the Maximum value.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the upper limit for PIM route interfaces on all VRFs to 200000:

```
RP/0/RSP0/CPU0:router# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# global maximum route-interfaces 200000
```
global maximum bsr crp-cache threshold

To configure the global maximum bsr crp-cache threshold limit that are allowed by Protocol Independent Multicast (PIM) for all VRFs, use the `global maximum bsr crp-cache threshold` command in PIM configuration mode. To return to the default behavior, use the `no` form of this command.

```
[global] maximum [{bsr crp-cache threshold}]
no [global] maximum [{bsr crp-cache threshold}]
```

Syntax Description

- **global**: (Optional) Configures the maximum value for CRP cache and threshold limit to the sum of the caches in all VRFs.
- **crp-cache**: Specifies the CRP cache value. The range is from 1 to 10000.
- **threshold**: Specifies the threshold value for the crp-cache value. Range is between 1 to the set crp-cache value.

Command Default

No default behavior or values.

Command Modes

PIM configuration

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `global maximum bsr` command is used to the threshold limits for the crp-cache levels.

Use the `global` keyword to configure the maximum value for CRP cache and threshold limit to the sum of the caches in all VRF. However, each VRF, including the default, will still have its own smaller maximum and threshold values. To set the maximum and threshold values in the default VRF, you should omit the `global` keyword.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

Examples

The following example shows how to set a crp-cache of 2000 and the threshold level to 500 for the crp-cache in the router PIM configuration mode.
The following example shows how to set a crp-cache of 2000 and the threshold level to 500 for the crp-cache in the router PIM configuration mode in VRF sub-mode:

```
RP/0/RSP0/CPU0:router# router pim
RP/0/RSP0/CPU0:router(config-pim)# global maximum bsr crp-cache 2000 threshold 500

The following configuration shows how to set the maximum and threshold level in the default VRF, while all VRFs together have a larger global maximum and threshold level:

```
RP/0/RSP0/CPU0:router# router pim
RP/0/RSP0/CPU0:router(config-pim)# address-family ipv4
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# global maximum bsr crp-cache 600 threshold 550
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# maximum bsr crp-cache 500 threshold 450
```
# global maximum group-mappings bsr threshold

To configure the global maximum group-mappings and the threshold levels that are allowed by Protocol Independent Multicast (PIM) for all VRFs, use the `global maximum group-mappings bsr threshold` command in PIM configuration mode. To return to the default behavior, use the `no` form of this command.

```
[global maximum [{group-mappings bsr threshold}]
no  global maximum [{group-mappings bsr threshold}]
```

## Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bsr</td>
<td>Specifies the bsr value. Range is 1 to 10000.</td>
</tr>
<tr>
<td>threshold</td>
<td>Specifies the threshold value for the bsr value. Range is between 1 to the set bsr value.</td>
</tr>
</tbody>
</table>

## Command Default

No default behavior or values.

## Command Modes

PIM configuration

## Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.2.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

## Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `global maximum group-mappings` command is used to the threshold limits for the crp-cache levels.

## Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

## Examples

The following example shows how to set a bsr of 2000 and the threshold level to 500 for the bsr in the router PIM configuration mode.

```
RP/0/RSP0/CPU0:router#  router pim
RP/0/RSP0/CPU0:router(config-pim)#  global maximum group-mappings bsr
RP/0/RSP0/CPU0:router(config-pim)#  global maximum group-mappings bsr 2000 threshold ?
<1-2000>  Threshold value
RP/0/RSP0/CPU0:router(config-pim)#  global maximum group-mappings bsr 2000 threshold 500
RP/0/RSP0/CPU0:router(config-pim)#
```

The following example shows how to set a crp-cache of 2000 and the threshold level to 500 for the crp-cache in the router PIM configuration mode in VRF sub-mode.
RP/0/RSP0/CPU0:router# router pim
RP/0/RSP0/CPU0:router (config-pim)# address-family ipv4
RP/0/RSP0/CPU0:router (config-pim-default-ipv4)# global maximum bsr-crp-cache 2000 threshold 500
RP/0/RSP0/CPU0:router (config-pim-default-ipv4)# maximum bsr-crp-cache 1800 threshold 450
### hello-interval (PIM)

To configure the frequency of Protocol Independent Multicast (PIM) hello messages, use the `hello-interval` command in the appropriate configuration mode. To return to the default behavior, use the `no` form of this command.

```
hello-interval  seconds
no hello-interval
```

**Syntax Description**
- `seconds` Interval at which PIM hello messages are sent. Range is 1 to 3600.

**Command Default**
- Default is 30 seconds.

**Command Modes**
- PIM interface configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Routers configured for IP multicast send PIM hello messages to establish PIM neighbor adjacencies and to determine which router is the designated router (DR) for each LAN segment (subnet).

To establish these adjacencies, at every hello period, a PIM multicast router multicasts a PIM router-query message to the All-PIM-Routers (224.0.0.13) multicast address on each of its multicast-enabled interfaces.

PIM hello messages contain a hold-time value that tells the receiver when the neighbor adjacency associated with the sender should expire if no further PIM hello messages are received. Typically the value of the hold-time field is 3.5 times the interval time value, or 120 seconds if the interval time is 30 seconds.

Use the `show pim neighbor` command to display PIM neighbor adjacencies and elected DRs.

**Note**

If you configure the `hello-interval` command in PIM configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces from PIM interface configuration mode.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the PIM hello message interval to 45 seconds. This setting is adopted by all interfaces excluding the 60 second interval time set for Packet-over-SONET/SDH (POS) interface 0/1/0/0:
**hello-interval (PIM)**

RP/0/RSP0/CPU0:router(config)# **router pim**
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# **hello-interval 45**
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# **interface pos 0/1/0/0**
RP/0/RSP0/CPU0:router(config-pim-ipv4-if)# **hello-interval 60**

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dr-priority, on page 418</td>
<td>Configures the designated router (DR) priority on a Protocol Independent Multicast (PIM) router.</td>
<td></td>
</tr>
<tr>
<td>show pim neighbor, on page 469</td>
<td>Displays the Protocol Independent Multicast (PIM) neighbors discovered by means of PIM hello messages.</td>
<td></td>
</tr>
</tbody>
</table>
interface (PIM)

To configure Protocol Independent Multicast (PIM) interface properties, use the `interface` command in PIM configuration mode. To disable multicast routing on an interface, use the `no` form of this command.

```
interface type interface-path-id
no interface type interface-path-id
```

### Syntax Description

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>type</code></td>
<td>Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td><code>interface-path-id</code></td>
<td>Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note**  
Use the `show interfaces` command in EXEC mode to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

### Command Default

No default behavior or values

### Command Modes

PIM configuration

### Command History

**Release**  
3.7.2  
This command was introduced.

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the `interface` command to configure PIM routing properties for specific interfaces. Specifically, this command can be used to override the global settings for the following commands:

- dr-priority
- hello-interval
- join-prune-interval

Use the `interface` command also to enter PIM interface configuration mode.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example shows how to enter interface configuration mode to configure PIM routing properties for specific interfaces:

```
RP/0/RSP0/CPU0:router(config)# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# interface pos 0/1/0/0
```
RP/0/RSP0/CPU0:router
/CPU0:router(config-pim-ipv4-if)#

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>dr-priority, on page 418</td>
<td>Configures the designated router (DR) priority on a Protocol Independent Multicast (PIM) router.</td>
</tr>
<tr>
<td></td>
<td>hello-interval (PIM), on page 425</td>
<td>Configures the frequency of Protocol Independent Multicast (PIM) hello messages.</td>
</tr>
<tr>
<td></td>
<td>join-prune-interval, on page 429</td>
<td>Configures the join and prune interval time for Protocol Independent Multicast (PIM) protocol traffic.</td>
</tr>
</tbody>
</table>
join-prune-interval

To configure the join and prune interval time for Protocol Independent Multicast (PIM) protocol traffic, use the `join-prune-interval` command in the appropriate configuration mode. To return to the default behavior, use the `no` form of this command.

```
join-prune-interval  seconds
no  join-prune-interval
```

**Syntax Description**
- `seconds` Interval, in seconds, at which PIM multicast traffic can join or be removed from the shortest path tree (SPT) or rendezvous point tree (RPT). Range is 10 to 600.

**Command Default**
- If this command is not specified in PIM interface configuration mode, the interface adopts the join and prune interval parameter specified in PIM configuration mode.
- If this command is not specified in PIM configuration mode, the join and prune interval is 60 seconds.

**Command Modes**
- PIM interface configuration
- PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Note**
If this command is configured in PIM configuration mode, parameters are inherited by all new and existing interfaces. You can override these parameters on individual interfaces from PIM interface configuration mode.

The `join-prune-interval` command is used to configure the frequency at which a PIM sparse-mode router sends periodic join and prune messages.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to change the join and prune interval time to 90 seconds on Packet-over-SONET/SDH (POS) interface 0/1/0/0:

```
RP/0/RSP0/CPU0:router(config)# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# interface pos 0/1/0/0
RP/0/RSP0/CPU0:router(config-pim-ipv4-if)# join-prune-interval 90
```
join-prune-mtu

To configure the maximum size of a PIM Join/Prune message, use the `join-prune-mtu` command in the appropriate mode. To return to the default value, use the `no` form of the command.

```
join-prune-mtu  value
no join-prune-mtu  value
```

**Syntax Description**

```
value   Join-prune MTU in bytes. Range is 576 to 65535.
```

**Command Default**

65535 bytes

**Command Modes**

Router PIM configuration mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.1</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The actual maximum size used for PIM Join/Prune messages is the smaller of the, IP MTU value of the interface and the join-prune-mtu value. In normal operation without this configuration, the PIM Join/Prune packet is packed with Join/Prune messages until the interface MTU size limit is reached. This can lead to large PIM Join/Prune message packets getting sent out, which may affect the processing efficiency on some neighboring routers. Configuring the maximum size of a PIM Join/Prune message helps controlling the MTU size of the PIM Join/Prune packet getting sent out.

**Task ID**

```
Task ID      Operation
-------------
multicast   read,
            write
```

**Example**

This example shows how to use the `join-prune mtu` command:

```
RP/0/RSP0/CPU0:router (config-pim) # join-prune-mtu 1000
```
maximum register-states

To configure the maximum number of sparse-mode source register states that is allowed by Protocol Independent Multicast (PIM), use the `maximum register-states` command in PIM configuration mode. To return to the default behavior, use the `no` form of this command.

```
maximum register-states number
no maximum register-states
```

**Syntax Description**

- `number`  
  Maximum number of PIM sparse-mode source register states. Range is 0 to 75000.

**Command Default**

- `number` : 20000

**Command Modes**

PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `maximum register-states` command is used to set an upper limit for PIM register states. When the limit is reached, PIM discontinues route creation from PIM register messages.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to set the upper limit for PIM register states to 10000:

```
RP/0/RSP0/CPU0:router# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# maximum register-states 10000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show pim summary, on page 488</td>
<td>Displays configured Protocol Independent Multicast (PIM) out-of-resource (OOR) limits and current counts.</td>
</tr>
</tbody>
</table>
maximum route-interfaces

To configure the maximum number of route interface states that is allowed by Protocol Independent Multicast (PIM), use the **maximum route-interfaces** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

```
maximum route-interfaces number
no maximum route-interfaces
```

**Syntax Description**

- **number**: Maximum number of PIM route interface states. Range is 1 to 600000.

**Command Default**

- **number**: 30000

**Command Modes**

- PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The **maximum route-interfaces** command is used to set an upper limit for route interface states. When the limit is reached, PIM discontinues route interface creation for its topology table.

**Task ID**

- **Task ID**: multicast
- **Operations**: read, write

**Examples**

The following example shows how to set the upper limit for PIM route interface states to 200000:

```
RP/0/RSP0/CPU0:router# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# maximum route-interfaces 200000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show pim summary, on page 488</td>
<td>Displays configured Protocol Independent Multicast (PIM) out-of-resource (OOR) limits and current counts.</td>
</tr>
</tbody>
</table>
maximum routes

To configure the maximum number of routes that is allowed by Protocol Independent Multicast (PIM), use the `maximum routes` command in PIM configuration mode. To return to the default behavior, use the `no` form of this command.

```
maximum routes number
no maximum routes
```

**Syntax Description**
- `number`: Maximum number of PIM routes. Range is 1 to 200000.

**Command Default**
- `number`: 100000

**Command Modes**
- PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `maximum routes` command is used to set an upper limit for PIM routes. When the limit is reached, PIM discontinues route creation for its topology table.

**Examples**

The following example shows how to set the upper limit for PIM routes to 200000:

```
RP/0/RSP0/CPU0:router# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# maximum routes 200000
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show pim summary, on page 488</td>
<td>Displays configured Protocol Independent Multicast (PIM) out-of-resource (OOR) limits and current counts.</td>
</tr>
</tbody>
</table>
To perform a fast convergence (multicast-only fast reroute, or MoFRR) of specified routes/flows when a failure is detected on one of multiple equal-cost paths between the router and the source, use the `mofrr` command under PIM address-family IPv4 configuration submode.

```
mofrr acl_name
no mofrr acl_name
```

### Syntax Description

- `acl_name` Specifies the flows \((S, G)\) s to be enabled by MoFRR.

### Command Default

MoFRR is not enabled by default.

If no VRF is specified, the default VRF is operational.

### Command Modes

- PIM vrf configuration
- PIM address-family IPv4 configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Release 3.9.0</td>
</tr>
<tr>
<td></td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

MoFRR is a mechanism in which two copies of the same multicast stream flow through disjoint paths in the network. At the point in the network (usually the PE closer to the receivers) where the two streams merge, one of the streams is accepted and forwarded on the downstream links, while the other stream is discarded. When a failure is detected in the primary stream due to a link or node failure in the network, MoFRR instructs the forwarding plane to start accepting packets from the backup stream (which now becomes the primary stream).

MoFRR is triggered when the hardware detects traffic loss on the primary path of a given flow or route. Traffic loss is defined as no data packet having been received for 30 ms. When MoFRR is triggered, the primary and secondary reverse-path forwarding (RPF) interfaces are exposed to the forwarding plane and switchover occurs entirely at the hardware level.

### Note

MoFRR supports all ECMP hashing algorithms except the source-only hash algorithm. The secondary path is chosen by running the same algorithm on the set of paths that does not include the primary path.
### Examples

The following example shows how to configure MoFRR:

```plaintext
RP/0/RSP0/CPU0:router# router pim
RP/0/RSP0/CPU0:router(config-pim)# mofrr rib acl-green

RP/0/RSP0/CPU0:router# router pim
RP/0/RSP0/CPU0:router(config-pim)# address-family ipv4
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# mofrr acl-green
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mfib counter</td>
<td>Displays Multicast Forwarding Information Base (MFIB) counter statistics for packets that have dropped.</td>
</tr>
<tr>
<td>show mfib route</td>
<td>Displays route entries in the MFIB.</td>
</tr>
<tr>
<td>show mrrib route</td>
<td>Displays all entries in the Multicast Routing Information Base (MRIB).</td>
</tr>
<tr>
<td>show pim rpf hash, on page 480</td>
<td>Displays MoFRR hashing information for Routing Information Base (RIB) lookups used to predict RPF next-hop paths for routing tables in PIM.</td>
</tr>
<tr>
<td>show pim rpf summary, on page 486</td>
<td>Displays summary information about the interaction of PIM with the RIB.</td>
</tr>
<tr>
<td>show pim topology detail, on page 496</td>
<td>Displays detailed PIM routing topology information that includes references to the tables in which reverse path forwarding (RPF) lookups occurred for specific topology route entries.</td>
</tr>
<tr>
<td>show pim topology, on page 490</td>
<td>Displays PIM routing topology table information for a specific group or all groups.</td>
</tr>
</tbody>
</table>
neighbor-check-on-recv enable

To block the receipt of join and prune messages from non-Protocol Independent Multicast (PIM) neighbors, use the **neighbor-check-on-recv enable** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

```
neighbor-check-on-recv enable
no neighbor-check-on-recv enable
```

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
Join and prune messages that are sent from non-PIM neighbors are received and not rejected.

**Command Modes**
PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to enable PIM neighbor checking on received join and prune messages:

```
RP/0/RSP0/CPU0:router# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# neighbor-check-on-recv enable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>neighbor-check-on-send enable</strong>, on page 437</td>
<td>Enables Protocol Independent Multicast (PIM) neighbor checking when sending join and prune messages.</td>
</tr>
</tbody>
</table>
neighbor-check-on-send enable

To enable Protocol Independent Multicast (PIM) neighbor checking when sending join and prune messages, use the `neighbor-check-on-send enable` command in PIM configuration mode. To return to the default behavior, use the `no` form of this command.

```
neighbor-check-on-send enable
no neighbor-check-on-send enable
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

Join and prune messages are sent to non-PIM neighbors.

**Command Modes**

PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable PIM neighbor checking when sending join and prune messages:

```
RP/0/RSP0/CPU0:router# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# neighbor-check-on-send enable
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>neighbor-check-on-recv enable, on page 436</td>
<td>Blocks the receipt of join and prune messages from non-Protocol Independent Multicast (PIM) neighbors.</td>
</tr>
</tbody>
</table>
neighbor-filter

To filter Protocol Independent Multicast (PIM) neighbor messages from specific IP addresses, use the `neighbor-filter` command in PIM configuration mode. To return to the default behavior, use the `no` form of this command.

```
neighbor-filter access-list
no neighbor-filter
```

**Syntax Description**

- `access-list`: Number or name of a standard IP access list that denies PIM packets from a source.

