Cisco IOS IP Multicast Command Reference

December 2010

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

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

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

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

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

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

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at 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. (1005R)

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

Cisco IOS IP Multicast Command Reference
© 2007–2010 Cisco Systems, Inc. All rights reserved.

CONTENTS

IP Multicast Commands IMC-1

beacon (multicast routing monitor) IMC-2

class-map type multicast-flows IMC-4

clear ip cgmp IMC-6

clear ip dvmrp route IMC-7

clear ip igmp group IMC-8

clear ip igmp snooping filter statistics IMC-10

clear ip igmp snooping statistics IMC-11

clear ip mfib counters IMC-12

clear ip mrm status-report IMC-14

clear ip mroute IMC-15

clear ip msdp peer IMC-17

clear ip msdp sa-cache IMC-18

clear ip msdp statistics IMC-20

clear ip multicast limit IMC-21

clear ip multicast redundancy statistics IMC-22

clear ip pgm host IMC-23

clear ip pgm router IMC-24

clear ip pim auto-rp IMC-25

clear ip pim interface count IMC-26

clear ip pim rp-mapping IMC-27

clear ip pim snooping statistics IMC-28

clear ip pim snooping vlan IMC-29

clear ip rtp header-compression IMC-31

clear ip sap IMC-32

clear ip sdr IMC-33

clear mls ip multicast bidir-rpcache IMC-34

clear mls ip multicast group IMC-35

clear mls ip multicast statistics IMC-36

clear router-guard ip multicast statistics IMC-37

group (multicast-flows) IMC-38
ip cgmp IMC-40
ip domain multicast IMC-42
ip dvmrp accept-filter IMC-43
ip dvmrp auto-summary IMC-45
ip dvmrp default-information IMC-47
ip dvmrp interoperability IMC-49
ip dvmrp metric IMC-50
ip dvmrp metric-offset IMC-52
ip dvmrp output-report-delay IMC-53
ip dvmrp reject-non-pruners IMC-55
ip dvmrp routehog-notification IMC-57
ip dvmrp route-limit IMC-59
ip dvmrp summary-address IMC-61
ip dvmrp unicast-routing IMC-63
ip igmp access-group IMC-65
ip igmp explicit-tracking IMC-68
ip igmp helper-address IMC-70
ip igmp helper-address (UDL) IMC-72
ip igmp immediate-leave IMC-74
ip igmp immediate-leave group-list IMC-76
ip igmp join-group IMC-77
ip igmp last-member-query-count IMC-79
ip igmp last-member-query-interval IMC-81
ip igmp limit (global) IMC-83
ip igmp limit (interface) IMC-85
ip igmp mroute-proxy IMC-88
ip igmp proxy-service IMC-90
ip igmp querier-timeout IMC-92
ip igmp query-interval IMC-95
ip igmp query-max-response-time IMC-98
ip igmp snooping IMC-99
ip igmp snooping access-group IMC-101
ip igmp snooping explicit-tracking IMC-103
ip igmp snooping fast-leave IMC-105

ip igmp snooping flooding **IMC-107**
ip igmp snooping l2-entry-limit **IMC-108**
ip igmp snooping last-member-query-interval **IMC-109**
ip igmp snooping limit **IMC-111**
ip igmp snooping limit track **IMC-113**
ip igmp snooping minimum-version **IMC-114**
ip igmp snooping mrouter **IMC-115**
ip igmp snooping querier **IMC-117**
ip igmp snooping rate **IMC-119**
ip igmp snooping report-suppression **IMC-120**
ip igmp snooping source-only-learning age-timer **IMC-121**
ip igmp snooping ssm-safe-reporting **IMC-122**
ip igmp snooping vlan **IMC-123**
ip igmp snooping vlan immediate-leave **IMC-125**
ip igmp snooping vlan mrouter **IMC-127**
ip igmp snooping vlan static **IMC-129**
ip igmp ssm-map **IMC-131**
ip igmp ssm-map enable **IMC-133**
ip igmp ssm-map query dns **IMC-135**
ip igmp ssm-map static **IMC-137**
ip igmp static-group **IMC-139**
ip igmp tcn query **IMC-142**
ip igmp unidirectional-link **IMC-143**
ip igmp v3lite **IMC-145**
ip igmp version **IMC-146**
ip mfib **IMC-148**
ip mfib cef **IMC-149**
ip mfib forwarding **IMC-151**
ip mrm **IMC-153**
ip mrm accept-manager **IMC-155**
ip mrm manager **IMC-157**
ip mroute **IMC-158**
ip mroute-cache **IMC-162**
ip msdp border **IMC-164**
ip msdp cache-rejected-sa **IMC-166**

ip msdp cache-sa-state **IMC-168**
ip msdp default-peer **IMC-170**
ip msdp description **IMC-172**
ip msdp filter-sa-request **IMC-173**
ip msdp keepalive **IMC-175**
ip msdp mesh-group **IMC-177**
ip msdp originator-id **IMC-179**
ip msdp password peer **IMC-181**
ip msdp peer **IMC-183**
ip msdp redistribute **IMC-185**
ip msdp rpf rfc3618 **IMC-188**
ip msdp sa-filter in **IMC-190**
ip msdp sa-filter out **IMC-192**
ip msdp sa-limit **IMC-194**
ip msdp sa-request **IMC-196**
ip msdp shutdown **IMC-198**
ip msdp timer **IMC-199**
ip msdp ttl-threshold **IMC-201**
ip multicast boundary **IMC-203**
ip multicast cache-headers **IMC-207**
ip multicast default-rpf-distance **IMC-209**
ip multicast group-range **IMC-211**
ip multicast hardware-switching non-rpf aging **IMC-213**
ip multicast hardware-switching replication-mode **IMC-214**
ip multicast heartbeat **IMC-216**
ip multicast helper-map **IMC-218**
ip multicast limit **IMC-221**
ip multicast limit cost **IMC-225**
ip multicast mrinfo-filter **IMC-228**
ip multicast multipath **IMC-230**
ip multicast rate-limit **IMC-233**
ip multicast redundancy routeflush maxtime **IMC-235**
ip multicast route-limit **IMC-237**
ip multicast rpf backoff **IMC-238**
ip multicast rpf interval **IMC-240**

ip multicast rpf mofrr **IMC-242**
ip multicast rpf proxy vector **IMC-244**
ip multicast rpf select **IMC-247**
ip multicast rpf select topology **IMC-249**
ip multicast topology **IMC-250**
ip multicast ttl-threshold **IMC-251**
ip multicast use-functional **IMC-253**
ip multicast-routing **IMC-254**
ip pgm host **IMC-256**
ip pgm router **IMC-260**
ip pim **IMC-261**
ip pim accept-register **IMC-265**
ip pim accept-rp **IMC-267**
ip pim autorp listener **IMC-269**
ip pim bidir-enable **IMC-270**
ip pim bidir-neighbor-filter **IMC-272**
ip pim bidir-offer-interval **IMC-275**
ip pim bidir-offer-limit **IMC-276**
ip pim border **IMC-277**
ip pim bsr-border **IMC-278**
ip pim bsr-candidate **IMC-280**
ip pim dm-fallback **IMC-283**
ip pim dr-priority **IMC-285**
ip pim log-neighbor-changes **IMC-286**
ip pim minimum-vc-rate **IMC-287**
ip pim multipoint-signalling **IMC-288**
ip pim nbma-mode **IMC-289**
ip pim neighbor-filter **IMC-290**
ip pim passive **IMC-292**
ip pim query-interval **IMC-294**
ip pim register-rate-limit **IMC-297**
ip pim register-source **IMC-299**
ip pim rp-address **IMC-301**
ip pim rp-announce-filter **IMC-304**
ip pim rp-candidate **IMC-307**

ip pim send-rp-announce IMC-310
ip pim send-rp-discovery IMC-313
ip pim snooping (global configuration) IMC-315
ip pim snooping (interface configuration) IMC-316
ip pim snooping dr-flood IMC-318
ip pim snooping suppress sgr-prune IMC-319
ip pim sparse sg-expiry-timer IMC-320
ip pim spt-threshold IMC-322
ip pim ssm IMC-324
ip pim state-refresh disable IMC-326
ip pim state-refresh origination-interval IMC-328
ip pim v1-rp-reachability IMC-330
ip pim vc-count IMC-331
ip pim version IMC-332
ip rgmp IMC-333
ip sap cache-timeout IMC-335
ip sap listen IMC-336
ip sdr cache-timeout IMC-338
ip sdr listen IMC-339
ip service reflect IMC-340
ip urd IMC-342
manager IMC-344
mdt data IMC-346
mdt default IMC-348
mdt log-reuse IMC-350
mdt preference IMC-351
mls ip multicast (global configuration) IMC-353
mls ip multicast (interface configuration) IMC-356
mls ip multicast bidir gm-scan-interval IMC-357
mls ip multicast connected IMC-358
mls ip multicast consistency-check IMC-360
mls ip multicast flow-stat-timer IMC-362
mls ip multicast non-rpf aging IMC-363
mls ip multicast replication-mode IMC-364
mls ip multicast sso IMC-366

mls ip multicast stub **IMC-368**
mls ip multicast threshold **IMC-370**
mode bypass **IMC-371**
mpls mldp forwarding recursive **IMC-373**
mpls mldp logging notifications **IMC-374**
mpls mldp path **IMC-375**
mrinfo **IMC-377**
mrm **IMC-379**
mstat **IMC-380**
mtrace **IMC-382**
receivers **IMC-384**
router-guard ip multicast **IMC-387**
router-guard ip multicast switchports **IMC-388**
senders **IMC-390**
show ip dvmrp route **IMC-392**
show ip igmp groups **IMC-394**
show ip igmp interface **IMC-397**
show ip igmp membership **IMC-400**
show ip igmp snooping **IMC-403**
show ip igmp snooping explicit-tracking **IMC-406**
show ip igmp snooping filter **IMC-408**
show ip igmp snooping mrouter **IMC-411**
show ip igmp snooping rate-limit **IMC-413**
show ip igmp snooping statistics **IMC-414**
show ip igmp ssm-mapping **IMC-416**
show ip igmp static-group class-map **IMC-419**
show ip igmp udlr **IMC-421**
show ip mcache **IMC-423**
show ip mfib **IMC-425**
show ip mfib active **IMC-427**
show ip mfib count **IMC-429**
show ip mfib interface **IMC-432**
show ip mfib route **IMC-435**
show ip mfib status **IMC-437**
show ip mfib summary **IMC-438**

show ip mpacket IMC-440
show ip mr proxy IMC-442
show ip mrib client IMC-444
show ip mrib route IMC-446
show ip mrib route summary IMC-448
show ip mrm interface IMC-449
show ip mrm manager IMC-451
show ip mrm status-report IMC-453
show ip mroute IMC-455
show ip msdp count IMC-466
show ip msdp peer IMC-468
show ip msdp rpf-peer IMC-470
show ip msdp sa-cache IMC-472
show ip msdp summary IMC-476
show ip multicast IMC-478
show ip multicast interface IMC-480
show ip multicast redundancy state IMC-483
show ip multicast redundancy statistics IMC-490
show ip multicast rpf tracked IMC-495
show ip multicast topology IMC-496
show ip pgm host defaults IMC-498
show ip pgm host sessions IMC-501
show ip pgm host traffic IMC-504
show ip pgm router IMC-506
show ip pim boundary IMC-510
show ip pim bsr-router IMC-512
show ip pim interface IMC-514
show ip pim mdt bgp IMC-520
show ip pim mdt history IMC-521
show ip pim mdt receive IMC-523
show ip pim mdt send IMC-525
show ip pim neighbor IMC-527
show ip pim rp IMC-530
show ip pim rp mapping IMC-533
show ip pim rp-hash IMC-535

show ip pim rp-hash (BSR) IMC-537
show ip pim snooping IMC-539
show ip pim tunnel IMC-543
show ip pim vc IMC-545
show ip rpf IMC-547
show ip rpf events IMC-552
show ip rpf select IMC-554
show ip sap IMC-556
show ip sdr IMC-559
show mls ip multicast IMC-560
show mls ip multicast bidir IMC-563
show mls ip multicast rp-mapping IMC-565
show mls ip multicast sso IMC-567
show mpls mldp bindings IMC-569
show mpls mldp count IMC-571
show mpls mldp database IMC-572
show mpls mldp label release IMC-574
show mpls mldp neighbors IMC-575
show mpls mldp root IMC-577
show platform software multicast ip bidir IMC-578
show platform software multicast ip capability IMC-580
show platform software multicast ip complete IMC-582
show platform software multicast ip connected IMC-585
show platform software multicast ip interface IMC-587
show platform software multicast ip partial IMC-589
show platform software multicast ip source IMC-591
show platform software multicast ip statistics IMC-593
show platform software multicast ip summary IMC-595
show platform software multicast ip vrf IMC-597
show router-guard IMC-600
snmp-server enable traps mvpn IMC-602
snmp-server enable traps pim IMC-604
tunnel udlr address-resolution IMC-606
tunnel udlr receive-only IMC-607
tunnel udlr send-only IMC-610

udp-port **IMC-612**

IP Multicast Commands

beacon (multicast routing monitor)

To change the frequency, duration, or scope of beacon messages that the Manager sends to Test Senders and Test Receivers during a Multicast Routing Monitor (MRM) test, use the **beacon** command in MRM manager configuration mode. To restore the default settings, use the **no** form of this command.

beacon [**interval** *seconds*] [**holdtime** *seconds*] [**ttl** *ttl-value*]

no beacon [**interval** *seconds*] [**holdtime** *seconds*] [**ttl** *ttl-value*]

Syntax Description

interval *seconds*	(Optional) Specifies the frequency of beacon messages (in seconds). The range is from 1 to 1800. By default, beacon messages are sent at an interval of 60 seconds, meaning that one beacon message is sent every 60 seconds.
holdtime *seconds*	(Optional) Specifies the length of the test period (in seconds). The Test Sender and Test Receiver are respectively sending and receiving test data constantly during the hold time. The range is from 1800 to 4294967295. By default, the duration of a test period is 86400 seconds (1 day).
ttl *ttl-value*	(Optional) Specifies the time-to-live (TTL) value of the beacon messages. The range is from 1 to 255. By default, the TTL for beacon messages is 32 hops.

Command Default

Beacon messages are sent at an interval of 60 seconds. The duration of a test period is 86400 seconds (1 day). The TTL for beacon messages is 32 hops.

Command Modes

MRM manager configuration (config-mrm-manager)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The beacon message functions like a keepalive message. The Manager multicasts beacon messages to the Test Sender and Test Receiver. Beacon messages include the sender requests and receiver requests to start the test, thus providing redundancy in case the Test Sender or Test Receiver goes down.

Examples

The following example shows how to customize the Manager to send beacon messages every 30 minutes (1800 seconds), for a test period of 12 hours (43,200 seconds), with a TTL of 40 hops:

```
ip mrm manager test
 beacon interval 1800 holdtime 43200 ttl 40
```

Related Commands

Command	Description
manager	Specifies that an interface is the Manager for MRM, and specifies the multicast group address the Test Receiver will listen to.

class-map type multicast-flows

To enter multicast-flows class-map configuration mode to create or modify an Internet Group Management Protocol (IGMP) static group class map, use the **class-map type multicast-flows** command in global configuration mode. To delete an IGMP static group range class map, use the **no** form of this command.

class-map type multicast-flows *class-map-name*

no class-map type multicast-flows *class-map-name*

Syntax Description

class-map-name	Name of the IGMP static group class map to be created or modified.

Command Default

No IGMP static group class maps are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXF5	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Use the **class-map type multicast-flows** command to enter multicast-flows class-map configuration mode to create or modify IGMP static group class maps.

Unlike quality of service (QoS) class maps, which you define by specifying numerous match criteria, you define IGMP static group class maps by specifying multicast groups entries (group addresses, group ranges, Source Specific Multicast [SSM] channels, and SSM channel ranges). The **group** command is used to define the group entries to be associated with a class map.

After using the **class-map type multicast-flows** command to specify the name of the IGMP static group class map to be created or modified, use the following forms of the **group** command in multicast-flows class-map configuration mode to define the group entries to be associated with the class map:

- **group** *group-address*

  Defines a group address to be associated with an IGMP static group class map.

- **group** *group-address* **to** *group-address*

  Defines a range of group addresses to be associated with an IGMP static group class map.

- **group** *group-address* **source** *source-address*

  Defines an SSM channel to be associated with an IGMP static group class map.

- **group** *group-address* **to** *group-address* **source** *source-address*

Defines a range of SSM channels to be associated with an IGMP static group class map.

Unlike QoS class maps, IGMP static group range class maps are not configured in traffic policies. Rather, the **ip igmp static-group** command has been extended to support IGMP static group ranges. After creating an IGMP static group class map, you can attach the class map to interfaces using the **ip igmp static-group** command with the **class-map** keyword and *class-map-name* argument. Once a class map is attached to an interface, all group entries defined in the class map become statically connected members on the interface and are added to the IGMP cache and IP multicast route (mroute) table.

Additional Guidelines for Configuring IGMP Static Group Class Maps

- Only one IGMP static group class map can be attached to an interface.
- If an IGMP static group class map is modified (that is, if group entries are added to or removed from the class map using the **group** command), the group entries that are added to or removed from the IGMP static group class map are added to or deleted from the IGMP cache and the IP multicast route (mroute) table, respectively.
- If an IGMP static group class map attached to an interface is replaced on the interface by another class map using the **ip igmp static-group** command, the group entries associated with the old class map are removed, and the group entries defined in the new class map are added to the IGMP cache and mroute table.
- The **ip igmp static-group** command accepts an IGMP static group class map for the *class-map-name* argument, regardless of whether the class map configuration exists. If a class map attached to an interface does not exist, the class map remains inactive. Once the class map is configured, all group entries associated with the class map are added to the IGMP cache and mroute table.
- If a class map is removed from an interface using the **no** form of the **ip igmp static-group** command, all group entries defined in the class map are removed from the IGMP cache and mroute tables.

Use the **show ip igmp static-group class-map** command to display the contents of IGMP static group class map configurations and information about the interfaces using class maps.

Examples

The following example shows how to create a class map named static1 and enter multicast-flows class-map configuration mode:

```
class-map type multicast-flows static1
```

The following example shows how to define a range of SSM channels to be associated with an IGMP static group class map:

```
group 192.0.2.0 source 192.0.2.10
```

Related Commands

Command	Description
group (multicast-flows)	Defines the group entries to be associated with an IGMP static group class map.
ip igmp static-group	Configures static group membership entries on an interface.
show ip igmp static-group class-map	Displays the contents of IGMP static group class map configurations and the interfaces using class maps.

clear ip cgmp

To clear all group entries from the caches of Catalyst switches, use the **clear ip cgmp** command in privileged EXEC mode.

clear ip cgmp [*interface-type interface-number*]

Syntax Description

interface-type interface-number	(Optional) Interface type and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command sends a Cisco Group Management Protocol (CGMP) leave message with a group address of 0000.0000.0000 and a unicast address of 0000.0000.0000. This message instructs the switches to clear all group entries they have cached.

If an interface type and number are specified, the leave message is sent only on that interface. Otherwise, it is sent on all CGMP-enabled interfaces.

Examples

The following example clears the CGMP cache:

```
Router# clear ip cgmp
```

Related Commands

Command	Description
ip cgmp	Enables CGMP on an interface of a router connected to a Catalyst 5000 switch.

clear ip dvmrp route

Note The **clear ip dvmrp route** command is not available in 12.2(33)SRB, 15.0(1)M, and later 12.2SR, 15.0M, and T releases.

To delete routes from the Distance Vector Multicast Routing Protocol (DVMRP) routing table, use the **clear ip dvmrp route** command in privileged EXEC mode.

clear ip dvmrp route {***** | *route*}

Syntax Description

*****	Clears all routes from the DVMRP table.
route	Name of the longest matched route to be cleared. Can be an IP address, a network number, or an IP Domain Name System (DNS) name.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was removed.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was removed.

Examples

The following example shows how to delete route 10.1.1.1 from the DVMRP routing table:

```
Router# clear ip dvmrp route 10.1.1.1
```

clear ip igmp group

To delete entries from the Internet Group Management Protocol (IGMP) cache, use the **clear ip igmp group** command in privileged EXEC mode.

clear ip igmp [**vrf** *vrf-name*] **group** [*group-name group-address* | *interface-type interface-number*]

Cisco 7600 Series

clear ip igmp [**vrf** *vrf-name*] **group** [*interface interface-number* | *group-name* | *group-address*] [**loopbap** *interface-number* | **null** *interface-number* | **port-channel** *number* | **vlan** *vlan-id*]

Defaults

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
group-name	(Optional) Name of the multicast group, as defined in the Domain Name System (DNS) hosts table or with the **ip host** command.
group-address	(Optional) Address of the multicast group. This is a multicast IP address in four-part dotted-decimal notation.
interface-type interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, and **tengigabitethernet**.
loopback *interface-number*	(Optional) Specifies the loopback interface; valid values are from 0 to 2147483647.
null *interface-number*	(Optional) Specifies the null interface; the valid value is 0.
port-channel *number*	(Optional) Specifies the channel interface; valid values are a maximum of 64 values ranging from 1 to 256.
vlan *vlan-id*	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

Defaults

When this command is entered with no keywords or arguments, all entries are deleted from the IGMP cache.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720 in Cisco IOS Release 12.2(14)SX. The **vrf** *vrf-name* keyword and argument are not supported in this release.
12.2(17d)SXB	Support for the Supervisor Engine 2 was added in Cisco IOS Release 12.2(17d)SXB. The **vrf** *vrf-name* keyword and argument are not supported in this release.
12.2(18)SXE	The **vrf** keyword and *vrf-name* argument were integrated into Cisco IOS Release 12.2(18)SXE on the Supervisor Engine 720 only.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

The IGMP cache contains a list of the multicast groups of which hosts on the directly connected LAN are members. If the router has joined a group, that group is also listed in the cache.

To delete all entries from the IGMP cache, specify the **clear ip igmp group** command with no arguments.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Examples

The following example shows how to clear entries for the multicast group 224.0.255.1 from the IGMP cache:

```
Router# clear ip igmp group 224.0.255.1
```

Cisco 7600 Series

This example shows how to clear the IGMP-group cache entries from a specific interface of the IGMP-group cache:

```
Router# clear ip igmp group gigabitethernet 2/2
Router#
```

Related Commands

Command	Description
ip host	Defines a static host name-to-address mapping in the host cache.
show ip igmp groups	Displays the multicast groups that are directly connected to the router and that were learned through IGMP.
show ip igmp interface	Displays multicast-related information about an interface.
show ip cache flow	Displays the multicast groups with receivers that are directly connected to the router and that were learned through IGMP.

clear ip igmp snooping filter statistics

To clear Internet Group Management Protocol (IGMP) filtering statistics, use the **clear ip igmp snooping filter statistics** command in privileged EXEC mode.

clear ip igmp snooping filter statistics interface *type mod/port* [**vlan** *vlan-id*]

Syntax Description

interface *type*	Interface type; possible valid values are **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel** *num*, and **vlan** *vlan-id*.
mod/port	Module and port number.
vlan *vlan-id*	(Optional) Specifies the Layer 2 VLAN identification.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Examples

This example shows how to clear statistics for all access ports and for all VLANs on all trunk ports:

```
Router# clear ip igmp snooping filter statistics
```

This example shows how to clear statistics for one particular access port or for all VLANs on one particular trunk port:

```
Router# clear ip igmp snooping filter statistics interface gigabitethernet 3/2
```

This example shows how to clear statistics for one particular VLAN on a trunk port:

```
Router# clear ip igmp snooping filter statistics interface gigabitethernet 3/2 vlan 100
```

Related Commands

Command	Description
ip igmp snooping access-group	Configures an IGMP group access group.
ip igmp snooping limit	Limits the number of IGMP groups or channels allowed on an interface.
ip igmp snooping minimum-version	Filters on the IGMP protocol.

clear ip igmp snooping statistics

To clear the IGMP-snooping statistics, use the **clear ip igmp snooping statistics** command in privileged EXEC mode.

clear ip igmp snooping statistics [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id*	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you do not enter a VLAN, the IGMP-snooping statistics for all VLANs is cleared.

Examples

This example shows how to clear the IGMP-snooping statistics for all VLANs:

```
Router# clear ip igmp snooping statistics
```

This example shows how to clear the IGMP-snooping statistics for a specific VLAN:

```
Router# clear ip igmp snooping statistics vlan 300
```

Related Commands

Command	Description
show ip igmp snooping statistics	Displays information about IGMPv3 statistics.

clear ip mfib counters

To reset all active IPv4 Multicast Forwarding Information Base (MFIB) traffic counters, use the **clear ip mfib counters** command in privileged EXEC mode.

clear ip mfib [**vrf** {*vrf-name* | *****}] **counters** [*group-address/mask* | *group-address* [*source-address*] | *source-address group-address*]

Syntax Description

vrf {*vrf-name* | ***** }	(Optional) Clears active IPv4 MFIB traffic counters associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances. After specifying the optional **vrf** keyword, you must specify either: • *vrf-name*—Name of an MVRF. Clears active MFIB traffic counters for the MVRF specified for the *vrf-name* argument. • *****—Clears active MFIB traffic counters for all MVRFs.
group-address/mask	(Optional) Multicast group address followed by a forward slash (*/*) and group mask, in dotted decimal notation, referred to as a (*, G/mask) entry.
group-address	(Optional) Multicast group address.
source-address	(Optional) Multicast source address.

Command Default

When this command is entered with no optional keywords or arguments, all active IPv4 MFIB traffic counters for all multicast tables are reset.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Use the **clear ip mfib counters** command to reset all active IPv4 MFIB traffic counters.

This command will reset the active IPv4 MFIB traffic counters displayed in the output of the following commands:

- **show ip mfib**
- **show ip mfib active**
- **show ip mfib count**

Examples

The following example shows how to reset all active MFIB traffic counters for all multicast tables:

```
Router# clear ip mfib counters
```

Related Commands

Command	Description
show ip mfib	Displays the forwarding entries and interfaces in the IPv4 MFIB.
show ip mfib active	Displays information from the IPv4 MFIB about the rate at which active multicast sources are sending to multicast groups.
show ip mfib count	Displays a summary of traffic statistics from the IPv4 MFIB about multicast sources and groups.

clear ip mrm status-report

To clear the Multicast Routing Monitor (MRM) status report cache, use the **clear ip mrm status-report** command in privileged EXEC mode.

clear ip mrm status-report [*ip-address*]

Syntax Description

ip-address	(Optional) IP address of the Test Receiver for which to clear status reports from the MRM status report cache.

Command Default

If no IP address is specified for the optional *ip-address* argument, all status reports are cleared from the MRM status report cache.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **clear ip mrm status-report** command to clear the MRM status report cache.

Use the **clear ip mrm status-report** command with the *ip-address* argument to clear only the status reports sent by the Test Receiver at the specified IP address. If no IP address is specified for the optional *ip-address* argument, all status reports are cleared from the MRM status report cache.

Use the **show ip mrm status-report** to display the status reports in the MRM status report cache.

Examples

The following example shows how to clear status reports sent by a specific Test Receiver from the MRM status report cache. In this example, the status reports sent by the Test Receiver at 172.16.0.0 are cleared from the MRM status report cache.

```
Router# clear ip mrm status-report 172.16.0.0
```

Related Commands

Command	Description
show ip mrm status-report	Displays the status reports in the MRM status report cache.

clear ip mroute

To delete entries from the IP multicast routing table, use the **clear ip mroute** command in privileged EXEC mode.

clear ip mroute [**vrf** *vrf-name*] {***** | *group*} [*source*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
*	Deletes all entries from the IP multicast routing table.
group	Name or IP address of the multicast group; see the "Usage Guidelines" section for additional information.
source	(Optional) Name or address of a multicast source that is sending to the group; see the "Usage Guidelines" section for additional information.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	The effect of this command was modified. If IP multicast Multilayer Switching (MMLS) is enabled, using this command now clears both the multicast routing table on the MMLS rendezvous point (RP) and all multicast MLS cache entries for all Multicast MLS-Switching Engines (MMLS-SEs) that are performing multicast MLS for the MMLS-RP. That is, the original clearing occurs, and the derived hardware switching table is also cleared.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The *group* argument specifies one of the following:

- Name of the multicast group as defined in the DNS hosts table or with the **ip host** command.
- IP address of the multicast group in four-part, dotted notation.

If you specify a *group* name or address, you can also enter the *source* argument to specify a name or address of a multicast source that is sending to the group. A source does not need to be a member of the group.

Examples

The following example shows how to delete all entries from the IP multicast routing table:

```
Router# clear ip mroute *
```

The following example shows how to delete all sources on the 228.3.0.0 subnet that are sending to the multicast group 224.2.205.42 from the IP multicast routing table. This example shows how to delete all sources on network 228.3, not individual sources.

```
Router# clear ip mroute 224.2.205.42 228.3.0.0
```

Related Commands

Command	Description
ip host	Defines a static host name-to-address mapping in the host cache.
mls rp ip multicast	Enables IP multicast MLS (hardware switching) on an external or internal router in conjunction with Layer 3 switching hardware for the Catalyst 5000 switch.
show ip mroute	Displays the contents of the IP multicast routing table.

clear ip msdp peer

To clear the TCP connection to the specified Multicast Source Discovery Protocol (MSDP) peer, use the **clear ip msdp peer** command in privileged EXEC mode.

clear ip msdp [**vrf** *vrf-name*] **peer** {*peer-address* | *peer-name*}

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or name of the MSDP peer to which the TCP connection is cleared.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command closes the TCP connection to the peer, resets all the MSDP peer statistics, and clears the input and output queues to and from the MSDP peer.