**Command Default**

PIM neighbor messages are not filtered.

**Command Modes**

PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `neighbor-filter` command is used to prevent unauthorized routers on the LAN from becoming PIM neighbors. Hello messages from addresses specified in the command are ignored.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure PIM to ignore all hello messages from IP address 10.0.0.1:

```
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# neighbor-filter 1
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# exit
RP/0/RSP0/CPU0:router(config)# ipv4 access-list 1
RP/0/RSP0/CPU0:router(config-ipv4-acl)# deny ipv4 any 10.0.0.1/24
```
**nsf lifetime (PIM)**

To configure the nonstop forwarding (NSF) timeout value for the Protocol Independent Multicast (PIM) process, use the `nsf lifetime` command in PIM configuration mode. To return to the default behavior, use the `no` form of this command.

```
nsf lifetime seconds
no nsf lifetime
```

**Syntax Description**

- `seconds` Maximum time for NSF mode in seconds. Range is 10 to 600.

**Command Default**

- `seconds`: 120

**Command Modes**

- PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

While in PIM NSF mode, PIM is recovering multicast routing topology from the network and updating the Multicast Routing Information Base (MRIB). After the PIM NSF timeout value is reached, PIM signals the MRIB and resumes normal operation.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following command shows how to set the PIM NSF timeout value to 30 seconds:

```
RP/0/RSP0/CPU0:router(config)# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# nsf lifetime 30
```

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>nsf (multicast)</code></td>
<td>Turns on NSF capability for the multicast routing system.</td>
</tr>
<tr>
<td><code>show igmp nsf</code></td>
<td>Displays the state of NSF operation in IGMP.</td>
</tr>
<tr>
<td><code>show mfb nsf</code></td>
<td>Displays the state of NSF operation for the MFIB line cards.</td>
</tr>
<tr>
<td><code>show mrib nsf</code></td>
<td>Displays the state of NSF operation in the MRIB.</td>
</tr>
<tr>
<td><code>show pim nsf, on page 472</code></td>
<td>Displays the state of NSF operation for PIM.</td>
</tr>
</tbody>
</table>
old-register-checksum

To configure a Cisco IOS XR designated router (DRs) in a network where the rendezvous point is running an older version of Cisco IOS software, use the `old-register-checksum` command in PIM configuration mode. To return to the default behavior, use the `no` form of this command.

```
old-register-checksum
no old-register-checksum
```

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
No default behavior or values

**Command Modes**
PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Cisco IOS XR software accepts register messages with checksum on the Protocol Independent Multicast (PIM) header and the next 4 bytes only. This differs from the Cisco IOS method that accepts register messages with the entire PIM message for all PIM message types. The `old-register-checksum` command generates and accepts registers compatible with Cisco IOS software. This command is provided entirely for backward compatibility with Cisco IOS implementations.

**Note**
To allow interoperability with Cisco IOS rendezvous points running older software, run this command on all DRs in your network running Cisco IOS XR software. Cisco IOS XR register messages are incompatible with Cisco IOS software.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**
The following example shows how to set a source designated router (DR) to generate a register compatible with an earlier version of Cisco IOS XR PIM rendezvous point:

```
RP/0/RSP0/CPU0:router(config)# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# old-register-checksum
```
**router pim**

To enter Protocol Independent Multicast (PIM) configuration mode, use the **router pim** command in global configuration mode. To return to the default behavior, use the no form of this command.

```
router pim [address family {ipv4|ipv6}]
no router pim [address family {ipv4|ipv6}]
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-family</td>
<td>(Optional) Specifies which address prefixes to use.</td>
</tr>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IPv4 address prefixes.</td>
</tr>
<tr>
<td>ipv6</td>
<td>(Optional) Specifies IPv6 address prefixes.</td>
</tr>
</tbody>
</table>

**Command Default**

The default is IPv4 address prefixes.

**Command Modes**

Global configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
<tr>
<td>Release 4.2.0</td>
<td>The ipv6 keyword was added.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

From PIM configuration mode, you can configure the address of a rendezvous point (RP) for a particular group, configure the nonstop forwarding (NSF) timeout value for the PIM process, and so on.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

This example shows how to enter PIM configuration mode for IPv4 address prefixes:

```
RP/0/RSP0/CPU0:router(config)# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)#
```

This example shows how to enter PIM configuration mode for IPv4 address prefixes and specify the `address-family ipv6` keywords:

```
RP/0/RSP0/CPU0:router(config)# router pim address-family ipv4
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)#
```
RP/0/RSP0/CPU0:router(config)# router pim address-family ipv6
RP/0/RSP0/CPU0:router(config-pim-default-ipv6)#
rp-address

To statically configure the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for a particular group, use the **rp-address** command in PIM configuration mode. To return to the default behavior, use the **no** form of this command.

```
rp-address ip-address [group-access-list] [override] [bidir]
no rp-address ip-address [group-access-list] [override] [bidir]
```

**Syntax Description**

- **ip-address**  
  IP address of a router to be a PIM rendezvous point. This address is a unicast IP address in four-part dotted-decimal notation.

- **group-access-list**  
  (Optional) Name of an access list that defines for which multicast group the rendezvous point should be used. This list is a standard IP access list.

- **override**  
  (Optional) Indicates that if there is a conflict, the rendezvous point configured with this command prevails over the rendezvous point learned through the auto rendezvous point (Auto-RP) or BSR mechanism.

- **bidir**  
  (Optional) Configures a bidirectional (bidir) rendezvous point.

**Command Default**

No PIM rendezvous points are preconfigured.

**Command Modes**

PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| 3.7.2   | This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

All routers within a common PIM sparse mode (PIM-SM) require the knowledge of the well-known PIM rendezvous point address. The address is learned through Auto-RP, BSR, or is statically configured using this command.

If the optional **group-access-list-number** argument is not specified, the rendezvous point for the group is applied to the entire IP multicast group range (224.0.0.0/4).

You can configure a single rendezvous point to serve more than one group. The group range specified in the access list determines the PIM rendezvous point group mapping. If no access list is specified, the rendezvous point default maps to 224/4.

If the rendezvous point for a group is learned through a dynamic mechanism, such as Auto-RP, this command might not be required. If there is a conflict between the rendezvous point configured with this command and one learned by Auto-RP, the Auto-RP information is used unless the **override** keyword is specified.
Examples

The following example shows how to set the PIM rendezvous point address to 10.0.0.1 for all multicast groups:

```plaintext
RP/0/RSP0/CPU0:router(config)# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# rp-address 10.0.0.1
```

The following example shows how to set the PIM rendezvous point address to 172.16.6.21 for groups 225.2.2.0 - 225.2.2.255:

```plaintext
RP/0/RSP0/CPU0:router(config)# ipv4 access-list 1
RP/0/RSP0/CPU0:router(config-ipv4-acl)# permit ipv4 any 225.2.2.0 0.0.0.255
RP/0/RSP0/CPU0:router(config-ipv4-acl)# exit
RP/0/RSP0/CPU0:router(config)# router pim
RP/0/RSP0/CPU0:router(config-pim-ipv4)# rp-address 172.16.6.21
RP/0/RSP0/CPU0:router(config-pim-ipv4)#
RP/0/RSP0/CPU0:router(config)# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# rp-address 172.16.6.21
```

Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4 access-list</td>
<td>Defines a standard IP access list. For more information, see IP Addresses and Services Command Reference for Cisco ASR 9000 Series Routers</td>
</tr>
</tbody>
</table>
To assign a route policy in PIM to select a reverse-path forwarding (RPF) topology, use the `rpf topology route-policy` command in PIM command mode. To disable this configuration, use the `no` form of this command.

```
rpf topology route-policy policy-name
no rpf topology route-policy policy-name
```

**Syntax Description**

- **policy-name** (Required) Name of the specific route policy that you want PIM to associate with a reverse-path forwarding topology.

**Command Default**

No default behavior or values

**Command Modes**

- PIM configuration
- PIM address-family configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

For information about routing policy commands and how to create a routing policy, see *Routing Command Reference for Cisco ASR 9000 Series Routers* and *Routing Configuration Guide for Cisco ASR 9000 Series Routers*.

To assign a route policy using an IPv6 address family prefix, you must enter the command as shown in the Examples section.

**Examples**

The following examples show how to associate a specific routing policy in PIM with a RPF topology table for IPv4 address family prefixes:

```
RP/0/RSP0/CPU0:router(config)# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# rpf topology route-policy mypolicy
RP/0/RSP0/CPU0:router(config-pim-default-ipv6)# router pim address-family ipv6
RP/0/RSP0/CPU0:router(config-pim-default-ipv6)# rpf topology route-policy mypolicy
```
**rpf-redirect**

To assign a rpf-redirect route policy in PIM, use the `rpf-redirect route-policy` command in PIM command mode. To disable this configuration, use the `no` form of this command.

```
rpf-redirect route-policy policy-name
no rpf-redirect route-policy policy-name
```

**Syntax Description**

- `policy-name` (Required) Name of the specific route policy that you want PIM to associate with a reverse-path forwarding topology.

**Command Default**

No default behavior or values

**Command Modes**

- PIM configuration
- PIM address-family configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

For information about routing policy commands and how to create a routing policy, see *Routing Command Reference for Cisco ASR 9000 Series Routers* and *Routing Configuration Guide for Cisco ASR 9000 Series Routers*.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Example**

The following example shows how to associate a specific rpf-redirect routing policy to an rpf-redirect bundle for IPv4 address family prefixes:

```
RP/0/RSP0/CPU0:router(config)# router pim
RP/0/RSP0/CPU0:router(config-pim)#address-family ipv4
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# rpf-redirect route-policy <route-policy>
```
To enable Reverse Path Forwarding (RPF) vector signaling for Protocol Independent Multicast (PIM), use the `rpf-vector` command in PIM configuration mode. To return to the default behavior, use the `no` form of this command.

```
  rpf-vector
  no rpf-vector
```

**Syntax Description**

This command has no keywords or arguments.

**Command Default**

By default, RPF vector signaling is disabled.

**Command Modes**

PIM configuration

**Command History**

```
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>
```

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

RPF vector is a PIM proxy that lets core routers without RPF information forward join and prune messages for external sources (for example, a Multiprotocol Label Switching [MPLS]-based BGP-free core, where the MPLS core router is without external routes learned from Border Gateway Protocol [BGP]).

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to enable RPF vector:

```
RP/0/RSP0/CPU0:router(config)# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# rpf-vector
```
To configure the deny range of the static Protocol Independent Multicast (PIM) rendezvous point (RP), use the `rp-static-deny` command in PIM configuration mode. To return to the default behavior, use the `no` form of this command.

```
rp-static-deny access-list
no rp-static-deny
```

**Syntax Description**

- `access-list`: Name of an access list. This list is a standard IP access list.

**Command Default**

No default behavior or values

**Command Modes**

PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

- `multicast`: read, write

**Examples**

The following example shows how to configure the PIM RP deny range:

```
RP/0/RSP0/CPU0:router(config)# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# rp-static-deny listA
```
show auto-rp candidate-rp

To display the group ranges that this router represents (advertises) as a candidate rendezvous point (RP), use the `show auto-rp candidate-rp` command in EXEC mode.

```
show auto-rp [ipv4] candidate-rp
```

**Syntax Description**
- `ipv4` (Optional) Specifies IPv4 address prefixes.

**Command Default**
IPv4 addressing is the default.

**Command Modes**
EXEC

**Command History**
- **Release** 3.7.2 This command was introduced.

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `show auto-rp candidate-rp` command displays all the candidate rendezvous points configured on this router.

Information that is displayed is the time-to-live (TTL) value; the interval from which the rendezvous point announcements were sent; and the mode, such as Protocol Independent Multicast (PIM) sparse mode (SM), to which the rendezvous point belongs.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**
The following is sample output from the `show auto-rp candidate-rp` command:

```
RP/0/RSP0/CPU0:router# show auto-rp candidate-rp
Group Range Mode Candidate RP ttl interval
224.0.0.0/4 SM 10.0.0.6 30 30
```

This table describes the significant fields shown in the display.

**Table 31: show auto-rp candidate-rp Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Range</td>
<td>Multicast group address and prefix for which this router is advertised as a rendezvous point.</td>
</tr>
</tbody>
</table>
## show auto-rp candidate-rp

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mode</td>
<td>PIM protocol mode for which this router is advertised as a rendezvous point, either PIM-SM or bidirectional PIM (bidir).</td>
</tr>
<tr>
<td>Candidate RP</td>
<td>Address of the interface serving as a rendezvous point for the range.</td>
</tr>
<tr>
<td>ttl</td>
<td>TTL scope value (in router hops) for Auto-RP candidate announcement messages sent out from this candidate rendezvous point interface.</td>
</tr>
<tr>
<td>interval</td>
<td>Time between candidate rendezvous point announcement messages for this candidate rendezvous point interface.</td>
</tr>
</tbody>
</table>
**show pim context**

To show the reverse path forwarding (RPF) table information configured for a VRF context, use the `show pim context` command in EXEC mode.

```plaintext
show pim [vrf vrf-name] [ipv4] context
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.

**Command Default**

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

**Command Modes**

EXEC

**Command History**

- **Release 3.7.2** This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

- `multicast` read

**Examples**

The following example illustrates output from use of the `show pim context` command:

```plaintext
RP/0/RSP0/CPU0:router# show pim context

VRF ID: 0x60000000
Table ID: 0xe0000000
Remote Table ID: 0xe0800000
MDT Default Group : 0.0.0.0
MDT handle: 0x0
Context Active, ITAL Active
Routing Enabled
Registered with MRIB
Not owner of MDT Interface
Raw socket req: T, act: T, LPTS filter req: T, act: T
UDP socket req: T, act: T, UDP vbind req: T, act: T
Mhost Default Interface : Null {publish pending: F}
Remote MDT Default Group : 0.0.0.0
Neighbor-filter: -
```
The following table gives the field descriptions for the `show pim context` command output:

**Table 32: show pim context Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF ID</td>
<td>VPN routing and forwarding instance identification.</td>
</tr>
<tr>
<td>Table ID</td>
<td>Identification of unicast default table as of VRF context activation.</td>
</tr>
<tr>
<td>Remote Table ID</td>
<td>Identifies the table ID of the opposite address family.</td>
</tr>
<tr>
<td></td>
<td>For example, the remote table ID for the VRF context of the</td>
</tr>
<tr>
<td>MDT Default Group</td>
<td>Identifies the multicast distribution tree (MDT) group configured as the default for use by the VRF.</td>
</tr>
<tr>
<td>MDT handle</td>
<td>Identifies the handle for multicast packets to be passed through the MDT interface.</td>
</tr>
<tr>
<td>Context Active</td>
<td>Identifies whether or not the VRF context was activated.</td>
</tr>
<tr>
<td>ITAL Active</td>
<td>Identifies whether or not the VRF is registered with ITAL. If it is, this signifies that the VRF is configured globally.</td>
</tr>
<tr>
<td>Routing Enabled</td>
<td>Identifies whether or not PIM is enabled in the VRF.</td>
</tr>
<tr>
<td>Registered with MRIB</td>
<td>Identifies whether or not the VRF is registered with Multicast Routing Information Base (MRIB).</td>
</tr>
<tr>
<td>Not owner of MDT interface</td>
<td>Identifies a process as not being the owner of the MDT interface.</td>
</tr>
<tr>
<td></td>
<td>The owner is either the PIM or the PIM IPv6 process.</td>
</tr>
<tr>
<td>Owner of MDT interface</td>
<td>Identifies the owner of the MDT interface.</td>
</tr>
<tr>
<td></td>
<td>The owner is either the PIM or the PIM IPv6 process.</td>
</tr>
<tr>
<td>Raw socket req:</td>
<td>Raw socket operations requested.</td>
</tr>
<tr>
<td>act:</td>
<td>Action: Indicates whether or not the operations were performed.</td>
</tr>
<tr>
<td>T; F</td>
<td>True; False</td>
</tr>
<tr>
<td>LPTS filter req</td>
<td>Identifies whether or not the VRF was requested to be added to the socket.</td>
</tr>
<tr>
<td>UDP socket req</td>
<td>Identifies whether or not a UDP socket was requested.</td>
</tr>
<tr>
<td>UDP vbind req</td>
<td>Identifies whether or not the VRF was added to the UDP socket.</td>
</tr>
<tr>
<td>Reg Inj socket req</td>
<td>This Boolean indicates whether or not the register inject socket, used for PIM register messages, was requested.</td>
</tr>
<tr>
<td>Reg Inj LPTS filter req</td>
<td>Indicates whether or not the VRF was added to the register inject socket.</td>
</tr>
<tr>
<td><strong>Field</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>---------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mhost Default Interface</td>
<td>Identifies the default interface to be used for multicast host (Mhost).</td>
</tr>
<tr>
<td>Remote MDT Default Group</td>
<td>Identifies the MDT transiting this VRF or address family in use by the remote</td>
</tr>
<tr>
<td></td>
<td>address family.</td>
</tr>
<tr>
<td>Neighbor-filter</td>
<td>Name of the neighbor filter used to filter joins or prunes from neighbors. If the</td>
</tr>
<tr>
<td></td>
<td>there is no neighbor filter, the output reads: &quot;-&quot;.</td>
</tr>
</tbody>
</table>
show pim context table

To display a summary list of all tables currently configured for a VRF context, use the `show pim context table` command in EXEC mode.

```
show pim [vrf vrf-name] [ipv4] context table
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.

**Command Default**

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

**Command Modes**

EXEC

**Command History**

- **Release 3.7.2** This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following example illustrates the output for PIM table contexts for a VRF default after using the `show pim context table` command:

```
RP/0/RSP0/CPU0:router# show pim ipv4 context table

PIM Table contexts for VRF default

<table>
<thead>
<tr>
<th>Table</th>
<th>TableID</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4-Unicast-default</td>
<td>0xe0000000</td>
<td>Active</td>
</tr>
<tr>
<td>IPv4-Multicast-default</td>
<td>0xe0100000</td>
<td>Active</td>
</tr>
<tr>
<td>IPv4-Multicast-t201</td>
<td>0xe010000b</td>
<td>Active</td>
</tr>
<tr>
<td>IPv4-Multicast-t202</td>
<td>0xe010000c</td>
<td>Active</td>
</tr>
<tr>
<td>IPv4-Multicast-t203</td>
<td>0xe010000d</td>
<td>Active</td>
</tr>
<tr>
<td>IPv4-Multicast-t204</td>
<td>0xe010000e</td>
<td>Active</td>
</tr>
<tr>
<td>IPv4-Multicast-t205</td>
<td>0xe010000f</td>
<td>Active</td>
</tr>
<tr>
<td>IPv4-Multicast-t206</td>
<td>0xe0100010</td>
<td>Active</td>
</tr>
<tr>
<td>IPv4-Multicast-t207</td>
<td>0xe0100011</td>
<td>Active</td>
</tr>
<tr>
<td>IPv4-Multicast-t208</td>
<td>0x00000000</td>
<td>Inactive</td>
</tr>
<tr>
<td>IPv4-Multicast-t209</td>
<td>0x00000000</td>
<td>Inactive</td>
</tr>
<tr>
<td>IPv4-Multicast-t210</td>
<td>0x00000000</td>
<td>Inactive</td>
</tr>
</tbody>
</table>
```
### Table 33: show pim ipv4 context table Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table</td>
<td>Context table name.</td>
</tr>
<tr>
<td>Table ID</td>
<td>RSI table ID for the table.</td>
</tr>
<tr>
<td>Status</td>
<td>Identifies whether or not the context table is active or inactive. The table displays “Active” if it was globally configured under a given VRF, and if RSI considers it to be active. The table displays “Inactive” if the opposite is true.</td>
</tr>
</tbody>
</table>
show pim global summary

To display configured Protocol Independent Multicast (PIM) out-of-resource (OOR) limits and current counts for all VRFs, use the `show pim global summary` command in EXEC mode.

**Syntax Description**
This command has no keywords or arguments.

**Command Default**
None

**Command Modes**
EXEC mode

**Command History**
<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
Use the `show pim global summary` command to display global limits that are shared by all VRFs.

**Task ID**
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**
The following is sample output from the `show pim global summary` command that shows PIM routes, with the maximum number of routes allowed being 100000:

```
RP/0/RSP0/CPU0:router# show pim global summary
PIM Global Summary
PIM State Counters
     Routes  Current   Maximum  Warning-threshold
         8     100000    100000
     Topology Interface States  8     300000    300000
     SM Registers                0     20000     20000
     AutoRP Group Ranges         0       500      450
     BSR Group Ranges            0       500      450
     BSR C-RP caches             0       100      0
```

This table describes the significant fields shown in the display.

**Table 34: show pim global summary Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routes</td>
<td>Current number of routes (in the PIM topology table) and the maximum allowed before the creation of new routes is prohibited to avoid out-of-resource (OOR) conditions.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Topology Interface States</td>
<td>Current total number of interfaces (in the PIM topology table) present in all route entries and the maximum allowed before the creation of new routes is prohibited to avoid OOR conditions.</td>
</tr>
<tr>
<td>SM Registers</td>
<td>Current number of sparse mode route entries from which PIM register messages are received and the maximum allowed before the creation of new register states is prohibited to avoid OOR conditions.</td>
</tr>
<tr>
<td>AutoRP Group Ranges</td>
<td>Current number of sparse mode group range-to-rendezvous point mappings learned through the auto-rendezvous point (Auto-RP) mechanism and the maximum allowed before the creation of new group ranges is prohibited to avoid OOR conditions.</td>
</tr>
<tr>
<td>Warning-threshold</td>
<td>Maximum number of multicast routes that can be configured per router.</td>
</tr>
<tr>
<td>BSR Group Ranges</td>
<td>The number of BSR groups and the maximum set range.</td>
</tr>
<tr>
<td>BSR C-RP caches</td>
<td>The number of candidate-RP caches in BSR and the maximum set range.</td>
</tr>
</tbody>
</table>
show pim group-map

To display group-to-PIM mode mapping, use the show pim group-map command in EXEC mode.

show pim [vrf vrf-name] [ipv4] group-map [ip-address-name] [info-source]

Syntax Description

- **vrf vrf-name**: (Optional) Specifies a VPN routing and forwarding (VRF) instance.

- **ipv4**: (Optional) Specifies IPv4 address prefixes.

- **ip-address-name**: (Optional) IP address name as defined in the Domain Name System (DNS) hosts table or with the domain ipv4 host in the format A.B.C.D.

- **info-source**: (Optional) Displays the group range information source.

Command Default

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

Command Modes

EXEC

Command History

Release 3.7.2 This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The show pim group-map command displays all group protocol address mappings for the rendezvous point. Mappings are learned from different clients or through the auto rendezvous point (Auto-RP) mechanism.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

Examples

The following is sample output from the show pim group-map command:

RP/0/RSP0/CPU0:router# show pim group-map

IP PIM Group Mapping Table
(* indicates group mappings being used)
(+ indicates BSR group mappings active in MRIB)

<table>
<thead>
<tr>
<th>Group Range</th>
<th>Proto</th>
<th>Client</th>
<th>Groups</th>
<th>RP address</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>224.0.1.39/32*</td>
<td>DM</td>
<td>perm</td>
<td>1</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>224.0.1.40/32*</td>
<td>DM</td>
<td>perm</td>
<td>1</td>
<td>0.0.0.0</td>
<td></td>
</tr>
<tr>
<td>224.0.0.0/24*</td>
<td>NO</td>
<td>perm</td>
<td>0</td>
<td>0.0.0.0</td>
<td></td>
</tr>
</tbody>
</table>
In lines 1 and 2, Auto-RP group ranges are specifically denied from the sparse mode group range.

In line 3, link-local multicast groups (224.0.0.0 to 224.0.0.255 as defined by 224.0.0.0/24) are also denied from the sparse mode group range.

In line 4, the Protocol Independent Multicast (PIM) Source Specific Multicast (PIM-SSM) group range is mapped to 232.0.0.0/8.

Line 5 shows that all the remaining groups are in sparse mode mapped to rendezvous point 10.10.3.2.

This table describes the significant fields shown in the display.

**Table 35: show pim group-map Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Range</td>
<td>Multicast group range that is mapped.</td>
</tr>
<tr>
<td>Proto</td>
<td>Multicast forwarding mode.</td>
</tr>
<tr>
<td>Client</td>
<td>States how the client was learned.</td>
</tr>
<tr>
<td>Groups</td>
<td>Number of groups from the PIM topology table.</td>
</tr>
<tr>
<td>RP address</td>
<td>Rendezvous point address.</td>
</tr>
<tr>
<td>Info</td>
<td>RPF interface used and the PIM-SM Reverse Path Forwarding (RPF) information toward the rendezvous point.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rp-address, on page 443</td>
<td>Configures the address of a PIM rendezvous point for a particular group.</td>
</tr>
<tr>
<td>show pim range-list, on page 476</td>
<td>Displays the range-list information for PIM.</td>
</tr>
</tbody>
</table>
**show pim interface**

To display information about interfaces configured for Protocol Independent Multicast (PIM), use the `show pim interface` command in EXEC mode.

```
show pim [vrf vrf-name] [ipv4] interface [type interface-path-id|state-on|state-off] [detail]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a VPN routing and forwarding (VRF) instance.</td>
</tr>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IPv4 address prefixes.</td>
</tr>
<tr>
<td>type</td>
<td>(Optional) Interface type. For more information, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>interface-path-id</td>
<td>(Optional) Physical interface or virtual interface. Note: Use the <code>show interfaces</code> command in EXEC mode to see a list of all interfaces currently configured on the router. For more information about the syntax for the router, use the question mark (?) online help function.</td>
</tr>
<tr>
<td>state-on</td>
<td>(Optional) Displays only interfaces from which PIM is enabled and active.</td>
</tr>
<tr>
<td>state-off</td>
<td>(Optional) Displays only interfaces from which PIM is disabled or inactive.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Displays detailed address information.</td>
</tr>
</tbody>
</table>

**Command Default**

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `show pim interface` command displays neighboring information on all PIM-enabled interfaces, such as designated router (DR) priority and DR election winner.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>
Examples

The following is sample output from the `show pim interface` command:

```
RP/0/RSP0/CPU0:router# show pim interface

+-----------+-----------------+-------------+-------------+-------------+-------------+-------------+
| Address   | Interface       | PIM Nbr Count | Hello Intvl | DR Prior    |
|-----------|-----------------|-------------|-------------|-------------|-------------|
| 172.29.52.127 | MgmtEth0/0/CP0/0 | off 0       | 30 1        | not elected |
| 10.6.6.6  | Loopback0       | off 0       | 30 1        | not elected |
| 0.0.0.0   | Loopback61      | off 0       | 30 1        | not elected |
| 10.46.4.6 | ATM0/2/0/0.1    | off 0       | 30 1        | not elected |
| 10.46.5.6 | ATM0/2/0/0.2    | off 0       | 30 1        | not elected |
| 10.46.6.6 | ATM0/2/0/0.3    | off 0       | 30 1        | not elected |
| 10.46.7.6 | ATM0/2/0/0.4    | off 0       | 30 1        | not elected |
| 10.46.8.6 | ATM0/2/0/3.1    | off 0       | 30 1        | not elected |
| 10.46.9.6 | ATM0/2/0/3.2    | off 0       | 30 1        | not elected |
| 10.56.16.6| Serial10/3/2/1  | off 0       | 30 1        | not elected |
| 10.56.4.2 | Serial10/3/0/0/0:0 | off 0 | 30 1  | not elected |
| 10.56.4.6 | Serial10/3/0/1:0 | off 0 | 30 1  | not elected |
| 10.56.4.10| Serial10/3/0/2:0 | off 0 | 30 1  | not elected |
| 10.56.4.14| Serial10/3/0/2:1 | off 0 | 30 1  | not elected |
| 10.56.4.18| Serial10/3/0/2:2 | off 0 | 30 1  | not elected |
| 10.56.4.22| Serial10/3/0/2:3 | off 0 | 30 1  | not elected |
| 10.56.4.26| Serial10/3/0/3:2 | off 0 | 30 1  | not elected |
| 10.56.4.30| Serial10/3/0/3:3 | off 0 | 30 1  | not elected |
| 10.56.8.2 | Serial10/3/0/1:0 | off 0 | 30 1  | not elected |
| 10.56.12.6| Serial10/3/2/0.1 | off 0 | 30 1  | not elected |
| 10.56.13.6| Serial10/3/2/0.2 | off 0 | 30 1  | not elected |
| 10.56.14.6| Serial10/3/2/0.3 | off 0 | 30 1  | not elected |
| 10.56.15.6| Serial10/3/2/0.4 | off 0 | 30 1  | not elected |
| 10.67.4.6 | POS0/4/1/0      | off 0       | 30 1        | not elected |
| 10.67.8.6 | POS0/4/1/1      | off 0       | 30 1        | not elected |
+-----------+-----------------+-------------+-------------+-------------+-------------+
```

This table describes the significant fields shown in the display.