Examples

The following example shows how to clear the TCP connection to the MSDP peer at 10.3.32.154:

```
Router# clear ip msdp peer 10.3.32.154
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

clear ip msdp sa-cache

To clear Multicast Source Discovery Protocol (MSDP) Source-Active (SA) cache entries, use the **clear ip msdp sa-cache** command in privileged EXEC mode.

clear ip msdp [**vrf** *vrf-name*] **sa-cache** [*group-address* | *group-name*]

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
group-address | *group-name*	(Optional) Multicast group address or name for which SA entries are cleared from the SA cache.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

In order to have any SA entries in the cache to clear, SA caching must have been enabled with the **ip msdp cache-sa-state** command.

If no multicast group is identified by group address or name, all SA cache entries are cleared.

Examples

The following example shows how to clear the SA entries for the multicast group 10.3.50.152 from the cache:

```
Router# clear ip msdp sa-cache 10.3.50.152
```

Related Commands

Command	Description
ip host	Configures an MSDP peer.
ip msdp cache-sa-state	Enables the router to create SA state.
show ip msdp sa-cache	Displays (S, G) state learned from MSDP peers.

clear ip msdp statistics

To clear statistics counters for one or all of the Multicast Source Discovery Protocol (MSDP) peers without resetting the sessions, use the **clear ip msdp statistics** command in privileged EXEC mode.

clear ip msdp [**vrf** *vrf-name*] **statistics** [*peer-address* | *peer-name*]

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	(Optional) Address or name of the MSDP peers whose statistics counters, reset count, and input/output count are cleared.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example shows how to clear the counters for the peer named peer1:

```
Router# clear ip msdp statistics peer1
```

Related Commands

Command	Description
show ip msdp sa-cache	Displays (S, G) state learned from MSDP peers.

clear ip multicast limit

To reset the exceeded counter for per interface mroute state limiters, use the **clear ip multicast limit** command in privileged EXEC mode.

clear ip multicast limit [*type number*]

Syntax Description

type number	(Optional) Interface type and number for which to reset the exceeded counter for per interface mroute state limiters.

Command Default

The exceeded counter for all per interface mroute state limiters are reset.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the **clear ip multicast limit** command to reset the exceeded counter for per interface mroute state limiters (configured with the **ip multicast limit** command) that are displayed in the output of the **show ip multicast limit** command. The exceeded counter tracks the total number of times that the limit configured for the per interface mroute state limiter has been exceeded. Each time an mroute is denied due to the configured limit being reached, the exceeded counter is increased by a value of 1.

Specifying an interface for the optional *type* and *number* resets the exceeded counter for only per interface mroute state limiters configured on the specified interface. When no interface is specified for the optional *type* and *number* argument, the **clear ip multicast limit** command resets the exceeded counters globally (for all per interface mroute state limiters configured on the router).

Examples

The following example shows how to reset exceeded counters for mroute state limiters configured on Gigabit Ethernet interface 1/0:

```
clear ip multicast limit GigabitEthernet1/0
```

Related Commands

Command	Description
debug ip mrouting limits	Displays debugging information about configured per interface mroute state limiters and bandwidth-based multicast CAC policies.
ip multicast limit	Configures per interface mroute state limiters.
ip multicast limit cost	Applies costs to per interface mroute state limiters.
show ip multicast limit	Displays statistics about configured per interface mroute state limiters.

clear ip multicast redundancy statistics

To clear IP multicast redundancy statistics, use the **clear ip multicast redundancy statistics** command in privileged EXEC mode.

clear ip multicast redundancy statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Examples

The following example shows how to clear IP multicast redundancy statistics:

```
Router# clear ip multicast redundancy statistics
```

Related Commands

Command	Description
show ip multicast redundancy statistics	Displays IP multicast redundancy statistics.

clear ip pgm host

Note Support for the PGM Host feature has been removed. Use of this command is not recommended.

To reset Pragmatic General Multicast (PGM) Host connections to their default values and to clear traffic statistics, use the **clear ip pgm host** command in privileged EXEC mode.

clear ip pgm host {**defaults** | **traffic**}

Syntax Description

defaults	Resets all PGM Host connections to their default values.
traffic	Clears all PGM Host traffic statistics.

Defaults

No default behavior or values

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command should be used only in rare cases or during debugging. A reason to reset all PGM Host connections to their default values is to eliminate configuration errors in one step. A reason to clear traffic statistics is to make diagnostic testing easier.

Examples

The following example resets all PGM Host connections to their default values:

```
Router# clear ip pgm host defaults
```

The following example clears all PGM Host traffic statistics:

```
Router# clear ip pgm host traffic
```

Related Commands

Command	Description
ip pgm host	Enables PGM Host.
show ip pgm host defaults	Displays default values for PGM Host traffic.
show ip pgm host traffic	Displays PGM Host traffic statistics.

clear ip pgm router

To clear Pragmatic General Multicast (PGM) traffic statistics, use the **clear ip pgm router** command in privileged EXEC mode.

clear ip pgm router [**traffic** [*interface-type interface-number*] | **rtx-state** [*group-address*]]

Syntax Description

traffic [*interface-type interface-number*]	(Optional) Specifies the interface type and number whose PGM traffic statistics are cleared. If no interface type and number are provided, all traffic statistics are cleared.
rtx-state [*group-address*]	(Optional) Specifies the IP address of the multicast group whose PGM resend state is cleared. If no group address is provided, all resend state is cleared. Clearing resend state means the router will not forward any retransmissions corresponding to that state.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command should be used only in rare cases or during debugging. Normally, the resend state memory is freed automatically when the information is no longer useful. Also, using this command briefly affects the normal PGM behavior.

A reason to clear traffic statistics is to make diagnostic testing easier.

A reason to clear state might be to free the memory consumed by such state. PGM resend state times out if no traffic keeps it alive.

Examples

The following example clears all PGM resend state from the router:

```
Router# clear ip pgm router rtx-state
```

Related Commands

Command	Description
ip pgm router	Enables PGM Router Assist and thereby allows PGM to operate more efficiently on the router.
show ip pgm router	Displays PGM Reliable Transport Protocol state and statistics.

clear ip pim auto-rp

The **clear ip pim auto-rp** command is replaced by the **clear ip pim rp-mapping** command. See the **clear ip pim rp-mapping** command for more information.

clear ip pim interface count

To clear all line card counts or packet counts, use the **clear ip pim interface count** command in user EXEC or privileged EXEC mode.

clear ip pim interface count

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.2(11)GS	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command on a Router Processor (RP) to delete all multicast distributed switching (MDS) statistics for the entire router.

Examples

The following example shows how to clear all the line card packets counts:

```
Router# clear ip pim interface count
```

Related Commands

Command	Description
clear ip mds forwarding	Clears all routes from the MFIB table of a line card and resynchronizes it with the RP.

clear ip pim rp-mapping

To delete group-to-rendezvous point (RP) mapping entries from the RP mapping cache, use the **clear ip pim rp-mapping** command in privileged EXEC mode.

clear ip pim [**vrf** *vrf-name*] **rp-mapping** [*ip-address*]

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
ip-address	(Optional) IP address of the RP about which to clear associated group-to-RP mappings. If this argument is omitted, all group-to-RP mapping entries are cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.1	The **clear ip pim auto-rp** command was deprecated and replaced by the **clear ip pim rp-mapping** command.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **clear ip pim rp-mapping** command replaces the **clear ip pim auto-rp** command.

The **clear ip pim rp-mapping** command deletes group-to-RP mapping entries learned by Auto-RP or by a bootstrap router (BSR) from the RP mapping cache.

Use the **show ip pim rp** command to display active RPs that are cached with associated multicast routing entries.

Examples

The following example shows how to clear all group-to-RP entries from the RP mapping cache:

```
Router# clear ip pim rp-mapping
```

Related Commands

Command	Description
show ip pim rp	Displays active RPs that are cached with associated multicast routing entries.

clear ip pim snooping statistics

To delete the IP PIM-snooping global statistics, use the **clear ip pim snooping statistics** command in privileged EXEC mode.

clear ip pim snooping statistics

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to clear the IP PIM statistics:

```
Router# clear ip pim snooping statistics
```

Related Commands

Command	Description
ip pim snooping (global configuration mode)	Enables PIM snooping globally.
show ip pim snooping statistics	Displays statistical information about IP PIM snooping.

clear ip pim snooping vlan

To delete the IP PIM-snooping entries on a specific VLAN, use the **clear ip pim snooping vlan** command in privileged EXEC mode.

clear ip pim snooping vlan *vlan-id* **mac-address** *gda-address*

clear ip pim snooping vlan *vlan-id* **mroute** {***** | {*group-addr src-addr*} {{**downstream-neighbor**} *ip-addr*} | {**upstream-neighbor** *ip-addr*}}}

clear ip pim snooping vlan *vlan-id* **neighbor** {***** | *ip-addr*}

Syntax Description

vlan-id	VLAN ID; valid values are from 1 to 4094.
mac-address *gda-address*	Specifies the multicast group MAC address to delete.
mroute *	Deletes all mroute entries.
mroute *group-addr src-addr*	Deletes the mroute entries at the specified group and source IP address.
downstream-neighbor *ip-addr*	Deletes the entries at the specified downstream neighbor originating the join/prune message.
upstream-neighbor *ip-addr*	Deletes the entries at the specified upstream neighbor receiving the join/prune message.
neighbor *	Deletes all neighbors.
neighbor *ip-addr*	Deletes the neighbor at the specified IP address.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to clear the IP PIM-snooping entries on a specific VLAN:

```
Router# clear ip pim snooping vlan 25
```

Related Commands

Command	Description
ip pim snooping (interface configuration mode)	Enables PIM snooping on a specific interface.
show ip pim snooping	Displays information about IP PIM snooping.

clear ip rtp header-compression

To clear Real-Time Transport Protocol (RTP) header compression structures and statistics, use the **clear ip rtp header-compression** command in privileged EXEC mode.

clear ip rtp header-compression [*interface-type interface-number*]

Syntax Description

interface-type interface-number	(Optional) Interface type and number.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If this command is used without an interface type and number, it clears all RTP header compression structures and statistics.

Examples

The following example clears RTP header compression structures and statistics for serial interface 0:

```
Router# clear ip rtp header-compression serial 0
```

Related Commands

Command	Description
ip rtp header-compression	Enables RTP header compression.

clear ip sap

To delete a Session Announcement Protocol (SAP) cache entry or the entire SAP cache, use the **clear ip sap** command in privileged EXEC mode.

clear ip sap [*group-address* | **"***session-name***"**]

Syntax Description

group-address	(Optional) Deletes all sessions associated with the IP group address.
"*session-name***"**	(Optional) Session name to be deleted by the SAP cache entry. The session name is enclosed in quotation marks (**" "**) that the user must enter.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	The **clear ip sdr** command was introduced.
12.2	The **clear ip sdr** command was replaced by the **clear ip sap** command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If no arguments or keywords are used with this command, the system deletes the entire SAP cache.

Examples

The following example clears the SAP cache:

```
Router# clear ip sap "Sample Session"
```

Related Commands

Command	Description
ip sap cache-timeout	Limits how long a SAP cache entry stays active in the cache.
ip sap listen	Enables the Cisco IOS software to listen to session directory announcements.
show ip sap	Displays the SAP cache.

clear ip sdr

The **clear ip sdr** command is replaced by the **clear ip sap** command. See the description of the **clear ip sap** command in this chapter for more information.

clear mls ip multicast bidir-rpcache

To clear all Bidir rendezvous-point cache entries, use the **clear mls ip multicast bidir-rpcache** command in privileged EXEC mode.

clear mls ip multicast bidir-rpcache

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to reset the Bidir counters:

```
Router# clear mls ip multicast bidir-rpcache
```

Related Commands

Command	Description
show mls ip multicast bidir	Displays the Bidir hardware-switched entries.

clear mls ip multicast group

To delete an IP multicast group, use the **clear mls ip multicast group** command in privileged EXEC mode.

clear mls ip multicast group {*ip-name* | *group-address*}

Syntax Description

ip-name	Host IP name.
group-address	Address of the multicast group in four-part, dotted notation.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17b)SXA	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to delete an IP multicast group:

```
Router# clear mls ip multicast group 224.0.255.1
```

Related Commands

Command	Description
show mls ip multicast group	Displays the entries for a specific multicast-group address.

clear mls ip multicast statistics

To reset the IP-multicast statistics counters, use the **clear mls ip multicast statistics** command in privileged EXEC mode.

clear mls ip multicast statistics

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to reset the IP-multicast statistics counters:

```
Router# clear mls ip multicast statistics
```

Related Commands

Command	Description
show mls ip multicast	Displays the MLS IP information.

clear router-guard ip multicast statistics

To clear router guard statistics, use the **clear router-guard ip multicast statistics** command in privileged EXEC mode.

clear router-guard ip multicast statistics [**interface** *type mod/port* [**vlan** *vlan-id*]]

Syntax Description

interface *type*	(Optional) Interface type; possible valid values are **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel** *num*, and **vlan** *vlan-id*.
mod/port	Module and port number.
vlan *vlan-id*	(Optional) Specifies the Layer 2 VLAN identification.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Examples

This example shows how to clear router guard statistics for all access ports and for all VLANs on all trunk ports:

```
Router# clear router-guard ip multicast statistics
```

This example shows how to clear router guard statistics for one particular access port or for all VLANs on one particular trunk port:

```
Router# clear router-guard ip multicast statistics interface gigabitethernet 3/2
```

This example shows how to clear router guard statistics for one particular VLAN on a trunk port:

```
Router# clear router-guard ip multicast statistics interface gigabitethernet 3/2 vlan 100
```

Related Commands

Command	Description
ip igmp snooping limit	Limits the number of IGMP groups or channels allowed on an interface.
ip igmp snooping minimum-version	Filters on the IGMP protocol.
router-guard ip multicast switchports	Configures an IGMP group access group.

group (multicast-flows)

To define the group entries to be associated with an Internet Group Management Protocol (IGMP) static group class map, use the **group** command in class-map multicast-flows configuration mode. To delete an entry from an IGMP static group class map, use the **no** form of this command.

group *group-address* [**to** *group-address*] [**source** *source-address*]

no group *group-address* [**to** *group-address*] [**source** *source-address*]

Syntax Description

group-address	Group address to be associated with an IGMP static group class map.
to *group-address*	(Optional) Defines a range of multicast groups to be associated with an IGMP static group class map.
source *source-address*	(Optional) Defines a (S, G) channel or a range of (S, G) channels to be associated with an IGMP static group class map.

Command Default

No group entries are defined in IGMP static group class maps.

Command Modes

Class-map multicast-flows configuration (config-mcast-flows-cmap)

Command History

Release	Modification
12.2(18)SXF5	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Use the **group** command to define group entries to be associated with an IGMP static group class map. You can use this command only after entering the **class-map type multicast-flows** command to enter multicast-flows class-map configuration mode to create or modify an IGMP static group class map.

Once you enter multicast-flows class-map configuration mode, use the following forms of the **group** command to define the group entries to be associated with an IGMP static group class map:

- **group** *group-address*

  Defines a group address to be associated with an IGMP static group class map.

- **group** *group-address* **to** *group-address*

  Defines a range of group addresses to be associated with an IGMP static group class map.

- **group** *group-address* **source** *source-address*

  Defines an SSM channel to be associated with an IGMP static group class map.

- **group** *group-address* **to** *group-address* **source** *source-address*

Defines a range of SSM channels to be associated with an IGMP static group class map.

After creating an IGMP static group class map, you can attach the class map to interfaces using the **ip igmp static-group** command with the **class-map** keyword and *class-map-name* argument. Once a class map is attached to an interface, all group entries defined in the class map become statically connected members on the interface and are added to the IGMP cache and IP multicast route (mroute) table.

Examples

The following example shows how to define a range of group addresses to be associated with an IGMP static group class map named test:

```
class-map type multicast-flows test
 group 227.7.7.7 to 227.7.7.9
```

Related Commands

Command	Description
class-map type multicast-flows	Enters multicast-flows class-map configuration mode to create or modify IGMP static group class maps.
ip igmp static-group	Configures static group membership entries on an interface.
show ip igmp static-group class-map	Displays the contents of IGMP static group class map configurations and the interfaces using class maps.

ip cgmp

To enable Cisco Group Management Protocol (CGMP) on an interface of a router connected to a Cisco Catalyst switch, use the **ip cgmp** command in interface configuration mode. To disable CGMP routing, use the **no** form of this command.

ip cgmp [**proxy** | **router-only**]

no ip cgmp

Syntax Description

proxy	(Optional) Enables CGMP and the CGMP proxy function.
router-only	(Optional) Enables the router to send only CGMP self-join and CGMP self-leave messages.

Defaults

CGMP is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2	The **router-only** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

When enabled on an interface, this command triggers a CGMP join message. This command should be used only on 802 media (that is, Ethernet, FDDI, or Token Ring) or ATM. When a **no ip cgmp** command is issued, a triggered CGMP leave message is sent for the MAC address on the interface for group 0000.0000.0000 (all groups). CGMP can run on an interface only if Protocol Independent Multicast (PIM) is configured on the same interface.

A Cisco router will send CGMP join messages in response to receiving Internet Group Management Protocol (IGMP) reports from IGMP-capable members. Only the CGMP querier Cisco router sends these CGMP join messages on behalf of hosts.

The **ip cgmp router-only** command enables the routers in a VLAN to send only CGMP self-join and CGMP self-leave messages—no other types of CGMP messages will be sent. This feature allows other CGMP-capable routers to learn about multicast router ports. If the **ip cgmp router-only** command is not available on any of the external routers in the network, the **ip cgmp** command can be used instead. Issuing the **ip cgmp** command on a router enables that router to send CGMP self-join and CGMP self-leave messages as well as other types of CGMP messages.

When the **proxy** keyword is specified, the CGMP proxy function is also enabled. That is, any router that is not CGMP-capable will be advertised by the proxy router. The proxy router advertises the existence of other non-CGMP-capable routers by sending a CGMP join message with the MAC address of the non-CGMP-capable router and a group address of 0000.0000.0000.

Initially supported is Distance Vector Multicast Routing Protocol (DVMRP) proxying. If a DVMRP report is received from a router that is not a PIM router, a Cisco IGMP querier will advertise the MAC address of the DVMRP router in a CGMP join message with the group address 0000.0000.0000.

To perform CGMP proxy, a Cisco router must be the IGMP querier. If you configure the **ip cgmp proxy** command, you must manipulate the IP addresses so that a Cisco router will be the IGMP querier, which might be the highest or lowest IP address, depending on which version of IGMP is being run on the network. An IGMP Version 2 querier is selected based on the lowest IP addressed router on the interface. An IGMP Version 1 querier is selected based on the multicast routing protocol used on the interface.

When multiple Cisco routers are connected to a switched network and the **ip cgmp proxy** command is needed, we recommend that all routers be configured in the following manner:

- With the same CGMP option.
- To have precedence of becoming IGMP querier over non-Cisco routers.

Examples

The following example enables CGMP:

```
ip cgmp
```

The following example enables CGMP and CGMP proxy:

```
ip cgmp proxy
```

ip domain multicast

To change the domain prefix used by the Cisco IOS software for Domain Name Service (DNS)-based Source Specific Multicast (SSM) mapping, use the **ip domain multicast** command in global configuration mode. To revert to the default domain prefix, use the **no** form of this command.

ip domain multicast *domain-prefix*

no domain multicast *domain-prefix*

Syntax Description

domain-prefix	Name of the domain prefix to be used for DNS-based SSM mapping. The default is in-addr.arpa.

Command Default

By default, the Cisco IOS software uses the ip-addr.arpa domain prefix.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18) SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to change the domain prefix used by Cisco IOS software when DNS-based SSM mapping is configured. When a router attempts DNS-based SSM mapping for an IP group address (G = G1.G2.G3.G4), the router queries the domain name server for IP address resource records ("IP A" RRs) for the domain G4.G3.G2.G1 *domain-prefix*.

Examples

The following example shows how to change the domain prefix used for DNS-based SSM mapping to ssm-map.cisco.com:

```
ip domain multicast ssm-map.cisco.com
```

Related Commands

Command	Description
ip igmp ssm-map enable	Enables SSM mapping for groups in a configured SSM range.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip dvmrp accept-filter

Note The **ip dvmrp accept-filter** command is not available in 12.2(33)SRB, 15.0(1)M, and later 12.2SR, 15.0M, and T releases.

To configure an acceptance filter for incoming Distance Vector Multicast Routing Protocol (DVMRP) reports, use the **ip dvmrp accept-filter** command in interface configuration mode. To disable this filter, use the **no** form of this command.

ip dvmrp accept-filter *access-list* [*distance* | **neighbor-list** *access-list*]

no ip dvmrp accept-filter *access-list* [*distance* | **neighbor-list** *access-list*]

Syntax Description

access-list	Access list number or name. A value of 0 means that all sources are accepted with the configured distance.
distance	(Optional) Administrative distance to the destination.
neighbor-list *access-list*	(Optional) Number of a neighbor list. DVMRP reports are accepted only by those neighbors on the list.

Defaults

All destination reports are accepted with a distance of 0. Default settings accept reports from all neighbors.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The **neighbor-list** keyword and *access-list* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was removed.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was removed.

Usage Guidelines

Any sources that match the access list are stored in the DVMRP routing table with the *distance* argument.

The *distance* value is used to compare with the same source in the unicast routing table. The route with the lower distance (either the route in the unicast routing table or that in the DVMRP routing table) takes precedence when computing the Reverse Path Forwarding (RPF) interface for a source of a multicast packet.

By default, the administrative distance for DVMRP routes is 0, which means that they always take precedence over unicast routing table routes. If you have two paths to a source, one through unicast routing (using Protocol Independent Multicast [PIM] as the multicast routing protocol) and another path using DVMRP (unicast and multicast routing), and if you want to use the PIM path, use the **ip dvmrp accept-filter** command to increase the administrative distance for DVMRP routes.

Examples

The following example shows how to apply an access list such that the RPF interface used to accept multicast packets will be through an Enhanced Interior Gateway Routing Protocol (IGRP)/PIM path. The Enhanced IGRP unicast routing protocol has a default administrative distance of 90.

```
ip dvmrp accept-filter 1 100
access-list 1 permit 0.0.0.0 255.255.255.255
```

The following example shows how to apply access list 57 to an interface and set a distance of 4:

```
access-list 57 permit 172.16.0.0 0.0.255.255
access-list 57 permit 192.168.0.0 0.0.0.255
access-list 57 deny 10.0.0.0 255.255.255.255
 ip dvmrp accept-filter 57 4
```

Related Commands

Command	Description
distance (IP)	Defines an administrative distance.
ip dvmrp metric	Configures the metric associated with a set of destinations for DVMRP reports.
show ip dvmrp route	Displays the contents of the DVMRP routing table.
tunnel mode	Sets the encapsulation mode for the tunnel interface.

ip dvmrp auto-summary

Note The **ip dvmrp auto-summary** command is not available in 12.2(33)SRB, 15.0(1)M, and later 12.2SR, 15.0M, and T releases.

To enable Distance Vector Multicast Routing Protocol (DVMRP) automatic summarization if it was disabled, use the **ip dvmrp auto-summary** command in interface configuration mode. To disable this function, use the **no** form of this command.

ip dvmrp auto-summary

no ip dvmrp auto-summary

Syntax Description

This command has no arguments or keywords.

Defaults

DVMRP automatic summarization is enabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was removed.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was removed.

Usage Guidelines

DVMRP automatic summarization occurs when a unicast subnet route is collapsed into a classful network number route. This situation occurs when the subnet is a different network number than the IP address of the interface (or tunnel) over which the advertisement is sent. If the interface is unnumbered, the network number of the numbered interface the unnumbered interface points to is compared to the subnet.

Disable this function if the information you want to send using the **ip dvmrp summary-address** command is the same as the information that would be sent using DVMRP automatic summarization.

Examples

The following example shows how to disable DVMRP automatic summarization:

```
no ip dvmrp auto-summary
```

Related Commands

Command	Description
ip dvmrp summary-address	Configures a DVMRP summary address to be advertised out the interface.

ip dvmrp default-information

Note The **ip dvmrp default-information** command is not available in 12.2(33)SRB, 15.0(1)M, and later 12.2SR, 15.0M, and T releases.

To advertise network 0.0.0.0 to Distance Vector Multicast Routing Protocol (DVMRP) neighbors on an interface, use the **ip dvmrp default-information** command in interface configuration mode. To prevent the advertisement, use the **no** form of this command.

ip dvmrp default-information {**originate** | **only**}

no ip dvmrp default-information {**originate** | **only**}

Syntax Description

originate	Specifies that other routes more specific than 0.0.0.0 may be advertised.
only	Specifies that no DVMRP routes other than 0.0.0.0 are advertised.

Defaults

Network 0.0.0.0 is not advertised to DVMRP neighbors on an interface.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was removed.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was removed.

Usage Guidelines

This command should be used only when the router is a neighbor to mrouted version 3.6 devices. The mrouted protocol is a public domain implementation of DVMRP.

You can use the **ip dvrmrp metric** command with the **ip dvmrp default-information** command to tailor the metric used when advertising the default route 0.0.0.0. By default, metric 1 is used.

Examples

The following example shows how to configure a router to advertise network 0.0.0.0, in addition to other networks, to DVMRP neighbors:

```
ip dvmrp default-information originate
```

Related Commands

Command	Description
ip dvmrp metric	Configures the metric associated with a set of destinations for DVMRP reports.

ip dvmrp interoperability

To enable Distance Vector Multicast Routing Protocol (DVMRP) interoperability, use the **ip dvmrp interoperability** command in global configuration mode. To disable DVMRP interoperatibility, use the **no** form of this command.

ip dvmrp [**vrf** *vrf-name*] **interoperability**

no ip dvmrp [**vrf** *vrf-name*] **interoperability**

Syntax Description

vrf *vrf-name*	Enables DVMRP interoperability for the Multicast Virtual Private Network virtual routing and forwarding (MVRF) instance specified for the *vrf-name* argument.

Command Default

DVMRP interoperability is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXF7	This command was introduced.

Usage Guidelines

Use the **ip dvmrp interoperability** command to enable DVMRP interoperability.

Note Prior to the introduction of this command, DVMRP interoperability was enabled by default and could not be effectively disabled.

When DVMRP interoperability is disabled, the router will not process DVMRP packets (probe, report, prune, or graft packets) but will still process packets that are received from **mtrace** and **mrinfo** multicast backbone (MBONE) commands.

When upgrading the router to a Cisco IOS software release where DVMRP is disabled by default, if any DVMRP commands are configured, the **ip dvmrp interoperability** command will automatically be nvgened during reboot.

Note If you have DVMRP commands configured and you want to disable DVMRP, you must disable DVMRP interoperability *and* remove all DVMRP commands from the configuration. If you do not remove all DVMRP commands from the configuration, DVMRP interoperability will be reenabled upon the next reboot.

Examples

The following example shows how to enable DVMRP interoperability:

```
Router(config)# ip dvmrp interoperability
```

ip dvmrp metric

Note The **ip dvmrp metric** command is not available in 12.2(33)SRB, 15.0(1)M, and later 12.2SR, 15.0M, and T releases.

To configure the metric associated with a set of destinations for Distance Vector Multicast Routing Protocol (DVMRP) reports, use the **ip dvmrp metric** command in interface configuration mode. To disable this function, use the **no** form of this command.

ip dvmrp metric *metric* [**route-map** *map-name*] [**mbgp**] [**mobile**] [**list** *access-list-number*] [*protocol process-id*] | **dvmrp**]

no ip dvmrp metric *metric* [**route-map** *map-name*] [**mbgp**] [**mobile**] [**list** *access-list-number*] [*protocol process-id*] | **dvmrp**]

Syntax Description

metric	Metric associated with a set of destinations for DVMRP reports. It can be a value from 0 to 32. A value of 0 means that the route is not advertised. A value of 32 is equivalent to infinity (unreachable).
route-map *map-name*	(Optional) Names a route map. If you specify this keyword and argument, only the destinations that match the route map are reported with the configured metric. Unicast routes are subject to route map conditions before being injected into DVMRP. Route maps cannot be used for DVMRP routes.
mbgp	(Optional) Configures redistribution of only IP version 4 (IPv4) multicast routes into DVMRP.
mobile	(Optional) Configures redistribution of only mobile routes into DVMRP.
list *access-list-number*	(Optional) Names an access list. If you specify this keyword and argument, only the multicast destinations that match the access list are reported with the configured metric. Any destinations not advertised because of split horizon do not use the configured metric.
protocol	(Optional) Name of a unicast routing protocol. Available protocols are: **bgp**, **dvmrp**, **eigrp**, **isis, mobile, odr**, **ospf**, **rip**, or **static**. If you specify these values, only routes learned by the specified routing protocol are advertised in DVMRP report messages.
process-id	(Optional) Process ID number of the unicast routing protocol.
dvmrp	(Optional) Allows routes from the DVMRP routing table to be advertised with the configured *metric* value, or filtered.

Defaults

No metric value is preconfigured. Only directly connected subnets and networks are advertised to neighboring DVMRP routers.

Command Modes

Interface configuration

Command History

Release	Modification
10.2	This command was introduced.
11.1	The **route-map** keyword was added.
11.1(20)CC	This **mbgp** keyword was added.
12.0(7)T	This **mbgp** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was removed.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was removed.

Usage Guidelines

When Protocol Independent Multicast (PIM) is configured on an interface and DVMRP neighbors are discovered, the Cisco IOS software sends DVMRP report messages for directly connected networks. The **ip dvmrp metric** command enables DVMRP report messages for multicast destinations that match the access list. Usually, the metric for these routes is 1. Under certain circumstances, you might want to tailor the metric used for various unicast routes. This command lets you configure the metric associated with a set of destinations for report messages sent out this interface.

You can use the *access-list-number* argument in conjunction with the *protocol* and *process-id* arguments to selectively list the destinations learned from a given routing protocol.

To display DVMRP activity, use the **debug ip dvmrp** command.

Examples

The following example shows how to connect a PIM cloud to a DVMRP cloud. Access list 1 permits the sending of DVMRP reports to the DVMRP routers advertising all sources in the 172.16.35.0 network with a metric of 1. Access list 2 permits all other destinations, but the metric of 0 means that no DVMRP reports are sent for these destinations.

```
access-list 1 permit 172.16.35.0 0.0.0.255
access-list 1 deny 0.0.0.0 255.255.255.255
access-list 2 permit 0.0.0.0 255.255.255.255
interface tunnel 0
 ip dvmrp metric 1 list 1
 ip dvmrp metric 0 list 2
```

The following example shows how to redistribute IPv4 multicast routes into DVMRP neighbors with a metric of 1:

```
interface tunnel 0
 ip dvmrp metric 1 mbgp
```

Related Commands

Command	Description
debug ip dvmrp	Displays information on DVMRP packets received and sent.
ip dvmrp accept-filter	Configures an acceptance filter for incoming DVMRP reports.

ip dvmrp metric-offset

Note The **ip dvmrp metric-offset** command is not available in 12.2(33)SRB, 15.0(1)M, and later 12.2SR, 15.0M, and T releases.

To change the metrics of advertised Distance Vector Multicast Routing Protocol (DVMRP) routes and thus favor or not favor a certain route, use the **ip dvmrp metric-offset** command in interface configuration mode. To restore the default values, use the **no** form of this command.

ip dvmrp metric-offset [**in** | **out**] *increment*

no ip dvmrp metric-offset

Syntax Description

in	(Optional) Adds the *increment* value to incoming DVMRP reports and is reported in mrinfo replies. The default for **in** is 1.
out	(Optional) Adds the *increment* value to outgoing DVMRP reports for routes from the DVMRP routing table. The default for **out** is 0.
increment	Value added to the metric of a DVMRP route advertised in a report message.

Defaults

If neither **in** nor **out** is specified, **in** is the default.
in: 1
out: 0

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was removed.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was removed.

Usage Guidelines

Use this command to influence which routes are used, as you prefer. The DVMRP metric is in hop count.

Examples

The following example shows how to add a value of 10 to incoming DVMRP reports:

```
ip dvmrp metric-offset 10
```

ip dvmrp output-report-delay

Note The **ip dvmrp output-report-delay** command is not available in 12.2(33)SRB, 15.0(1)M, and later 12.2SR, 15.0M, and T releases.

To configure an interpacket delay of a Distance Vector Multicast Routing Protocol (DVMRP) report, use the **ip dvmrp output-report-delay** command in interface configuration mode. To restore the default values, use the **no** form of this command.

ip dvmrp output-report-delay *milliseconds* [*burst*]

no ip dvmrp output-report-delay *milliseconds* [*burst*]

Syntax Description

milliseconds	Number of milliseconds that elapse between transmissions of a set of DVMRP report packets. The number of packets in the set is determined by the *burst* argument. The default number of milliseconds is 100 milliseconds.
burst	(Optional) The number of packets in the set being sent. The default is 2 packets.

Defaults

milliseconds: 100 milliseconds
burst: 2 packets

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was removed.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was removed.

Usage Guidelines

The delay is the number of milliseconds that elapse between transmissions of sets of packets that constitute a report. The number of packets in the set is determined by the *burst* value.

You might want to change the default values, depending on the CPU and buffering of the mrouted machine.

Examples

The following example shows how to set the interpacket delay to 200 milliseconds and the burst size to 3 packets. For this example, at the periodic DVMRP report interval, if six packets are built, three packets will be sent, then a delay of 200 milliseconds will occur, and then the next three packets will be sent.

```
ip dvmrp output-report-delay 200 3
```

ip dvmrp reject-non-pruners

Note The **ip dvmrp reject-non-pruners** command is not available in 12.2(33)SRB, 15.0(1)M, and later 12.2SR, 15.0M, and T releases.

To configure the router so that it will not peer with a Distance Vector Multicast Routing Protocol (DVMRP) neighbor if that neighbor does not support DVMRP pruning or grafting, use the **ip dvmrp reject-non-pruners** command in interface configuration mode. To disable the function, use the **no** form of this command.

ip dvmrp reject-non-pruners

no ip dvmrp reject-non-pruners

Syntax Description

This command has no arguments or keywords.

Defaults

Routers peer with DVMRP neighbors that do not support DVMRP pruning or grafting.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was removed.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was removed.

Usage Guidelines

By default, the router accepts all DVMRP neighbors as peers, regardless of their DVMRP capability or lack thereof.

Use this command to prevent a router from peering with a DVMRP neighbor if that neighbor does not support DVMRP pruning or grafting. If the router receives a DVMRP probe or report message without the Prune-Capable flag set, the router logs a syslog message and discards the message.

This command prevents peering with neighbors only. If there are any nonpruning routers multiple hops away (downstream toward potential receivers) that are not rejected, then a nonpruning DVMRP network might still exist.

Examples

The following example shows how to configures the router not to peer with DVMRP neighbors that do not support pruning or grafting:

```
ip dvmrp reject-non-pruners
```

ip dvmrp routehog-notification

Note The **ip dvmrp route-hog notification** command is not available in 12.2(33)SRB, 15.0(1)M, and later 12.2SR, 15.0M, and T releases.

To change the number of Distance Vector Multicast Routing Protocol (DVMRP) routes allowed before a syslog warning message is issued, use the **ip dvmrp routehog-notification** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip dvmrp routehog-notification *route-count*

no ip dvmrp routehog-notification

Syntax Description

route-count	Number of routes allowed before a syslog message is triggered. The default is 10,000 routes.

Defaults

10,000 routes

Command Modes

Global configuration

Command History

Release	Modification
10.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was removed.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was removed.

Usage Guidelines

This command configures how many DVMRP routes are accepted on each interface within an approximate 1-minute period before a syslog message is issued, warning that a route surge might be occurring. The warning is typically used to detect quickly when routers have been misconfigured to inject a large number of routes into the multicast backbone (MBONE).

The **show ip igmp interface** command displays a running count of routes. When the count is exceeded, an "*** ALERT ***" is appended to the line.

Examples

The following example shows how to lower the threshold to 8000 routes:

```
ip dvmrp routehog-notification 8000
```

Related Commands

Command	Description
show ip igmp interface	Displays multicast-related information about an interface.

ip dvmrp route-limit

Note The **ip dvmrp route-limit** command is not available in 12.2(33)SRB, 15.0(1)M, and later 12.2SR, 15.0M, and T releases.

To change the limit on the number of Distance Vector Multicast Routing Protocol (DVMRP) routes that can be advertised over an interface enabled to run DVMRP, use the **ip dvmrp route-limit** command in global configuration mode. To configure no limit, use the **no** form of this command.

ip dvmrp route-limit *count*

no ip dvmrp route-limit

Syntax Description

count	Number of DVMRP routes that can be advertised. The default is 7000 routes.

Defaults

count: 7000 routes

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was removed.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was removed.

Usage Guidelines

Interfaces enabled to run DVMRP include a DVMRP tunnel, an interface where a DVMRP neighbor has been discovered, and an interface configured to run the **ip dvmrp unicast-routing** command.

The **ip dvmrp route-limit** command is automatically generated to the configuration file when at least one interface is enabled for multicast routing. This command is necessary to prevent misconfigured **ip dvmrp metric** commands from causing massive route injection into the multicast backbone (MBONE).

Examples

The following example shows how to configure the limit of DMVRP routes that can be advertised to 5000:

```
ip dvmrp route-limit 5000
```

Related Commands

Command	Description
ip dvmrp metric	Configures the metric associated with a set of destinations for DVMRP reports.
ip dvmrp unicast-routing	Enables DVMRP unicast routing on an interface.

ip dvmrp summary-address

Note The **ip dvmrp summary-address** command is not available in 12.2(33)SRB, 15.0(1)M, and later 12.2SR, 15.0M, and T releases.

To configure a Distance Vector Multicast Routing Protocol (DVMRP) summary address to be advertised out the interface, use the **ip dvmrp summary-address** command in interface configuration mode. To remove the summary address, use the **no** form of this command.

ip dvmrp summary-address *summary-address mask* [**metric** *value*]

no ip dvmrp summary-address *summary-address mask* [**metric** *value*]

Syntax Description

summary-address	Summary IP address that is advertised instead of the more specific route.
mask	Mask on the summary IP address.
metric *value*	(Optional) Metric that is advertised with the summary address. The default is 1.

Defaults

metric *value*: 1

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was removed.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was removed.

Usage Guidelines

If there is at least a single, more specific route in the unicast routing table that matches the specified *address* and *mask* arguments, the summary is advertised. Routes in the DVMRP routing table are not candidates for summarization.

When the **metric** keyword is specified, the summary is advertised with that metric value.

Multiple summary addresses can be configured on an interface. When multiple overlapping summary addresses are configured on an interface, the one with the longest mask takes preference.

Examples

The following example configures the DVMRP summary address 172.16.0.0 to be advertised out the interface:

```
ip dvmrp summary-address 172.16.0.0 255.255.0.0 metric 1
```

Related Commands

Command	Description
ip dvmrp auto-summary	Enables DVMRP automatic summarization if it was disabled.

ip dvmrp unicast-routing

Note The **ip dvmrp unicast-routing** command is not available in 12.2(33)SRB, 15.0(1)M, and later 12.2SR, 15.0M, and T releases.

To enable Distance Vector Multicast Routing Protocol (DVMRP) unicast routing on an interface, use the **ip dvmrp unicast-routing** command in interface configuration mode. To disable this function, use the **no** form of this command.

ip dvmrp unicast-routing

no ip dvmrp unicast-routing

Syntax Description

This command has no arguments or keywords.

Defaults

DVMRP unicast routing on an interface is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was removed.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was removed.

Usage Guidelines

Enabling DVMRP unicast routing means that routes in DVMRP report messages are cached by the router in a DVMRP routing table. When Protocol Independent Multicast (PIM) is running, these routes may get preference over routes in the unicast routing table. This capability allows PIM to run on the multicast backbone (MBONE) topology when it is different from the unicast topology.

DVMRP unicast routing can run on all interfaces, including generic routing encapsulation (GRE) tunnels. On DVMRP tunnels, it runs by virtue of DVMRP multicast routing. This command does not enable DVMRP multicast routing among Cisco routers. However, if there is a DVMRP-capable multicast router, the Cisco router will do PIM and DVMRP multicast routing interaction.

Examples

The following example shows how to enable DVMRP unicast routing:

```
ip dvmrp unicast-routing
```

Related Commands

Command	Description
ip dvmrp route-limit	Changes the limit on the number of DVMRP routes that can be advertised over an interface enabled to run DVMRP.

ip igmp access-group

To restrict hosts (receivers) on a subnet to joining only multicast groups that are permitted by a standard IP access list or to restrict hosts (receivers) on a subnet to membership to only the (S,G) channels that are permitted by an extended IP access list, use the **ip igmp access-group** command in interface configuration mode. To disable this control, use the **no** form of this command.

ip igmp access-group *access-list*

no ip igmp access-group *access-list*

Syntax Description

access-list	Access list number or name.

Command Default

Disabled (no access lists are configured for receiver access control).

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	Extended access list support was added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Use the **ip igmp access-group** command to filter groups from Internet Group Management Protocol (IGMP) reports by use of a standard access list or to filter sources and groups from IGMPv3 reports by use of an extended access list. This command is used to restrict hosts on a subnet to joining only multicast groups that are permitted by a standard IP access list or to restrict hosts on a subnet to membership to only those (S, G) channels that are permitted by an extended IP access list.

IGMP Version 3 (IGMPv3) accommodates extended access lists, which allow you to leverage an important advantage of Source Specific Multicast (SSM) in IPv4, that of basing access on source IP address. Prior to this feature, an IGMP access list accepted only a standard access list, allowing membership reports to be filtered based only on multicast group addresses.

IGMPv3 allows multicast receivers not only to join to groups, but to groups including or excluding sources. For appropriate access control, it is therefore necessary to allow filtering of IGMPv3 messages not only by group addresses reported, but by group and source addresses. IGMP extended access lists

introduce this functionality. Using SSM with an IGMP extended access list allows you to permit or deny source S and group G (S, G) in IGMPv3 reports, thereby filtering SSM traffic based on source address, group address, or both.

Source Addresses in IGMPv3 Reports for ASM Groups

Additionally, IGMP extended access lists can be used to permit or filter traffic based on (0.0.0.0, G); that is, (*, G), in IGMP reports that are non-SSM, such as Any Source Multicast (ASM).

Note The permit and deny statements equivalent to (*, G) are **permit host 0.0.0.0 host** *group-address* and **deny host 0.0.0.0 host group** *group-address*, respectively.

Filtering applies to IGMPv3 reports for both ASM and SSM groups, but it is most important for SSM groups because multicast routing ignores source addresses in IGMPv3 reports for ASM groups. Source addresses in IGMPv3 membership reports for ASM groups are stored in the IGMP cache (as displayed with the **show ip igmp membership** command), but PIM-based IP multicast routing considers only the ASM groups reported. Therefore, adding filtering for source addresses for ASM groups impacts only the IGMP cache for ASM groups.

How IGMP Checks an Extended Access List

When an IGMP extended access list is referenced in the **ip igmp access-group** command on an interface, the (S, G) pairs in the permit and deny statements of the extended access list are matched against the (S, G) pair of the IGMP reports received on the interface. The first part of the extended access list clause controls the source, and the second part of the extended access list clause controls the multicast group.

Specifically, if an IGMP report with (S1, S2...Sn, G) is received, first the group (0, G) is checked against the access list statements. If the group is denied, the entire IGMP report is denied. If the group is permitted, each individual (S, G) pair is checked against the access list. Denied sources are taken out of the IGMP report, thereby denying any sources that match the access list from sending to the group.

Note The convention (0, G) means (*, G), which is a wildcard source with a multicast group number.

Examples

The following example shows how to configure a standard access list to filter the groups that are available on an interface for receivers to join. In this example, Ethernet interface 1/3 is configured to restrict receivers from joining groups in the range 226.1.0.0 through 226.1.255.255. Receivers are permitted to join all other groups on Ethernet interface 1/3.

```
access-list 1 deny 226.1.0.0 0.0.255.255
access-list 1 permit any log
!
interface ethernet 1/3
 ip igmp access-group 1
```

Note Access lists are very flexible; there is a seemingly limitless combination of permit and deny statements one could use in an access list to filter multicast traffic. The examples in this section simply provide a few examples of how it can be done.

The following example shows how to deny all states for a group G. In this example, FastEthernet interface 0/0 is configured to filter all sources for SSM group 232.2.2.2 in IGMPv3 reports, which effectively denies this group.

```
ip access-list extended test1
 deny igmp any host 232.2.2.2
 permit igmp any any
!
interface FastEthernet0/0
 ip igmp access-group test1
!
```

The following example shows how to deny all states for a source S. In this example, Ethernet interface 1/1 is configured to filter all groups for source 10.2.1.32 in IGMPv3 reports, which effectively denies this source.

```
ip access-list extended test2
 deny igmp host 10.2.1.32 any
 permit igmp any any
!
interface Ethernet1/1
 ip igmp access-group test2
```

The following example shows how to permit all states for a group G. In this example, Ethernet interface 1/1 is configured to accept all sources for SSM group 232.1.1.10 in IGMPv3 reports, which effectively accepts this group altogether.

```
ip access-list extended test3
 permit igmp any host 232.1.1.10
!
interface Ethernet1/1
 ip igmp access-group test3
```

The following example shows how to permit all states for a source S. In this example, Ethernet interface 1/2 is configured to accept all groups for source 10.6.23.32 in IGMPv3 reports, which effectively accepts this source altogether.

```
!
ip access-list extended test4
 permit igmp host 10.6.23.32 any
!
interface Ethernet1/2
 ip igmp access-group test4
!
```

The following example shows how to filter a particular source S for a group G. In this example, Ethernet interface 0/3 is configured to filter source 232.2.2.2 for SSM group 232.2.30.30 in IGMPv3 reports.

```
ip access-list extended test5
 deny igmp host 10.4.4.4 host 232.2.30.30
 permit igmp any any
!
interface Ethernet0/3
 ip igmp access-group test5
```

ip igmp explicit-tracking

To enable explicit tracking of hosts, groups, and channels for Internet Group Management Protocol Version 3 (IGMPv3), use the **ip igmp explicit-tracking** command in interface configuration mode. To disable this capability, use the **no** form of this command.

ip igmp explicit-tracking

no ip igmp explicit-tracking

Syntax Description

This command has no arguments or keywords.

Command Default

Explicit tracking of hosts, groups and channels for IGMPv3 is disabled.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.0(19)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Use the **ip igmp explicit-tracking** command to enable a multicast router to explicitly track the membership of multicast hosts in a particular multiaccess network. This capability enables the router to track each individual host that is joined to a particular group or channel and to achieve minimal leave latencies when hosts leave a multicast group or channel.

Note Before configuring the **ip igmp explicit-tracking** command, IGMP must be enabled (IGMP is enabled by enabling PIM on an interface using the **ip pim** command). In addition, IGMPv3 should be configured on the interface. To configure IGMPv3, use the **ip igmp version 3** command in interface configuration mode.

Note When explicit tracking is enabled, the router uses more memory than if explicit tracking is disabled because the router must store the membership state of all hosts on the interface.

To monitor the IGMP membership of hosts, use the **show ip igmp membership** command.

Examples

The following example shows how to enable explicit tracking. The example shows a basic configuration for enabling IP multicast with SSM, IGMPv3, and explicit tracking.

```
ip multicast-routing
interface ethernet 0
 description access network to desktop systems
 ip address 10.1.0.1 255.255.255.0
 ip pim sparse-dense-mode
 ip mroute-cache
 ip igmp version 3
 ip igmp explicit-tracking
interface ethernet 1
 description backbone interface no connected hosts
 ip address 10.10.0.1 255.255.255.0
 ip pim sparse-dense-mode
 ip mroute-cache
ip pim ssm default
```

Related Commands

Command	Description
ip igmp version	Configures the version of IGMP that the router uses.
ip pim	Enables PIM on an interface.
show ip igmp membership	Displays the IGMP membership information for multicast groups and (S, G) channels.

ip igmp helper-address

To cause the system to forward all Internet Group Management Protocol (IGMP) host reports and leave messages received on the interface to the specified IP address, use the **ip igmp helper-address** command in interface configuration mode. To disable such forwarding, use the **no** form of this command.

ip igmp helper-address *ip-address*

no ip igmp helper-address

Syntax Description

ip-address	IP address to which IGMP host reports and leave messages are forwarded. Specify the IP address of an interface on the central router.

Defaults

IGMP host reports and leave messages are not forwarded.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

This command and the **ip pim neighbor-filter** command together enable stub multicast routing. The IGMP host reports and leave messages are forwarded to the IP address specified. The reports are re-sent out the next hop interface toward the IP address, with the source address of that interface. This command enables a type of “dense-mode” join, allowing stub sites not participating in Protocol Independent Multicast (PIM) to indicate membership in IP multicast groups.

Examples

The following example enables stub multicast routing on Router A, which has an outgoing interface with IP address 10.0.0.1. Router B is a central router with an incoming interface with address 10.0.0.2. Access list 1 filters PIM messages from the source (stub Router A).

Router A Configuration

```
ip multicast-routing
 ip pim dense-mode
 ip igmp helper-address 10.0.0.2
```

Router B Configuration

```
ip multicast-routing
 ip pim dense-mode : or ip pim sparse-mode
 ip pim neighbor-filter 1
access-list 1 deny 10.0.0.1
```

Related Commands

Command	Description
ip pim neighbor-filter	Prevents a router from participating in PIM (for example, to configure stub multicast routing).

ip igmp helper-address (UDL)

To configure Internet Group Management Protocol (IGMP) helpering as required for IGMP unidirectional link routing (UDLR), use the **ip igmp helper-address** command in interface configuration mode. To disable such report forwarding, use the **no** form of this command.

ip igmp helper-address udl *interface-type interface-number*

no ip igmp helper-address

Syntax Description

udl *interface-type interface-number*	Specifies the interface type and number of a unidirectional interface.

Defaults

No forwarding occurs.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is required on a downstream router on each interface connected to a potential multicast receiver. The command allows the downstream router to helper IGMP reports received from hosts to an upstream router connected to a unidirectional link (UDL) associated with the configured *interface-type* and *interface-number* arguments.

Examples

The following example configures a helper address on a downstream router:

```
ip multicast-routing
!
! Interface that receiver is attached to, configure for IGMP reports to be
! helpered for the unidirectional interface.
!
interface ethernet 0
 description Forward IGMP reports from this interface to UDL querier
 ip address 10.0.0.2 255.0.0.0
 ip pim sparse-dense-mode
 ip igmp helper-address udl serial 0
```

Related Commands

Command	Description
ip igmp proxy-service	Enables the mroute proxy service.
ip igmp unidirectional-link	Configures an interface to be unidirectional and enables it for IGMP UDLR.

ip igmp immediate-leave

To minimize the leave latency of Internet Group Management Protocol (IGMP) memberships when IGMP Version 2 is used and only one receiver host is connected to each interface, use the **ip igmp immediate-leave** command in global or interface configuration mode. To disable this feature, use the **no** form of this command.

ip igmp immediate-leave group-list *access-list*

no ip igmp immediate-leave

Syntax Description

group-list *access-list*	Specifies a standard access list number or name that defines multicast groups in which the immediate leave feature is enabled.

Defaults

This command is disabled.

Command Modes

Global configuration (config)
Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

You cannot configure this command in both interface and global configuration mode.

When this command is not configured, the router will send an IGMP group-specific query message upon receipt of an IGMP Version 2 (IGMPv2) group leave message. The router will stop forwarding traffic for that group only if no host replies to the query within the timeout period. The timeout period is determined by the **ip igmp last-member-query-interval** command and the IGMP robustness variable, which is defined by the IGMP specification. By default, the timeout period in Cisco IOS software is approximately 2.5 seconds.

If this command is configured, the router assumes that only one host has joined the group and stops forwarding the group's traffic immediately upon receipt of an IGMPv2 group leave message.

Global Configuration Mode

When this command is configured in global configuration mode, it applies to all IGMP-enabled interfaces. Any existing configuration of this command in interface configuration mode will be removed from the configuration. Also, any new configuration of this command in interface configuration mode will be ignored.

Interface Configuration Mode

When this command is configured in interface configuration mode, it applies to an individual interface. Configure this command on an interface if only one IGMP-enabled neighbor is connected to the interface. The neighbor can be either a host or switch running IGMP Snooping. When the **ip igmp immediate-leave** command is enabled on an interface, the router will not send IGMP group-specific host queries when an IGMP Version 2 leave group message is received from that interface. Instead, the router will immediately remove the interface from the IGMP cache for that group and send Protocol Independent Multicast (PIM) prune messages toward sources if this interface was the last one to join that group.

Examples

The following example shows how to enable the immediate leave feature on all interfaces for all multicast groups:

```
Router(config)# ip multicast-routing
Router(config)# ip igmp immediate-leave group-list all-groups

Router(config)# interface ethernet 0
Router(config-if)# ip address 10.0.10.1 255.255.255.0
Router(config-if)# ip pim sparse-dense mode
Router(config-if)# exit
Router(config)# ip access-list standard all-groups
Router(config)# permit 224.0.0.0 15.255.255.255
```

The following example shows how to enable the immediate leave feature on an interface for a specific range of multicast groups. In this example, the router assumes that the tv-groups access list consists of groups that have only one host membership at a time per interface:

```
Router(config)# ip multicast-routing
Router(config)# interface ethernet 0
Router(config-if)# ip address 10.0.10.1 255.255.255.0
Router(config-if)# ip pim sparse-dense-mode
Router(config-if)# ip igmp immediate-leave group-list tv-groups
Router(config-if)# exit
Router(config)# ip access-list standard tv-groups
Router(config)# permit 239.192.20.0 0.0.0.255
```

Related Commands

Command	Description
ip igmp last-member-query-interval	Configures the frequency at which the router sends IGMP group-specific host query messages.

ip igmp immediate-leave group-list

To enable the immediate processing of the IGMP leave-group messages, use the **ip igmp immediate-leave group-list** command in global or interface configuration mode. To return to the default settings, use the **no** form of this command.

ip igmp immediate-leave group-list *acl*

no ip igmp immediate-leave group-list *acl*

Syntax Description

acl	Specifies the group ACL number; see the "Usage Guidelines" section for valid values.

Defaults

Disabled

Command Modes

Global or interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

If you enter the **ip igmp immediate-leave group-list** command, you must enter this command in VLAN interface configuration mode only.

Valid values for the *acl* argument are as follows:

- Access-list number—1 to 99
- Expanded range access-list number—1300 to 1999
- Name of the standard IP access list

You can configure one or the other but not both configuration modes at the same time.

You can enter the *acl* to restrict the immediate-leave behavior to a simple access list for multicast groups. The IGMP leave-group messages for multicast groups that are not permitted by the *acl* has the standard inquiry mechanism/leave latency.

Examples

This example shows how to enable the immediate processing of the IGMP leave-group messages:

```
Router(config)# ip igmp immediate-leave group-list 3
```

ip igmp join-group

To configure an interface on the router to join the specified group or channel, use the **ip igmp join-group** command in interface configuration mode. To cancel membership in a multicast group, use the **no** form of this command.

ip igmp join-group *group-address* [**source** *source-address*]

no ip igmp join-group *group-address* [**source** *source-address*]

Syntax Description

group-address	Multicast group address.
source *source-address*	(Optional) Specifies a multicast source address. This keyword and argument pair can be used to enable the router to provide INCLUDE mode capability for the (S, G) channel specified for the *group-address* and *source-address* arguments.

Command Default

No multicast group memberships are predefined.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
10.0	This command was introduced.
12.3(14)T	This command was modified. The **source** keyword and *source-address* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRE	This command was modified. The **source** keyword and *source-address* argument were added.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Use the **ip igmp join-group** command to configure an interface on the router to join the specified group or channel. With this method, the router accepts the multicast packets in addition to forwarding them. Accepting the multicast packets prevents the router from fast switching.

In support of the IGMPv3 Host Stack feature, the **source** keyword and *source-address* argument were added to the **ip igmp join-group** command to add INCLUDE mode capability to the IGMPv3 host stack for SSM groups.

The IGMPv3 Host Stack feature enables routers or switches to function as multicast network endpoints or hosts. The feature adds INCLUDE mode capability to the IGMPv3 host stack for SSM groups. Enabling the IGMPv3 host stack ensures that hosts on a LAN can leverage SSM by enabling the router or switch to initiate IGMPv3 joins, such as in environments where fast channel change is required in a SSM deployments.

Note Multiple **ip igmp join-group** command configurations with different source addresses for the same group are supported.

When the IGMPv3 Host Stack feature is configured, an IGMPv3 membership report is sent when one of the following events occurs:

- When the **ip igmp join-group** command is configured for a group and source and there is no existing state for this (S, G) channel, an IGMPv3 report of group record type ALLOW_NEW_SOURCES for the source specified is sent on that interface.
- When the **no** form of the **ip igmp join-group** command is configured for a group and source and there is state for this (S, G) channel, an IGMPv3 report of group record type BLOCK_OLD_SOURCES for the source specified is sent on that interface.
- When a query is received, an IGMPv3 report is sent as defined in RFC 3376.

Examples

The following example shows how to configure a router to forward multicast traffic in the absence of directly connected IGMP hosts using the **ip igmp join-group** command. With this method, the router accepts the multicast packets in addition to forwarding them. Accepting the multicast packets prevents the router from fast switching. In this example, Fast Ethernet interface 0/0 on the router is configured to join the group 225.2.2.2.

```
interface FastEthernet0/0
 ip igmp join-group 225.2.2.2
```

The following example shows how to add INCLUDE mode capability to the IGMPv3 host stack for SSM groups:

```
interface FastEthernet0/0
 ip igmp join-group 232.2.2.2 source 10.1.1.1
 ip igmp join-group 232.2.2.2 source 10.5.5.5
 ip igmp join-group 232.2.2.2 source 10.5.5.6
 ip igmp join-group 232.2.2.4 source 10.5.5.5
 ip igmp join-group 232.2.2.4 source 10.5.5.6
 ip igmp version 3
```

Related Commands

Command	Description
ip igmp static-group	Configures static group membership entries on an interface.

ip igmp last-member-query-count

To configure the number of times that the router sends Internet Group Management Protocol (IGMP) group-specific or group-source-specific (with IGMP version 3) query messages in response to receiving a group-specific or group-source-specific leave message, use the **ip igmp last-member-query-count** command in interface configuration mode. To set this interval to the default value, use the **no** form of this command.

ip igmp last-member-query-count *lmqc*

no ip igmp last-member-query-count *lmqc*

Syntax Description

lmqc	Last member query count. The number of times, from 1 through 7, that the router sends group- or group-source-specific queries upon receipt of a message indicating a leave.

Defaults

LMQC is 2

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

When a router receives an IGMP version 2 (IGMPv2) or IGMP version 3 (IGMPv3) message indicating that a host wants to leave a group, source, or channel, it sends last-member-query-count group- or group-source-specific IGMP query messages at intervals of igmp-last-member-interval milliseconds. If no response is received after this period, the router stops forwarding for the group, source, or channel.

Caution Do not set the LMQC to 1, because in this situation the loss of a single packet—the query packet from the router to the host or the report packet from the host to the router—may result in traffic forwarding being stopped, even there is still a receiver. Traffic will continue to be forwarded after the next general query sent by the router, but the interval during which a receiver may not receive the query could be as long as 1 minute (with the default query interval).

The leave latency in Cisco IOS software may increase by up to one last member query interval (LMQI) value when the router is processing more than one leave within a LMQI. In this case, the average leave latency is determined by the (LMQC + 0.5) * LMQI. The result is that the default leave latency can range from 2.0 to 3.0 seconds with an average of 2.5 seconds under a higher load of IGMP leave processing. The leave latency under load for the minimum LMQI value of 100 msec and a LMQC of 1 is from 100 to 200 milliseconds, with an average of 150 milliseconds. This is done to limit the impact of higher rates of IGMP leave messages.

If no response is received after this period, the router will stop forwarding traffic for that group, source, or channel only if no host replies to the query within the timeout period. The timeout period is determined by the **ip igmp last-member-query-interval** and the **ip igmp last-member-query-count** commands.

Examples

The following example changes the number of times that the router sends group-specific or group-source-specific query messages to 5:

```
interface tunnel 0
 ip igmp last-member-query-count 5
```

Related Commands

Command	Description
ip igmp explicit-tracking	Enables explicit tracking of hosts, groups, and channels for IGMPv3.
ip igmp immediate-leave	Minimizes the leave latency of IGMP memberships when IGMPv2 is used and only one receiver host is connected to each interface.
ip igmp last-member-query-interval	Configures the interval at which the router sends IGMP group-specific or group-source-specific (with IGMPv3) query messages

ip igmp last-member-query-interval

To configure the interval at which the router sends Internet Group Management Protocol (IGMP) group-specific or group-source-specific (with IGMP Version 3) query messages, use the **ip igmp last-member-query-interval** command in interface configuration mode. To set this interval to the default value, use the **no** form of this command.

ip igmp last-member-query-interval *interval*

no ip igmp last-member-query-interval *interval*

Syntax Description

interval	Interval, in milliseconds, at which IGMP group-specific host query messages are sent. The interval value is an integer from 100 to 25,500. The *interval* argument in 12.0 S, 12.1 E, 12.2, and 12.2 S releases is an integer from 100 through 65,535.

Defaults

interval: 1000 milliseconds (1 second)

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.1	This command was introduced.
12.2(4)T	The highest *interval* integer value accepted was changed from 65,535 to 25,500.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

When a router receives an IGMP Version 2 (IGMPv2) or IGMP Version 3 (IGMPv3) message indicating that a host wants to leave a group, source, or channel, it sends last-member-query-count group, group-specific, or source-specific IGMP query messages at intervals set by the **ip igmp last-member-query-interval** command. If no response is received after this period, the router stops forwarding for the group, source, or channel.

The leave latency in Cisco IOS software may increase by up to one last member query interval (LMQI) value when the router is processing more than one leave within a LMQI. In this case, the average leave latency is determined by the (last member query count + 0.5) * LMQI. The result is that the default leave latency can range from 2.0 to 3.0 seconds with an average of 2.5 seconds under a higher load of IGMP leave processing. The leave latency under load for the minimum LMQI value of 100 msec and a last member query count of 1 is from 100 to 200 milliseconds, with an average of 150 milliseconds. This is done to limit the impact of higher rates of IGMP leave messages.

If no response is received after this period, the router will stop forwarding traffic for that group, source, or channel only if no host replies to the query within the timeout period. The timeout period is determined by the **ip igmp last-member-query-interval** and the **ip igmp last-member-query-count** commands.

Examples

The following example changes the IGMP group-specific host query message interval to 2000 milliseconds (2 seconds):