**Table 36: show pim interface Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>IP address of the interface.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface type and number that is configured to run PIM.</td>
</tr>
<tr>
<td>PIM</td>
<td>PIM is turned off or turned on this interface.</td>
</tr>
<tr>
<td>Nbr Count</td>
<td>Number of PIM neighbors in the neighbor table for the interface.</td>
</tr>
<tr>
<td>Hello Intvl</td>
<td>Frequency, in seconds, of PIM hello messages, as set by the <code>ip pim hello-interval</code> command in interface configuration mode.</td>
</tr>
<tr>
<td>DR Priority</td>
<td>Designated router priority is advertised by the neighbor in its hello messages.</td>
</tr>
</tbody>
</table>
### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show pim neighbor, on page 469</td>
<td>Displays the Protocol Independent Multicast (PIM) neighbors discovered by means of PIM hello messages.</td>
</tr>
</tbody>
</table>
show pim join-prune statistic

To display Protocol Independent Multicast (PIM) join and prune aggregation statistics, use the `show pim join-prune statistics` command in EXEC mode.

```
show pim [vrf vrf-name] [ipv4] join-prune statistic [type interface-path-id]
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `type` (Optional) Interface type. For more information, use the question mark (?) online help function.
- `interface-path-id` (Optional) Physical interface or virtual interface.

**Note** Use the `show interfaces` command in EXEC mode to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

**Command Default**

IP addressing is the default. If no VRF is specified, the default VRF is operational.

**Command Modes**

EXEC

**Command History**

Release 3.7.2 This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `show pim join-prune statistics` command displays the average PIM join and prune groups for the most recent packets (in increments of 1000/10000/50000) that either were sent out or received from each PIM interface. If fewer than 1000/10000/50000 join and prune group messages are received since PIM was started or the statistics were cleared, the join-prune aggregation shown in the command display is zero (0).

Because each PIM join and prune packet can contain multiple groups, this command can provide a snapshot view of the average pace based on the number of join and prune packets, and on the consideration of the aggregation factor of each join and prune packet.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show pim join-prune statistics` command with all router interfaces specified:
show pim join-prune statistic

RP/0/RSP0/CPU0:router#  show pim join-prune statistics

PIM Average Join/Prune Aggregation for last (100/1K/10K) packets

<table>
<thead>
<tr>
<th>Interface</th>
<th>MTU</th>
<th>Transmitted</th>
<th>Received</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loopback0</td>
<td>1514</td>
<td>0 / 0 / 0</td>
<td>0 / 0 / 0</td>
</tr>
<tr>
<td>Encapstunnel0</td>
<td>0</td>
<td>0 / 0 / 0</td>
<td>0 / 0 / 0</td>
</tr>
<tr>
<td>Decapstunnel0</td>
<td>0</td>
<td>0 / 0 / 0</td>
<td>0 / 0 / 0</td>
</tr>
<tr>
<td>Loopback1</td>
<td>1514</td>
<td>0 / 0 / 0</td>
<td>0 / 0 / 0</td>
</tr>
<tr>
<td>POS0/3/0/0</td>
<td>4470</td>
<td>0 / 0 / 0</td>
<td>0 / 0 / 0</td>
</tr>
<tr>
<td>POS0/3/0/3</td>
<td>4470</td>
<td>0 / 0 / 0</td>
<td>0 / 0 / 0</td>
</tr>
</tbody>
</table>

This table describes the significant fields shown in the display.

Table 37: show pim join-prune statistics Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Interface from which statistics were collected.</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum transmission unit (MTU) in bytes for the interface.</td>
</tr>
<tr>
<td>Transmitted</td>
<td>Number of join and prune states aggregated into transmitted messages in the last 1000/10000/50000 transmitted join and prune messages.</td>
</tr>
<tr>
<td>Received</td>
<td>Number of join and prune states aggregated into received messages in the last 1000/10000/50000 received join and prune messages.</td>
</tr>
</tbody>
</table>
show pim rpf-redirect

To display the maximum bandwidth, the bandwidth used by traffic flowing through the local box, and the bandwidth used by other routers sharing the PIM bundle member interfaces of all members of bundles known to the system, use show pim rpf-redirect command in EXEC mode.

show pim ipv4 rpf-redirect

Syntax Description

ipv4  (Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

Example

The following sample output from the show pim rpf-redirect command displays statistics about the PIM bundles:

RP/0/RSP0/CPU0:router#show pim rpf-redirect

Mon Aug 11 16:50:35.811 IST

PIM RPF-Redirect bundle database

<table>
<thead>
<tr>
<th>Member</th>
<th>Available/Allocated Bandwidth (Kbps)</th>
<th>Available/Allocated Threshold Bandwidth (Kbps)</th>
<th>Local / Network Bandwidth (Kbps)</th>
<th>Total Bandwidth (Kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bundle: east</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Gi0/0/0/0</td>
<td>100000/100000</td>
<td>80000/80000</td>
<td>0/0</td>
<td>0</td>
</tr>
</tbody>
</table>

where, Available/Allocated Bandwidth (kbps) is the total multicast bandwidth (in kbps) available/allocated for multicast transmission; Available/Threshold Bandwidth (kbps) is the multicast bandwidth threshold beyond which the redirects are enabled, displays the available and the threshold bandwidth (kbps); Local/Network Bandwidth (kbps) is the difference between the Allocated Bandwidth and Available Bandwidth; and the Total Bandwidth (kbps) is represented by the Local/Network Bandwidth.
show pim rpf-redirect route

To display the content of the snooping database, use `show pim rpf-redirect` command in EXEC mode.

```
show pim  ipv4 rpf-redirect route
```

**Syntax Description**

`ipv4`  (Optional) Specifies IPv4 address prefixes.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 4.3.0</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>
show pim mstatic

To display multicast static routing information, use the show pim mstatic command in EXEC mode.

```
show pim [ipv4] mstatic [ipv4]
```

Syntax Description

- `ipv4` (Optional) Specifies IPv4 address prefixes.

Command Default

IPv4 addressing is the default.

Command Modes

EXEC

Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The show pim mstatic command is used to view all the multicast static routes. Multicast static routes are defined by the static-rpf command.

Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

Examples

The following is sample output from the show pim mstatic command that shows how to reach IP address 10.0.0.1:

```
RP/0/RSP0/CPU0:router# show pim mstatic

IP Multicast Static Routes Information
* 10.0.0.1/32 via pos0/1/0/1 with nexthop 172.16.0.1 and distance 0
```

This table describes the significant fields shown in the display.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1</td>
<td>Destination IP address</td>
</tr>
<tr>
<td>pos0/1/0/1</td>
<td>Interface that is entered to reach destination IP address 10.0.0.1</td>
</tr>
<tr>
<td>172.16.0.1</td>
<td>Next-hop IP address to enter to reach destination address 10.0.0.1</td>
</tr>
</tbody>
</table>
Field | Description
--- | ---
0 | Distance of this mstatic route.

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>static-rpf</td>
<td>Configures a static Reverse Path Forwarding (RPF) rule for a specified prefix mask.</td>
</tr>
</tbody>
</table>
show pim neighbor

To display the Protocol Independent Multicast (PIM) neighbors discovered by means of PIM hello messages, use the `show pim neighbor` command in EXEC mode.

```
show pim [vrf vrf-name] [ipv4] neighbor [type interface-path-id] [{count|detail}]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vrf vrf-name</td>
<td>(Optional) Specifies a VPN routing and forwarding (VRF) instance.</td>
</tr>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IPv4 address prefixes.</td>
</tr>
<tr>
<td>type interface-path-id</td>
<td>(Optional) Physical interface or virtual interface.</td>
</tr>
</tbody>
</table>

**Note** Use the `show interfaces` command in EXEC mode to see a list of all interfaces currently configured on the router.

For more information about the syntax for the router, use the question mark (?) online help function.

<table>
<thead>
<tr>
<th>Command Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.</td>
<td></td>
</tr>
</tbody>
</table>

**Command Modes**

EXEC

**Command History**

Release 3.7.2 This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

```
Task ID Operations
multicast read
```

**Examples**

The following is sample output from the `show pim neighbor` command:
```plaintext
RP/0/RSP0/CPU0:router# show pim neighbor

Neighbor Address  Interface     Uptime   Expires  DR  pri  Bidir  Flags
172.17.1.2*      Loopback1    03:41:22  00:01:43  1   (DR)  B
172.17.2.2*      Loopback2    03:41:20  00:01:31  1   (DR)  B
172.17.3.2*      Loopback3    03:41:18  00:01:28  1   (DR)  B
10.10.1.1         POS0/2/0/0   03:40:36  00:01:41  1   B
10.10.1.2*        POS0/2/0/0   03:41:28  00:01:32  1   (DR)  B
10.10.2.2*        POS0/2/0/2   03:41:26  00:01:36  1   B
10.10.2.3         POS0/2/0/2   03:41:25  00:01:29  1   (DR)  B
PIM neighbors in VRF default
Neighbor Address  Interface     Uptime   Expires  DR  pri  Flags
10.6.6.6*         Loopback0    4w1d     00:01:24  1   (DR)  B
10.16.8.1         GigabitEthernet0/4/0/2 3w2d  00:01:24  1   B
10.16.8.6*        GigabitEthernet0/4/0/2 3w2d  00:01:28  1   (DR)  B
192.168.66.6*     GigabitEthernet0/4/0/0.7 4w1d  00:01:28  1   (DR)
B P
192.168.67.6*     GigabitEthernet0/4/0/0.8 4w1d  00:01:40  1   (DR)
B P
192.168.68.6*     GigabitEthernet0/4/0/0.9 4w1d  00:01:24  1   (DR)
B P
PIM neighbors in VRF default
Neighbor Address  Interface     Uptime   Expires  DR  pri  Flags
28.28.9.2*       GigabitEthernet0/2/0/9  00:39:34  00:01:40  1   (DR)  B A
10.1.1.1         GigabitEthernet0/2/0/19  00:49:30  00:01:42  1   B A
10.1.1.2*        GigabitEthernet0/2/0/19  00:50:01  00:01:41  1   (DR)  B A
2.2.2.2*         Loopback0     00:50:01  00:01:42  1   (DR)  B A

The following is sample output from the show pim neighbor command with the count option:

RP/0/RSP0/CPU0:router# show pim neighbor count

Interface  Nbr count
POS0/3/0/0  1
Loopback1  1
Total Nbrs  2

This table describes the significant fields shown in the display.

Table 39: show pim neighbor Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neighbor Address</td>
<td>IP address of the PIM neighbor.</td>
</tr>
<tr>
<td>Interface</td>
<td>Interface type and number on which the neighbor is reachable.</td>
</tr>
<tr>
<td>Uptime</td>
<td>Time the entry has been in the PIM neighbor table.</td>
</tr>
<tr>
<td>Expires</td>
<td>Time until the entry is removed from the IP multicast routing table.</td>
</tr>
</tbody>
</table>
```
### Field Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DR pri</td>
<td>DR priority sent by the neighbor in its hello messages. If this neighbor is elected as the DR on the interface, it is annotated with “(DR)” in the command display.</td>
</tr>
<tr>
<td>Nbr count</td>
<td>Number of PIM neighbors in the neighbor table for all interfaces on this router.</td>
</tr>
</tbody>
</table>

#### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show pim interface, on page 460</td>
<td>Displays information about interfaces configured for Protocol Independent Multicast (PIM).</td>
</tr>
</tbody>
</table>
show pim nsf

To display the state of nonstop forwarding (NSF) operation for Protocol Independent Multicast (PIM), use the `show pim nsf` command in EXEC mode.

```
show pim [ipv4] nsf
```

**Syntax Description**

- `ipv4` (Optional) Specifies IPv4 address prefixes.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
</table>
| 3.7.2   | This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `show pim nsf` command displays the current multicast NSF state for PIM. For multicast NSF, the state may be normal or activated for nonstop forwarding. The latter state indicates that recovery is in progress due to a failure in the Multicast Routing Information Base (MRIB) or PIM. The total NSF timeout and time remaining are displayed until NSF expiration.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show pim nsf` command:

```
RP/0/RSP0/CPU0:router# show pim nsf

IP PIM Non-Stop Forwarding Status:
Multicast routing state: Non-Stop Forwarding Activated
NSF Lifetime: 00:02:00
NSF Time Remaining: 00:01:56
```
This table describes the significant fields shown in the display.

Table 40: show pim nsf Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Multicast routing state</td>
<td>PIM state is in NSF recovery mode (Normal or Non-Stop Forwarding Activated).</td>
</tr>
<tr>
<td>NSF Lifetime</td>
<td>Total NSF lifetime (seconds, hours, and minutes) configured for PIM.</td>
</tr>
<tr>
<td>NSF Time Remaining</td>
<td>Time remaining in NSF recovery for PIM if NSF recovery is activated.</td>
</tr>
</tbody>
</table>
show pim nsr

To display the nonstop routing (NSR) information for Protocol Independent Multicast (PIM), use the `show pim nsr` command in EXEC mode.

```
show pim [ipv4|ipv6] nsr
```

**Syntax Description**

- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `ipv6` (Optional) Specifies IPv6 address prefixes.

**Command Default**
IPv4 addressing is the default.

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `show pim nsr` command displays the current multicast NSR state for PIM. For multicast NSR, the state may be Ready or Not activated for non-stop routing. The latter state indicates that recovery is in progress due to a failure in the Multicast Routing Information Base (MRIB) or PIM. The total NSR timeout and time remaining are displayed until NSR expiration.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show pim nsr` command:

```
RP/0/RSP0/CPU0:router# show pim nsr

PIM NSR Data:
State : Ready
RMF Timer : N [-]
RMF Notif done : Y
Last RMF rdy : 4w0d [1]
Last RMF not rdy : Never [0]
Last conn up : Never [0]
Last conn down : Never [0]
```
This table describes the significant fields shown in the display.

**Table 41: show pim nsr Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Multicast Non-Stop Routing State: Ready or Not Ready</td>
</tr>
<tr>
<td>RMF Timer</td>
<td>Whether RMF timer is running or not, indicates either Yes or No</td>
</tr>
<tr>
<td>RMF Notify done</td>
<td>RMF notification received: Yes or No</td>
</tr>
<tr>
<td>Last RMF ready</td>
<td>The Time when the last RMF ready notification was received: Yes, No, or Never. The number in the brackets indicate the number of times the RMF ready notification was received. Yes, No, or Never respectively.</td>
</tr>
<tr>
<td>Last RMF not ready</td>
<td>The Time when the last RMF ready notification was received: Yes, No, or Never. The number in the brackets indicate the number of times the RMF not ready notification was issued.</td>
</tr>
<tr>
<td>Last connection up</td>
<td>The Time when the last RMF ready notification was received: Yes, No, or Never. The number in the brackets indicate the number of times the RMF not ready notification was received.</td>
</tr>
<tr>
<td>Last connection down</td>
<td>Whether the Last connection down notification is issued: Yes, No, or Never. The number in the brackets indicate the number of times the RMF not ready notification was received.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show msdp nsr</td>
<td>Displays the state of NSR operation for MSDP.</td>
</tr>
<tr>
<td>show mrib nsr</td>
<td>Displays the state of NSR operation in MRIB.</td>
</tr>
<tr>
<td>show igmp nsr</td>
<td>Displays the state of NSR operation for IGMP.</td>
</tr>
</tbody>
</table>
show pim range-list

To display range-list information for Protocol Independent Multicast (PIM), use the `show pim range-list` command in EXEC mode.

```
show pim [vrf vrf-name] [ipv4] range-list [config] [ip-address-name]
```

**Syntax Description**

- **vrf vrf-name** (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- **ipv4** (Optional) Specifies IPv4 address prefixes.
- **config** (Optional) Displays PIM command-line interface (CLI) range-list information.
- **ip-address-name** (Optional) IP address of the rendezvous point.

**Command Default**

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `show pim range-list` command is used to determine the multicast forwarding mode to group mapping. The output also indicates the rendezvous point (RP) address for the range, if applicable. The `config` keyword means that the particular range is statically configured.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show pim range-list` command:

```
RP/0/RSP0/CPU0:router# show pim range-list

config SSM Exp: never Src: 0.0.0.0
  230.0.0.0/8 Up: 03:47:09
config BD RP: 172.16.1.3 Exp: never Src: 0.0.0.0
  239.0.0.0/8 Up: 03:47:16
config SM RP: 172.18.2.6 Exp: never Src: 0.0.0.0
  235.0.0.0/8 Up: 03:47:09
```
This table describes the significant fields shown in the display.