```
interface tunnel 0
 ip igmp last-member-query-interval 2000
```

Related Commands

Command	Description
ip igmp explicit-tracking	Enables explicit tracking of hosts, groups, and channels for IGMPv3.
ip igmp immediate-leave	Minimizes the leave latency of IGMP memberships when IGMPv2 is used and only one receiver host is connected to each interface.
ip igmp last-member-query-count	Configures the number of times that the router sends IGMP group-specific or group-source-specific (with IGMP version 3) query messages.

ip igmp limit (global)

To configure a global limit on the number of multicast route (mroute) states created as a result of Internet Group Management Protocol (IGMP) membership reports (IGMP joins), use the **ip igmp limit** command in global configuration mode. To remove the limit imposed by the global IGMP state limiter, use the **no** form of this command.

ip igmp limit *number*

no ip igmp limit *number*

Syntax Description

number	Maximum number of IGMP membership reports that can be cached. The range is from 1 to 64000.

Command Default

A global IGMP state limiter is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to configure a global limit on the number of mroute states created as a result of IGMP membership reports (IGMP joins). When configured globally, the limit is referred to as a global IGMP state limiter. Membership reports exceeding the configured limits are not entered into the IGMP cache. This command can be used to prevent DoS attacks.

Note IGMP state limiters impose limits on the number of mroute states resulting from IGMP, IGMP v3lite, and URL Rendezvous Directory (URD) membership reports on a global or per interface basis.

Use the **ip igmp limit** (interface) command to configure a per interface limit on the number mroute states created as a result of IGMP membership reports (IGMP joins).

Note When configuring IGMP state limiters, you can only configure one global limit on a router and one limit per interface.

The mechanics of IGMP state limiters are as follows:

- Each time a router receives an IGMP membership report for a particular group or channel, the Cisco IOS software checks to see if either the limit for the global IGMP state limiter or the limit for the per interface IGMP state limiter has been reached.
  - If only a global IGMP state limiter has been configured and the limit has not been reached, IGMP membership reports are honored. When the configured limit has been reached, subsequent IGMP membership reports are then ignored (dropped) and a warning message in one of the following formats is generated:

    ```
    %IGMP-6-IGMP_GROUP_LIMIT: IGMP limit exceeded for <group (*, group address)> on
    <interface type number> by host <ip address>
    ```
    or

    ```
    %IGMP-6-IGMP_CHANNEL_LIMIT: IGMP limit exceeded for <channel (source address,
    group address)> on <interface type number> by host <ip address>
    ```

  - If only per interface IGMP state limiters are configured, then each limit is only counted against the interface on which it was configured.
  - If both a global IGMP state limiter and per interface IGMP state limiters are configured, the limits configured for the per interface IGMP state limiters are still enforced but are constrained by the global limit.
- If a per interface IGMP state limiter has been configured using the **ip igmp limit** (interface) command, the Cisco IOS software also checks to see if an access control list (ACL) is specified (with the optional **except** keyword and *access-list* argument) to prevent groups or channels from being counted against the interface limit.
  - If an ACL has been configured and the group or channel in the IGMP membership report matches, then the state for the IGMP membership is counted against the global limit and not the interface limit.
  - If no ACL has been configured, the per interface IGMP state limiter accounts for all IGMP membership reports that do not exceed the configured limit.

Examples

The following example shows how to configure a global IGMP state limiter that limits the number of mroute states created as result of IGMP membership reports to 300:

```
ip igmp limit 300
```

Related Commands

Command	Description
ip igmp limit (interface)	Limits the number of mroute states created as a result of IGMP membership reports on a per interface basis.
show ip igmp groups	Displays information about the status and configuration of IGMP and multicast routing on interfaces.

ip igmp limit (interface)

To configure a per interface limit on the number of multicast route (mroute) states created as a result of Internet Group Management Protocol (IGMP) membership reports (IGMP joins), use the **ip igmp limit** command in interface configuration mode. To remove the limit imposed by a per interface IGMP state limiter, use the **no** form of this command.

ip igmp limit *number* [**except** *access-list*]

no ip igmp limit *number* [**except** *access-list*]

Syntax Description

number	Maximum number of IGMP states allowed on a router or interface. The range is from 1 to 64000.
except *access-list*	(Optional) Prevent groups or channels from being counted against the interface limit. A standard or an extended access control list (ACL) can be specified for the *access-limit* argument. • A standard ACL can be used to define the (*, G) state to be excluded from the limit on an interface. • An extended ACLs can be used to define the (S, G) state to be excluded from the limit on an interface. An extended ACL also can be used to define the (*, G) state to be excluded from the limit on an interface, by specifying 0.0.0.0 for the source address and source wildcard—referred to as (0, G)—in the permit or deny statements that compose the extended access list.

Command Default

No per interface IGMP state limiters are configured.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Use this command to configure per interface limits on the number mroute states created as a result of IGMP membership reports (IGMP joins). When configured on an interface, the limit is referred to as a *per interface IGMP state limiter*. Membership reports exceeding the configured limits for the interface are not entered into the IGMP cache. This command can be used to prevent DoS attacks or to provide a multicast Call Admission Control (CAC) mechanism in network environments where all the multicast flows roughly utilize the same amount of bandwidth.

Note IGMP state limiters impose limits on the number of mroute states resulting from IGMP, IGMP v3lite, and URD membership reports on a global or per interface basis.

For the required *number* argument, specify a limit on the number of IGMP membership reports that can be cached for the specified interface. The range is from 1 to 64000.

Use the optional **except** *access-list* keyword and argument to prevent groups or channels from being counted against the interface limit. A standard or an extended ACL can be specified.

- A standard ACL can be used to define the (*, G) state to be excluded from the limit on an interface.
- An extended ACLs can be used to define the (S, G) state to be excluded from the limit on an interface. An extended ACL also can be used to define the (*, G) state to be excluded from the limit on an interface, by specifying 0.0.0.0 for the source address and source wildcard—referred to as (0, G)—in the permit or deny statements that compose the extended access list.

Use the **ip igmp limit** (global) command to configure a global limit on the number of mroute states created as a result of IGMP membership reports (IGMP joins).

Note When configuring IGMP state limiters, you can only configure one global limit on a router and one limit per interface.

The mechanics of IGMP state limiters are as follows:

- Each time a router receives an IGMP membership report for a particular group or channel, the Cisco IOS software checks to see if either the limit for the global IGMP state limiter or the limit for the per interface IGMP state limiter has been reached.
  - If only a global IGMP state limiter has been configured and the limit has not been reached, IGMP membership reports are honored. When the configured limit has been reached, subsequent IGMP membership reports are then ignored (dropped) and a warning message in one of the following formats is generated:

    ```
    %IGMP-6-IGMP_GROUP_LIMIT: IGMP limit exceeded for <group (*, group address)> on
    <interface type number> by host <ip address>
    ```
    or
    ```
    %IGMP-6-IGMP_CHANNEL_LIMIT: IGMP limit exceeded for <channel (source address,
    group address)> on <interface type number> by host <ip address>
    ```

  - If only per interface IGMP state limiters are configured, then each limit is only counted against the interface on which it was configured.
  - If both a global IGMP state limiter and per interface IGMP state limiters are configured, the limits configured for the per interface IGMP state limiters are still enforced but are constrained by the global limit.

- If a per interface IGMP state limiter has been configured using the **ip igmp limit** (interface) command, the Cisco IOS software also checks to see if an ACL is specified (with the optional **except** keyword and *access-list* argument) to prevent groups or channels from being counted against the interface limit.
  - If an ACL has been configured and the group or channel in the IGMP membership report matches, then the state for the IGMP membership is counted against the global limit and not the interface limit.
  - If no ACL has been configured, the per interface IGMP state limiter accounts for all IGMP membership reports that do not exceed the configured limit.

Examples

The following example shows how configure a per interface limiter that limits the number of mroute states created as result of IGMP membership reports on Gigabit Ethernet interface 0/1 to 100:

```
interface GigabitEthernet 0/1
 ip igmp limit 100
```

Related Commands

Command	Description
ip igmp limit (global)	Globally limits the number of IGMP states resulting from IGMP membership reports (IGMP joins).
show ip igmp groups	Displays the multicast groups with receivers that are directly connected to the router and that were learned through IGMP.
show ip igmp interface	Displays information about the status and configuration of IGMP and multicast routing on interfaces.

ip igmp mroute-proxy

To enable Internet Group Management Protocol (IGMP) report forwarding of proxied (*, G) multicast static route (mroute) entries, use the **ip igmp mroute-proxy** command in interface configuration mode. To disable this service, use the **no** form of this command.

ip igmp mroute-proxy *interface-type interface-number*

no ip igmp mroute-proxy *interface-type interface-number*

Syntax Description

interface-type interface-number	Interface type and number.

Defaults

The command is disabled.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

When used with the **ip igmp proxy-service** interface command, this command enables forwarding of IGMP reports to a proxy service interface for all (*, G) forwarding entries for this interface in the multicast forwarding table.

Examples

The following example shows how to configure the **ip igmp mroute-proxy** command on Ethernet interface 1 to request that IGMP reports be sent to loopback interface 0 for all groups in the mroute table that are forwarded to Ethernet interface 1. This example also shows how to configure the **ip igmp proxy-service** command on loopback interface 0 to enable the forwarding of IGMP reports out the interface for all groups on interfaces registered through the **ip igmp mroute-proxy** command.

```
interface loopback 0
ip address 10.7.1.1 255.255.255.0
ip pim dense-mode
ip igmp helper-address udl ethernet 0
ip igmp proxy-service
!
interface ethernet 0
```

```
ip address 10.2.1.1 255.255.255.0
ip pim dense-mode
ip igmp unidirectional link
!
interface ethernet 1
ip address 10.1.1.1 255.255.255.0
ip pim sparse-mode
ip igmp mroute-proxy loopback 0
```

Related Commands

Command	Description
ip igmp proxy-service	Enables the mroute proxy service.
ip igmp unidirectional-link	Configures an interface to be unidirectional and enables it for IGMP UDLR.

ip igmp proxy-service

To enable the mroute proxy service, use the **ip igmp proxy-service** command in interface configuration mode. To disable forwarding, use the **no** form of this command.

ip igmp proxy-service

no ip igmp proxy-service

Syntax Description

This command has no arguments or keywords.

Defaults

The command is disabled.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Based on the Internet Group Management Protocol (IGMP) query interval, the router periodically checks the multicast static route (mroute) table for (*, G) forwarding entries that match interfaces configured with the **ip igmp mroute-proxy** command. Where there is a match, one IGMP report is created and received on this interface. The **ip igmp proxy-service** command is intended to be used with the **ip igmp helper-address (UDL)** command, in which case the IGMP report would be forwarded to an upstream router.

Examples

The following example shows how to configure the **ip igmp mroute-proxy** command on Ethernet interface 1 to request that IGMP reports be sent to loopback interface 0 for all groups in the mroute table that are forwarded to Ethernet interface 1. This example also shows how to configure the **ip igmp proxy-service** command on loopback interface 0 to enable the forwarding of IGMP reports out the interface for all groups on interfaces registered through the **ip igmp mroute-proxy** command.

```
interface loopback 0
ip address 10.7.1.1 255.255.255.0
ip pim dense-mode
ip igmp helper-address udl ethernet 0
ip igmp proxy-service
!
```

```
interface ethernet 0
ip address 10.2.1.1 255.255.255.0
ip pim dense-mode
ip igmp unidirectional link
!
interface ethernet 1
ip address 10.1.1.1 255.255.255.0
ip pim sparse-mode
ip igmp mroute-proxy loopback 0
```

Related Commands

Command	Description
ip igmp helper-address (UDL)	Configures IGMP helpering as required for IGMP UDLR.
ip igmp mroute-proxy	Enables IGMP report forwarding of proxied (*, G) mroute entries.
ip igmp unidirectional-link	Configures an interface to be unidirectional and enables it for IGMP UDLR.

ip igmp querier-timeout

Note We recommend that you do not change the default IGMP querier timeout period; however, if the query interval is modified using the **ip igmp query-interval** command, the timeout period will automatically adjust to two times the query interval.

To configure the timeout period before the router triggers Internet Group Management Protocol (IGMP) querier reelection for the interface, use the **ip igmp querier-timeout** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip igmp querier-timeout *seconds*

no ip igmp querier-timeout

Syntax Description

seconds	Number of seconds that router waits before the router triggers IGMP querier reelection for the interface. The range is from 60 to 300.

Command Default

The default timeout period is two times the IGMP query interval. By default, the query interval is 60 seconds, so the default timeout period is 120 seconds.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Use the **ip igmp querier-timeout** command to configure the timeout period before the router triggers IGMP querier reelection for the interface. The IGMP querier timeout period applies to routers on the subnet that are not currently acting as the IGMP querier.

Note We recommend that you use the default IGMP query interval and IGMP querier timeout period.

By default, a router on the subnet that is not currently acting as the querier waits twice the query interval specified by the **ip igmp query-interval** command, after which, if it has heard no queries, it triggers IGMP reelection. The router with the lowest IP address on the subnet is elected the IGMP querier. By default, the **ip igmp query-interval** defaults to 60 seconds, which means the **ip igmp querier-timeout** defaults to 120 seconds.

If the IGMP query interval and IGMP querier timeout period are modified on an interface, the following conditions apply:

- By default, if the query interval is modified using the **ip igmp query-interval** command, the timeout period will automatically adjust to two times the query interval; the adjusted timeout period, however, will *not* be reflected in the interface configuration.
  - To confirm that the timeout period adjusted to two times the modified query interval, you can use the **show ip igmp interface** command; the output for this command displays the IGMP query interval and timeout period being used for the interface.
  - If you would like to have the ability to view the modified IGMP querier timeout period in the interface configuration, you can manually configure the timeout period using the **ip igmp querier-timeout** command. For the *seconds* argument, specify a value that is two times the modified query interval.
- If the timeout period is modified using the **ip igmp querier-timeout** command, the query interval will *not* automatically adjust to be in proportion with the modified timeout period (half of the timeout period), so it is possible to override the default timeout period of two times the query interval.

Note If the timeout period is modified for the **ip igmp querier-timeout** command, we recommend that it be changed in proportion to the IGMP query interval.

- If the IGMP query interval is modified, the modified query interval must be greater than the IGMP maximum query response time (which is controlled using the **ip igmp max-response-time** command).

Examples

The following example shows how to configure the router to wait 240 seconds from the time it received the last query before it triggers the IGMP election process. In this example, the IGMP timeout period is modified in proportion to the IGMP query interval.

Note By default, when the query interval is modified, the timeout period will automatically adjust to two times the query interval. The adjusted timeout period, however, will not be reflected in the respective interface configuration. For this case, to have the ability to view the modified timeout period in the configuration, you can manually configure the **ip igmp querier-timeout** command in proportion to the modified query interval.

```
interface GigabitEthernet1/1
 ip igmp query-interval 120
 ip igmp querier-timeout 240
```

The following example shows how to configure the router to wait 250 seconds from the time it received the last query before it triggers the IGMP election process. In this example, the default IGMP query interval of 60 seconds is being used on the interface because it has not been modified (using the **ip igmp**

query-interval command). When the timeout period is modified, the query interval will not automatically adjust to be in proportion to the timeout period (half of the timeout period), so in this example the default timeout period of two times the query interval is overridden.

Note If the timeout period is modified for the **ip igmp querier-timeout** command, we recommend that it be changed in proportion to the IGMP query interval.

```
interface GigabitEthernet0/1
 ip igmp querier-timeout 250
```

Related Commands

Command	Description
ip igmp max-response-time	Configures the maximum response time advertised in IGMP queries.
ip igmp query-interval	Configures the frequency at which the IGMP querier sends IGMP host-query messages from an interface.
show ip igmp interface	Displays information about the status and configuration of IGMP and multicast routing on interfaces.

ip igmp query-interval

Note We recommend that you do not change the default IGMP query interval.

To configure the frequency at which the IGMP querier sends Internet Group Management Protocol (IGMP) host-query messages from an interface, use the **ip igmp query-interval** command in interface configuration mode. To restore the default IGMP query interval, use the **no** form of this command.

ip igmp query-interval *seconds*

no ip igmp query-interval

Syntax Description

seconds	Frequency, in seconds, at which the router sends IGMP query messages from the interface. The range is from 1 to 18000. The default is 60.

Command Default

The default IGMP query interval is 60 seconds.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
10.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Use the **ip igmp query-interval** command to configure the frequency at which the IGMP querier sends IGMP host-query messages from an interface. The IGMP querier sends query-host messages to discover which multicast groups have members on the attached networks of the router.

Note We recommend that you use the default IGMP query interval and timeout period.

The Cisco IOS software uses a default IGMP query interval of 60 seconds, which is different from the RFC standard default of 125 seconds. Using a lower default IGMP query interval of 60 seconds allows routers to stop forwarding traffic faster when a member crashes without sending leaves (in IGMPv2 or IGMPv3 environment), or if using IGMPv1: 3 * 60 seconds versus 3 * 125 seconds.

If a lower version IGMP-enabled interface (that is, an interface running IGMPv1 or v2) receives a higher version IGMP query (IGMPv3) with a different query interval, the following events will occur:

- An error message in the following format will be displayed:

```
%IGMP-3-QUERY_INT_MISMATCH: Received a non-matching query interval <interval in
seconds>, from querier address <ip-address>
```

- If the query interval on the lower version IGMP-enabled interface has not been modified, the default query interval will appear under its respective interface configuration.
- If the query interval on the IGMP-enabled interface has been modified, the configured query interval will be updated to show the configured query interval under its respective interface configuration.

Note The **show ip igmp interface** command displays both the configured query interval and the received query interval in its output.

Be careful when increasing the query interval in an environment with IGMPv2 routers (the default) and Layer 2 (L2) snooping switches: An IGMPv2 snooping switch needs to know the query interval of the IGMP querier, because it is not signaled in IGMP messages (in IGMPv3 it is). The IGMP snooping switch will time out membership state based on what it thinks the query interval is. If the querier uses a query interval larger than what the IGMP snooping switch assumes, then this may lead to an unexpected timeout of multicast state on the IGMP snooping switch.

Note The default IGMP query interval on Cisco routers of 60 seconds is never an issue with Cisco IGMP snooping switches because they either assume a 60 second-interval or will try to determine the query interval by measuring the interval between IGMP general queries.

Be careful decreasing the query interval because it increases the processing load on the router (total number of IGMP reports received over a period of time)—especially on routers with a large number of interfaces and hosts connected to it (for example, a broadband aggregation router).

If the IGMP query interval and IGMP querier timeout period are modified on an interface, the following conditions apply:

- By default, if the query interval is modified using the **ip igmp query-interval** command, the timeout period will automatically adjust to two times the query interval; the adjusted timeout period, however, will *not* be reflected in the interface configuration.
  - To confirm that the timeout period adjusted to two times the modified query interval, you can use the **show ip igmp interface** command; the output for this command displays the IGMP query interval and timeout period being used for the interface.
  - If you would like to have the ability to view the modified IGMP querier timeout period in the interface configuration, you can manually configure the timeout period using the **ip igmp querier-timeout** command. For the *seconds* argument, specify a value that is two times the modified query interval.
- If the timeout period is modified using the **ip igmp querier-timeout** command, the query interval will *not* automatically adjust to be in proportion with the modified timeout period (half of the timeout period), so it is possible to override the default timeout period of two times the query interval.

Note If the timeout period is modified for the **ip igmp querier-timeout** command, we recommend that it be changed in proportion to the IGMP query interval.

- If the IGMP query interval is modified, the modified query interval must be greater than the IGMP maximum query response time (which is controlled using the **ip igmp max-response-time** command).

Examples

The following example shows how to increase the frequency at which the IGMP querier sends IGMP host-query messages to 120 seconds. The IGMP timeout period will automatically adjust to two times the configured query interval (240 seconds, in this example).

```
interface tunnel 0
 ip igmp query-interval 120
```

Related Commands

Command	Description
ip igmp max-response-time	Configures the maximum response time advertised in IGMP queries.
ip igmp querier-timeout	Configures the timeout period before the router triggers IGMP querier reelection for the interface.
show ip igmp interface	Displays information about the status and configuration of IGMP and multicast routing on interfaces.

ip igmp query-max-response-time

To configure the maximum response time advertised in Internet Group Management Protocol (IGMP) queries, use the **ip igmp query-max-response-time** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip igmp query-max-response-time *seconds*

no ip igmp query-max-response-time

Syntax Description

seconds	Maximum response time, in seconds, advertised in IGMP queries. The default value is 10 seconds.

Defaults

seconds: 10 seconds

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

This command is valid only when IGMP Version 2 is running.

This command controls the period during which the responder can respond to an IGMP query message before the router deletes the group.

Examples

The following example configures a maximum response time of 8 seconds:

```
ip igmp query-max-response-time 8
```

Related Commands

Command	Description
ip pim query-interval	Configures the frequency of PIM router query messages.
show ip igmp groups	Displays the multicast groups that are directly connected to the router and that were learned through IGMP.

ip igmp snooping

To globally enable Internet Group Management Protocol (IGMP) snooping, use the **ip igmp snooping** command in global configuration mode. To disable IGMP snooping, use the **no** form of this command.

ip igmp snooping

no ip igmp snooping

Syntax Description

This command has no arguments or keywords.

Defaults

By default, IGMP snooping is globally enabled.

Cisco 7600 Series

IGMP snooping is not configured on multicast routers.

Command Modes

Global configuration

Cisco 7600 Series

Interface configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to 12.2(17d)SXB.

Usage Guidelines

When IGMP snooping is globally enabled, it enables IGMP snooping on all the existing VLAN interfaces. When IGMP snooping is globally disabled, it disables IGMP snooping on all the existing VLAN interfaces.

Use the **show ip igmp snooping** privileged EXEC command to verify your IGMP settings.

The configuration is saved in NVRAM.

Cisco 7600 Series

Before you can enable IGMP snooping on the Cisco 7600 series routers, you must configure the VLAN interface for multicast routing.

Examples

The following example shows how to globally enable IGMP snooping:

```
Router(config)# ip igmp snooping
```

The following example shows how to globally disable IGMP snooping:

```
Router(config)# no ip igmp snooping
```

Related Commands

Command	Description
ip igmp snooping fast-leave	Enables the IGMPv3-snooping fast-leave processing.
ip igmp snooping vlan	Enables IGMP snooping on a VLAN interface.
ip igmp snooping vlan immediate-leave	Enables IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
show ip igmp snooping	Displays the IGMP snooping configuration.

ip igmp snooping access-group

To configure a Internet Group Management Protocol (IGMP) group access group, use the **ip igmp snooping access-group** command in interface configuration mode. To remove the IGMP group access group, use the **no** form of this command.

ip igmp snooping access-group {*acl-num* | *acl-name*} [**vlan** *vlan-id*]

no ip igmp snooping access-group {*acl-num* | *acl-name*} [**vlan** *vlan-id*]

Syntax Description

acl-num	Number of the Access Control List (ACL); valid values are from 1 to 199.
acl-name	Name of the ACL.
vlan *vlan-id*	(Optional) Specifies the Layer 2 VLAN that packets arrive on if the switch port is a trunk port and applies the filter to that VLAN.

Command Default

This command has no default settings.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

Internet group management protocol (IGMP) filtering allows you to configure filters on a per-port basis, a per-Switched Virtual Interface (SVI) basis, or both.

IGMP filtering is supported for IPv4 only.

You can list several groups or channels if you configure multiple access control entries in the access control list. Depending on the ACL configuration of either the **permit** or **deny** configuration, the corresponding group or channel is allowed or denied. The ACL you specify can be a simple or an extended ACL.

This command can be entered on the following basis:

- Per-SVI basis.
- Per-Layer 2-switchport basis.
- Per-Layer 2-VLAN basis. The **vlan** keyword allows you to apply the filter only to the IGMP packets arriving on the specified Layer 2 VLAN if the switch port is a trunk port.
- Per-SVI basis as a default filter for all switch ports in access mode under that SVI and for all trunk ports that carry the corresponding VLAN for that VLAN only.

- Per-switch port basis as follows:
  - If the switch port is in access mode, this filter overrides any default SVI filter.
  - If the switch port is in trunk mode, this filter acts as a default for all VLANs on that trunk and overrides any default SVI filter.
- Per-Layer 2-VLAN basis. The filter applies only if the switch port is in trunk mode, and overrides any trunk default filter.

Examples

This example shows how to configure an IGMP group access group:

```
Router(config-if)# ip igmp snooping access-group 44
```

This example shows how to configure an IGMP group access group and apply the filter only to the IGMP packets arriving on the specified Layer 2 VLAN if the switch port is a trunk port:

```
Router(config-if)# no ip igmp snooping access-group 44 vlan 244
```

Related Commands

Command	Description
ip igmp snooping limit	Limits the number of IGMP groups or channels allowed on an interface.
ip igmp snooping minimum-version	Filters on the IGMP protocol.
show ip igmp snooping filter	Displays the IGMP filtering rules.

ip igmp snooping explicit-tracking

To enable explicit host tracking, use the **ip igmp snooping explicit-tracking** command in interface configuration mode. To disable the explicit host tracking, use the **no** form of this command.

ip igmp snooping explicit-tracking

no ip igmp snooping explicit-tracking

Syntax Description

This command has no arguments or keywords.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Explicit host tracking is supported only with IGMPv3 hosts.

When you enable explicit host tracking and the Cisco 7600 series router is working in proxy-reporting mode, the router may not be able to track all the hosts that are behind a VLAN interface. In proxy-reporting mode, the Cisco 7600 series router forwards only the first report for a channel to the router and suppresses all other reports for the same channel.

With IGMPv3 proxy reporting, the Cisco 7600 series router does proxy reporting for unsolicited reports and reports that are received in the general query interval.

Proxy reporting is turned on by default. When you disable proxy reporting, the Cisco 7600 series router works in transparent mode and updates the IGMP snooping database as it receives reports and forwards this information to the upstream router. The router can then explicitly track all reporting hosts.

Disabling explicit tracking disables fast-leave processing and proxy reporting.

IGMPv3 supports explicit host tracking of membership information on any port. The explicit host-tracking database is used for fast-leave processing for IGMPv3 hosts, proxy reporting, and statistics collection. When you enable explicit host tracking on a VLAN, the IGMP snooping software processes the IGMPv3 report that it receives from a host and builds an explicit host-tracking database that contains the following information:

- The port that is connected to the host.
- The channels that are reported by the host.
- The filter mode for each group that is reported by the host.

- The list of sources for each group that is reported by the hosts.
- The router filter mode of each group.
- For each group, the list of hosts that request the source.

Examples

This example shows how to enable IGMPv3-explicit host tracking:

```
Router(config-if)# ip igmp snooping explicit-tracking
```

This example shows how to disable IGMPv3-explicit host tracking:

```
Router(config-if)# no ip igmp snooping explicit-tracking
```

Related Commands

Command	Description
ip igmp snooping limit track	Limits the size of the explicit-tracking database.
show ip igmp snooping explicit-tracking	Displays the information about the explicit host-tracking status for IGMPv3 hosts.

ip igmp snooping fast-leave

To enable the IGMPv3-snooping fast-leave processing, use the **ip igmp snooping fast-leave** command in interface configuration mode. To disable fast-leave processing, use the **no** form of this command.

ip igmp snooping fast-leave

no ip igmp snooping fast-leave

Syntax Description

This command has no arguments or keywords.

Defaults

The defaults are as follows:

- IGMP version 2—Disabled
- IGMP version 3—Enabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

Enter this command in VLAN interface configuration mode only.

Note Fast-leave processing is enabled by default. To disable fast-leave processing, you must enter the **no ip igmp snooping fast-leave** command to disable fast-leave processing.

You should use the IGMPv3-snooping fast-leave processing when there is a single receiver for the MAC group for a specific VLAN.

Examples

This example shows how to enable IGMPv3-snooping fast-leave processing:

```
Router(config-if)# ip igmp snooping fast-leave
```

This example shows how to disable IGMPv3-snooping fast-leave processing:

```
Router(config-if)# no ip igmp snooping fast-leave
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
ip igmp snooping explicit-tracking	Enables explicit host tracking.
show ip igmp interface	Displays the information about the IGMP-interface status and configuration.
show mac-address-table	Displays the information about the MAC-address table.

ip igmp snooping flooding

To configure periodic flooding of multicast packets, use the **ip igmp snooping flooding** command in interface configuration mode. To disable periodic flooding, use the **no** form of this command.

ip igmp snooping flooding [**timer** *seconds*]

no ip igmp snooping flooding

Syntax Description

timer *seconds*	(Optional) Specifies the interval between flooding in a 24-hour period for source-only entries; valid values are from 0 to 86400 seconds.

Defaults

The defaults are as follows:

- Disabled.
- If enabled, *seconds* is 600 seconds (10 minutes).

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

This command is supported on source-only VLANs.

You can enter **0** seconds to disable flooding. If you enter a maximum of 86400 seconds, flooding would occur once every 24 hours.

Examples

This example shows how to specify the interval between flooding in a 24-hour period:

```
Router(config-if)# ip igmp snooping flooding timer 300
```

ip igmp snooping l2-entry-limit

To configure the maximum number of Layer 2 entries that can be created by the Cisco 7600 series router, use the **ip igmp snooping l2-entry-limit** command in global configuration mode.

ip igmp snooping l2-entry-limit *max-entries*

Syntax Description

max-entries	Maximum number of Layer 2 entries that can be created by the Cisco 7600 series router; valid values are from 1 to 100000.

Defaults

15488 Layer 2 entries

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to configure the maximum number of Layer 2 entries that can be created by the Cisco 7600 series router:

```
Router(config)# ip igmp snooping l2-entry-limit 25000
```

Related Commands

Command	Description
show ip igmp interface	Displays the information about the IGMP-interface status and configuration.

ip igmp snooping last-member-query-interval

To configure the last member query interval for IGMP snooping, use the **ip igmp snooping last-member-query-interval** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

ip igmp snooping last-member-query-interval *interval*

no ip igmp snooping last-member-query-interval

Syntax Description

interval	Interval for the last member query; valid values are from 100 to 999 milliseconds in multiples of 100 milliseconds.