**Table 42: show pim range-list Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>config</td>
<td>Group range was learned by means of configuration.</td>
</tr>
<tr>
<td>SSM</td>
<td>PIM mode is operating in Source Specific Multicast (SSM) mode. Other modes are Sparse-Mode (SM) and bidirectional (BD) mode.</td>
</tr>
<tr>
<td>Exp: never</td>
<td>Expiration time for the range is “never”.</td>
</tr>
<tr>
<td>Src: 0.0.0.0</td>
<td>Advertising source of the range.</td>
</tr>
<tr>
<td>230.0.0.0/8</td>
<td>Group range: address and prefix.</td>
</tr>
<tr>
<td>Up: 03:47:09</td>
<td>Total time that the range has existed in the PIM group range table. In other words, the uptime in hours, minutes, and seconds.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show pim group-map, on page 458</td>
<td>Displays group-to-PIM mode mapping.</td>
</tr>
</tbody>
</table>
**show pim rpf**

To display information about reverse-path forwarding (RPF) in one or more routing tables within Protocol Independent Multicast (PIM), use the `show pim rpf` command in EXEC mode.

```
show pim [vrf vrf-name] {ipv4} {multicast|safi-all|unicast} [topology {table-name|all}] rpf [ip-address/name]
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `multicast` (Optional) Specifies a multicast secondary address family (SAFI).
- `safi-all` (Optional) Specifies a secondary address family (SAFI) wildcard.
- `unicast` (Optional) Specifies a unicast secondary address family (SAFI).
- `topology` (Optional) Specifies the display of multitopology routing table information.
- `table-name` Name of the specific multitopology table to show.
- `all` Specifies that detailed information be displayed for all multitopology routing tables in PIM.
- `ip-address/name` (Optional) IP address or name, or both, for the default or selected route policy with the domain IPv4 host in the format `A.B.C.D`

**Note**
The `ip-address` argument can also be a Protocol Independent Multicast (PIM) rendezvous point (RP) address.

**Command Default**
IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>
The following example shows output from the `show pim rpf` command:

```
RP/0/RSP0/CPU0:router# show pim rpf
Table: IPv4-Unicast-default
* 61.61.1.10/32 [90/181760]
  via GigabitEthernet0/1/0/1.201 with rpf neighbor 11.21.0.20
  via GigabitEthernet0/1/0/1.202 with rpf neighbor 11.22.0.20
  via GigabitEthernet0/1/0/1.203 with rpf neighbor 11.23.0.20
* 61.61.1.91/32 [90/181760]
  via GigabitEthernet0/1/0/1.201 with rpf neighbor 11.21.0.20
  via GigabitEthernet0/1/0/1.202 with rpf neighbor 11.22.0.20
  via GigabitEthernet0/1/0/1.203 with rpf neighbor 11.23.0.20
* 61.61.1.92/32 [90/181760]
  via GigabitEthernet0/1/0/1.201 with rpf neighbor 11.21.0.20
  via GigabitEthernet0/1/0/1.202 with rpf neighbor 11.22.0.20
  via GigabitEthernet0/1/0/1.203 with rpf neighbor 11.23.0.20
* 61.61.1.93/32 [90/181760]
  via GigabitEthernet0/1/0/1.201 with rpf neighbor 11.21.0.20
  via GigabitEthernet0/1/0/1.202 with rpf neighbor 11.22.0.20
  via GigabitEthernet0/1/0/1.203 with rpf neighbor 11.23.0.20
```
show pim rpf hash

To display information for Routing Information Base (RIB) lookups used to predict RPF next-hop paths for routing tables in Protocol Independent Multicast (PIM), use the **show pim rpf hash** command in EXEC mode.

```plaintext
show pim [vrf vrf-name] [ipv4] [multicast|safi-all|unicast] [topology {table-name|all}] rpf hash root/group ip-address/name [hash-mask-length bit-length|mofrr]
```

**Syntax Description**

- **vrf vrf-name**: (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- **ipv4**: (Optional) Specifies IPv4 address prefixes.
- **multicast**: (Optional) Specifies a multicast secondary address family (SAFI).
- **safi-all**: (Optional) Specifies a secondary address family (SAFI) wildcard.
- **unicast**: (Optional) Specifies a unicast secondary address family (SAFI).
- **topology**: (Optional) Specifies the display of multitopology routing table information.
- **table-name**: Name of the specific multitopology table to show.
- **all**: Specifies that detailed information be displayed for all multitopology routing tables in PIM.
- **root/group ip-address/group-name**: Root or group address, or both, for the default or selected route policy. IP address is as defined in the Domain Name System (DNS) hosts table or with the domain **ipv4** host in the format *A.B.C.D.*
- **hash-mask-length bit-length**: (Optional) Specifies the bootstrap router (BSR) hash mask length to be applied to the next-hop hashing. Default is the BSR hash mask length known for the matching group range (or host mask length if BSR is not configured for the range). The range in bit length is 0 to 32.
- **mofrr**: (Optional) Specifies MOFRR hashing.

**Command Default**

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.
The `show pim rpf hash` command lets you predict the way routes balance across Equal-Cost Multipath (ECMP) next hops. It does not require that route to exist in the Multicast Routing Information Base (MRIB) at the time.

When using the `ip-address` argument for a (*,G) route, use the rendezvous point address and omit the `group-address` argument. For (S,G) routes, use the `ip-address` and the `group-address` arguments.

### Task ID

#### Operations

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

### Examples

When you use the `show pim rpf hash` command, Cisco IOS XR software displays statistics regarding route policy invocations in topology tables:

```
RP/0/RSP0/CPU0:router# show pim rpf hash 10.0.0.1 239.0.0.1
Multipath RPF selection is enabled.
RPF next-hop neighbor selection result: POS0/2/0/0,10.1.0.1
```

The following example shows the results from use of the `mofrr` keyword:

```
RP/0/RSP0/CPU0:router# show pim rpf hash 11.11.0.4 226.1.1.2 mofrr
Table: IPv4-Unicast-default
Multipath RPF selection is enabled.
RPF next-hop neighbor selection result: POS0/2/0/0,10.1.0.1
Secondary RPF next-hop neighbor selection result: GigabitEthernet0/4/0/4,55.55.55.101
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>show pim rpf</code>, on page 478</td>
<td>Displays information about reverse-path forwarding (RPF) in one or more routing tables within Protocol Independent Multicast (PIM).</td>
</tr>
</tbody>
</table>
show pim rpf route-policy statistics

To display statistics for reverse-path forwarding (RPF) route policy invocations in Protocol Independent Multicast (PIM) routing tables, use the `show pim rpf route-policy statistics` command in EXEC mode.

```
show pim [vrf vrf-name] [ipv4] rpf route-policy statistics
```

**Syntax Description**
- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.

**Command Default**
IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

**Command Modes**
EXEC

**Command History**
- **Release** 3.7.2  This command was introduced.

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**
- `Task ID`  Operations
  - `multicast`  read

**Examples**
The following sample output from the `show pim rpf route-policy statistics` command displays statistics about route policy invocations in topology tables:

```
RP/0/RSP0/CPU0:router# show pim mt4-p201 rpf route-policy statistics

RPF route-policy statistics for VRF default:
  Route-policy name: mt4-p201
  Number of lookup requests 25
  Pass 25, Drop 0
  Default RPF Table selection 5, Specific RPF Table selection 20
```

This table describes the significant fields shown in the display.

**Table 43: show pim rpf route-policy statistics Field Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route-policy name</td>
<td>Name of a specific route policy.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Number of lookup requests</td>
<td>Number of times the route policy was run to determine the RPF table.</td>
</tr>
<tr>
<td>Pass</td>
<td>Number of (S,G) entries that were passed by the route policy.</td>
</tr>
<tr>
<td>Drop</td>
<td>Number of (S,G) entries that were dropped by the route policy.</td>
</tr>
<tr>
<td>Default RPF Table selection/Specific RPF Table selection</td>
<td>When an (S,G) entry is accepted by the route policy, it can either select the default RPF table (can be either the unicast default or multicast default table) or any specific named or default RPF table. The last line of output indicates the number of entries that fall into these two categories.</td>
</tr>
</tbody>
</table>
show pim rpf route-policy test

To test the outcome of a route-policy with reverse-path forwarding (RPF), use the `show pim rpf route-policy test` command in EXEC mode.

```
show pim [vrf vrf-name] [ipv4] rpf route-policy test src-ip-address/grp-address
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `src-ip-address/grp-address` Source or group address, or both, for the default or selected route policy, as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format `A.B.C.D`.

**Command Default**

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following sample output from the `show pim rpf route-policy test` command displays the RPF table selected by the route policy for a given source and/or group address:

```
RP/0/RSP0/CPU0:router# show pim ipv4 rpf route-policy test 10.11.11.11 225.2.0.1

RPF route-policy test for VRF default:
  Route-policy name: mt4-p2
  Source 10.11.11.11, Group 225.2.0.1
  Result: Pass
  Default RPF Table selected
  RPF Table: IPv4-Unicast-default (Created, Active)
```
This table describes the significant fields shown in the display.

Table 44: show pim rpf route-policy test Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route-policy name</td>
<td>Name of a specific route policy.</td>
</tr>
<tr>
<td>Source</td>
<td>Source IP name for the route policy.</td>
</tr>
<tr>
<td>Group</td>
<td>Group IP name for the route policy.</td>
</tr>
<tr>
<td>Result</td>
<td>Specifies whether the (S,G) entry was accepted by the route policy.</td>
</tr>
<tr>
<td>Default RPF Table</td>
<td>Specifies whether the (S,G) entry uses the default or a specific RPF table.</td>
</tr>
<tr>
<td>RPF Table</td>
<td>Specifies which RPF table was selected, and whether or not the table was created in PIM and is active.</td>
</tr>
</tbody>
</table>
show pim rpf summary

To display summary information about the interaction of Protocol Independent Multicast (PIM) with the Routing Information Base (RIB), including the convergence state, current default RPF table, and the number of source or rendezvous point registrations created, use the `show pim rpf summary` command in EXEC mode.

```
show pim [vrf vrf-name] [ipv4] [{multicast|safi-all|unicast}] [topology {table-name|all}] rpf summary
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `multicast` (Optional) Specifies a multicast secondary address family (SAFI).
- `safi-all` (Optional) Specifies a secondary address family (SAFI) wildcard.
- `unicast` (Optional) Specifies a unicast secondary address family (SAFI).
- `topology` (Optional) Specifies the display of multitopology routing table information.
- `table-name` Name of the specific multitopology table to show.
- `all` Specifies that detailed information be displayed for all multitopology routing tables in PIM.

**Command Default**

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

```
Task ID  Operations
multicast  read
```

**Examples**

The following sample output shows RPF information for multiple tables. The first part of the output example describes VRF-level information. The remainder consists of information specific to one or more tables.
RPF table indicates the table in which the RPF lookup was performed for this route entry.

RP/O/RSP0/CPU0:router# show pim ipv4 unicast topology all rpf summary

MBGP Not configured
    OSPF Mcast-intact Not configured
    ISIS Mcast-intact Not configured
    ISIS Mcast Topology Not configured

PIM RPFs registered with Unicast RIB table

Default RPF Table: IPv4-Unicast-default
    RIB Convergence Timeout Value: 00:30:00
    RIB Convergence Time Left: 00:00:00
    Multipath RPF Selection is Enabled

Table: IPv4-Multicast-default
    PIM RPF Registrations = 0
    RIB Table converged

Table: IPv4-Multicast-t300
    PIM RPF Registrations = 3
    RIB Table converged

Table: IPv4-Multicast-t310
    PIM RPF Registrations = 5
    RIB Table converged

Table: IPv4-Multicast-t320
    PIM RPF Registrations = 5
    RIB Table converged

The first part of the output example describes VRF-level information. The remainder consists of information specific to one or more tables.

The following example shows the sample output for `show pim rpf summary` command:

RP/O/RSP0/CPU0:router# show pim rpf summary

MBGP Not configured
    OSPF Mcast-intact Configured
    ISIS Mcast-intact Not configured
    ISIS Mcast Topology Not configured
    MoFRR Flow-based Configured
    MoFRR RIB Not configured

PIM RPFs registered with Multicast RIB table

Default RPF Table: IPv4-Multicast-default
    RIB Convergence Timeout Value: 00:30:00
    RIB Convergence Time Left: 00:00:00
    Multipath RPF Selection is Disabled

Table: IPv4-Multicast-default
    PIM RPF Registrations = 3
    RIB Table converged
show pim summary

To display configured Protocol Independent Multicast (PIM) out-of-resource (OOR) limits and current counts, use the `show pim summary` command in EXEC mode.

```
show pim [vrf vrf-name] [ipv4] summary
```

**Syntax Description**

<table>
<thead>
<tr>
<th>vrf vrf-name</th>
<th>(Optional) Specifies a VPN routing and forwarding (VRF) instance associated with this count.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IPv4 address prefixes.</td>
</tr>
</tbody>
</table>

**Command Default**

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

**Command Modes**

EXEC mode

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

The `show pim summary` command is used to identify configured OOR information for the PIM protocol, such as number of current and maximum routes.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>multicast</td>
</tr>
<tr>
<td></td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show pim summary` command that shows PIM routes, with the maximum number of routes allowed being 100000:

```
RP/0/RSP0/CPU0:router# show pim summary

PPIM Summary for VRF:default

PIM State Counters

<table>
<thead>
<tr>
<th>Type</th>
<th>Current</th>
<th>Maximum</th>
<th>Warning-threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routes</td>
<td>4</td>
<td>100000</td>
<td>100000</td>
</tr>
<tr>
<td>Topology Interface States</td>
<td>4</td>
<td>300000</td>
<td>300000</td>
</tr>
<tr>
<td>SM Registers</td>
<td>1</td>
<td>20000</td>
<td>20000</td>
</tr>
<tr>
<td>AutoRP Group Ranges</td>
<td>0</td>
<td>500</td>
<td>450</td>
</tr>
<tr>
<td>BSR Group Ranges</td>
<td>9</td>
<td>500</td>
<td>450</td>
</tr>
<tr>
<td>BSR C-RP caches</td>
<td>9</td>
<td>100</td>
<td>100</td>
</tr>
</tbody>
</table>
```
This table describes the significant fields shown in the display.

**Table 45: show pim summary Field Descriptions**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routes</td>
<td>Current number of routes (in the PIM topology table) and the maximum allowed before the creation of new routes is prohibited to avoid OOR conditions.</td>
</tr>
<tr>
<td>Routes x Interfaces</td>
<td>Current total number of interfaces (in the PIM topology table) present in all route entries and the maximum allowed before the creation of new routes is prohibited to avoid OOR conditions.</td>
</tr>
<tr>
<td>SM Registers</td>
<td>Current number of sparse mode route entries from which PIM register messages are received and the maximum allowed before the creation of new register states is prohibited to avoid OOR conditions.</td>
</tr>
<tr>
<td>AutoRP Group Ranges</td>
<td>Current number of sparse mode group range-to-rendezvous point mappings learned through the auto-rendezvous point (Auto-RP) mechanism and the maximum allowed before the creation of new group ranges is prohibited to avoid OOR conditions.</td>
</tr>
<tr>
<td>Warning-threshold</td>
<td>Maximum number of multicast routes that can be configured per router.</td>
</tr>
<tr>
<td>BSR Group Ranges</td>
<td>The number of BSR groups and the set range.</td>
</tr>
<tr>
<td>BSR C-RP caches</td>
<td>The number of candidate-RP caches in BSR and the set range.</td>
</tr>
</tbody>
</table>
show pim topology

To display Protocol Independent Multicast (PIM) routing topology table information for a specific group or all groups, use the `show pim topology` command in EXEC mode.

```
show pim [vrf vrf-name] [ipv4] topology [src-ip-address / grp-address]
```

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vrf vrf-name</code></td>
<td>(Optional) Specifies a VPN routing and forwarding (VRF) instance.</td>
</tr>
<tr>
<td><code>ipv4</code></td>
<td>(Optional) Specifies IPv4 address prefixes.</td>
</tr>
<tr>
<td><code>src-ip-address / grp-address</code></td>
<td>Source IP address or group IP address, as defined in the Domain Name System (DNS) hosts table or with the domain IPv4 host in the format A.B.C.D.</td>
</tr>
</tbody>
</table>

| Command Default | IPv4 addressing is the default. If no VRF is specified, the default VRF is operational. |
| Command Modes | EXEC |

| Command History | Release 3.7.2 This command was introduced. |

| Usage Guidelines | To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance. |
| Use the PIM routing topology table to display various entries for a given group, (*, G), (S, G), and (S, G) RPT, each with its own interface list. |
| PIM communicates the contents of these entries through the Multicast Routing Information Base (MRIB), which is an intermediary for communication between multicast routing protocols, such as PIM; local membership protocols, such as Internet Group Management Protocol (IGMP); and the multicast forwarding engine of the system. |
| The MRIB shows on which interface the data packet should be accepted and on which interfaces the data packet should be forwarded, for a given (S, G) entry. Additionally, the Multicast Forwarding Information Base (MFIB) table is used during forwarding to decide on per-packet forwarding actions. |
| When multicast-only fast reroute (MoFRR) feature is enabled, the `show pim topology` command shows the SGs that are configured for MoFRR. For information about the MoFRR primary and secondary paths, see the description of the command `show pim topology detail`, on page 496. |

| Note | For forwarding information, use the `show mfib route` and `show mrib route` commands. |
The following is sample output from the `show pim topology` command:

```
RP/0/RSP0/CPU0# show pim topology

IP PIM Multicast Topology Table
Entry state: 
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
RR - Register Received, SR - Sending Registers, E - MSDP External, EX - Extranet
DCC - Don't Check Connected,
ME - MDT Encap, MD - MDT Decap,
MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
II - Internal Interest, ID - Internal Dissinterest,
LH - Last Hop, AS - Assert, AB - Admin Boundary

(*,239.9.9.9) SPT SM Up: 00:00:13
JP: Join(never) RPF: Loopback1,11.0.0.1* Flags: KAT(00:03:16) RA RR
No interfaces in immediate olist

(*,239.9.9.9) SM Up: 4d14h RP: 11.0.0.1*
JP: Join(never) RPF: Decapstunnel0,11.0.0.1 Flags: LH
POS0/3/0/0 4d14h fwd LI II LH

(*,224.0.1.39) DM Up: 02:10:38 RP: 0.0.0.0
JP: Null(never) RPF: Null,0.0.0.0 Flags: DSS
POS0/2/0/0 02:10:38 off LI II LH

(*,224.0.1.40) DM Up: 03:54:23 RP: 0.0.0.0
JP: Null(never) RPF: Null,0.0.0.0 Flags: DSS
POS0/2/0/0 03:54:23 off LI II LH
POS0/2/0/2 03:54:14 off LI
POS0/4/0/0 03:53:37 off LI

(*,239.100.1.11) BD Up: 03:51:35 RP: 200.6.1.6
JP: Join(00:00:24) RPF: POS0/4/0/0,10.10.4.6 Flags:
POS0/2/0/0 03:42:05 fwd Join(00:03:18)
POS0/2/0/2 03:51:35 fwd Join(00:02:54)
POS0/2/0/2 03:51:39 RP: 200.6.2.6
JP: Join(00:00:50) RPF: POS0/4/0/0,10.10.4.6 Flags:
POS0/2/0/0 02:36:09 fwd Join(00:03:20)
POS0/2/0/2 03:42:04 fwd Join(00:03:16)

The following example shows output for a MoFRR convergence:

RP/0/RSP0/CPU0# show pim topology 239.1.1.1

IP PIM Multicast Topology Table
Entry state: 
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
MF - MoFRR Enabled, MFP - Primary MoFRR,
MFB - Backup MoFRR, MFA - Active MoFRR,
RR - Register Received, SR - Sending Registers, E - MSDP External,
```
DCC - Don't Check Connected,
ME - MDT Encap, MD - MDT Decap,
MT - Crossed Data MDT threshold, MA - Data MDT group assigned

Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
II - Internal Interest, ID - Internal Dissinterest,
LH - Last Hop, AS - Assert, AB - Admin Boundary

(192.1.1.2,239.1.1.1) SPT SSM Up: 13:54:06
JP: Join(00:00:41) RPF: GigabitEthernet0/5/0/3.3,100.100.0.10 MoFRR RIB, Flags:
GigabitEthernet0/5/0/1 13:54:06 fwd LI LH
RP/0/4/CP00:Sunnyvale#show pim topology 239.1.1.1 detail

IP PIM Multicast Topology Table
Entry state: (*,S,G) [RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
RR - Register Received, SR - Sending Registers, E - MSDP External,
DCC - Don't Check Connected,
ME - MDT Encap, MD - MDT Decap,
MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
II - Internal Interest, ID - Internal Dissinterest,
LH - Last Hop, AS - Assert, AB - Admin Boundary

(192.1.1.2,239.1.1.1) SPT SSM Up: 13:54:10
JP: Join(00:00:37) RPF: GigabitEthernet0/5/0/1 13:54:06 fwd LI LH
GigabitEthernet0/5/0/3.3 13:54:10 fwd LI LH

The following example shows a sample output for flow-based MoFRR:

RP/0/RSP0/CP00:router# show pim topology

IP PIM Multicast Topology Table
Entry state: (*,S,G) [RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
RA - Really Alive, IA - Inherit Alive, LH - Last Hop
DSS - Don't Signal Sources, RR - Register Received
SR - Sending Registers, E - MSDP External, EX - Extranet
DCC - Don't Check Connected, ME - MDT Encap, MD - MDT Decap
MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
II - Internal Interest, ID - Internal Dissinterest,
LH - Last Hop, AS - Assert, AB - Admin Boundary, EX - Extranet

(*,224.0.1.40) DM Up: 00:31:45 RP: 0.0.0.0
JP: Null(never) RPF: Null,0.0.0.0 Flags: LH DSS
GigabitEthernet0/0/0/8 00:31:45 off LI II LH

(20.20.20.1,225.0.0.1) SPT SM Up: 00:31:39
JP: Join(00:00:09) RPF: GigabitEthernet0/0/0/28,20.20.20.1 MoFRR, Flags:
GigabitEthernet0/0/0/28 00:31:39 fwd LI LH

(20.20.20.1,225.0.0.2) SPT SM Up: 00:31:39
JP: Join(00:00:09) RPF: GigabitEthernet0/0/0/28,20.20.20.1 MoFRR, Flags:
GigabitEthernet0/0/0/28 00:31:39 fwd LI LH

If the option detail is issued, then the secondary RPF of MoFRR route will be shown in the console.
show pim topology detail

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive
RA - Really Alive, IA - Inherit Alive, LH - Last Hop
DSS - Don’t Signal Sources, RR - Register Received
SR - Sending Registers, E - MSDP External, EX - Extranet
DCC - Don’t Check Connected, ME - MDT Encap, MD - MDT Decap
MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
II - Internal Interest, ID - Internal Dissinterest,
LH - Last Hop, AS - Assert, AB - Admin Boundary, EX - Extranet
(*,224.0.1.40) DM Up: 03:16:10 RP: 0.0.0.0
JP: Null(never) RPF: Null,0.0.0.0 Flags: LH DSS
RPF Table: None
   GigabitEthernet0/0/0/8 03:16:10 off LI II LH

(20.20.20.1,225.0.0.1) SPT SM Up: 03:16:04
JP: Join(00:00:45) RPF: GigabitEthernet0/0/0/8,20.20.20.1 MoFRR, Flags:
RPF Table: IPv4-Unicast-default
RPF Secondary: GigabitEthernet0/0/0/18,20.20.20.1
   GigabitEthernet0/0/0/28 03:16:04 fwd LI LH

(20.20.20.1,225.0.0.2) SPT SM Up: 03:16:04
JP: Join(00:00:45) RPF: GigabitEthernet0/0/0/8,20.20.20.1 MoFRR, Flags:
RPF Table: IPv4-Unicast-default
RPF Secondary: GigabitEthernet0/0/0/18,20.20.20.1
   GigabitEthernet0/0/0/28 03:16:04 fwd LI LH

This table describes the significant fields shown in the display. It includes fields that do not appear
in the example, but that may appear in your output.

Table 46: show pim topology Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(11.0.0.1,239.9.9.9)SPT</td>
<td>Entry state. Source address, group address, and tree flag (shortest path tree or rendezvous point tree) for the route entry. Note that the tree flag may be missing from the entry.</td>
</tr>
<tr>
<td>SM</td>
<td>Entry protocol. PIM protocol mode in which the entry operates: sparse mode (SM), source specific multicast (SSM), bidirectional (BD), or dense-mode (DM).</td>
</tr>
<tr>
<td>Up: 00:00:13</td>
<td>Entry uptime. Time (in hours, minutes, and seconds) this entry has existed in the topology table.</td>
</tr>
<tr>
<td>RP: 11.0.0.1*</td>
<td>Entry information. Additional information about the route entry. If route entry is a sparse mode or bidirectional PIM route, the RP address is given.</td>
</tr>
<tr>
<td>JP: Null(never)</td>
<td>Entry join/prune state. Indicates if and when a join or prune message is sent to the RPF neighbor for the route.</td>
</tr>
<tr>
<td>MoFRR RIB, Flags:</td>
<td>Indicates whether the (S,G) route is a RIB-based MoFRR route.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>MoFRR, Flags:</td>
<td>Indicates whether the (S,G) route is a flow-based MoFRR route. By default,</td>
</tr>
<tr>
<td></td>
<td>a flow-based MoFRR route will be a RIB-based MoFRR route but not in the</td>
</tr>
<tr>
<td></td>
<td>reverse way.</td>
</tr>
<tr>
<td>RPF Table</td>
<td>IPv4 Unicast default.</td>
</tr>
<tr>
<td>RPF Secondary</td>
<td>Secondary path interface</td>
</tr>
<tr>
<td>Entry Information Flags</td>
<td></td>
</tr>
<tr>
<td>KAT - Keep Alive Timer</td>
<td>The keepalive timer tracks whether traffic is flowing for the (S, G) route</td>
</tr>
<tr>
<td></td>
<td>on which it is set. A route does not time out while the KAT is running. The</td>
</tr>
<tr>
<td></td>
<td>KAT runs for 3.5 minutes, and the route goes into KAT probing mode for</td>
</tr>
<tr>
<td></td>
<td>as long as 65 seconds. The route is deleted if no traffic is seen during</td>
</tr>
<tr>
<td></td>
<td>the probing interval, and there is no longer any reason to keep the route—</td>
</tr>
<tr>
<td></td>
<td>for example, registers and (S, G) joins.</td>
</tr>
<tr>
<td>AA - Assume Alive</td>
<td>Flag that indicates that the route was alive, but recent confirmation of</td>
</tr>
<tr>
<td></td>
<td>traffic flow was not received.</td>
</tr>
<tr>
<td>PA - Probe Alive</td>
<td>Flag that indicates that the route is probing the data plane to determine</td>
</tr>
<tr>
<td></td>
<td>if traffic is still flowing for this route before it is timed out.</td>
</tr>
<tr>
<td>RA - Really Alive</td>
<td>Flag that indicates that the source is confirmed to be sending traffic for</td>
</tr>
<tr>
<td></td>
<td>the route.</td>
</tr>
<tr>
<td>LH - Last Hop</td>
<td>Flag that indicates that the entry is the last-hop router for the entry.</td>
</tr>
<tr>
<td></td>
<td>If (S, G) routes inherit the LH olist from an (*, G) route, the route entry</td>
</tr>
<tr>
<td></td>
<td>LH flag appears only on the (*, G) route.</td>
</tr>
<tr>
<td>IA - Inherit Alive</td>
<td>Flag that indicates a source VPN routing and forwarding (VRF) route with</td>
</tr>
<tr>
<td></td>
<td>the KAT active.</td>
</tr>
<tr>
<td>DSS - Don’t Signal Sources</td>
<td>Flag that may be set on the last-hop (*, G) entries that indicates that new</td>
</tr>
<tr>
<td></td>
<td>matching sources should not be signaled from the forwarding plane.</td>
</tr>
<tr>
<td>DCC - Don’t Check Connected</td>
<td>Flag that is set when the KAT probes, which indicates that the connected</td>
</tr>
<tr>
<td></td>
<td>check for new sources should be omitted in the forwarding plane.</td>
</tr>
<tr>
<td>RR - Register Received</td>
<td>Flag that indicates the RP has received and answered PIM register</td>
</tr>
<tr>
<td></td>
<td>messages for this (S, G) route.</td>
</tr>
<tr>
<td>SR - Sending Registers</td>
<td>Flag that indicates that the first-hop DR has begun sending registers for</td>
</tr>
<tr>
<td></td>
<td>this (S, G) route, but has not yet received a Register-Stop message.</td>
</tr>
<tr>
<td>E - MSDP External</td>
<td>Flag that is set on those entries that have sources, learned through</td>
</tr>
<tr>
<td></td>
<td>Multicast Source Discovery Protocol (MSDP), from another RP.</td>
</tr>
<tr>
<td>ME - MDT Encap</td>
<td>Flag that indicates a core encapsulation route for a multicast distribution</td>
</tr>
<tr>
<td></td>
<td>tree (MDT).</td>
</tr>
<tr>
<td>MD - MDT Decap</td>
<td>Flag that indicates a core decapsulation route for an MDT.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------</td>
<td>-------------</td>
</tr>
<tr>
<td>MT - Crossed Data MDT threshold</td>
<td>Flag that indicates that traffic on this route passed a threshold for the data MDT.</td>
</tr>
<tr>
<td>MA - Data MDT group assigned</td>
<td>Flag that indicates a core encapsulation route for the data MDT.</td>
</tr>
<tr>
<td>POS0/2/0/0 Interface name. Name of an interface in the interface list of the entry.</td>
<td>Time (in hours, minutes, and seconds) this interface has existed in the entry.</td>
</tr>
<tr>
<td>Interface forwarding status. Outgoing forwarding status of the interface for the entry is “fwd” or “off”.</td>
<td></td>
</tr>
</tbody>
</table>

**Interface Information Flags**

<table>
<thead>
<tr>
<th>Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LI - Local Interest</td>
<td>Flag that indicates that there are local receivers for this entry on this interface, as reported by Internet Group Management Protocol (IGMP).</td>
</tr>
<tr>
<td>LD - Local Disinterest</td>
<td>Flag that indicates that there is explicit disinterest for this entry on this interface, as reported by IGMP exclude mode reports.</td>
</tr>
<tr>
<td>Il - Internal Interest</td>
<td>Flag that indicates that the host stack of the router has internal receivers for this entry.</td>
</tr>
<tr>
<td>Id - Internal Disinterest</td>
<td>Flag that indicates that the host stack of the router has explicit internal disinterest for this entry.</td>
</tr>
<tr>
<td>LH - Last Hop</td>
<td>Flag that indicates that this interface has directly connected receivers and this router serves as a last hop for the entry. If the (S, G) outgoing interface list is inherited from a (<em>, G) route, the LH flag is set on the (</em>, G) outgoing LH interface.</td>
</tr>
<tr>
<td>AS - Assert</td>
<td>Flag that indicates that a PIM assert message was seen on this interface and the active PIM assert state exists.</td>
</tr>
<tr>
<td>AB - Administrative Boundary</td>
<td>Flag that indicates that forwarding on this interface is blocked by a configured administrative boundary for this entry’s group range.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mftb route</td>
<td>Displays all entries in the MFIB table.</td>
</tr>
</tbody>
</table>
show pim topology detail

To display detailed Protocol Independent Multicast (PIM) routing topology information that includes references to the tables in which reverse path forwarding (RPF) lookups occurred for specific topology route entries, use the `show pim topology detail` command in EXEC mode.

```
show pim [vrf vrf-name] [ipv4] topology detail
```

**Syntax Description**
- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.

**Command Default**
IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Release 3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the PIM topology table to display various entries for a given group, (*, G), (S, G), and (S, G)RPT, each with its own interface list.

PIM communicates the contents of these entries through the Multicast Routing Information Base (MRIB), which is an intermediary for communication between multicast routing protocols, such as PIM; local membership protocols, such as Internet Group Management Protocol (IGMP); and the multicast forwarding engine of the system.

The MRIB shows on which interface the data packet should be accepted and on which interfaces the data packet should be forwarded, for a given (S, G) entry. Additionally, the Multicast Forwarding Information Base (MFIB) table is used during forwarding to decide on per-packet forwarding actions.

When the multicast-only fast reroute (MoFRR) feature is enabled, the `show pim topology detail` command shows the primary and secondary paths for SGs configured for MoFRR.