Defaults

1000 milliseconds (1 second); see the "Usage Guidelines" section for additional information.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When a multicast host leaves a group, the host sends an IGMP leave. To check if this host is the last to leave the group, an IGMP query is sent out when the leave is seen and a timer is started. If no reports are received before the timer expires, the group record is deleted.

The *interval* is the actual time that the Cisco 7600 series router waits for a response for the group-specific query.

If you enter an interval that is not a multiple of 100, the interval is rounded to the next lowest multiple of 100. For example, if you enter 999, the interval is rounded down to 900 milliseconds.

If you enable IGMP fast-leave processing and you enter the **no igmp snooping last-member-query-interval** command, the interval is set to 0 seconds; fast-leave processing always assumes higher priority.

Even though the valid interval range is 100 to 1000 milliseconds, you cannot enter a value of **1000**. If you want this value, you must enter the **no ip igmp snooping last-member-query-interval** command and return to the default value (1000 milliseconds).

Examples

This example shows how to configure the last-member-query-interval to 200 milliseconds:

```
Router(config-if)# ip igmp snooping last-member-query-interval 200
```

Related Commands

Command	Description
ip igmp snooping fast-leave	Enables the IGMP v3-snooping fast-leave processing.
show ip igmp interface	Displays the information about the IGMP-interface status and configuration.

ip igmp snooping limit

To limit the number of Internet Group Management Protocol (IGMP) groups or channels allowed on an interface, use the **ip igmp snooping limit** command in interface configuration mode. To remove the IGMP group access group, use the **no** form of this command.

ip igmp snooping limit *num* [**except** {*acl-num* | *acl-name*}] [**vlan** *vlan-id*]

no ip igmp snooping limit *num* [**except** {*acl-num* | *acl-name*}] [**vlan** *vlan-id*]

Syntax Description

num	Maximum number of groups or channels allowed on this interface; valid values are 1 to 64000.
except *acl-num*	(Optional) Specifies the group to exempt from the limit; valid values are from 1 to 199.
except *acl-name*	(Optional) Specifies the name of the Access Control List (ACL) to exempt from the limit.
vlan *vlan-id*	(Optional) Specifies the Layer 2 VLAN that packets arrive on if the switch port is a trunk port and applies the filter to that VLAN.

Command Default

This command has no default settings.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

Note If joins are received for (*,G1) and (S1,G1) on the same interface, these joins are counted as two separate joins. If the limit on an interface has been set to two, and the joins are received for (*,G1) and (S1,G1), all other joins (for groups/channels different from these two) are discarded.

IGMP filtering allows you to configure filters on a per-port basis, a per-Switched Virtual Interface (SVI) basis, or both.

IGMP filtering is supported for IPv4 only.

You can enter this command based on the following:

- Per-SVI basis.
- Per-Layer 2-switchport basis.
- Per-Layer 2-VLAN basis. The **vlan** keyword allows you to apply the filter only to the IGMP packets arriving on the specified Layer 2 VLAN if the switch port is a trunk port.

- Per-SVI basis as a default filter for all switch ports in access mode under that SVI and for all trunk ports that carry the corresponding VLAN for that VLAN only.
- Per-switch port basis as follows:
  - If the switch port is in access mode, this filter overrides any default SVI filter.
  - If the switch port is in trunk mode, this filter acts as a default for all VLANs on that trunk and overrides any default SVI filter.
- Per-Layer 2-VLAN basis. The filter applies only if the switch port is in trunk mode, and overrides any trunk default filter.

Examples

This example shows how to limit the number of IGMP groups or channels allowed on an interface:

```
Router(config-if)# ip igmp snooping limit 4400
```

This example shows how to limit the number of IGMP groups or channels allowed on an interface except for a specific ACL:

```
Router(config-if)# ip igmp snooping limit 1300 except test1
```

Related Commands

Command	Description
ip igmp snooping access-group	Configures an IGMP group access group.
ip igmp snooping minimum-version	Filters on the IGMP protocol.
show ip igmp snooping filter	Displays the IGMP filtering rules.

ip igmp snooping limit track

To limit the size of the explicit-tracking database, use the **ip igmp snooping limit track** command in global configuration mode. To return to the default settings, use the **no** form of this command.

ip igmp snooping limit track *max-entries*

no ip igmp snooping limit track

Syntax Description

max-entries	Maximum number of entries in the explicit-tracking database; valid values are from 0 to 128000 entries.

Defaults

max-entries is 32000.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Each entry in the explicit-tracking database is identified by the source IP, group IP, port, VLAN, and reporter IP.

When you set the *max-entries* to 0, explicit-tracking is disabled.

When the explicit-tracking database exceeds the configured *max-entries*, a syslog message is generated.

When you reduce the *max-entries*, the explicit-tracking database does not decrease in size immediately. The explicit-tracking database gradually shrinks as reporters time out.

Examples

This example shows how to configure the maximum number of entries in the explicit-tracking database:

```
Router(config)# ip igmp snooping limit track 20000
```

Related Commands

Command	Description
ip igmp snooping explicit-tracking	Enables explicit host tracking.
show ip igmp snooping explicit-tracking vlan	Displays information about the explicit host-tracking for IGMPv3 hosts.

ip igmp snooping minimum-version

To filter on the Internet Group Management Protocol (IGMP) protocol, use the **ip igmp snooping minimum-version** command in interface configuration mode. To stop filtering on the IGMP protocol, use the **no** form of this command.

ip igmp snooping minimum-version {**2** | **3**}

no ip igmp snooping minimum-version {**2** | **3**}

Syntax Description

2	Filters out all IGMPv1 hosts.
3	Filters out all IGMPv1 and IGMPv2 hosts.

Command Default

This command has no default settings.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

This command is allowed on a per-switched virtual interface (SVI) basis only.

Examples

This example shows how to filter out all IGMPv1 hosts:

```
Router(config-if)# ip igmp snooping minimum-version 2
```

Related Commands

Command	Description
ip igmp snooping access-group	Configures an IGMP group access group.
ip igmp snooping limit	Limits the number of IGMP groups or channels allowed on an interface.
show ip igmp snooping filter	Displays the IGMP filtering rules.

ip igmp snooping mrouter

To configure a Layer 2 port as a multicast router port, use the **ip igmp snooping mrouter** command in interface configuration mode. To remove the configuration, use the **no** form of this command.

ip igmp snooping mrouter {**interface** *type number* | **port-channel** *number* | **learn** {**cgmp** | **pim-dvmrp**}}

no ip igmp snooping mrouter {**interface** *type number* | **port-channel** *number* | **learn** {**cgmp** | **pim-dvmrp**}}

Syntax Description

interface	Specifies the next-hop interface to the multicast router.
type	Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, and **tengigabitethernet**. See the "Usage Guidelines" section for additional valid values.
number	Module and port number; see the "Usage Guidelines" section for valid values.
port-channel *number*	Specifies the port-channel number; valid values are a maximum of 64 values ranging from 1 to 256.
learn	Specifies the learning method for the multicast router.
cgmp	Specifies the snooping Cisco Group Management Protocol (CGMP) packets for the multicast router.
pim-dvmrp	Specifies the snooping Protocol Independent Multicast-Distance Vector Multicast Routing Protocol (PIM-DVMRP) packets for the multicast router.

Command Default

Specifies the snooping PIM-DVMRP packets for the multicast router.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB. The **learn cgmp** and **learn pim-dvmrp** options have been superseded. Multicast router ports will default to auto-learn through PIM or IGMP packets.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(24)T	This command was integrated into a release earlier than Cisco IOS Release 12.4(24)T.

Usage Guidelines

The valid values for *interface* include the **ge-wan**, **atm**, and **pos** keywords that are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Enter this command in VLAN interface configuration mode only.

The interface to the router must be in the VLAN where you are entering the command, the interface must be administratively up, and the line protocol must be up.

The *number* argument designates the module and port number. Valid values for *number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The CGMP learning method can decrease control traffic.

The learning method that you configure is saved in NVRAM.

Static connections to multicast routers are supported only on switch ports.

Examples

The following example shows how to specify the next-hop interface to the multicast router:

```
Router(config-if)# ip igmp snooping mrouter interface fastethernet 5/6
```

The following example shows how to specify the learning method for the multicast router:

```
Router(config-if)# ip igmp snooping mrouter learn cgmp
```

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping.
ip igmp snooping fast-leave	Enables the IGMPv3-snooping fast-leave processing.
show ip igmp snooping mrouter	Displays the information about the dynamically learned and manually configured multicast router interfaces.

ip igmp snooping querier

To enable multicast support within a subnet when no multicast routing protocol is configured in the VLAN or subnet, use the **ip igmp snooping querier** command in interface configuration mode. To disable multicast support within a subnet when no multicast routing protocol is configured, use the **no** form of this command.

ip igmp snooping querier

no ip igmp snooping querier

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Enter this command in VLAN interface configuration mode only.

You enable IGMP snooping on the Cisco 7600 series router, and disable PIM on the VLAN.

Configure the VLAN in global configuration mode.

Configure an IP address on the VLAN interface. When enabled, the IGMP-snooping querier uses the IP address as the query source address. If no IP address is configured on the VLAN interface, the IGMP-snooping querier does not start. The IGMP-snooping querier disables itself if you clear the IP address. When enabled, the IGMP-snooping querier restarts if you configure an IP address.

The IGMP-snooping querier supports IGMPv2.

When enabled, the IGMP-snooping querier does the following:

- Does not start if it detects IGMP traffic from a multicast router.
- Starts after 60 seconds when no IGMP traffic is detected from a multicast router.
- Disables itself if it detects IGMP traffic from a multicast router.

QoS does not support IGMP packets when IGMP snooping is enabled.

You can enable the IGMP-snooping querier on all the Cisco 7600 series routers in the VLAN. One Cisco 7600 series router is elected as the querier.

If multicast routers are not present on the VLAN or subnet, the Cisco 7600 series router becomes the IGMP querier for the VLAN when you enable the IGMP-snooping querier.

If you disable the IGMP-snooping querier, IGMP snooping functions only when you configure PIM in the subnet.

You can enter the **ip igmp snooping querier** command at any time, but the IGMP-snooping querier starts only when no other multicast routers are present in the VLAN or subnet.

You can use this command as an alternative to configuring PIM in a subnet; use this command when the multicast traffic does not need to be routed but you would like support for IGMP snooping on Layer 2 interfaces in your network.

Examples

This example shows how to enable the IGMP-snooping querier on the VLAN:

```
Router(config-if)# ip igmp snooping querier
```

Related Commands

Command	Description
show ip igmp snooping mrouter	Displays the information about the dynamically learned and manually configured multicast router interfaces.

ip igmp snooping rate

To set the rate limit for IGMP-snooping packets, use the **ip igmp snooping rate** command in global configuration mode. To disable the software rate limiting, use the **no** form of this command.

ip igmp snooping rate *pps*

no ip igmp snooping rate

Syntax Description

pps	Rate limit of incoming IGMP messages; valid values are from 100 to 6000 packets per second.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to enable software rate limiting:

```
Router(config)# ip igmp snooping rate 500
```

This example shows how to disable software rate limiting:

```
Router(config)# no ip igmp snooping rate
```

Related Commands

Command	Description
show ip igmp snooping rate-limit	Displays the information about the IGMP-snooping rate limit.

ip igmp snooping report-suppression

To turn on IP IGMP snooping report suppression, use the **ip igmp snooping report-suppression** command in interface configuration mode. To turn off report suppression, use the **no** form of this command.

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SXF	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you enable report suppression for all host reports responding to a general query, IP IGMP snooping forwards the first report only and suppresses the remaining reports to constrain IGMP traffic to the multicast router.

Examples

This example shows how to enable IP IGMP snooping report suppression:

```
Router(config)# ip igmp snooping report-suppression
```

This example shows how to disableIP IGMP snooping report suppression:

```
Router(config)# no ip igmp snooping report-suppression
```

ip igmp snooping source-only-learning age-timer

To flood multicast packets periodically to a Layer 2 segment that has only multicast sources and no receivers connected to it, use the **ip igmp snooping source-only-learning age-timer** command in global configuration mode. To return to the default settings, use the **no** form of this command.

ip igmp snooping source-only-learning age-timer *seconds*

no ip igmp snooping source-only-learning age-timer

Syntax Description

seconds	Source-only entries age timer value in seconds; valid values are from 0 to 86400 seconds.

Defaults

seconds is 600 seconds (10 minutes).

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE2	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

There are two source-only timers that run in an alternating fashion; the source_only_age_timer and the source_only_delete_timer. The value that you configure by entering the **ip igmp snooping source-only-learning age-timer** command sets the source_only_age_timer. The source_only_delete_timer has a fixed, nonconfigurable value of 5 minutes (300 seconds).

The expiration of one timer starts the other timer. At any time, only one timer is running.

Setting the age-timer to 0 stops the flooding in the source-only VLAN.

Note Setting the age-timer to a nonzero value causes flooding to occur every x (configured value) + 5 minutes (source_only_delete_timer) interval.

Examples

This example shows how to flood multicast packets periodically:

```
Router(config)# ip igmp snooping source-only-learning age-timer 300
```

This example shows how to return to the default settings:

```
Router(config)# no ip igmp snooping source-only-learning age-timer
```

ip igmp snooping ssm-safe-reporting

To enable SSM-safe reporting in the presence of a mix of IGMPv2 and IGMPv3 hosts, use the **ip igmp snooping ssm-safe-reporting** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

ip igmp snooping ssm-safe-reporting

no ip igmp snooping ssm-safe-reporting

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXE	This command was deprecated.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

When you configure SSM-safe reporting, IGMPv3 becomes the group mode in the Cisco 7600 series router or the router even in the presence of IGMPv2 hosts.

A Layer-3 SVI must be configured for any Layer 2 VLAN that supports mixed-IGMPv3 receivers.

Within an SSM group, an IGMPv2 host does not receive the requested traffic until an IGMPv3 host that is connected to the same Cisco 7600 series router is receiving the same group traffic. When the last IGMPv3 host leaves the group, the IGMPv2 host stops receiving traffic for that group.

Examples

This example shows how to enable SSM-safe reporting:

```
Router(config-if)# ip igmp snooping ssm-safe-reporting
```

ip igmp snooping vlan

To enable Internet Group Management Protocol (IGMP) snooping on a specific VLAN, use the **ip igmp snooping vlan** command in global configuration mode. To disable IGMP snooping on a VLAN interface, use the **no** form of this command.

ip igmp snooping vlan *vlan-id*

no ip igmp snooping vlan *vlan-id*

Syntax Description

vlan-id	VLAN ID value. The range is from 1 to 1001. Do not enter leading zeroes.

Defaults

By default, IGMP snooping is enabled when each VLAN is created.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

This command automatically configures the VLAN if it is not already configured. The configuration is saved in NVRAM.

Examples

The following example shows how to enable IGMP snooping on VLAN 2:

```
Router(config)# ip igmp snooping vlan 2
```

The following example shows how to disable IGMP snooping on VLAN 2:

```
Router(config)# no ip igmp snooping vlan 2
```

Related Commands

Command	Description
ip igmp snooping	Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN.
ip igmp snooping vlan immediate-leave	Enables IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.

Command	Description
ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
show ip igmp snooping	Displays the IGMP snooping configuration.

ip igmp snooping vlan immediate-leave

To enable Internet Group Management Protocol (IGMP) Immediate-Leave processing on a VLAN interface, use the **ip igmp snooping vlan immediate-leave** command in global configuration mode. To disable Immediate-Leave processing on the VLAN interface, use the **no** form of this command.

ip igmp snooping vlan *vlan-id* **immediate-leave**

no ip igmp snooping vlan *vlan-id* **immediate-leave**

Syntax Description

vlan-id	VLAN ID value. The range is between 1 to 1001. Do not enter leading zeroes.

Defaults

By default, IGMP Immediate-Leave processing is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

Use Immediate-Leave processing only when there is only one IP multicast receiver present on every port in the VLAN. The Immediate-Leave configuration is saved in NVRAM.

Immediate-Leave processing is supported only with IGMP version 2 hosts.

Examples

The following example shows how to enable IGMP Immediate-Leave processing on VLAN 1:

```
Router(config)# ip igmp snooping vlan 1 immediate-leave
```

The following example shows how to disable IGMP Immediate-Leave processing on VLAN 1:

```
Router(config)# no ip igmp snooping vlan 1 immediate-leave
```

Related Commands

Command	Description
ip igmp snooping	Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.

Command	Description
ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
show ip igmp snooping	Displays the IGMP snooping configuration.
show mac-address-table multicast	Displays the Layer 2 multicast entries for a VLAN.

ip igmp snooping vlan mrouter

To add a multicast router port and to configure the multicast router learning method, use the **ip igmp snooping vlan mrouter** command in global configuration mode. To remove the configuration, use the **no** form of this command.

ip igmp snooping vlan *vlan-id* **mrouter** {**interface** *interface-id* | **learn pim-dvmrp**}

no ip igmp snooping vlan *vlan-id* **mrouter** {**interface** *interface-id* | **learn pim-dvmrp**}

Syntax Description

vlan-id	Specifies the VLAN ID. The range is from 1 to 1001. Do not enter leading zeroes.
interface *interface-id*	Specifies the interface of the member port that is configured to a static router port.
learn pim-dvmrp	Specifies the multicast router snooping PIM-DVMRP packets multicast router learning method.

Defaults

The default learning method is **pim-dvmrp**.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

The configured learning method is saved in NVRAM.

Static connections to multicast routers are supported only on switch ports.

Examples

The following example shows how to configure Fast Ethernet interface 0/6 as a multicast router port:

```
Router(config)# ip igmp snooping vlan 1 mrouter interface fastethernet0/6
```

Related commands

Command	Description
ip igmp snooping	Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN.
ip igmp snooping vlan	Enables IGMP snooping on the VLAN interface.
ip igmp snooping vlan immediate-leave	Configures IGMP Immediate-Leave processing.
ip igmp snooping vlan static	Configures a Layer 2 port as a member of a group.
show ip igmp snooping mrouter	Displays the statically and dynamically learned multicast router ports.

ip igmp snooping vlan static

To add a Layer 2 port as a member of a multicast group, use the **ip igmp snooping vlan static** command in global configuration mode. To remove the configuration, use the **no** form of this command.

ip igmp snooping vlan *vlan-id* **static** *mac-address* **interface** *interface-id*

no ip igmp snooping vlan *vlan-id* **static** *mac-address* **interface** *interface-id*

Syntax Description

vlan-id	Specifies the VLAN ID. The range is 1 to 1001. Do not enter leading zeroes.
mac-address	Specifies the static group MAC address.
interface *interface-id*	Specifies the interface configured to a static router port.

Defaults

No Layer 2 ports are configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

This command is used to statically configure the IP multicast group member ports.

The static ports and groups are saved in NVRAM.

Static connections to multicast routers are supported only on switch ports.

Use the **show mac-address-table multicast** privileged EXEC command to verify your Layer 2 multicast entries.

Examples

The following example shows how to statically configure a host on an interface:

```
Router(config)# ip igmp snooping vlan 1 static 0100.5e02.0203 interface fastethernet0/6
Configuring port FastEthernet 0/6 on group 0100.5e02.0203
```

Related Commands

Command	Description
ip igmp snooping	Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN.
ip igmp snooping vlan	Enables IGMP snooping on the VLAN interface.
ip igmp snooping vlan immediate-leave	Configures IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
show mac-address-table multicast	Displays the Layer 2 multicast entries for a VLAN.

ip igmp ssm-map

To enable and configure SSM mapping, use the **ip igmp ssm-map** command in global configuration mode. To disable SSM mapping, use the **no** form of this command.

ip igmp ssm-map {**enable** | **query dns** | **static** {*group-access-list* | *group-access-list-name*} *source-address*}

no ip igmp ssm-map {**enable** | **query dns**}

Syntax Description

enable	Enables SSM group to the source mapping.
query dns	Enables the DNS lookup.
static	Specifies an SSM static group to the source mapping.
group-access-list	Group access list to map to the source address.
group-access-list-name	Name of the group access list to map to the source address.
source-address	Source address.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

By default, the locally configured static SSM mappings and the DNS server are queried. Local configured mappings have priority over dynamic mappings. If a DNS server is not available, you may want to disable DNS server lookups. To disable DNS lookups, use the **no ip igmp ssm-map query dns** command.

If a DNS server is not available, a locally configured static SSM mapping database is used to query. A database query uses the group address and receives the source list in return. As soon as the static SSM mappings are configured, the maps are used for the lookups. To build a static SSM mappings database, use the following commands:

ip igmp ssm-map static *acl-1 source-1-ip-address*

ip igmp ssm-map static *acl-2 source-2-ip-address*

The ACL specifies the group or groups that have to be mapped to the listed source. Because the content servers may send out more then one stream with the same source address, the access list is used to group the multicast destination addresses together. You can use wildcards if the addresses are contiguous.

If multiple sources have to be joined for a multicast group address, you must place the group in all ACLs that are associated with the source address. In the example above, if group G must join sources 1 and 2, the group address must be placed in both acl-1 and acl-2.

When you enable SSM mapping using the **ip igmp ssm-map enable** command, but the source mapping list is empty for the group, enter the **no ip igmp ssm-map query dns** command. The **ip igmp ssm-map enable** command is supported on statically configured SSM-mapped source entries only.

Examples

This example shows how to enable an SSM group to the source mapping:

```
Router(config)# ip igmp ssm-map enable
```

This example shows how to enable DNS lookups:

```
Router(config)# ip igmp ssm-map query dns
```

This example shows how to build a static SSM mapping database:

```
Router(config)# ip igmp ssm-map static acl1 255.255.255.0
Router(config)# ip igmp ssm-map static acl2 255.255.255.0
```

This example shows how to disable an SSM group to the source mapping:

```
Router(config)# no ip igmp ssm-map enable
```

This example shows how to disable DNS lookups:

```
Router(config)# no ip igmp ssm-map query dns
```

ip igmp ssm-map enable

To enable Source Specific Multicast (SSM) mapping for groups in a configured SSM range, use the **ip igmp ssm-map enable** command in global configuration mode. To disable SSM mapping, use the **no** form of this command.

ip igmp [**vrf** *vrf-name*] **ssm-map enable**

no ip igmp [**vrf** *vrf-name*] **ssm-map enable**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Defaults

This command is disabled by default. If this command is enabled, Domain Name System (DNS)-based SSM mapping is the default.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18) SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to enable SSM mapping for groups in the configured SSM range. SSM mapping is applied only to received Internet Group Management Protocol (IGMP) version 1 or IGMP version 2 membership reports.

SSM mapping is compatible with URL Rendezvous Directory (URD) and IGMPv3 lite. SSM mapping is needed only in the router connecting to the receivers. No support is needed in any other routers in the network. SSM mapping can be configured only globally and cannot be configured per interface.

Use the **vrf** *vrf-name* keyword and argument to enable SSM mapping for a particular VRF.

Examples

The following example shows how to enable SSM mapping:

```
ip igmp ssm-map enable
```

The following example shows how to enable SSM mapping for the VRF named vrf1:

```
ip igmp vrf vrf1 ssm-map enable
```

Related Commands

Command	Description
ip domain multicast	Changes the domain prefix used by Cisco IOS software for DNS-based SSM mapping.
ip igmp ssm-map query dns	Configures DNS-based SSM mapping.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.
ip pim ssm	Defines the SSM range of IP multicast addresses.

ip igmp ssm-map query dns

To configure Domain Name System (DNS)-based Source Specific Multicast (SSM) mapping, use the **ip igmp ssm-map query dns** command in global configuration mode. To disable DNS-based SSM mapping, use the **no** form of this command.

ip igmp [**vrf** *vrf-name*] **ssm-map query dns**

no ip igmp [**vrf** *vrf-name*] **ssm-map query dns**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Defaults

This command is enabled by default when the **ip igmp ssm-map enable** command is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18) SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to enable DNS-based SSM mapping. Disable DNS-based SSM mapping if you want to rely only on statically configured SSM mapping. By default, the router will use both DNS-based SSM mapping and statically configured SSM mapping. If DNS-based SSM mapping is not explicitly disabled, the router will first try to find any statically mapped sources for the group and, if it does not find any, will use DNS-based SSM mapping.

This command is enabled by default when the **ip igmp ssm-map enable** command is configured. Use the **no ip igmp ssm-map query dns** command to disable DNS-based SSM mapping. When DNS-based SSM mapping is disabled, SSM mapping is performed only on SSM sources mapped by the **ip igmp ssm-map static** command.

To configure DNS-based SSM mapping, the router needs to find at least one correctly configured DNS server. The router can discover the DNS server by configuring the **ip name-server** global configuration command or by being directly connected to the DNS server.

Note It is recommended to always configure the IP addresses of the DNS servers with the **ip name-server** command to prevent the router from sending each DNS query broadcast to all connected interfaces.

Only the **no** form of this command is saved to the running configuration.

Use the **vrf** *vrf-name* keyword and argument to enable DNS-based SSM mapping for a particular VRF.

Examples

The following example shows how to configure DNS-based SSM mapping:

```
ip name-server 10.0.0.0
ip igmp ssm-map enable
ip igmp ssm-map query dns
```

The following example shows how to configure DNS-based SSM mapping for a VRF named vrf1:

```
ip name-server 10.0.0.0
ip igmp ssm-map enable
ip igmp vrf vrf1 ssm-map query dns
```

Related Commands

Command	Description
ip domain multicast	Changes the domain prefix used by Cisco IOS software for DNS-based SSM mapping.
ip igmp ssm-map enable	Enables SSM mapping for groups in a configured SSM range.
ip igmp ssm-map static	Enables static SSM mapping.
ip igmp static-group	Configures the router to be a statically connected member of the specified group on the interface.
ip name-server	Specifies the address of one or more name servers to use for name and address resolution.

ip igmp ssm-map static

To enable static Source Specific Multicast (SSM) mappings, use the **ip igmp ssm-map static** command in global configuration mode. To disable a static SSM mapping, use the **no** form of this command.

ip igmp ssm-map [**vrf** *vrf-name*] **static** *access-list source-address*

no ip igmp ssm-map [**vrf** *vrf-name*] **static** *access-list source-address*

Syntax Description

vrf *vrf-name*	(Optional) Specifies that the static SSM mapping be applied to the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
access-list	Access list (ACL) to apply to the static SSM mapping.
source-address	Source address to use for the groups defined in the ACL specified for the *access-list* argument.

Command Default

No static SSM mappings are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18) SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **ip igmp ssm-map static** command to configure static SSM mappings. Before configuring static SSM mappings, you must first globally enable SSM mapping with the **ip igmp ssm-map enable** command. When static SSM mappings are configured and the router receives an Internet Group Management Protocol (IGMP) membership report for a group G in the configured SSM range, the router tries to determine the source address or addresses associated with the group G by walking the configured **ip igmp ssm-map static** commands. If the group G matches the ACL in a configured static SSM mapping, then the source address (specified for the *source-address* argument in the **ip igmp ssm-map static** command) associated with the SSM mapping is statically mapped to the group G. If multiple static SSM mappings are configured, and a group G is permitted by multiple ACLs, the source addresses associated with all matching ACLs in configured SSM mappings are used (that is, the group G is statically mapped to those sources). The maximum number of configured static SSM mappings for each group is 20.

When both static SSM mappings and Domain Name System (DNS) SSM mappings are configured, static SSM mappings take precedence over the DNS mappings. If a router receives an IGMP membership report for a group G that does not match any of ACLs configured in static SSM mappings, the router then will revert to querying the DNS for the address mapping.

Use the **vrf** *vrf-name* keyword and argument to configure SSM static mapping for a particular MVRF.

Examples

The following example shows how to enable static SSM mapping. In this example, the router is configured to statically map groups that match ACL 11 to source address 172.16.8.11 and to statically map groups that match ACL 10 to source address 172.16.8.10.

```
ip igmp ssm-map enable
ip igmp ssm-map static 11 172.16.8.11
ip igmp ssm-map static 10 172.16.8.10
```

The following example shows how to enable static SSM mapping for an MVRF. In this example, the router is configured to statically maps groups within the MVRF named test that match ACL 12 to source address 172.16.8.12.

```
ip igmp ssm-map enable
ip igmp ssm-map vrf test static 12 172.16.8.12
```

Related Commands

Command	Description
ip igmp ssm-map enable	Enables SSM mapping for groups in a configured SSM range.
ip igmp ssm-map query dns	Configures DNS-based SSM mapping.
ip igmp static-group	Configures the router to be a statically connected member of the specified group on the interface, or to statically forward for a multicast group onto the interface.
ip pim ssm	Defines the SSM range of IP multicast addresses.

ip igmp static-group

To configure static group membership entries on an interface, use the **ip igmp static-group** command in interface configuration mode. To delete static group membership entries, use the **no** form of this command.

ip igmp static-group {***** | *group-address* [**source** {*source-address* | **ssm-map**}] | **class-map** *class-map-name*}

no ip igmp static-group {***** | *group-address* [**source** {*source-address* | **ssm-map**}] | **class-map** *class-map-name*}

Syntax Description

*****	Places the interface into all created multicast route (mroute) entries.
group-address	IP multicast group address to configure as a static group member on the interface.
source	(Optional) Statically forwards a (S, G) channel out of the interface.
source-address	(Optional) IP address of a system where multicast data packets originate.
ssm-map	(Optional) Configures Source Specific Multicast (SSM) mapping to be used on the interface to determine the source associated with this group. The resulting (S, G) channels are statically forwarded.
class-map *class-map-name*	Attaches an Internet Group Management Protocol (IGMP) static group range class map to the interface.

Command Default

No static group membership entries are configured on interfaces.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
11.2	This command was introduced.
12.3(2)T	This command was modified. The **ssm-map** keyword was added.
12.2(18)S	This command was modified. The **ssm-map** keyword was added.
12.2(18)SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF5	This command was modified. The **class-map** keyword and *class-map-name* argument were added.
15.0(1)M	This command was modified. The **class-map** keyword and *class-map-name* argument were added.
12.2(33)SRE	This command was modified. The **class-map** keyword and *class-map-name* argument were added.

Release	Modification
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Use the **ip igmp static-group** command to configure static group membership entries on an interface. When you configure the **ip igmp static-group** command, packets to the group are fast-switched out the interface, provided that packets were received on the correct reverse path forwarding (RPF) interface. Once configured, static group membership entries are added to the IGMP cache and mroute table.

Configuring the **ip igmp static-group** command is unlike configuring the **ip igmp join-group** command, which allows the router to join the multicast group. This configuration of the **ip igmp static-group** command would cause the upstream routers to maintain the multicast routing table information for that group, which would ensure that all the paths to that multicast group are active.

If you configure the **ip igmp join-group** command for the same group address as the **ip igmp static-group** command, the **ip igmp join-group** command takes precedence, and the group behaves like a locally joined group.

Use the **ip igmp static-group** command with the **ssm-map** keyword to configure static traffic forwarding with SSM mapping on the last hop router. Static traffic forwarding can be used in conjunction with SSM mapping to statically forward SSM traffic for certain groups. When static traffic forwarding with SSM mapping is configured, the last hop router uses Domain Name System (DNS)-based SSM mapping to determine the sources associated with a group. The resulting (S, G) channels are then statically forwarded.

Use the **ip igmp static-group class-map** command with the **class-map** keyword and *class-map-name* argument to attach an IGMP static group class map to an interface. Once attached, all groups entries that are defined in the class map become static members on the interface and are added to the IGMP cache and to the mroute table.

Examples

The following example shows how to configure group address 239.100.100.101 on Ethernet interface 0:

```
interface ethernet 0
 ip igmp static-group 239.100.100.101
```

The following example shows how to configure group address 239.1.2.1 to use SSM mapping for statically forwarded groups on Ethernet interface 0:

```
interface ethernet 0
 ip igmp static-group 239.1.2.1 source ssm-map
```

The following example shows how to attach an IGMP static group range class map named static1 to GigabitEthernet interface 1/1:

```
interface GigabitEthernet1/1
 ip igmp static-group class-map static1
```

Related Commands

Command	Description
class-map type multicast-flows	Enters multicast-flows class-map configuration mode to create or modify IGMP static group class maps.
ip igmp join-group	Causes the router to join a multicast group.
ip igmp ssm-map enable	Enables SSM mapping for groups in a configured SSM range.
ip igmp ssm-map query dns	Configures DNS-based SSM mapping.
ip igmp ssm-map static	Enables static SSM mapping.
ip pim ssm	Defines the SSM range of IP multicast addresses.

ip igmp tcn query

To configure the number of IGMP topology change queries to be executed during a set interval time, use the **ip igmp tcn query** command. To disable IGMP topology change queries, use the **no** form of this command.

ip igmp tcn query {**count** *count* | **interval** *interval*}

no ip igmp tcn query {**count** | **interval**}

Syntax Description

count *count*	Specifies the number of queries needed to stop flooding multicast traffic after a TCN event; valid values are from 1 to 10.
interval *interval*	Specifies the time until the IGMP TCN querier expires; valid values are from 1 to 255 seconds.

Command Default

Disabled

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.2(18)ZY	Support for this command was introduced.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

The **ip igmp tcn query** command applies only to Layer 2 switch ports and EtherChannels; it does not apply to routed ports, VLAN interfaces, or Layer 3 channels.

Use **ip igmp tcn query count** command to control the time that multicast traffic is flooded after a TCN event. If you set the TCN flood query count to 1 by using the **ip igmp tcn query count** command, the flooding stops after receiving 1 general query. If you set the count to 7, the flooding of multicast traffic due to the TCN event lasts until 7 general queries are received. Groups are relearned based on the general queries received during the TCN event.

Examples

This example shows how to set the number of queries to be executed:

```
Router(config)# ip igmp tcn query count 5
Router(config)#
```

This example shows how to set the time until the query expires to 120 seconds:

```
Router(config)# ip igmp tcn query interval 120
Router(config)#
```

ip igmp unidirectional-link

To configure an interface to be unidirectional and enable it for Internet Group Management Protocol (IGMP) unidirectional link routing (UDLR), use the **ip igmp unidirectional-link** command in interface configuration mode. To disable the unidirectional link (UDL), use the **no** form of this command.

ip igmp unidirectional-link

no ip igmp unidirectional-link

Syntax Description

This command has no arguments or keywords.

Defaults

No UDLR occurs.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

One example of when you might configure this command is if you have traffic traveling via a satellite.

If you have a small number of receivers, another way to achieve UDLR is to configure a UDLR tunnel. See the descriptions of the **tunnel udlr receive-only** and **tunnel udlr send-only** commands.

Examples

The following example configures an upstream router with UDLR on serial interface 0:

```
ip multicast-routing
!
! Unidirectional link
!
interface serial 0
 description Unidirectional to downlink-rtr
 ip address 10.0.0.1 255.0.0.0
 ip pim sparse-dense-mode
 ip igmp unidirectional-link
 no keepalive
```

Related Commands

Command	Description
ip igmp helper-address (UDL)	Configures IGMP helpering as required for IGMP UDLR.
ip igmp mroute-proxy	Enables IGMP report forwarding of proxied (*, G) mroute entries.
ip igmp proxy-service	Enables the mroute proxy service.
ip multicast default-rpf-distance	Changes the distance given to the default RPF interface when configuring IGMP UDLR.
show ip igmp udlr	Displays UDLR information for directly connected multicast groups on interfaces that have a UDL helper address configured.
tunnel udlr receive-only	Configures a unidirectional, GRE tunnel to act as a back channel that can receive messages, when another interface is configured for UDLR to send messages.
tunnel udlr send-only	Configures a unidirectional, GRE tunnel to act as a back channel that can send messages, when another interface is configured for UDLR to receive messages.

ip igmp v3lite

To enable acceptance and processing of Internet Group Management Protocol Version 3 lite (IGMP v3lite) membership reports on an interface, use the **ip igmp v3lite** command in interface configuration mode. To disable IGMP v3lite, use the **no** form of this command.

ip igmp v3lite

no ip igmp v3lite

Syntax Description

This command has no arguments or keywords.

Defaults

IGMPv3 lite membership reports are not accepted and processed.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

To use this command, you must define a Source Specific Multicast (SSM) range of IP addresses using the **ip pim ssm** global configuration command. When IGMP v3lite is enabled, it is supported in the SSM range of addresses only.

Examples

The following example shows how to configure IGMP v3lite on Ethernet interface 3/1:

```
interface ethernet 3/1
ip igmp v3lite
```

Related Commands

Command	Description
ip pim ssm	Defines the SSM range of IP multicast addresses.

ip igmp version

To configure which version of Internet Group Management Protocol (IGMP) the router uses, use the **ip igmp version** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip igmp version {**1** | **2** | **3**}

no ip igmp version

Syntax Description

1	IGMP Version 1.
2	IGMP Version 2. This is the default.
3	IGMP Version 3.

Defaults

Version 2

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
11.1	This command was introduced.
12.1(5)T	The **3** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

All routers on the subnet must support the same version. The router does not automatically detect Version 1 routers and switch to Version 1 as did earlier releases of the Cisco IOS software. Hosts can have any IGMP version (1, 2, or 3) and the router will correctly detect their presence and query them appropriately.

Some commands require IGMP Version 2 or 3, such as the **ip igmp query-max-response-time** and **ip igmp query-timeout** commands.

Examples

The following example configures the router to use IGMP Version 3:

```
ip igmp version 3
```

Related Commands

Command	Description
ip igmp query-max-response-time	Configures the maximum response time advertised in IGMP queries.
ip igmp query-timeout	Configures the timeout time before the router takes over as the querier for the interface, after the previous querier has stopped querying.
show ip igmp groups	Displays the multicast groups that are directly connected to the router and that were learned through IGMP.
show ip igmp interface	Displays multicast-related information about an interface.

ip mfib

To reenable IPv4 multicast forwarding on the router, use the **ip mfib** command in global configuration mode. To disable IPv4 multicast forwarding, use the **no** form of this command.

ip mfib

no ip mfib

Syntax Description

This command has no arguments or keywords.

Command Default

IPv4 multicast forwarding is enabled automatically when IPv4 multicast routing is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

After you have enabled the **ip multicast-routing** command, IPv4 multicast forwarding is enabled. Because IPv4 multicast forwarding is enabled by default, use the **no** form of the **ip mfib** command to disable IPv4 multicast forwarding.

Examples

The following example shows how to disable IPv4 multicast forwarding:

```
Router(config)# no ip mfib
```

Related Commands

Command	Description
ip multicast-routing	Enables IP multicast routing.

ip mfib cef

To reenable IPv4 Multicast Forwarding Information Base (MFIB) interrupt-level IP multicast forwarding of incoming packets or outgoing packets on a specific interface, use the **ip mfib cef input** command in interface configuration mode. To disable IPv4 MFIB interrupt-level IP multicast forwarding of incoming or outgoing packets on the interface, use the **no** form of this command.

ip mfib cef {**input** | **output**}

no ip mfib cef {**input** | **output**}

Syntax Description

input	Enables IPv4 MFIB interrupt-level IP multicast forwarding of incoming packets.
output	Enables IPv4 MFIB interrupt-level IP multicast forwarding of outgoing packets.

Command Default

Cisco Express Forwarding (CEF)-based (interrupt-level) forwarding of incoming packets and outgoing packets is enabled by default on interfaces that support it.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

After you have enabled the **ip multicast-routing** command, IPv4 MFIB interrupt-level switching of both incoming packets and outgoing packets is enabled by default on interfaces that support it.

Use the **no** form of the **ip mfib cef** command with the **input** keyword to disable IPv4 MFIB interrupt switching of incoming packets on a specific interface.

Use the **no** form of the **ip mfib cef** command with the **output** keyword to disable IPv4 MFIB interrupt switching of outgoing packets on a specific interface.

Use the **show ip mfib interface** command to display IPv4 MFIB-related information about interfaces and their forwarding status.

Examples

The following example shows how to disable MFIB interrupt-level IP multicast forwarding of incoming packets on Gigabit Ethernet interface 0/0:

```
interface GigabitEthernet0/0
 no ip mfib cef input
```

The following example shows how to disable MFIB interrupt-level IP multicast forwarding of outgoing packets on Gigabit Ethernet interface 0/0:

```
interface GigabitEthernet0/0
 no ip mfib cef output
```

Related Commands

Command	Description
ip multicast-routing	Enables IP multicast routing
show ip mfib interface	Displays IPv4 MFIB-related information about interfaces and their forwarding status.

ip mfib forwarding

To reenable IPv4 multicast forwarding of packets received from or destined for the specified interface, use the **ip mfib forwarding** command in interface configuration mode. To disable multicast forwarding of multicast packets received from or destined for the specified interface, use the **no** form of this command.

ip mfib forwarding {**input** | **output**}

no ip mfib forwarding {**input** | **output**}

Syntax Description

input	Enables IPv4 multicast forwarding of packets received from an interface.
output	Enables IPv4 multicast forwarding of packets destined for an interface.

Command Default

IPv4 multicast forwarding is enabled automatically on all interfaces when IPv4 multicast routing is enabled.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	Support was not added for Cisco 7600 routers.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Because multicast forwarding is enabled automatically on all interfaces when IPv4 multicast routing is enabled using the **ip multicast-routing** command, the **ip mfib forwarding** command is used to reenable multicast forwarding of packets received from or destined for an interface, if it has been previously disabled.

Use the **no ip mfib forwarding** command with the **input** keyword to disable IPv4 multicast forwarding of packets received from an interface, although the specified interface will still continue to receive multicast packets destined for applications on the router itself.

Use the **no ip mfib forwarding** command with the **output** keyword to disable IPv4 multicast forwarding of packets destined for an interface.

Examples

The following example shows how to disable IPv4 multicast forwarding of packets received from Gigabit Ethernet interface 0/0:

```
interface GigabitEthernet0/0
 no ip mfib forwarding input
```

The following example shows how to disable IPv4 multicast forwarding of packets destined for Gigabit Ethernet interface 0/0:

```
interface GigabitEthernet0/0
 no ip mfib forwarding output
```

Related Commands

Command	Description
ip multicast-routing	Enables IP multicast routing.

ip mrm

To configure an interface to operate as a Test Sender or Test Receiver, or both, for Multicast Routing Monitor (MRM) tests, use the **ip mrm** command in interface configuration mode. To remove the interface as a Test Sender or Test Receiver, use the **no** form of this command.

ip mrm {**test-sender** | **test-receiver** | **test-sender-receiver**}

no ip mrm

Syntax Description

test-sender	Configures the interface to operate as a Test Sender.
test-receiver	Configures the interface to operate as a Test Receiver.
test-sender-receiver	Configures the interface to operate as both a Test Sender and Test Receiver (for different groups).

Command Default

No interface is configured to operate as a Test Sender or a Test Receiver, or both, for MRM.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Test Sender and Test Receiver can be either a router or a host.

If a router (or host) belongs to more than one test group, it can be a Test Sender for one group and a Test Receiver for the other group. It, however, cannot be the Test Sender and Test Receiver for the same group.

Examples

The following example shows how to configure an interface to operate as a Test Sender. In this example, Ethernet interface 0 is configured to operate as a Test Sender.

```
interface ethernet 0
 ip mrm test-sender
```

Related Commands

Command	Description
receivers	Establishes Test Receivers for MRM.
senders	Establishes Test Senders for MRM.

ip mrm accept-manager

To configure a Test Sender or Test Receiver to accept requests only from Managers that pass an access list, use the **ip mrm accept-manager** command in global configuration mode. To remove the restriction, use the **no** form of this command.

ip mrm accept-manager *access-list* [**test-sender** | **test-receiver**]

no ip mrm accept-manager *access-list*

Syntax Description

access-list	Number or name of an IP access list used to restrict Managers.
test-sender	(Optional) Applies the access list only to the Test Sender.
test-receiver	(Optional) Applies the access list only to the Test Receiver.

Command Default

Test Senders and Test Receivers respond to all Managers.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to control which Managers a Test Sender or Test Receiver must respond to.

If neither the **test-sender** nor **test-receiver** keyword is configured, the access list applies to both.

Examples

The following example shows how to configure a Test Sender to respond only to Managers that pass an access list. In this example, the Test Sender is configured to respond only to the Managers that pass the ACL named supervisor.

```
ip mrm accept-manager supervisor
!
ip access-list standard supervisor
 remark Permit only the Manager from the Central Office
 permit 172.18.2.4
!
```

Related Commands

Command	Description
ip mrm	Configures an interface to operate as a Test Sender or Test Receiver, or both, for MRM.

ip mrm manager

To specify the Multicast Routing Monitor (MRM) test to be created or modified and enter MRM manager configuration mode, use the **ip mrm manager** command in global configuration mode. To remove the test, use the **no** form of this command.

ip mrm manager *test-name*

no ip mrm manager *test-name*

Syntax Description

test-name	Name of the MRM test to be created or modified.

Command Default

No MRM tests are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip mrm manager** command to specify the name of the MRM test to be created or modified and enter MRM manager configuration mode where you specify the parameters of the MRM test.

Examples

The following example shows how to enter MRM manager configuration mode for the MRM test named test1:

```
Router(config)# ip mrm manager test1
Router(config-mrm-manager)#
```

Related Commands

Command	Description
mrm	Starts or stops an MRM test.
show ip mrm manager	Displays test information for MRM.

ip mroute

To configure a static multicast route (mroute), use the **ip mroute** command in global configuration mode. To remove the static mroute, use the **no** form of this command.

ip mroute [**vrf** *vrf-name*] *source-address mask* {**fallback-lookup** {**global** | **vrf** *vrf-name*} | [*protocol*] {*rpf-address* | *interface-type interface-number*}} [*distance*]

no ip mroute [**vrf** *vrf-name*] *source-address mask* [**fallback-lookup** {**global** | **vrf** *vrf-name*} | [*protocol*] [*distance*]

Cisco IOS Release 12.2(33)SRB and Subsequent 12.2SR Releases

ip mroute [**vrf** *vrf-name*] *source-address mask* {**fallback-lookup** {**global** | **vrf** *vrf-name*} | *rpf-address* | *interface-type interface-number*} [*distance*]

no ip mroute [**vrf** *vrf-name*] *source-address mask*

Syntax Description

vrf *vrf-name*	(Optional) Configures a static mroute in the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
source-address	Source IP address of a multicast source or source IP route prefix.
mask	Mask associated with the source IP address or source IP route prefix.
fallback-lookup {**global** | **vrf** *vrf-name*}	Specifies that the Reverse Path Forwarding (RPF) lookup originating in the receiver MVRF instance to continue and be resolved in either the global table or in the source MVRF instance. If you specify the **fallback-lookup** keyword, you must specify one of the following keywords and arguments: • **global**—Specifies that the source MVRF is in the global table. • **vrf** *vrf-name*—Specifies a VRF as the source MVRF.
protocol	(Optional) Unicast routing protocol or route map used to further tune the matching of source addresses.
rpf-address	IP address to be used as the RPF address. The interface associated with this IP address, thus, is used as the incoming interface for the mroute.
interface-type interface-number	Interface type and number to be used as the RPF interface for the mroute. A space is not needed between the values.
distance	(Optional) Administrative distance for the mroute. The value specified determines whether a unicast route, a Distance Vector Multicast Routing Protocol (DVMRP) route, or a static mroute should be used for the RPF lookup. The lower distances have better preference. If the static mroute has the same distance as the other RPF sources, the static mroute will take precedence. The range is from 0 to 255. The default is 0.

Command Default

No static mroutes are configured.

Command Modes Global configuration (config)

Command History

Release	Modification
11.0	This command was introduced.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(31)SB	This command was modified. The **fallback-lookup** and **global** keywords and the **vrf** keyword and *vrf-name* argument were added in support of the Multicast VPN Extranet Support feature.
12.2(33)SRB	This command was modified. The following protocol keywords were removed: **bgp**, **eigrp**, **isis**, **iso-igrp**, **mobile**, **odr**, **ospf**, **rip**, **route-map**, and **static**.
12.2(33)SXH	This command was modified. The **fallback-lookup** and **global** keywords and the **vrf** keyword and *vrf-name* argument were added in support of the Multicast VPN Extranet Support feature.
12.2(33)SRC	This command was modified. The **fallback-lookup** and **global** keywords and the **vrf** keyword and *vrf-name* argument were added in support of the Multicast VPN Extranet Support feature.
15.0(1)M	This command was modified. The **fallback-lookup** and **global** keywords and the **vrf** keyword and *vrf-name* argument were added in support of the Multicast VPN Extranet Support feature.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines The **ip mroute** command is used to configure static mroutes. Static mroutes are similar to unicast static routes but differ in the following ways:

- Static mroutes are used to calculate RPF information, not to forward traffic.
- Static mroutes cannot be redistributed.

Static mroutes are strictly local to the router on which they are defined. Because Protocol Independent Multicast (PIM) does not have its own routing protocol, there is no mechanism to distribute static mroutes throughout the network. Consequently, the administration of static mroutes tends to be more complicated then the administration of unicast static routes.

When static mroutes are configured, they are stored on the router in a separate table referred to as the *static mroute table*. When configured, the **ip mroute** command enters a static mroute into the static mroute table for the source address or source address range specified for the *source-address* and *mask* arguments. Sources that match the source address or that fall in the source address range specified for the *source-address* argument will RPF to either the interface associated with the IP address specified for the *rpf-address* argument or the local interface on the router specified for the *interface-type* and *interface-number* arguments. If an IP address is specified for the *rpf-address* argument, a recursive lookup is done from the unicast routing table on this address to find the directly connected neighbor.

The administrative distance of an mroute may be specified for the optional *distance* argument. If a value is not specified for the *distance* argument, the distance of the mroute defaults to zero. If the static mroute has the same distance as another RPF source, the static mroute will take precedence. There are only two exceptions to this rule: directly connected routes and the default unicast route.

Note The order that static mroutes are configured is important. The router searches the static mroute table in the order that they were configured. If a matching entry is found, the search terminates and the information in the matching static mroute is used.

Tip Remember that the distance of a matching mroute is compared to the distance of any other matching routes found in the other sources of RPF information. The static mroute is used if its distance is equal to or less than the distance of other routes.

For the Multicast VPN Extranet Support feature, the **fallback-lookup** and **global** keywords and an additional **vrf** keyword and *vrf-name* argument were added to the syntax of the **ip mroute** command. Use the **ip mroute** command with the **fallback-lookup** keyword and **vrf** *vrf-name* keyword and argument to specify the source MVRF. By default, extranet MVPN relies on the unicast routing policies to determine the RPF interface. When the RPF lookup originates in a receiver MVRF, and it finds that the RPF interface is not located in the same MVRF, the router uses the information in the Border Gateway Protocol (BGP) imported route to determine the source MVRF. The RPF lookup then continues and resolves in the source MVRF. In cases where the multicast and unicast topologies are incongruent, you can override the default behavior by configuring a static mroute in the receiver MVRF to explicitly specify the source MVRF using the **ip mroute** command with the **fallback-lookup** keyword and **vrf** *vrf-name* keyword and argument.

Static mroutes can also be configured to support RPF for extranet MVPN in the case where the source is present in an MVRF and the receiver is in the global table. In this case, because BGP does not allow VPNv4 routes to be imported into the IPv4 routing table, unicast cannot obtain the source MVRF information needed to resolve the RPF lookup. To enable the RPF lookup to be resolved in this case, a static mroute can be configured to explicitly specify the source MVRF using the **ip mroute** command with the **fallback-lookup** keyword and the **global** keyword.

In Release 12.2(33)SRB and subsequent 12.2SR releases, the following protocol keywords are no longer supported (to be consistent with the **ip route** command): **bgp**, **eigrp**, **isis**, **iso-igrp**, **mobile**, **odr**, **ospf**, **rip**, **route-map**, and **static**. Those keywords are still present in the online help as available keywords; however, if the **ip mroute** command is entered with one of those deprecated protocol keywords, the command will be rejected and the following error message will display on the console: “The option of specifying protocol is deprecated.”

Examples

The following example shows how to configure a static mroute. In this static mroute configuration, the source IP address 10.1.1.1 is configured to be reachable through the interface associated with IP address 10.2.2.2:

```
ip mroute 10.1.1.1 255.255.255.255 10.2.2.2
```

The following example shows how to configure a static mroute. In this static mroute configuration, sources in network 172.16.0.0 are configured to be reachable through the interface associated with IP address 172.30.10.13:

```
ip mroute 172.16.0.0 255.255.0.0 172.30.10.13
```

The following example shows how configure a static mroute. In this static mroute configuration (from an extranet MVPN configuration), RPF lookups originating in VPN-Y are configured to be resolved in VPN-X using the static mroute 192.168.1.1:

```
ip mroute vrf VPN-Y 192.168.1.1 255.255.255.255 fallback-lookup vrf VPN-X
```

ip mroute-cache

Note Effective with Cisco IOS Release 15.0(1)M and Cisco IOS Release 12.2(33)SRE, the **ip mroute-cache** command is not available in Cisco IOS software.

To configure IP multicast fast switching or multicast distributed switching (MDS), use the **ip mroute-cache** command in interface configuration mode. To disable either of these features, use the **no** form of this command.

ip mroute-cache [**distributed**]

no ip mroute-cache [**distributed**]

Syntax Description

distributed	(Optional) Enables MDS on the interface. In the case of Cisco 7500 series routers, this keyword is optional; if it is omitted, fast switching occurs. On the Cisco 12000 series, this keyword is required because the Cisco 12000 series does only distributed switching.

Command Default

On the Cisco 7500 series, IP multicast fast switching is enabled; MDS is disabled.
On the Cisco 12000 series, MDS is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2(11)GS	The **distributed** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.0(33)S	Support for IPv6 was added. This command was implemented on the Cisco 12000 series routers.
15.0(1)M	This command was removed.
12.2(33)SRE	This command was removed.

Usage Guidelines

On the Cisco 7500 Series

If multicast fast switching is disabled on an incoming interface for a multicast routing table entry, the packet will be sent at the process level for all interfaces in the outgoing interface list.

If multicast fast switching is disabled on an outgoing interface for a multicast routing table entry, the packet is process-level switched for that interface, but may be fast switched for other interfaces in the outgoing interface list.

When multicast fast switching is enabled (like unicast routing), debug messages are not logged. If you want to log debug messages, disable fast switching.

If MDS is not enabled on an incoming interface that is capable of MDS, incoming multicast packets will not be distributed switched; they will be fast switched at the Route Processor (RP). Also, if the incoming interface is not capable of MDS, packets will get fast switched or process switched at the RP.

If MDS is enabled on the incoming interface, but at least one of the outgoing interfaces cannot fast switch, packets will be process switched. We recommend that you disable fast switching on any interface when MDS is enabled.

On the Cisco 12000 Series

On the Cisco 12000 series router, all interfaces should be configured for MDS because that is the only switching mode.

Examples

The following example shows how to enable IP multicast fast switching on the interface:

```
ip mroute-cache
```

The following example shows how to disable IP multicast fast switching on the interface:

```
no ip mroute-cache
```

The following example shows how to enable MDS on the interface:

```
ip mroute-cache distributed
```

The following example shows how to disable MDS and IP multicast fast switching on the interface:

```
no ip mroute-cache distributed
```

ip msdp border

To configure a router that borders a Protocol Independent Multicast (PIM) sparse mode region and dense mode region to use Multicast Source Discovery Protocol (MSDP), use the **ip msdp border** command in global configuration mode. To prevent this action, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **border sa-address** *interface-type interface-number*

no ip msdp [**vrf** *vrf-name*] **border sa-address** *interface-type interface-number*

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
sa-address	Specifies the active source IP address.
interface-type interface-number	Interface type and number from which the IP address is derived and used as the rendezvous point (RP) address in Source-Active (SA) messages. Thus, MSDP peers can forward SA messages away from this border. The IP address of the interface is used as the originator ID, which is the RP field in the MSDP SA message. No space is needed between the values.

Defaults

The active sources in the dense mode region will not participate in MSDP.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command if you want the router to send SA messages for sources active in the PIM dense mode region to MSDP peers.

Specifying the interface-type and interface-number values allow the MSDP peers to forward source-active messages away from this border. The IP address of the interface is used as the originator ID, which is the rendezvous point field in the MSDP source-active message.

Note We recommend configuring the border router in the sparse mode domain to proxy-register sources in the dense mode domain, and have the sparse mode domain use standard MSDP procedures to advertise these sources.

Note If you use this command, you must constrain the sources advertised by using the **ip msdp redistribute** command. Configure the **ip msdp redistribute** command to apply to only local sources. Be aware that this configuration can result in (S, G) state remaining long after a source in the dense mode domain has stopped sending.

Note The **ip msdp originator-id** command also identifies an interface type and number to be used as the RP address. If both the **ip msdp border** and **ip msdp originator-id** commands are configured, the address derived from the **ip msdp originator-id** command determines the address of the RP.

Examples

In the following example, the local router is not an RP. It borders a PIM sparse mode region with a dense mode region. It uses the IP address of Ethernet interface 0 as the "RP" address in SA messages.

```
ip msdp border sa-address ethernet0
```

Related Commands

Command	Description
ip msdp originator-id	Allows an MSDP speaker that originates an SA message to use the IP address of its interface as the RP address in the SA message.
ip msdp redistribute	Configures which (S, G) entries from the multicast routing table are advertised in SA messages originated to MSDP peers.

ip msdp cache-rejected-sa

To cache Source-Active (SA) request messages rejected from Multicast Source Discovery Protocol (MSDP) peers, use the **ip msdp cache-rejected-sa** command in global configuration mode. To stop tracking SA request messages, use the **no** form of this command.

ip msdp cache-rejected-sa *number-of-entries*

no ip msdp cache-rejected-sa *number-of-entries*

Syntax Description

number-of-entries	Number of entries to be cached. The range is from 1 to 32766.

Defaults

Rejected SA request messages are not stored.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.1E	This command was integrated into Cisco IOS Release 12.1E.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip msdp cache-rejected-sa** command to configure the router to store SA messages that have been recently received from an MSDP peer but were rejected. Once this command is enabled, the router will maintain a rejected SAcache that stores the most recent rejected SA messages. The number of rejected SA message entries to be stored in the rejected SA cache is configured with the *number-of-entries* argument. If the rejected SA cache overflows, entries are overwritten, starting from the first entry.

Note Enabling the **ip msdp cache-rejected-sa** command will not impact the performance of MSDP.

Use the **show ip msdp sa-cache** command with the **rejected-sa** keyword to display SA messages rejected from MSDP peers.

Examples

The following example shows how to enable the router to store a maximum of 200 messages rejected from MSDP peers:

```
Router(config)# ip msdp cache-rejected-sa 200
```

Related Commands

Command	Description
show ip msdp sa-cache	Displays the (S, G) state learned from MSDP peers.

ip msdp cache-sa-state

To have the router create Source-Active (SA) state, use the **ip msdp cache-sa-state** command in global configuration mode.

ip msdp cache-sa-state [**vrf** *vrf-name*]

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Defaults

The router creates SA state for all Multicast Source Discovery Protocol (MSDP) SA messages it receives.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(7)	This command was modified such that it is enabled by default and cannot be disabled.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is automatically configured if at least one MSDP peer is configured. It cannot be disabled.

If you are running a version of Cisco IOS software prior to Release 12.1(7), we recommend enabling the **ip msdp cache-sa-state** command.

Examples

The following example shows how the **ip msdp cache-sa-state** command is enabled when an MSDP peer is configured:

```
.
.
.
ip classless
ip msdp peer 192.168.1.2 connect-source Loopback0
ip msdp peer 192.169.1.7
ip msdp mesh-group outside-test 192.168.1.2
ip msdp cache-sa-state
ip msdp originator-id Loopback0
```

Related Commands

Command	Description
clear ip msdp sa-cache	Clears MSDP SA cache entries.
ip msdp sa-request	Configures the router to send SA request messages to the MSDP peer when a new joiner from the group becomes active.
show ip msdp sa-cache	Displays (S, G) state learned from MSDP peers.

ip msdp default-peer

To define a default peer from which to accept all Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages, use the **ip msdp default-peer** command in global configuration mode. To remove the default peer, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **default-peer** {*peer-address* | *peer-name*} [**prefix-list** *list*]

no ip msdp [**vrf** *vrf-name*] **default-peer**

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or Domain Name System (DNS) name of the MSDP default peer.
prefix-list *list*	(Optional) Specifies the Border Gateway Protocol (BGP) prefix list that specifies that the peer will be a default peer only for the prefixes listed in the list specified by the *list* argument. A BGP prefix list must be configured for this **prefix-list** *list* keyword and argument to have any effect.

Defaults

No default MSDP peer exists.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

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

If only one MSDP peer is configured (with the **ip msdp peer** command), it will be used as a default peer. Therefore, you need not configure a default peer with this command.

If 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 if you intend to configure the **prefix-list** *list* keyword and argument with the **ip msdp default-peer** command.

If the **prefix-list** *list* keyword and argument are specified, SA messages originated from rendezvous points (RPs) specified by the **prefix-list** *list* keyword and argument will be accepted from the configured default peer. If the **prefix-list** *list* keyword and argument are specified but no prefix list is configured, the default peer will be used for all prefixes.

You can enter multiple **ip msdp default-peer** commands, with or without the **prefix-list** keyword, as follows. However, all commands must either have the keyword or all must not have the keyword.