**Note**
For forwarding information, use the `show mfib route` and `show mrib route` commands.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>
### Examples

The following is sample output from the `show pim topology detail` command, showing the RPF table information for each topology entry:

```
RP/0/RSP0/CPU0:router# show pim ipv4 topology detail

IP PIM Multicast Topology Table:
Entry state: (*,S,G) [RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
             RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
             RR - Register Received, SR - Sending Registers, E - MSDP External,
             DCC - Don't Check Connected,
             ME - MDT Encap, MD - MDT Decap,
             MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
                 II - Internal Interest, ID - Internal Dissinterest,
                 LH - Last Hop, AS - Assert, AB - Admin Boundary

(*,224.0.1.40) DM Up: 00:07:28 RP: 0.0.0.0
JP: Null(never) RPF: Null,0.0.0.0 Flags: LH DSS
RPF Table: None
GigabitEthernet0/1/0/1 00:07:28 off LI II LH
GigabitEthernet0/1/0/2 00:07:23 off LI LH
GigabitEthernet0/1/0/1.503 00:07:27 off LI LH

(11.11.11.1,232.5.0.2) SPT SSM Up: 00:07:21
JP: Join(now) RPF: GigabitEthernet0/1/0/1.203,11.23.0.20 Flags:
RPF Table: IPv4-Unicast-default
GigabitEthernet0/1/0/1.501 00:07:21 fwd LI LH

(61.61.0.10,232.5.0.3) SPT SSM Up: 00:11:57
JP: Join(now) RPF: Null,0.0.0.0 Flags:
RPF Table: None (Dropped due to route-policy)
No interfaces in immediate olist
```

The RPF table output in boldface indicates the table in which the RPF lookup occurred for this route entry.

### Note

The following example shows output for a MoFRR convergence:

```
RP/0/RSP0/CPU0:router# show pim topology 239.1.1.1 detail

IP PIM Multicast Topology Table:
Entry state: (*,S,G) [RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
             RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
             RR - Register Received, SR - Sending Registers, E - MSDP External,
             DCC - Don't Check Connected,
             ME - MDT Encap, MD - MDT Decap,
             MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
                 II - Internal Interest, ID - Internal Dissinterest,
                 LH - Last Hop, AS - Assert, AB - Admin Boundary

(192.1.1.2,239.1.1.1) SPT SSM Up: 13:54:06
JP: Join(00:00:41) RPF: GigabitEthernet0/5/0/3.3,100.100.0.10 MoFRR RIB, Flags:
```
GigabitEthernet0/5/0/1 13:54:06 fwd LI LH
RP/0/4/CPU0:Sunnyvale#show pim topology 239.1.1.1 detail

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
           RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
           RR - Register Received, SR - Sending Registers, E - MSDP External,
           DCC - Don't Check Connected,
           ME - MDT Encap, MD - MDT Decap,
           MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
                  II - Internal Interest, ID - Internal Dissinterest,
                  LH - Last Hop, AS - Assert, AB - Admin Boundary

(192.1.1.2,239.1.1.1) SPT SSM Up: 13:54:10
JP: Join(00:00:37) RPF: GigabitEthernet0/5/0/3.3,100.100.0.10 MoFRR RIB, Flags:
RPF Table: IPv4-Unicast-default
RPF Secondary: GigabitEthernet0/5/0/3.2,100.100.200.10
GigabitEthernet0/5/0/1 13:54:10 fwd LI LH

Table 46: show pim topology Field Descriptions, on page 493 describes the significant fields shown in the display, including those related to multicast-only fast reroute (MoFRR). This table includes fields that do not appear in the example, but that may appear in your output.

<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>show mfib route</td>
<td>Displays all entries in the MFIB table.</td>
</tr>
<tr>
<td></td>
<td>show mrib route</td>
<td>Displays all entries in the MRIB table.</td>
</tr>
</tbody>
</table>
show pim topology entry-flag

To display Protocol Independent Multicast (PIM) routing topology information for a specific entry flag, use the show pim topology entry-flag command in EXEC mode.

```
show pim [vrf vrf-name] [ipv4] topology entry-flag flag [{detail|route-count}]
```

**Syntax Description**

- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `flag` Configures a display of routes with the specified entry flag. Valid flags are the following:
  - AA — Assume alive
  - DCC — Don’t check connected
  - DSS — Don’t signal sources
  - E — MSDP External
  - EX — Extranet flag set
  - IA — Inherit except flag set
  - KAT — Keepalive timer
  - LH — Last hop
  - PA — Probe alive
  - RA — Really alive
  - RR — Registered receiver
  - SR — Sending registers
- `detail` (Optional) Specifies details about the entry flag information.
- `route-count` (Optional) Displays the number of routes in the PIM topology table.

**Command Default**

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the PIM topology table to display various entries for a given group, (*, G), (S, G), and (S, G)RPT, each with its own interface list.
PIM communicates the contents of these entries through the Multicast Routing Information Base (MRIB), which is an intermediary for communication between multicast routing protocols, such as PIM; local membership protocols, such as Internet Group Management Protocol (IGMP); and the multicast forwarding engine of the system.

The MRIB shows on which interface the data packet should be accepted and on which interfaces the data packet should be forwarded, for a given (S, G) entry. Additionally, the Multicast Forwarding Information Base (MFIB) table is used during forwarding to decide on per-packet forwarding actions.

For forwarding information, use the `show mfib route` and `show mrib route` commands.

Table 46: show pim topology Field Descriptions, on page 493 describes the significant fields shown in the display. This table includes fields that do not appear in the example, but that may appear in your output.
<table>
<thead>
<tr>
<th>Related Commands</th>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><code>show mrib route</code></td>
<td>Displays all entries in the MRIB table.</td>
</tr>
</tbody>
</table>
show pim topology interface-flag

To display Protocol Independent Multicast (PIM) routing topology information for a specific interface, use the `show pim topology` command in EXEC mode.

```
show pim [vrf vrf-name] [ipv4] topology interface-flag flag [{detail|route-count}]
```

**Syntax Description**
- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `flag` Configures a display of routes with the specified interface flag. Valid flags are the following:
  - `detail` (Optional) Displays details about the interface flag information.
  - `route-count` (Optional) Displays the number of routes in the PIM topology table.

**Command Default**
IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

**Command Modes**
EXEC

**Command History**
Release 3.7.2  This command was introduced.

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the PIM topology table to display various entries for a given group, (*, G), (S, G), and (S, G)RPT, each with its own interface list.

PIM communicates the contents of these entries through the Multicast Routing Information Base (MRIB), which is an intermediary for communication between multicast routing protocols, such as PIM; local membership protocols, such as Internet Group Management Protocol (IGMP); and the multicast forwarding engine of the system.

The MRIB shows on which interface the data packet should be accepted and on which interfaces the data packet should be forwarded, for a given (S, G) entry. Additionally, the Multicast Forwarding Information Base (MFIB) table is used during forwarding to decide on per-packet forwarding actions.

**Note**
For forwarding information, use the `show mfib route` and `show mrib route` commands.
## Examples

The following is sample output from the `show pim topology interface-flag` command:

```
RP/0/RSP0/CPU0:router# show pim topology interface-flag LI

IP PIM Multicast Topology Table
Entry state: (*/S,G) [RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive
  RA - Really Alive, IA - Inherit Alive, LH - Last Hop
  DSS - Don't Signal Sources, RR - Register Received
  SR - Sending Registers, E - MSDP External, EX - Extranet
  DCC - Don't Check Connected, ME - MDT Encap, MD - MDT Decap
  MT - Crossed Data MDT threshold, MA - Data MDT group assigned
Interface state: Name, Uptime, Fwd, Info
Interface flags: LI - Local Interest, LD - Local Dissinterest,
  II - Internal Interest, ID - Internal Dissinterest,
  LH - Last Hop, AS - Assert, AB - Admin Boundary, EX - Extranet

(*,224.0.1.39) DM Up: 00:27:27 RP: 0.0.0.0
JP: Null(never) RPF: Null,0.0.0.0 Flags: LH DSS
Loopback5 00:27:27 off LI II LH

(*,224.0.1.40) DM Up: 00:27:27 RP: 0.0.0.0
JP: Null(never) RPF: Null,0.0.0.0 Flags: LH DSS
Loopback5 00:27:26 off LI II LH
  GigabitEthernet0/2/0/2 00:27:27 off LI LH

(*,226.0.0.0) SM Up: 00:27:27 RP: 97.97.97.97*
JP: Join(never) RPF: Decapstunnel0,97.97.97.97 Flags: LH
Loopback5 00:27:27 fwd LI LH

(*,226.0.0.1) SM Up: 00:27:27 RP: 97.97.97.97*
JP: Join(never) RPF: Decapstunnel0,97.97.97.97 Flags: LH
Loopback5 00:27:27 fwd LI LH

(*,226.0.0.3) SM Up: 00:27:27 RP: 97.97.97.97*
JP: Join(never) RPF: Decapstunnel0,97.97.97.97 Flags: LH
Loopback5 00:27:27 fwd LI LH

(*,226.0.0.4) SM Up: 00:27:27 RP: 97.97.97.97*
JP: Join(never) RPF: Decapstunnel0,97.97.97.97 Flags: LH
Loopback5 00:27:27 fwd LI LH

(*,226.0.0.5) SM Up: 00:27:27 RP: 97.97.97.97*
JP: Join(never) RPF: Decapstunnel0,97.97.97.97 Flags: LH
Loopback5 00:27:27 fwd LI LH

(201.5.5.201,226.1.0.0)SPT SM Up: 00:27:27
JP: Join(never) RPF: Loopback5,201.5.5.201* Flags: KAT(00:00:34) RA RR (00:03:53)
  GigabitEthernet0/2/0/2 00:26:51 fwd Join(00:03:14)
Loopback5 00:27:27 fwd LI LH

(204.5.5.204,226.1.0.0)SPT SM Up: 00:27:27
JP: Join(now) RPF: GigabitEthernet0/2/0/2,44.44.44.103 Flags: E
  Loopback5 00:27:27 fwd LI LH
```
Table 46: show pim topology Field Descriptions, on page 493 describes the significant fields shown in the display. This table includes fields that do not appear in the example, but that may appear in your output.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show mrrib route</td>
<td>Displays all entries in the MRIB table.</td>
</tr>
</tbody>
</table>
show pim topology summary

To display summary information about the Protocol Independent Multicast (PIM) routing topology table, use the **show pim topology summary** command in EXEC mode.

```
show pim [vrf vrf-name] [ipv4] topology summary [detail]
```

**Syntax Description**
- `vrf vrf-name` (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `detail` (Optional) Displays details about the summary information.

**Command Default**
IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

**Command Modes**
EXEC

**Command History**
- **Release 3.7.2** This command was introduced.

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

Use the PIM topology table to display various entries for a given group, (*, G), (S, G), and (S, G)RPT, each with its own interface list.

PIM communicates the contents of these entries through the Multicast Routing Information Base (MRIB), which is an intermediary for communication between multicast routing protocols, such as PIM; local membership protocols, such as Internet Group Management Protocol (IGMP); and the multicast forwarding engine of the system.

The MRIB shows on which interface the data packet should be accepted and on which interfaces the data packet should be forwarded, for a given (S, G) entry. Additionally, the Multicast Forwarding Information Base (MFIB) table is used during forwarding to decide on per-packet forwarding actions.

**Note**
For forwarding information, use the **show mfib route** and **show mrib route** commands.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>
Examples

The following example represents sample output from the `show pim topology summary` command:

```
RP/0/RSP0/CPU0:router# show pim vrf svpn12 topology summary
Mon Feb  2 04:07:01.249 UTC
PIM TT Summary for VRF svpn12
   No. of group ranges = 9
   No. of (*,G) routes = 8
   No. of (S,G) routes = 2
   No. of (S,G)RPT routes = 0

OSPF Mcast-intact    Not configured
ISIS Mcast-intact    Not configured
ISIS Mcast Topology Not configured

Default RPF Table: IPv4-Unicast-default
RIB Convergence Timeout Value: 00:30:00
RIB Convergence Time Left:   00:28:32
Multipath RPF Selection is Enabled

Table: IPv4-Unicast-default
   PIM RPF Registrations = 13
   RIB Table converged

Table: IPv4-Multicast-default
   PIM RPF Registrations = 0
   RIB Table converged

For an example of detailed PIM topology output, see `show pim topology detail`, on page 496.
show pim traffic

To display Protocol Independent Multicast (PIM) traffic counter information, use the show pim traffic command in EXEC mode.

```
show pim [vrf vrf-name] [ipv4] traffic
```

**Syntax Description**

- **vrf vrf-name** (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- **ipv4** (Optional) Specifies IPv4 address prefixes.

**Command Default**

IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the show pim traffic command that displays a row for valid PIM packets, number of hello packets, and so on:

```
RP/0/RSP0/CPU0:router# show pim traffic

PIM Traffic Counters
Elapsed time since counters cleared: 1d01h

<table>
<thead>
<tr>
<th>Received</th>
<th>Sent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid PIM Packets</td>
<td>15759217</td>
</tr>
<tr>
<td>Hello</td>
<td>9207</td>
</tr>
<tr>
<td>Join-Prune</td>
<td>1076805</td>
</tr>
<tr>
<td>Data Register</td>
<td>14673205</td>
</tr>
<tr>
<td>Null Register</td>
<td>73205</td>
</tr>
<tr>
<td>Register Stop</td>
<td>0</td>
</tr>
<tr>
<td>Assert</td>
<td>0</td>
</tr>
<tr>
<td>Batched Assert</td>
<td>0</td>
</tr>
<tr>
<td>BSR Message</td>
<td>0</td>
</tr>
<tr>
<td>Candidate-RP Adv.</td>
<td>0</td>
</tr>
<tr>
<td>Join groups sent</td>
<td>0</td>
</tr>
<tr>
<td>Prune groups sent</td>
<td>0</td>
</tr>
</tbody>
</table>
```
This table describes the significant fields shown in the display.

### Table 47: show pim traffic Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elapsed time since counters cleared</td>
<td>Time (in days and hours) that had elapsed since the counters were cleared with the <code>clear pim counters</code> command.</td>
</tr>
<tr>
<td>Valid PIM Packets</td>
<td>Total PIM packets that were received and sent.</td>
</tr>
<tr>
<td>HelloJoin-PruneRegisterRegister StopAssert Bidir DF Election</td>
<td>Specific type of PIM packets that were received and sent.</td>
</tr>
<tr>
<td>Malformed Packets</td>
<td>Invalid packets due to format errors that were received and sent.</td>
</tr>
<tr>
<td>Bad Checksums</td>
<td>Packets received or sent due to invalid checksums.</td>
</tr>
<tr>
<td>Socket Errors</td>
<td>Packets received or sent due to errors from the router’s IP host stack sockets.</td>
</tr>
<tr>
<td>Packets dropped due to invalid socket</td>
<td>Packets received or sent due to invalid sockets in the router’s IP host stack.</td>
</tr>
<tr>
<td>Packets which couldn’t be accessed</td>
<td>Packets received or sent due to errors when accessing packet memory.</td>
</tr>
<tr>
<td>Packets sent on Loopback Errors</td>
<td>Packets received or sent due to use of loopback interfaces.</td>
</tr>
<tr>
<td>Packets received on PIM-disabled Interface</td>
<td>Packets received or sent due to use of interfaces not enabled for PIM.</td>
</tr>
<tr>
<td>Packets received with Unknown PIM Version</td>
<td>Packets received or sent due to invalid PIM version numbers in the packet header.</td>
</tr>
</tbody>
</table>

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear pim counters, on page 412</td>
<td>Clears Protocol Independent Multicast (PIM) counters and statistics.</td>
</tr>
</tbody>
</table>
show pim tunnel info

To display information for the Protocol Independent Multicast (PIM) tunnel interface, use the `show pim tunnel info` command in EXEC mode.