- When you use multiple **ip msdp default-peer** commands with the **prefix-list** keyword, all the default peers are used at the same time for different RP prefixes. This syntax is typically used in a service provider cloud that connects stub site clouds.
- When you use multiple **ip msdp default-peer** commands without the **prefix-list** keyword, a single active peer is used to accept all SA messages. If that peer goes down, then the next configured default peer accepts all SA messages. This syntax is typically used at a stub site.

Examples

The following example shows how to configure the router at IP address 192.168.1.3 as the default peer to the local router:

```
ip msdp peer 192.168.1.3
ip msdp peer 192.168.3.5
ip msdp default-peer 192.168.1.3
```

The following example shows how to configure two default peers:

```
ip msdp peer 172.18.2.3
ip msdp peer 172.19.3.5
ip msdp default-peer 172.18.2.3 prefix-list site-c
ip prefix-list site-a permit 172.18.0.0/16
ip msdp default-peer 172.19.3.5 prefix-list site-a
ip prefix-list site-c permit 172.19.0.0/16
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.
ip prefix-list	Creates a prefix list.

ip msdp description

To add descriptive text to the configuration for a Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp description** command in global configuration mode. To remove the description, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **description** {*peer-name* | *peer-address*} *text*

no ip msdp [**vrf** *vrf-name*] **description** {*peer-name* | *peer-address*}

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-name | *peer-address*	Peer name or address to which this description applies.
text	Description of the MSDP peer.

Defaults

No description is associated with an MSDP peer.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Configure a description to make the MSDP peer easier to identify. This description is displayed in the output of the **show ip msdp peer** command.

Examples

The following example shows how to configure the router at the IP address 172.17.1.2 with a description indicating it is a router at customer A:

```
ip msdp description 172.17.1.2 router at customer a
```

Related Commands

Command	Description
show ip msdp peer	Displays detailed information about the MSDP peer.

ip msdp filter-sa-request

To configure the router to send Source-Active (SA) request messages to the Multicast Source Discovery Protocol (MSDP) peer when a new joiner from a group becomes active, use the **ip msdp filter-sa-request** command in global configuration mode. To prevent this action, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **filter-sa-request** {*peer-address* | *peer-name*} [**list** *access-list*]

no ip msdp [**vrf** *vrf-name*] **filter-sa-request** {*peer-address* | *peer-name*}

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or name of the MSDP peer from which the local router requests SA messages when a new joiner for the group becomes active.
list *access-list*	(Optional) Specifies the standard IP access list number or name that describes a multicast group address. If no access list is specified, all SA request messages are ignored.

Defaults

By default, the router honors all SA request messages from peers. If this command is not configured, all SA request messages are honored. If this command is configured but no access list is specified, all SA request messages are ignored.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

By default, the router honors all SA request messages from peers. Use this command if you want to control exactly which SA request messages the router will honor.

If no access list is specified, all SA request messages are ignored. If an access list is specified, only SA request messages from those groups permitted will be honored, and all others will be ignored.

Examples

The following example shows how to configure the router to filter SA request messages from the MSDP peer at 172.16.2.2. SA request messages from sources on the network 192.168.22.0 pass access list 1 and will be honored; all others will be ignored.

```
ip msdp filter-sa-request 172.16.2.2 list 1
access-list 1 permit 192.4.22.0 0.0.0.255
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

ip msdp keepalive

To adjust the interval at which a Multicast Source Discovery Protocol (MSDP) peer will send keepalive messages and the interval at which the MSDP peer will wait for keepalive messages from other peers before declaring them down, use the **ip msdp keepalive** command in global configuration mode. To restore the default values, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **keepalive** {*peer-address* | *peer-name*} *keepalive-interval hold-time-interval*

no ip msdp [**vrf** *vrf-name*] **keepalive** {*peer-address* | *peer-name*}

Syntax Description

vrf *vrf-name*	(Optional) Configures the keepalive and hold-time intervals for the MSDP peer associated with the multicast VPN routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
peer-address | *peer-name*	IP address or Domain Name System (DNS) name of the MSDP peer whose keepalive timer and hold-time timer is to be adjusted.
keepalive-interval	Interval, in seconds, at which the MSDP peer will send keepalive messages. The range is from 1 to 60 seconds. The default is 60 seconds.
hold-time-interval	Interval, in seconds, at which the MSDP peer will wait for keepalive messages from other peers before declaring them down. The range is from 1 to 75 seconds. The default is 75 seconds.

Command Default

An MSDP peer sends keepalives messages at an interval of once every 60 seconds. The hold-time interval for an MSDP peer is set to 75 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E4	This command was introduced.
12.2(5)	This command was integrated into Cisco IOS Release 12.2(5).
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

Once an MSDP peering session is established, each side of the connection sends a keepalive message and sets a keepalive timer. If the keepalive timer expires, the local MSDP peer sends a keepalive message and restarts its keepalive timer; this interval is referred to as the keepalive interval. Use the

keepalive-interval argument to adjust the interval for which keepalive messages will be sent. The keepalive timer is set to the value specified for the *keepalive-interval* argument when the peer comes up. The keepalive timer is reset to the value of the *keepalive-interval* argument whenever an MSDP keepalive message is sent to the peer and reset when the timer expires. The keepalive timer is deleted when an MSDP peering session is closed. By default, the keepalive timer is set to 60 seconds.

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

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

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

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

Examples

The following example shows how to set the keepalive interval to 40 seconds and the hold-time interval to 55 seconds for the MSDP peer at 172.16.100.10:

```
ip msdp keepalive 172.16.100.10 40 55
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

ip msdp mesh-group

To configure a Multicast Source Discovery Protocol (MSDP) peer to be a member of a mesh group, use the **ip msdp mesh-group** command in global configuration mode. To remove an MSDP peer from a mesh group, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **mesh-group** *mesh-name* {*peer-address* | *peer-name*}

no ip msdp [**vrf** *vrf-name*] **mesh-group** *mesh-name* {*peer-address* | *peer-name*}

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
mesh-name	Name of the mesh group.
peer-address | *peer-name*	IP address or name of the MSDP peer to be a member of the mesh group.

Defaults

The MSDP peers do not belong to a mesh group.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

A mesh group is a group of MSDP speakers that have fully meshed MSDP connectivity among themselves. 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 achieve two goals:

- To reduce SA message flooding
- To simplify peer-Reverse Path Forwarding (RPF) flooding (no need to run Border Gateway Protocol [BGP] or multiprotocol BGP among MSDP peers)

Examples

The following example shows how to configure the MSDP peer at address 192.168.1.3 to be a member of the mesh group named internal:

```
ip msdp mesh-group internal 192.168.1.3
```

ip msdp originator-id

To allow a Multicast Source Discovery Protocol (MSDP) speaker that originates a Source-Active (SA) message to use the IP address of the interface as the rendezvous point (RP) address in the SA message, use the **ip msdp originator-id** command in global configuration mode. To prevent the RP address from being derived in this way, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **originator-id** *interface-type interface-number*

no ip msdp [**vrf** *vrf-name*] **originator-id** *interface-type interface-number*

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
interface-type interface-number	Interface type and number on the local router whose IP address is used as the RP address in SA messages. No space is needed between the values.

Defaults

The RP address is used as the originator ID.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **ip msdp originator-id** command identifies an interface type and number to be used as the RP address in an SA message.

Use this command if you want to configure a logical RP. Because only RPs and MSDP border routers originate SAs, there are times when it is necessary to change the ID used for this purpose.

If both the **ip msdp border sa-address** and **ip msdp originator-id** commands are configured the address derived from the **ip msdp originator-id** command determines the address of the RP to be used in the SA message.

Examples

The following example shows how to configure the IP address of Ethernet interface 1 as the RP address in SA messages:

```
ip msdp originator-id ethernet1
```

Related Commands

Command	Description
ip msdp border	Configures a router that borders a PIM sparse mode region and dense mode region to use MSDP.

ip msdp password peer

To enable message digest 5 (MD5) password authentication for TCP connections between two Multicast Source Discovery Protocol (MSDP) peers, use the **ip msdp password peer** command in global configuration mode. To disable this function, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **password peer** {*peer-name* | *peer-address*} [*encryption-type*] *string*

no ip msdp [**vrf** *vrf-name*] **password peer** {*peer-name* | *peer-address*} [*encryption-type*] *string*

Syntax Description

vrf *vrf-name*	(Optional) Enables MD5 password authentication for TCP connections between MSDP peers associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
{*peer-name* | *peer-address*}	The Domain Name System (DNS) name or IP address of the MSDP peer for which to enable MD5 password authentication.
encryption-type	(Optional) Single-digit number that defines whether the text immediately following is encrypted, and, if so, what type of encryption is used. Possible values are as follows: • **0**—Specifies that the text immediately following is not encrypted. • **7**—Specifies that the text is encrypted using an encryption algorithm defined by Cisco.
string	Case-sensitive or encrypted password.

Command Default

MD5 password authentication for TCP connections between MSDP peers is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

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

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

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

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

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

Configuring an MD5 Password in an Established MSDP Session

If you configure or change the password or key used for MD5 authentication between two MSDP peers, the local router will not tear down the existing session after you configure the password. The local router will attempt to maintain the peering session using the new password until the keepalive period expires. If the password is not entered or changed on the remote router before the keepalive period expires, the session will time out and the MSDP session will reset.

Examples

The following example shows how to configure an MD5 password for TCP connections to the MSDP peer at 10.3.32.152:

```
ip msdp password peer 10.3.32.152 0 test
```

Related Commands

Command	Description
show ip msdp peer	Displays detailed information about MSDP peers.

ip msdp peer

To configure a Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp peer** command in global configuration mode. To remove the peer relationship, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **peer** {*peer-name* | *peer-address*} [**connect-source** *interface-type interface-number*] [**remote-as** *as-number*]

no ip msdp [**vrf** *vrf-name*] **peer** {*peer-name* | *peer-address*}

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-name | *peer-address*	Domain Name System (DNS) name or IP address of the router that is to be the MSDP peer.
connect-source *interface-type interface-number*	(Optional) Specifies the interface type and number whose primary address becomes the source IP address for the TCP connection. This interface is on the router being configured.
remote-as *as-number*	(Optional) Specifies the autonomous system number of the MSDP peer. This keyword and argument are used for display purposes only.

Defaults

No MSDP peer is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The router specified should also be configured as a BGP neighbor.

The *interface-type* is on the router being configured.

If you are also BGP peering with this MSDP peer, you should use the same IP address for MSDP as you do for BGP. However, you are not required to run BGP or multiprotocol BGP with the MSDP peer, as long as there is a BGP or MBGP path between the MSDP peers. If there is no path, you must configure the **ip msdp default-peer** command.

The **remote-as** *as-number* keyword and argument are used for display purposes only.

A peer might appear to be in another autonomous system (other than the one it really resides in) when you have an MSDP peering session but do not have a BGP peer session with that peer. In this case, if the prefix of the peer is injected by another autonomous system, it displays as the autonomous system number of the peer.

Examples

The following example shows how to configure the router at the IP address 192.168.1.2 as an MSDP peer to the local router. The neighbor belongs to autonomous system 109.

```
ip msdp peer 192.168.1.2 connect-source ethernet 0/0
router bgp 110
 network 192.168.0.0
 neighbor 192.168.1.2 remote-as 109
 neighbor 192.168.1.2 update-source ethernet 0/0
```

The following example shows how to configure the router at the IP address 192.168.1.3 as an MSDP peer to the local router:

```
ip msdp peer 192.168.1.3
```

The following example shows how to configure the router at the IP address 192.168.1.4 to be an MSDP peer in autonomous system 109. The primary address of Ethernet interface 0/0 is used as the source address for the TCP connection.

```
ip msdp peer 192.168.1.4 connect-source ethernet 0/0 remote-as 109
```

Related Commands

Command	Description
ip msdp default-peer	Defines a default peer from which to accept all MSDP SA messages.
neighbor remote-as	Adds an entry to the BGP neighbor table.

ip msdp redistribute

To configure a filter to restrict which registered sources are advertised in SA messages, use the **ip msdp redistribute** command in global configuration mode. To remove the filter, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **redistribute** [**list** *access-list-name*] [**asn** *as-access-list-number*] [**route-map** *map-name*]

no ip msdp [**vrf** *vrf-name*] **redistribute**

Syntax Description

vrf *vrf-name*	(Optional) Specifies that the SA origination filter be applied to sources associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance.
list *access-list-name*	(Optional) Specifies that the router originate SA messages for local sources that are sending traffic to specific groups that match the (S, G) pairs defined in the extended access list.
asn *as-access-list-number*	(Optional) Specifies that the router originates SA messages that match the AS paths defined in the AS-path access list (configured using the **ip as-path** command). The AS-path access list number range is from 1 to 500. **Note** You can also specify a value of 0 after the **asn** keyword. If **asn 0** is specified, sources from all autonomous systems are advertised. This advertisement capability is useful when you are connecting a Protocol Independent Multicast (PIM) dense mode (PIM-DM) domain to a PIM sparse mode (PIM-SM) domain running MSDP or when you have configured MSDP on a router that is not configured with Border Gateway Protocol (BGP).
route-map *map-name*	(Optional) Specifies that the router originate SA messages for local sources that match the criteria defined in a route map.

Command Default

- If this command is not configured in a multicast network using MSDP to interconnect PIM-SM domains, only local sources are advertised in SA messages, provided the local sources are sending to groups for which the router is a rendezvous point (RP).
- If this command is not configured and if the **ip msdp border sa-address** command is configured, all local sources are advertised.
- If the **ip msdp redistribute** command is configured with no keywords and arguments, no multicast sources are advertised in SA messages.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

By default, an RP that is configured to run MSDP will originate SA messages for all local sources for which it is the RP. Local sources that register with an RP, therefore, will be advertised in SA messages, which in some cases is not desirable.

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

- You can prevent an RP from originating SA messages for local sources by configuring the **ip msdp redistribute** command without any keywords or arguments. Issuing this form of the command effectively prevents the router from advertising local sources in SA messages.

  Note When the **ip msdp redistribute** command is entered without any keywords or arguments, the router will still forward SA messages from other MSDP peers in the normal fashion; it will just not originate any SA messages for local sources.

- You can configure the router to originate SA messages for (S, G) pairs defined in an extended access list by configuring the **ip msdp redistribute** command with the optional **list** keyword and *access-list-name* argument. Issuing this form of the command effectively configures the router to originate SA messages for local sources that are sending traffic to specific groups that match (S, G) pairs defined in the extended access list. All other local sources will not be advertised in SA messages.
- You can configure the router to originate SA messages for AS paths defined in an AS-path access list by configuring the **ip msdp redistribute** command with the optional **asn** keyword and *as-access-list-number argument*. Issuing this form of the command effectively configures the router to originate SA messages for local sources that are sending traffic to specific groups that the match AS paths defined in an AS-path access list. All other local sources will not be advertised in SA messages.

  Note AS-path access lists are configured using the **ip as-path access-list** command.

- You can configure the router to originate SA messages for local sources that match the criteria defined in a route map by configuring the **ip msdp redistribute** command with the optional **route-map** keyword and *map-name* argument. Issuing this form of the command effectively configures the router to originate SA messages for local sources that match the criteria defined in the route map. All other local sources will not be advertised in SA messages.

Note You can configure an SA origination filter that includes an extended access list, an AS-path access list, and a route map (or a combination thereof). In that case, all conditions must be true before any local sources are advertised in SA messages.

Tip This command affects SA message origination, not SA message forwarding or receipt. If you want to control the forwarding of SA messages to MSDP peers or control the receipt of SA messages from MSDP peers, use the **ip msdp sa-filter out** command or the **ip msdp sa-filter in** command, respectively.

Examples

The following example shows how to configure which (S, G) entries from the mroute table are advertised in SA messages originated from AS 64512:

```
ip msdp redistribute route-map customer-sources

route-map customer-sources permit
match as-path 100

ip as-path access-list 100 permit ^64512$
```

Related Commands

Command	Description
ip as-path	Defines a BGP-related access list.
ip msdp border	Configures a router that borders a PIM sparse mode region and dense mode region to use MSDP.
ip msdp sa-filter in	Configures an incoming filter list for SA messages received from the specified MSDP peer.
ip msdp sa-filter out	Configures an outgoing filter list for SA messages sent to the MSDP peer.

ip msdp rpf rfc3618

To enable Multicast Source Discovery Protocol (MSDP) peers to be compliant with peer-Reverse Path Forwarding (RPF) forwarding rules specified in Internet Engineering Task Force (IETF) RFC 3618, use the **ip msdp rpf rfc3618** command in global configuration mode. To revert MSDP peers to non-IETF compliant peer-RPF forwarding rules, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **rpf rfc3618**

no ip msdp [**vrf** *vrf-name*] **rpf rfc3618**

Syntax Description

vrf *vrf-name*	(Optional) Enables MSDP peers associated with the Multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance specified for the *vrf-name* argument to be compliant with the peer-RPF forwarding rules specified in RFC 3618.

Command Default

MSDP peers are not compliant with peer-RPF forwarding rules specified in RFC 3618.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.0(27)S	This command was integrated into Cisco IOS Release 12.0(27)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use this command to enable MSDP peers to be compliant with peer-RPF forwarding rules specified in RFC 3618. Such compliance allows you to use Border Gateway Protocol (BGP) route reflectors without running MSDP on them. It also allows you to use an Interior Gateway Protocol (IGP) for the RPF check and thereby run peerings without BGP or Multicast Border Gateway Protocol (MBGP).

Examples

The following example shows how to enable MSDP peer-RPF forwarding rules that are compliant with RFC 3618:

```
ip msdp rpf rfc3618
```

Related Commands

Command	Description
show ip msdp rpf-peer	Displays the unique MSDP peer information from which the router will accept SA messages originating from the specified RP.

ip msdp sa-filter in

To configure an incoming filter list for Source-Active (SA) messages received from the specified Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp sa-filter in** command in global configuration mode. To remove the filter, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **sa-filter in** {*peer-address* | *peer-name*} [**list** *access-list-name*] [**route-map** *map-name*] [**rp-list** {*access-list-range* | *access-list-name*}] [**rp-route-map** *route-map reference*]

no ip msdp [**vrf** *vrf-name*] **sa-filter in** {*peer-address* | *peer-name*}

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or Domain Name System (DNS) name of the MSDP peer to which the SA messages are filtered.
list *access-list-name*	(Optional) Specifies the IP access list to pass certain source and group pairs.
route-map *map-name*	(Optional) Specifies the route map match criteria for passing certain source and group pairs.
rp-list	(Optional) Specifies an access list for an originating Route Processor.
access-list-range	Number assigned to an access list. The range is from 1 to 99.
access-list-name	Name assigned to an access list.
rp-route-map *route-map reference*	(Optional) Specifies the route map and route reference for passing through a route processor.

Command Default

No incoming messages are filtered; all SA messages are accepted from the peer.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was modified. Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **rp-list** keyword was added.

Usage Guidelines

If you use the **ip msdp sa-filter in** command without specifying access list name or route map match criteria, all source/group pairs from the peer are filtered.

If you use the **route-map** *map-name* keyword and argument pair, the specified MSDP peer passes only those SA messages that meet the match criteria.

If all match criteria are true, a **permit** keyword from the route map passes the routes through the filter. A **deny** keyword will filter routes.

Examples

The following example shows how to configure the router to filter all SA messages from the peer at 192.168.1.3:

```
Router> enable
Router# configure terminal
Router(config)# ip msdp peer 192.168.1.3 connect-source Ethernet 0/0
Router(config)# ip msdp sa-filter in 192.168.1.3
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.
ip msdp sa-filter out	Configures an outgoing filter list for SA messages sent to the specified MSDP peer.

ip msdp sa-filter out

To configure an outgoing filter list for Source-Active (SA) messages sent to the specified Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp sa-filter out** command in global configuration mode. To remove the filter, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **sa-filter out** {*peer-address* | *peer-name*} [**list** *access-list-name*] [**route-map** *map-name*] [**rp-list** {*access-list-range* | *access-list-name*}] [**rp-route-map** *route-map reference*]

no ip msdp [**vrf** *vrf-name*] **sa-filter out** {*peer-address* | *peer-name*}

Syntax Description

vrf	(Optional) Specifies the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or Domain Name System (DNS) name of the MSDP peer to which the SA messages are filtered.
list *access-list-name*	(Optional) Specifies the IP access list to pass certain source and group pairs.
route-map *map-name*	(Optional) Specifies the route map match criteria for passing certain source and group pairs.
rp-list	(Optional) Specifies an access list for an originating Route Processor.
access-list range	Number assigned to an access list. The range is from 1 to 99.
access-list name	Name assigned to an access list.
rp-route-map *route-map reference*	(Optional) Specifies the route map and route reference for passing through a route processor.

Command Default

No outgoing messages are filtered; all SA messages received are forwarded to the peer.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was modified. Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was modified. The **rp-list** keyword was added.

Usage Guidelines

If you use the **ip msdp sa-filter out** command without specifying access list name or route map match criteria, all source and group pairs from the peer are filtered. If you do specify an access-list name, the specified MSDP peer passes only those SA messages that pass the extended access list.

If you use the **route-map** *map-name* keyword and argument pair, the specified MSDP peer passes only those SA messages that meet the match criteria.

If both the **list** and **route-map** keywords are used, all conditions must be true to pass any source and group pairs in outgoing SA messages.

If all match criteria are true, a **permit** keyword from the route map will pass routes through the filter. A **deny** keyword will filter routes.

Examples

The following example shows how to permit only (S, G) pairs that pass access list 100 to be forwarded in an SA message to the peer at the IP address 192.168.1.5:

```
Router> enable
Router# configure terminal
Router(config)# ip msdp peer 192.168.1.5 connect-source ethernet 0/0
Router(config)# ip msdp sa-filter out 192.168.1.5 list 100
Router(config)# access-list 100 permit ip 172.1.0.0 0.0.255.255 224.2.0.0 0.0.255.255
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.
ip msdp sa-filter in	Configures an incoming filter list for SA messages received from the specified MSDP peer.

ip msdp sa-limit

To limit the number of Source Active (SA) messages that can be added to the SA cache from a specified Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp sa-limit** command in global configuration mode. To remove the limit imposed by the MSDP SA limiter, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **sa-limit** {*peer-name* | *peer-address*} *sa-limit*

no ip msdp [**vrf** *vrf-name*] **sa-limit** {*peer-name* | *peer-address*} *sa-limit*

Syntax Description

vrf *vrf-name*	(Optional) Specifies that the MSDP SA limiter be applied to the MSDP peer associated with Multicast Virtual Private Network (MVPN) virtual routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
peer-name | *peer-address*	Domain Name System (DNS) name or IP address of the MSDP peer for which to apply the MSDP SA limiter.
sa-limit	Maximum number of SA messages that can be accepted (cached) from the specified peer. The range is from 1 to 2147483646.

Command Default

No MSDP SA limiters are configured for MSDP peers.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(7)	This command was introduced.
12.0(15)S	This command was integrated into Cisco IOS Release 12.0(15)S.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(2)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(3)	This command was integrated into Cisco IOS Release 12.2(3).
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to configure MSDP SA limiters, which impose limits on the number of MSDP SA messages that an MSDP-enabled router can accept (can be cached) from an MSDP peer. This command provides a means to protect an MSDP-enabled router from denial of service (DoS) attacks.

Mechanics of MSDP SA Limiters

- When MSDP SA limiters are configured, the router maintains a per-peer count of SA messages stored in the SA cache.
- SA messages that exceed the limit configured for an MSDP peer are ignored.
- If the router receives SA messages in excess of the configured limit from an MSDP peer, a warning in the following format is generated (once a minute) until the cache is cleared:

```
%MSDP-4-SA_LIMIT: SA from peer <peer address or name>, RP <RP address> for <mroute>
exceeded sa-limit of <configured SA limit for MSDP peer>
```

Tips for Configuring MSDP SA Limiters

- We recommended that you configure MSDP SA limiters for all MSDP peerings on the router.
- An appropriately low MSDP SA limit should be configured on peerings with a stub MSDP region (an MSDP peer that may have some further downstream peers but does not act as a transit for SA messages across the rest of the Internet).
- An appropriately high SA limit should be configured for all MSDP peerings that act as transits for MSDP SA messages across the Internet.

The output of the **show ip msdp count**, **show ip msdp peer**, and **show ip msdp summary** commands will display the number of SA messages from each MSDP peer that is in the SA cache. If the **ip msdp sa-limit** command is configured, the output of the **show ip msdp peer** command will also display the value of the SA message limit for each MSDP peer.

Examples

The following example shows how to configure an MSDP SA limiter. In this example, an MSDP SA limiter is configured that imposes a limit of 100 SA messages from the MSDP peer at 192.168.10.1.

```
ip msdp sa-limit 192.168.10.1 100
```

Related Commands

Command	Description
show ip msdp count	Displays the number of sources and groups originated in MSDP SA messages.
show ip msdp peer	Displays detailed information about the MSDP peer.
show ip msdp summary	Displays MSDP peer status.

ip msdp sa-request

Note Effective with Cisco IOS Release 12.0(27)S, 12.2(20)S, 12.2(18)SXE, and 12.3(4)T, the **ip msdp sa-request** is not available in Cisco IOS software.

To configure the router to send Source-Active (SA) request messages to an Multicast Source Discovery Protocol (MSDP) peer when a new joiner from the group becomes active, use the **ip msdp sa-request** command in global configuration mode. To prevent this action, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **sa-request** {*peer-address* | *peer-name*}

no ip msdp [**vrf** *vrf-name*] **sa-request** {*peer-address* | *peer-name*}

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or name of the MSDP peer from which the local router requests SA messages when a new joiner for the group becomes active.

Defaults

The router does not send SA request messages to the MSDP peer.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.0(27)S	This command was removed from Cisco IOS Release 12.0(27)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(20)S	This command was removed from Cisco IOS Release 12.2(20)S.
12.2(18)SXE	This command was removed from Cisco IOS Release 12.2(18)SXE.
12.3(4)T	This command was removed from Cisco IOS Release 12.3(4)T.

Usage Guidelines

By default, the router does not send any SA request messages to its MSDP peers when a new member joins a group and wants to receive multicast traffic. The new member waits to receive any SA messages that eventually arrive.

Use this command if you want a new member of a group to learn the current, active multicast sources in a connected Protocol Independent Multicast sparse mode (PIM-SM) domain that are sending to a group. The router will send SA request messages to the specified MSDP peer when a new member joins a group. The peer replies with the information in its SA cache. If the peer does not have a cache configured, this command provides nothing.

An alternative to this command is using the **ip msdp cache-sa-state** command to have the router cache messages.

Examples

The following example shows how to configure the router to send SA request messages to the MSDP peer at the IP address 192.168.10.1:

```
ip msdp sa-request 192.168.10.1
```

Related Commands

Command	Description
ip msdp cache-sa-state	Enables the router to create SA state.
ip msdp peer	Configures an MSDP peer.

ip msdp shutdown

To administratively shut down a configured Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp shutdown** command in global configuration mode. To bring the peer back up, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **shutdown** {*peer-address* | *peer-name*}

no ip msdp [**vrf** *vrf-name*] **shutdown** {*peer-address* | *peer-name*}

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or name of the MSDP peer to shut down.

Defaults

No action is taken to shut down an MSDP peer.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example shows how to shut down the MSDP peer at IP address 192.168.7.20:

```
ip msdp shutdown 192.168.7.20
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

ip msdp timer

To adjust the interval at which Multicast Source Discovery Protocol (MSDP) peers will wait after peering sessions are reset before attempting to reestablish the peering sessions, use the **ip msdp timer** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **timer** *connection-retry-interval*

no ip msdp [**vrf** *vrf-name*] **timer**

Syntax Description

vrf *vrf-name*	(Optional) Sets the connection-retry interval for MSDP peers associated with the multicast VPN routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
connection-retry-interval	Interval, in seconds, at which MSDP peers will wait after peering sessions are reset before attempting to reestablish the peering sessions. The range is from 1 to 60 seconds. The default is 30 seconds.

Command Default

An MSDP peer will wait 30 seconds after a peering session is reset before attempting to reestablish the peering session with any peer.

Command Modes

Global configuration

Command History

Release	Modification
12.1(8a)E4	This command was introduced.
12.2(5)	This command was integrated into Cisco IOS Release 12.2(5).
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip msdp timer** command to adjust the interval at which all MSDP peers will wait after peering sessions are reset before attempting to reestablish the peering sessions. This interval is referred to as the connection-retry interval. By default, MSDP peers will wait 30 seconds after is session is reset before attempting to reestablish sessions with other peers. When the **ip msdp timer** command is configured, the configured connection-retry interval applies to all MSDP peering sessions on the router.

In network environments where fast recovery of Source-Active (SA) messages is required (such as in trading floor network environments), you may want to decrease the connection-retry interval to a time value less than the default value of 30 seconds.