```
show pim [vrf vrf-name] [ipv4] tunnel info {interface-unit|all} [netio]
```

**Syntax Description**

- **vrf vrf-name** (Optional) Specifies a VPN routing and forwarding (VRF) instance.
- **ipv4** (Optional) Specifies IPv4 address prefixes.
- **interface-unit** Name of virtual tunnel interface that represents the encapsulation tunnel or the decapsulation tunnel.
- **all** Specifies both encapsulation and decapsulation tunnel interfaces.
- **netio** (Optional) Displays information obtained from the Netio DLL.

**Command Default**
IPv4 addressing is the default. If no VRF is specified, the default VRF is operational.

**Command Modes**
EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

PIM register packets are sent through the virtual encapsulation tunnel interface from the source’s first-hop designated router (DR) router to the rendezvous point (RP). On the RP, a virtual decapsulation tunnel is used to represent the receiving interface of the PIM register packets. This command displays tunnel information for both types of interfaces.

Register tunnels are the encapsulated (in PIM register messages) multicast packets from a source that is sent to the RP for distribution through the shared tree. Registering applies only to sparse mode (SM), not to Source Specific Multicast (SSM).

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the `show pim tunnel info` command:
show pim tunnel info

RP/0/RSP0/CPU0:router# show pim tunnel info all

<table>
<thead>
<tr>
<th>Interface</th>
<th>RP Address</th>
<th>Source Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encapstunnel0</td>
<td>10.1.1.1</td>
<td>10.1.1.1</td>
</tr>
<tr>
<td>Decapstunnel0</td>
<td>10.1.1.1</td>
<td></td>
</tr>
</tbody>
</table>

This table describes the significant fields shown in the display.

Table 48: show pim tunnel info Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Name of the tunnel interface.</td>
</tr>
<tr>
<td>RP Address</td>
<td>IP address of the RP tunnel endpoint.</td>
</tr>
<tr>
<td>Source Address</td>
<td>IP address of the first-hop DR tunnel endpoint, applicable only to encapsulation interfaces.</td>
</tr>
</tbody>
</table>
spt-threshold infinity

To change the behavior of the last-hop router to always use the shared tree and never perform a shortest-path tree (SPT) switchover, use the `spt-threshold infinity` command in PIM configuration mode. To return to the default behavior, use the `no` form of this command.

```
spt-threshold infinity [group-list access-list]
no spt-threshold infinity
```

**Syntax Description**

- `group-list access-list` (Optional) Indicates the groups restricted by the access list.

**Command Default**

The last-hop Protocol Independent Multicast (PIM) router switches to the shortest-path source tree by default.

**Command Modes**

PIM configuration

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `spt-threshold infinity` command causes the last-hop PIM router to always use the shared tree instead of switching to the shortest-path source tree.

If the `group-list` keyword is not used, this command applies to all multicast groups.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

**Examples**

The following example shows how to configure the PIM source group grp1 to always use the shared tree:

```
RP/0/RSP0/CPU0:router(config)# router pim
RP/0/RSP0/CPU0:router(config-pim-default-ipv4)# spt-threshold infinity group-list grp1
```
To define the Protocol Independent Multicast (PIM)-Source Specific Multicast (SSM) range of IP multicast addresses, use the `ssm` command in the appropriate configuration mode. To return to the default behavior, use the `no` form of this command.

```
ssm [allow-override|disable|range access-list]
no ssm [allow-override|disable|range]
```

**Syntax Description**
- `allow-override` (Optional) Allows SSM ranges to be overridden by more specific ranges.
- `disable` (Optional) Disables SSM group ranges.
- `range access-list` (Optional) Specifies an access list describing group ranges for this router when operating in PIM SSM mode.

**Command Default**
Interface operates in PIM sparse mode (PIM-SM). IPv4 addressing is the default.

**Command Modes**
Multicast routing configuration
Multicast routing address-family configuration
Multicast VPN configuration

**Command History**
- **Release 3.7.2** This command was introduced.

**Usage Guidelines**
To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `ssm` command performs source filtering, which is the ability of a router to report interest in receiving packets from specific source addresses (or from all but the specific source addresses) to an IP multicast address. Unlike PIM-sparse mode (SM) that uses a rendezvous point (RP) and shared trees, PIM-SSM uses information on source addresses for a multicast group provided by receivers through the local membership protocol Internet Group Management Protocol (IGMP) and is used to directly build source-specific trees.

IGMP Version 3 must be enabled on routers that want to control the sources they receive through the network.

When multicast routing is enabled, the default is PIM-SSM enabled on the default SSM range, 232/8. SSM may be disabled with the `disable` form of the command, or any ranges may be specified in an access list with the `range` form. All forms of this command are mutually exclusive. If an access list is specified, the default SSM range is not used unless specified in the access list.

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>
The following example shows how to configure SSM service for the IP address range defined by access list 4, using the `ssm` command:

```
RP/0/RSP0/CPU0:router(config)# ipv4 access-list 4
RP/0/RSP0/CPU0:router(config-ipv4-acl)# permit ipv4 any 224.2.151.141
RP/0/RSP0/CPU0:router(config)# multicast-routing
RP/0/RSP0/CPU0:router(config-mcast)# ssm range 4
```
Multicast PIM Commands

ssm
Multicast Tool and Utility Commands

This chapter describes the commands used to troubleshoot multicast routing sessions on Cisco IOS XR Software.

For detailed information about multicast routing concepts, configuration tasks, and examples, refer to the *Implementing Multicast Routing on* configuration module in.

- mrinfo, on page 516
- mtrace, on page 518
- sap cache-timeout, on page 520
- sap listen, on page 521
- show sap, on page 522
mrinfo

To query neighboring multicast routers peering with the local router, use the mrinfo command in EXEC mode.

```mrinfo [ipv4] host-address [source-address]```

**Syntax Description**

- **ipv4** (Optional) Specifies IPv4 address prefixes.
- **host-address** Can be either the Domain Name System (DNS) name or IP address of a multicast router entered in **A.B.C.D** format.
  - **Note** If omitted, the router queries itself.
- **source-address** (Optional) Source address used on multicast routing information (mrinfo) requests. If omitted, the source is based on the outbound interface for the destination.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The mrinfo command determines which neighboring multicast routers are peering with a multicast router. You can query a multicast router with this command. The output format is identical to the multicast routed version of Distance Vector Multicast Routing Protocol (DVMRP). (The mrouted software is the UNIX software that implements DVMRP.)

**Task ID**

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>execute</td>
</tr>
</tbody>
</table>

**Examples**

The following is sample output from the mrinfo command. The first line shows the multicast configuration with version number and flags Parent Multicast Agent (PMA). The flags mean that the configuration is prune capable, mtrace capable, and SNMP capable. For each neighbor of the queried multicast router, the IP address of the queried router is displayed, followed by the IP address of the neighbor. The metric (cost of connect) and the threshold (multicast time to live) are displayed. Other information is available, such as whether this router is
  - Running the PIM protocol
  - An IGMP querier
  - A leaf router
RP/0/RSP0/CP0:router# mrinfo 192.168.50.1

192.168.50.1 (version 0.37.0) [flags: PMA]:
172.16.1.1 -> 172.16.1.1 [1/0/pim/querier/leaf]
172.16.2.2 -> 172.16.2.2 [1/0/pim/querier/leaf]
192.168.50.1 -> 192.168.50.1 [1/0/pim/querier]
192.168.50.1 -> 192.168.50.101 [1/0/pim/querier]
192.168.40.101 -> 192.168.40.1 [1/0/pim]
mtrace

To trace the path from a source to a destination branch for a multicast distribution tree, use the mtrace command in EXEC mode.

mtrace [ipv4] [vrf] source destination [group_addr] [resp_addr][ttl]

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipv4</td>
<td>(Optional) Specifies IPv4 address prefixes.</td>
</tr>
<tr>
<td>vrf</td>
<td>(Optional) Specifies the vrf table for the route lookup.</td>
</tr>
<tr>
<td>source</td>
<td>Domain Name System (DNS) name or the IP address of the multicast-capable source. This is a unicast address of the beginning of the path to be traced.</td>
</tr>
<tr>
<td>destination</td>
<td>DNS name or address of the unicast destination. This is a unicast address of the end of the path to be traced.</td>
</tr>
<tr>
<td>group_addr</td>
<td>(Optional) DNS name or multicast address of the group to be traced. Default address is 224.2.0.1 (the group used for MBONE Audio). When address 0.0.0.0 is used, the software invokes a weak mtrace. A weak mtrace is one that follows the Reverse Path Forwarding (RPF) path to the source, regardless of whether any router along the path has multicast routing table state.</td>
</tr>
<tr>
<td>resp_addr</td>
<td>(Optional) DNS name or multicast address of the querier address to receive response. If the querier is not reachable by the RP or the source, this value should be provided.</td>
</tr>
<tr>
<td>ttl</td>
<td>(Optional) Time-to-live (TTL) threshold for a multicast trace request. Range is 1 to 255 router hops.</td>
</tr>
</tbody>
</table>

Command Default

By default, this feature is disabled. IPv4 addressing is the default.

Command Modes

EXEC

Command History

Release 3.7.2 This command was introduced.

Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The trace request generated by the mtrace command is multicast to the multicast group to find the last-hop router to the specified destination. The trace follows the multicast path from destination to source by passing the mtrace request packet using unicast to each hop. Responses are unicast to the querying router by the first-hop router to the source. This command allows you to isolate multicast routing failures.

If no arguments are entered, the router interactively prompts you for them.

This command is identical in function to the UNIX version of mtrace.
Examples

The following is sample output from the mtrace command:

```
RP/0/RSP0/CPU0:router# mtrace 172.16.1.0 172.16.1.10 239.254.254.254
Type escape sequence to abort.
Mtrace from 172.16.1.0 to 172.16.1.10 via group 239.254.254.254
From source (?) to destination (?)
Querying full reverse path...

Switching to hop-by-hop:
  0  172.16.1.10
-1  172.17.20.101 PIM Reached RP/Core [172.16.1.0/24]
-2  172.18.10.1 PIM [172.16.1.0/32]
-3  172.16.1.0 PIM [172.16.1.0/32]

RP/0/RSP0/CPU0:router# mtrace vrf vrf1 172.16.1.0 172.16.1.10 239.254.254.254 45.244.244.244
```

Cisco ASR 9000 Series Aggregation Services Router Multicast Command Reference, Release 5.3.x
sap cache-timeout

To limit how long a Session Announcement Protocol (SAP) cache entry stays active in the cache, use the sap cache-timeout command in global configuration mode. To return to the default behavior, use the no form of this command.

```
sap cache-timeout minutes
no sap cache-timeout
```

**Syntax Description**

```
minutes  Time that a SAP cache entry is active in the cache. Range is 1 to 1440.
```

**Command Default**

```
minutes : 1440 (24 hours)
```

**Command Modes**

Global configuration

**Command History**

```
Release   Modification
-----   ------------------
Release 3.7.2  This command was introduced.
```

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The sap cache-timeout command defines how long session announcements are cached by the router. Active session announcements are periodically re-sent by the originating site, refreshing the cached state in the router. The minimum interval between announcements for a single group is 5 minutes. Setting the cache timeout to a value less than 30 minutes is not recommended. Set the cache timeout to 0 to keep entries in the cache indefinitely.

**Task ID**

```
<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>
```

**Examples**

The following example shows the SAP cache entry timeout being configured at 10 minutes:

```
RP/0/RSP0/CPU0:router(config)# sap cache-timeout 10
```
**sap listen**

To configure the Session Announcement Protocol (SAP) designated router (SDR) listener on a group address, use the `sap listen` command in global configuration mode. To return to the default behavior, use the `no` form of this command.

```
sap listen [{ip-addressname}]
```

### Syntax Description

- `ip-address` (Optional) Group IP address for an address range.
- `name` (Optional) Name of a prefix for an address range.

### Command Default

When no group address is configured, the SDR listener is configured on the global SAP announcement group (224.2.127.254).

### Command Modes

Global configuration

### Command History

<table>
<thead>
<tr>
<th>Release</th>
<th>Modification</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.7.2</td>
<td>This command was introduced.</td>
</tr>
</tbody>
</table>

### Usage Guidelines

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The `sap listen` command configures an SDR listener that listens to SAP announcements on the configured group address. The group IP address can be any group in the range from 224.2.128.0 to 224.2.255.255.

### Task ID

<table>
<thead>
<tr>
<th>Task ID</th>
<th>Operations</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>read, write</td>
</tr>
</tbody>
</table>

### Examples

The following example configures an SDR listener for group on IP address 224.2.127.254:

```
RP/0/RSP0/CPU0:router(config)# sap listen 224.2.127.254
```

### Related Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>show sap, on page 522</td>
<td>Displays the SAP sessions learned on the configured multicast groups.</td>
</tr>
</tbody>
</table>
show sap

To display the Session Announcement Protocol (SAP) sessions learned on the configured multicast groups, use the show sap command in EXEC mode.

```
show sap [ipv4] [group-address session-name] [detail]
```

**Syntax Description**

- `ipv4` (Optional) Specifies IPv4 address prefixes.
- `group-address` (Optional) Group IP address or name of the session that is learned.
- `session-name` (Optional) Session name.
- `detail` (Optional) Provides more SAP information.

**Command Default**

IPv4 addressing is the default.

**Command Modes**

EXEC

**Command History**

Release 3.7.2 This command was introduced.

**Usage Guidelines**

To use this command, you must be in a user group associated with a task group that includes appropriate task IDs. If the user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

The show sap command displays the sessions learned on the configured multicast groups. The detail keyword displays verbose session information.

Use the sap listen command to configure the SDR listener on a group IP address.

**Examples**

The following is sample output from the show sap command. Information is summarized and shows one entry.

```
RP/0/RSP0/CPU0:router# show sap

Sap Session Table Summary
Cisco Systems, Inc
Src: 192.168.30.101, Dst: 224.2.127.254, Last Heard: 00:00:23
Total Entries : 1
```
This table describes the significant fields shown in the display.

### Table 49: show sap Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Src</td>
<td>IP address of the host from which this session announcement was received.</td>
</tr>
<tr>
<td>Dst</td>
<td>Destination IP multicast group address where the announcement was sent.</td>
</tr>
<tr>
<td>Last Heard</td>
<td>Time (in hours, minutes, and seconds) when SAP announcements were last heard from the source.</td>
</tr>
<tr>
<td>Total Entries</td>
<td>Total number of entries displayed.</td>
</tr>
</tbody>
</table>

The following is sample output from the `show sap` command with the **detail** keyword specified for the SAP session, Cisco Systems, Inc.

```
RP/0/RSP0/CPU0:router# show sap detail
Sap Session Table
Session Name: Cisco Systems, Inc
Description: IPTV Streaming Video
Group: 225.225.225.1 TTL: 2
Announcement source: 192.30.30.101, Destination: 224.2.127.254
Created by: - 0050c200aabb 9 IN IP4 10.10.176.50
Session Permanent Attribute: packetsize:4416
Attribute: packetformat:RAW
Attribute: mux:m1s
Attribute: keywds:
Attribute: author:Cisco Systems, Inc
Attribute: copyright:Cisco Systems, Inc
Media : video, Transport Protocol : udp, Port : 444
Total Entries : 1
```

This table describes the significant fields shown in the display.

### Table 50: show sap detail Field Descriptions

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Name</td>
<td>Descriptive name of the SAP session.</td>
</tr>
<tr>
<td>Description</td>
<td>An expanded description of the session.</td>
</tr>
<tr>
<td>Group</td>
<td>IP multicast group addresses used for this session.</td>
</tr>
<tr>
<td>Announcement source</td>
<td>IP address of the host from which this session announcement was received.</td>
</tr>
<tr>
<td>Destination</td>
<td>Destination IP multicast group address that the announcement was sent to.</td>
</tr>
<tr>
<td>Created by</td>
<td>Information for identifying and tracking the session announcement.</td>
</tr>
<tr>
<td>Attribute</td>
<td>Indicates attributes specific to the session.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Media</td>
<td>Indicates the media type (audio, video, or data), transport port that the media stream is sent to, transport protocol used for these media (common values are User Datagram Protocol [UDP] and Real-Time Transport Protocol [RTP]/AVP), and list of media formats that each media instance can use. The first media format is the default format. Format identifiers are specific to the transport protocol used.</td>
</tr>
</tbody>
</table>

**Related Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sap listen, on page 521</td>
<td>Configures the SDR listener on a group IP address.</td>
</tr>
</tbody>
</table>