Examples

The following example shows how to set the connection-retry interval for all MSDP peers to 20 seconds:

```
ip msdp timer 20
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

ip msdp ttl-threshold

To limit which multicast data packets are sent in Source-Active (SA) messages to a Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp ttl-threshold** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **ttl-threshold** {*peer-address* | *peer-name*} *ttl-value*

no ip msdp [**vrf** *vrf-name*] **ttl-threshold** {*peer-address* | *peer-name*}

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
peer-address | *peer-name*	IP address or name of the MSDP peer to which the *ttl-value* argument value applies.
ttl-value	Time-to-live (TTL) value; valid values are from 0 to 255. The default value of the *ttl-value* argument is 0, meaning all multicast data packets are forwarded to the peer until the TTL is exhausted.

Defaults

ttl-value: 0

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command limits which multicast data packets are sent in data-encapsulated SA messages. Only multicast packets with an IP header TTL greater than or equal to the *ttl-value* argument are sent to the MSDP peer specified by the IP address or name.

Use this command if you want to use TTL to scope your multicast data traffic. For example, you could limit internal traffic to a TTL of 8. If you want other groups to go to external locations, you would need to send those packets with a TTL greater than 8.

The default value of the *ttl-value* argument is 0, which means that all multicast data packets are forwarded to the peer until the TTL is exhausted.

Examples

The following example shows how to configure a TTL threshold of 8 hops:

```
ip msdp ttl-threshold 192.168.1.5 8
```

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

ip multicast boundary

To configure an administratively scoped IPv4 multicast boundary, use the **ip multicast boundary** command in interface configuration mode. To remove the boundary, use the **no** form of this command.

ip multicast boundary *access-list* [**filter-autorp**]

no ip multicast boundary *access-list* [**filter-autorp**]

Cisco IOS 12.3(11)T and Subsequent T and Mainline Releases

ip multicast boundary *access-list* [**filter-autorp | in | out**]

no ip multicast boundary *access-list* [**filter-autorp | in | out**]

Syntax Description

access-list	Number or name identifying an access control list (ACL) that controls the range of group addresses or (S, G) traffic affected by the boundary.
filter-autorp	(Optional) Filters auto-rendezvous point (Auto-RP) messages denied by the boundary ACL.
in	(Optional) Filters source traffic coming into the interface that is denied by the boundary ACL.
out	(Optional) Prevents multicast route (mroute) states from being created on an interface by filtering Protocol Independent Multicast (PIM) joins and Internet Group Management Protocol (IGMP) reports for groups or channels that are denied by the boundary ACL.

Command Default

No administratively scoped boundaries are configured.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
11.1	This command was introduced.
12.0(22)S	The **filter-autorp** keyword was added.
12.1(12c)E	The **filter-autorp** keyword was integrated into Cisco IOS Release 12.1(12c)E.
12.2(11)	The **filter-autorp** keyword was integrated into Cisco IOS Release 12.2(11).
12.2(13)T	The **filter-autorp** keyword was integrated into Cisco IOS Release 12.2(13)T.
12.3(11)T	The **in** and **out** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Use the **ip multicast boundary** command to configure an administratively scoped boundary on an interface in order to filter source traffic coming into the interface and prevent mroute states from being created on the interface.

Note An IP multicast boundary enables reuse of the same multicast group address in different administrative domains.

A standard ACL is used with the **ip multicast boundary** command to define the group address range to be permitted or denied on an interface. An extended ACL is used with the **ip multicast boundary** to define (S, G) traffic to be permitted or denied on an interface. Extended ACLs can also be used to define the (*, G) state to be permitted or denied on an interface, by specifying **host 0.0.0.0** for the source address in the permit statements that compose the extended ACL.

When you configure IP multicast boundaries for (S, G) traffic in an Any Source Multicast (ASM) network environment—to ensure that the IP multicast boundaries function properly—you must configure an extended ACL on routers along the rendezvous point tree (RPT) that permits:

- (S, G) traffic by specifying the source and group address range in permit statements.
- (*, G) traffic by specifying **host 0.0.0.0** for the source address followed by the group address or group address range in permit statements.
- Traffic destined to the rendezvous point (RP) by including permit statements for (RP, G), where the IP address of the RP is specified for the source followed by the group address or group address range.

Note The IP multicast boundary guideline for ASM applies only to the routers on the RPT from the last-hop router to the RP. For routers on the RP-to-source branch, you need to define only the (S, G) traffic in the extended ACL (by specifying the source and group address range in permit statements).

When you configure IP multicast boundaries for (S, G) traffic in a Source Specific Multicast (SSM) network environment, you need to define only the (S, G) traffic to be permitted or denied on an interface in the extended ACL.

Note IP multicast boundaries filter data and control plane traffic including IGMP, PIM, and Auto-RP messages. PIM Register messages are sent using unicast and will *not* be filtered.

If you configure the **filter-autorp** keyword, the administratively scoped boundary also examines Auto-RP discovery and announcement messages and removes any Auto-RP group range announcements from the Auto-RP packets that are denied by the boundary ACL. An Auto-RP group range announcement is permitted and passed by the boundary only if all addresses in the Auto-RP group range are permitted by the boundary ACL. If any address is not permitted, the entire group range is filtered and removed from the Auto-RP message before the Auto-RP message is forwarded.

Note Extended ACLs cannot be used with the **filter-autorp** keyword because Auto-RP announcements do not contain source addresses.

In Cisco IOS software releases that do not support the **in** and **out** keywords, the IP multicast boundary both filters source traffic coming into the interface and prevents mroute states from being created on the interface.

In Cisco IOS releases that support the **in** and **out** keywords, these keywords are used as follows:

- The **in** keyword is used to filter source traffic coming into the interface.
- The **out** keyword is used to prevent mroute states from being created on an interface; that is, it will prevent IGMP reports and PIM joins from creating mroutes states for groups and channels denied by the boundary ACL, and the interface will not be included in the outgoing interface list (OIL).
- If a direction is not specified with the **ip multicast boundary** command, the IP multicast boundary both filters source traffic coming into the interface and prevents mroute states from being created on the interface.

In addition, the following rules govern the use of the **in**, **out**, and **filter-autorp** keywords with the **ip multicast boundary** command:

- The **in** and **out** keywords support standard or extended ACLs for (S, G) filtering.
- The **in** and **out** keywords support standard or extended ACLs for SSM filtering.
- One instance of the **in** and **out** keywords can be configured on an interface.
- Only standard ACLs are permitted with the use of the **filter-autorp** keyword.

In Cisco 7600 series routers:

- A deny any statement at the end of the boundary ACL will cause all multicast boundaries including the link local address in the range (224.0.0.0 - 224.0.0.255) to be dropped in the hardware.
- When the **ip multicast boundary** *access-list* [**filter-autorp**] command is configured with an empty ACL, it interferes in the proper functioning of Auto-RP in the hardware. Hence, it is important to specify the address you want to allow or deny in the access-list.

Note A maximum of three instances of an **ip multicast boundary** command is allowed on an interface: one instance of the command with the **in** keyword, one instance of the command with the **out** keyword, and one instance of the command with or without the **filter-autorp** keyword.

Examples

The following example shows how to set up an IP multicast boundary for all administratively scoped IPv4 multicast addresses by denying the entire administratively scoped IPv4 multicast address space (239.0.0.0/8). All other Class D addresses are permitted (224.0.0.0/4).

```
access-list 1 deny 239.0.0.0 0.255.255.255
access-list 1 permit 224.0.0.0 15.255.255.255
interface ethernet 0
 ip multicast boundary 1
```

The following example shows how to set up an IP multicast boundary in an SSM network environment. In this example, the IP multicast boundary is configured to permit mroute states for (172.16.2.201, 232.1.1.1) and (172.16.2.202, 232.1.1.1). All other (S, G) traffic is implicitly denied.

```
ip access-list extended acc_grp1
permit ip host 172.16.2.201 host 232.1.1.1
permit ip host 172.16.2.202 host 232.1.1.1
interface ethernet 2/3
 ip multicast boundary acc_grp1 out
```

The following example shows how to configure an IP multicast boundary in an ASM network environment. In this example, the IP multicast boundary configuration on the last-hop router is shown. The topology for this example is not illustrated; however, assume that the IP address of the RP in this scenario is 10.1.255.104. The IP multicast boundary is configured to filter outgoing IP multicast traffic on Fast Ethernet interface 0/0. The boundary ACL used for the IP multicast boundary in this scenario contains three permit statements:

- The first permit statement specifies the (S, G) traffic to be permitted.
- The second permit statement specifies the (RP, G) traffic to be permitted.
- The third permit statement specifies the (*, G) traffic to be permitted.

All other outgoing multicast traffic on this interface is implicitly denied.

```
ip access-list extended bndry-asm-3
 permit ip host 10.1.248.120 239.255.0.0 0.0.255.255
 permit ip host 10.1.255.104 239.255.0.0 0.0.255.255
 permit ip host 0.0.0.0 239.255.0.0 0.0.255.255
interface FastEthernet0/0
 ip multicast boundary bndry-asm-3 out
```

ip multicast cache-headers

Note Effective with Cisco IOS Release 15.0(1)M and Cisco IOS Release 12.2(33)SRE, the **ip multicast cache-headers** command is not available in Cisco IOS software.

To allocate a circular buffer to store IP multicast packet headers that the router receives, use the **ip multicast cache-headers** command in global configuration mode. To remove the buffer, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **cache-headers** [**rtp**]

no ip multicast [**vrf** *vrf-name*] **cache-headers** [**rtp**]

Syntax Description

vrf *vrf-name*	(Optional) Allocates a circular buffer to store IP multicast packet headers associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
rtp	(Optional) Caches Real-Time Transport Protocol (RTP) headers.

Defaults

The command is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.1	The **rtp** keyword was added.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was implemented on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was removed.
12.2(33)SRE	This command was removed.

Usage Guidelines

IP multicast packet headers can be stored in a cache and then displayed to determine the following information:

- Who is sending IP multicast packets to which groups
- Interpacket delay
- Duplicate IP multicast packets (if any)

- Multicast forwarding loops in your network (if any)
- Scope of the group
- User Datagram Protocol (UDP) port numbers
- Packet length

Use the **show ip mpacket** command to display the buffer.

Examples

The following example shows how to allocate a buffer to store IP multicast packet headers:

```
ip multicast cache-headers
```

Related Commands

Command	Description
show ip mpacket	Displays the contents of the circular cache header buffer.

ip multicast default-rpf-distance

When configuring Internet Group Management Protocol (IGMP) unidirectional link routing (UDLR), to change the distance given to the default Reverse Path Forwarding (RPF) interface, use the **ip multicast default-rpf-distance** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip multicast default-rpf-distance *distance*

no ip multicast default-rpf-distance *distance*

Syntax Description

distance	Distance given to the default RPF interface. The default value is 15.

Defaults

distance: 15

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is optional. If you want to receive all multicast traffic from all sources on the unidirectional link (UDL), as long as 15 is the lowest distance, you need not change the value of 15.

The default RPF interface is selected when an IGMP query message is received on a UDL and indicates to the router that all sources will use RPF to reach the UDL interface.

Any explicit sources learned by routing protocols will take preference as long as their distance is less than the *distance* argument configured with the **ip multicast default-rpf-distance** command.

You might consider changing the default value for one of the following reasons:

- To make IGMP prefer the UDL.
- To configure a value less than existing routing protocols.
- If you want to receive multicast packets from sources on interfaces other than the UDL interface. Configure a value greater than the distances of the existing routing protocols to make IGMP prefer the nonunidirectional link.

Examples

The following example configures a distance of 20:

```
ip multicast default-rpf-distance 20
```

Related Commands

Command	Description
ip igmp unidirectional-link	Configures an interface to be unidirectional and enables it for IGMP UDLR.

ip multicast group-range

To define a global range of IP multicast groups and channels to be permitted or denied, use the **ip multicast group-range** command in global configuration mode. To remove the global IP multicast address group range, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **group-range** *access-list*

no ip multicast [**vrf** *vrf-name*] **group-range**

Syntax Description

vrf *vrf-name*	(Optional) Applies the multicast group address range to group addresses associated with the Multicast Virtual Private Network (MVPN) routing and forwarding instance (MVRF) specified for the *vrf-name* argument.
access-list	Access control list (ACL) that defines the multicast groups to be permitted or denied.

Command Default

A global IP multicast group address range is not defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Use the **ip multicast group-range** command to define a global range of IP multicast groups and channels to be permitted or denied. This command is used to disable multicast protocol actions and traffic forwarding for unauthorized groups or channels for all interfaces on the router.

Use the optional **vrf** keyword with the *vrf-name* argument to apply an IP multicast group address range to the MVRF instance specified for the *vrf-name* argument.

For the required *access-list* argument, specify an access list that defines the multicast groups or channels to be permitted or denied globally:

- A standard ACL can be used to define the group address range to be permitted or denied globally.
- An extended ACL is used with the **ip multicast group-range** command to define (S, G) traffic to be permitted or denied globally. Extended ACLs can also be used to define the (*, G) state to be permitted or denied globally, by specifying **host 0.0.0.0** for the source address in the permit statements that compose the extended ACL.

Note When using the **ip multicast group-range** command to configure a multicast address group range in an AutoRP network, you must explicitly permit the AutoRP groups (39/40) in the access list that defines the range; if not, AutoRP packets will not be accepted or forwarded.

Note If AutoRP is enabled, but a specific group range is denied (for example, 224/8), an AutoRP message for that range will be accepted and the RP mapping will be put into the cache. However, state will not be created for those groups.

Examples

Allowing Groups 239/8 and AutoRP Groups (.39 and .40) to Operate in an Enterprise Network

The following example shows how to configure an IP multicast address group range that allows the 239/8 range and AutoRP groups to operate in an enterprise network:

```
ip multicast group-range 1

access-list 1 permit 224.0.1.39 0.0.0.0
access-list 1 permit 224.0.1.40 0.0.0.0
access-list 1 permit 239.0.0.0 0.255.255.255
```

Allowing Groups 239/8 in a Campus Network and Groups 239/9 on Interfaces Connected to Remote Branches

The following example shows how to configure an IP multicast group range that permits groups 239/8 in a campus network. For remote branches connected through Serial interface 0, an IP multicast boundary is configured to further refine the groups permitted to 239/9.

```
ip multicast group-range 1
access-list 1 permit 239.0.0.0 0.255.255.255

interface Serial 0
  ip multicast boundary 2
access-list 2 permit 239.128.0.0 0.127.255.255
```

Allowing Groups 239/8 Globally and AutoRP Groups (.39 and .40) on Core-Facing Interfaces

The following example shows how to configure an IP multicast group range that allows the 239/8 range. In this example, AutoRP groups are denied on access interfaces and permitted on core-facing interfaces. In addition, to permit AutoRP groups on core-facing interfaces, an IP multicast boundary is configured in this example that permits AutoRP groups (.39 and .40).

```
ip multicast group-range 1
access-list 1 permit 239.0.0.0 0.255.255.255

interface Ethernet 0
 description access interface
 ip pim sparse-mode

interface Ethernet 1
 description core facing interface
 ip multicast boundary 2

access-list 2 permit 224.0.1.39
access-list 2 permit 224.0.1.40
access-list 2 permit 239.0.0.0 0.255.255.255
```

ip multicast hardware-switching non-rpf aging

To configure the multicast hardware switching for rate-limiting of non-RP aging traffic, use the **ip multicast hardware-switching non-rpf aging** command in global configuration mode. To disable, use the **no** form of this command.

ip multicast hardware-switching non-rpf aging { **fast** *2-10* | **global** *0-180*}

no ip multicast hardware-switching non-rpf aging { **fast** *2-10* | **global** *0-180*}

Syntax Description

fast	Enables NON-RPF aging fast timer.
2-10	Fast aging timing interval.
global	Enables NON-RPF aging global timer.
0-180	Global aging time interval.

Defaults

The default state is OFF.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRE	Support for this command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to configure the multicast hardware switching for rate-limiting of non-RP traffic:

```
Router# enable
Router# configure terminal
Router(config)# ip multicast hardware-switching non-rp aging
```

Related Commands

Command	Description
ip multicast hardware-switching replication-mode	Switches hardware replication mode among auto-detection and ingress and egress replication.

ip multicast hardware-switching replication-mode

To switch hardware replication mode among auto-detection and ingress and egress replication, use the **ip multicast hardware-switching replication-mode** command in global configuration mode. To restore the system to automatic detection mode, use the **no** form of this command.

ip multicast hardware-switching replication-mode {**egress** | **ingress**}

no ip multicast hardware-switching replication-mode {**egress** | **ingress**}

Syntax Description

egress	Forces the system to the egress mode of replication.
ingress	Forces the system to the ingress mode of replication.

Defaults

The Supervisor Engine 720 automatically detects the replication mode based on the module types that are installed in the system. If all modules are capable of egress replication, the system uses egress-replication mode. If the supervisor engine detects the modules that are not capable of egress replication, the replication mode automatically switches to ingress replication.

If the system is functioning in the automatic-detection egress mode, and you install a module that cannot perform egress replication, the following occurs:

- The Cisco 7600 series router reverts to ingress mode.
- A system log is generated.
- A system reload occurs to revert to the old configuration.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRE	Support for this command was introduced on the Cisco 7600 series routers.

Usage Guidelines

This command is supported on Supervisor Engine 720, Supervisor Engine 32, Route Switching Processor 720, and compatible DFCDs.

Note During the change from egress- to ingress-replication mode, traffic interruptions may occur because the shortcuts are purged and reinstalled. To avoid interruptions in traffic forwarding, enter the **ip multicast hardware-switching replication-mode ingress** command.

If you enter the **no ip multicast hardware-switching replication-mode egress** command, only the forced-egress mode resets and not the forced-ingress mode.

If you enter the **no ip multicast hardware-switching replication-mode ingress** command, only the forced-ingress mode resets and not the forced-egress mode.

Examples

This example shows how to enable the ingress-replication mode:

```
Router# enable
Router# configure terminal
Router(config)# ip multicast hardware-switching replication-mode ingress
```

This example shows how to enable the egress-replication mode:

```
Router# enable
Router# configure terminal
Router(config)# ip multicast hardware-switching replication-mode egress
```

This example shows how to disable the current egress-replication mode and return to automatic detection mode:

```
Router# enable
Router# configure terminal
Router(config)# no ip multicast hardware-switching replication-mode egress
```

Related Commands

Command	Description
ip multicast hardware-switching non-rpf aging	Configures the multicast hardware switching for rate-limiting of non-RP aging traffic.

ip multicast heartbeat

To monitor the delivery of multicast traffic for a multicast group via Simple Network Management Protocol (SNMP) traps, use the **ip multicast heartbeat** command in global configuration mode. To disable the monitoring of multicast traffic for a multicast group, use the **no** form of this command.

ip multicast heartbeat *group-address minimum-number-intervals window-size seconds*

no ip multicast heartbeat *group-address*

Syntax Description

group-address	A multicast group Class D address, from 224.0.0.0 to 239.255.255.255.
minimum-number-intervals	Minimum number of intervals where a multicast heartbeat must be present. The range is from 1 to 100. **Note** The value specified for this argument must be less than or equal to the value specified for the *window-size* argument.
window-size	Number of intervals to monitor for a multicast heartbeat. The range is from 1 to 100. **Note** The value specified for this argument must be greater than or equal to the value specified for the *minimum-number-intervals* argument.
seconds	Length of an interval. The range is from 10 to 3600 seconds. **Note** The value entered for the *seconds* argument must be a multiple of 10.

Command Default

The monitoring of multicast traffic delivery via SNMP traps is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to configure a multicast router to send SNMP traps to a network management station (NMS) when multicast source traffic being sent to a multicast group fails to meet certain multicast delivery parameters.

When this command is configured, the router monitors multicast source traffic destined to the multicast group address specified for the *group-address* argument for the number of seconds configured for the *seconds* argument (the interval). The number of packets present in the interval is not as important as whether any multicast source packets destined to the group were forwarded at all during the interval. A "heartbeat" is present if at least one source packet sent to the group was forwarded during the interval.

Note A multicast heartbeat is determined by the counter of both the (*, G) and the (S, G) state of a group being tracked. An increment in the counters of any such state is considered to constitute forwarding for the group within the interval.

In addition to the required *seconds* argument value, two other required parameters must be configured: a value for the *minimum-number-intervals* argument and a value for the *window-size* argument. The *minimum-number-intervals* argument is used to specify the minimum number of intervals where a multicast heartbeat must be present. The *window-size* argument is used to specify the number of intervals to monitor for a multicast heartbeat (the interval window).

If after the interval window the router detected a heartbeat in fewer intervals than the minimum, an SNMP trap would be sent from this router to an NMS. The SNMP trap is used to indicate a loss of heartbeat. The SNMP trap triggered by this command is ciscoIpMRouteMissingHeartBeats, which is defined in CISCO-IPMROUTE-MIB.

The **ip multicast heartbeat** command will not create a multicast forwarding state in the router. Use the **ip igmp static-group** command on the router or on a downstream router to force forwarding of IP multicast traffic.

Use the **snmp-server enable traps** command with the **ipmulticast** keyword to enable the generation of traps associated with multicast heartbeat monitoring. Use the **snmp-server host** command to configure the sending of IP multicast traps to specific receiver hosts.

Use the **debug ip mhbeat** command to enable debugging output for IP multicast heartbeat monitoring.

Examples

The following example shows how to configure a multicast router to send SNMP traps to an NMS when multicast source traffic being sent to multicast group fails to meet certain multicast delivery parameters. In this example, a multicast router is configured to monitor the packets forwarded for group 239.1.1.53 in intervals of 10 seconds. If at least one packet is forwarded during two out of the last five intervals (the interval window), an SNMP trap will not be generated. An SNMP trap would be generated only if the router did not see packets forwarded during three or more of the 10-second intervals within the interval window of five samples.

```
snmp-server enable traps ipmulticast
ip multicast heartbeat 239.1.1.53 2 5 10
```

Related Commandsl

Command	Description
debug ip mhbeat	Enables debugging output for IP multicast heartbeat monitoring.
ip igmp static-group	Configures static group membership entries on an interface.
snmp-server enable traps	Enables the router to send SNMP traps.
snmp-server host	Specifies the recipient of an SNMP notification operation.

ip multicast helper-map

To allow IP multicast routing in a multicast-capable internetwork between two broadcast-only internetworks, use the **ip multicast helper-map** command in interface configuration mode. To disable this function, use the **no** form of this command.

ip multicast helper-map {*group-address broadcast-address* | **broadcast** *multicast-address*} *access-list* [**ttl** *remapping-value*]

no ip multicast helper-map {*group-address broadcast-address* | **broadcast** *multicast-address*} *access-list* [**ttl** *remapping-value*]

Syntax Description

group-address	Multicast group address of traffic to be converted to broadcast traffic. Use this value with the *broadcast-address* value.
broadcast-address	Address to which broadcast traffic is sent. Use this value with the *group-address* value.
broadcast	Specifies the traffic to be converted from broadcast to multicast. Use this keyword with the *multicast-address* value.
multicast-address	IP multicast address to which the converted traffic is directed. Use this value with the **broadcast** keyword.
access-list	IP extended access list number or name that controls which broadcast packets are translated, based on the User Datagram Protocol (UDP) port number.
ttl *remapping-value*	(Optional) Configures the Time-to-Live (TTL) value of multicast packets generated by the helper-map from incoming broadcast packets. Valid values are from 1 to 50 hops. The default TTL value is 1 hop.

Command Default

No conversion between broadcast and multicast occurs.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
11.1	This command was introduced.
12.2(18)SXF	Support for this command was introduced on the Supervisor Engine 720. The **ttl** keyword and *remapping-value* arguments were added.
12.4(6)T	The **ttl** keyword and *remapping-value* arguments were added.
12.4(7)	The **ttl** keyword and *remapping-value* arguments were added.
12.3(19)	The **ttl** keyword and *remapping-value* arguments were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

When a multicast-capable internetwork is between two broadcast-only internetworks, you can convert broadcast traffic to multicast at the first hop router, and convert it back to broadcast at the last hop router before delivering the packets to the broadcast clients. However, broadcast packets with the IP source address of 0.0.0.0 (such as a Dynamic Host Configuration Protocol [DHCP] request) will not be translated to any multicast group. Thus, you can take advantage of the multicast capability of the intermediate multicast internetwork. This feature prevents unnecessary replication at the intermediate routers and allows multicast fast switching in the multicast internetwork.

If you need to send a directed broadcast to the subnet, the outgoing interface of the last hop router can be configured with an IP broadcast address of x.x.x.255, where x.x.x.0 is the subnet that you are trying to reach; otherwise, the packet will be converted to 255.255.255.255.

By default, many broadcast applications use a default TTL value of 1. Because the helper-map applies the decremented TTL value of the incoming broadcast packet for the generated multicast packet, and most broadcast applications use a TTL value of 1 hop, broadcast packets may not be translated to multicast packets, and thus, may be dropped rather than forwarded. To circumvent this potential issue, you can manually configure the TTL value for broadcast packets being translated into multicast packets using the **ttl** keyword and *remapping-value* argument. For the *remapping-value* argument, specify a value that will enable the translated packets to reach multicast receivers.

Examples

The following example shows how to allow IP multicast routing in a multicast-capable internetwork between two broadcast-only internetworks.

In this example, assume that a server on the LAN connected to the Ethernet interface 0 of the first hop router is sending a UDP broadcast stream with a source address of 126.1.22.199 and a destination address of 126.1.22.255:4000. Based on that scenario, the configuration on the first hop router converts the broadcast stream arriving at incoming Ethernet interface 0 destined for UDP port 4000 to a multicast stream. The access list permits traffic being sent from the server at 126.1.22.199 being sent to 126.1.22.255:4000. The traffic is sent to group address 239.254.2.5. The **ip forward-protocol** command specifies the forwarding of broadcast messages destined for UDP port 4000.

The second configuration on the last hop router converts the multicast stream arriving at incoming Ethernet interface 1 back to broadcast at outgoing Ethernet interface 2. Again, not all multicast traffic emerging from the multicast cloud should be converted from multicast to broadcast, only the traffic destined for 126.1.22.255:4000.

The configurations for the first and last hop routers are as follows:

First Hop Router Configuration

```
interface ethernet 0
 ip address 126.1.22.1 255.255.255.0
 ip pim sparse-mode
 ip multicast helper-map broadcast 239.254.2.5 105
access-list 105 permit udp host 126.1.22.199 host 126.1.22.255 eq 4000
ip forward-protocol udp 4000
```

Last Hop Router Configuration

```
interface ethernet 1
 ip address 126.1.26.1 255.255.255.0
 ip pim sparse-mode
 ip multicast helper-map 239.254.2.5 126.1.28.255 105
```

```
interface ethernet 2
 ip address 126.1.28.1 255.255.255.0
 ip directed-broadcast
access-list 105 permit udp host 126.1.22.199 any eq 4000
ip forward-protocol udp 4000
```

Related Commands

Command	Description
ip directed-broadcast	Enables the translation of directed broadcast to physical broadcasts.
ip forward-protocol	Specifies which protocols and ports the router forwards when forwarding broadcast packets.

ip multicast limit

To configure per interface multicast route (mroute) state limiters, use the **ip multicast limit** command in interface configuration mode. To remove the limit imposed by a per interface mroute state limiter, use the **no** form of this command.

ip multicast limit [**connected** | **out** | **rpf**] *access-list max-entries*

no ip multicast limit [**connected** | **out** | **rpf**] *access-list max-entries*

Syntax Description

connected	(Optional) Limits mroute states created for an access control list (ACL)-classified set of multicast traffic on an incoming (Reverse Path Forwarding [RPF]) interface that is directly connected to a multicast source by accounting each time that an mroute permitted by the ACL is created or deleted.
out	(Optional) Limits mroute outgoing interface list (olist) membership on an outgoing interface for an ACL-classified set of multicast traffic by accounting each time that an mroute olist member permitted by the ACL is added or removed.
rpf	(Optional) Limits the number of mroute states created for an ACL-classified set of multicast traffic on an incoming (RPF) interface by accounting each time an mroute permitted by the ACL is created or deleted.
access-list	Number or name identifying the ACL that defines the set of multicast traffic to be applied to a per interface mroute state limiter.
max-entries	Maximum number of mroutes permitted by the per interface mroute state limiter. The range is from 0 to 2147483647.

Command Default

No per interface mroute state limiters are configured.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Use the **ip multicast limit** command to configure mroute state limiters on an interface.

The following forms of the **ip multicast limit** command are available to configure per interface mroute state limiters:

- **ip multicast limit** *access-list max-entries*

  This command limits mroute state creation for an ACL-classified set of traffic on an interface when the interface is an outgoing (egress) interface, and limits mroute outgoing interface list (olist) membership when the interface is an incoming (ingress) Reverse Path Forwarding (RPF) interface.

  This type of per interface mroute state limiter limits mroute state creation—by accounting each time an mroute permitted by the ACL is created or deleted—and limits mroute olist membership—by accounting each time that an mroute olist member permitted by the ACL is added or removed.

  Entering this form of the command (that is, with no optional keywords) is equivalent to specifying the **ip multicast limit rpf** and **ip multicast limit out** forms of the command.

- **ip multicast limit connected** *access-list max-entries*

  This command limits mroute state creation for an ACL-classified set of multicast traffic on an incoming (RPF) interface that is directly connected to a multicast source by accounting each time that an mroute permitted by the ACL is created or deleted.

- **ip multicast limit out** *access-list max-entries*

  This command limits mroute olist membership on an outgoing interface for an ACL-classified set of multicast traffic by accounting each time that an mroute olist member permitted by the ACL is added or removed.

- **ip multicast limit rpf** *access-list max-entries*

  This command limits mroute state creation for an ACL-classified set of multicast traffic on an incoming (RPF) interface by accounting each time an mroute permitted by the ACL is created or deleted.

For the required *access-list* argument, specify the ACL that defines the IP multicast traffic to be limited on an interface. A standard or extended ACL can be specified. Standard ACLs can be used to define the (*, G) state to be limited on an interface. Extended ACLs can be used to define the (S, G) state to be limited on an interface. Extended ACLs also can be used to define the (*, G) state to be limited on an interface, by specifying 0.0.0.0 for the source address and source wildcard—referred to as (0, G)—in the permit or deny statements that compose the extended access list.

Mechanics of Per Interface Mroute State Limiters

The mechanics of per interface mroute state limiters are as follows:

- Each time the state for an mroute is created or deleted and each time an olist member is added or removed, the Cisco IOS software searches for a corresponding per interface mroute state limiter that matches the mroute.
- In the case of the creation and deletion of mroutes, the Cisco IOS software searches for a per interface mroute state limiter configured on the incoming (RPF) interface that matches the mroute to be created or deleted. In the case of olist member addition or removal, the Cisco IOS software searches for a per interface mroute state limiter configured on the outgoing interface that matches the mroute to be added or removed.
- The Cisco IOS software performs a top-down search from the list of configured per interface mroute state limiters. Only per interface mroute state limiters that match the direction of traffic are considered. The first per interface mroute state limiter that matches is used for limiting (sometimes referred to as *accounting*). A match is found when the ACL permits the mroute state.

- When a match is found, the counter of the per interface mroute state limiter is updated (increased or decreased). If no per interface mroute state limiter is found that matches an mroute, no accounting is performed for the mroute (because there is no counter to update).
- The amount to update the counter with is called the *cost* (sometimes referred to as the *cost multiplier*). The default cost is 1.

Note A per interface mroute state limiter always allows the deletion of an mroute or the removal of an interface from the olist. In those cases, the respective per interface mroute state limiter decreases the counter by the value of the cost multiplier. In addition, RPF changes to an existing mroute are always allowed (in order to not affect existing traffic). However, a per interface mroute state limiter *only* allows the creation of an mroute or the addition of an mroute olist member if adding the cost does not exceed the maximum number of mroutes permitted.

Tips for Configuring Per Interface Mroute State Limiters

- To ensure that all mroutes are accounted, you can configure a per interface mroute state limiter whose ACL contains a **permit any** statement and set the maximum for the *max-entries* argument to 0. Configuring an mroute state limiter in this manner effectively denies all fall through states, which may be a way to prevent a multicast DoS attack in and out of the interface.
- When creating an ACL, remember that, by default, the end of the ACL contains an implicit **deny any** statement for everything if it did not find a match before reaching the end.
- An explicit deny statement for a specific mroute in an ACL can be used to specify the state that will not match the ACL (thus, preventing the ACL from being accounted). If an mroute matches a deny statement, the search immediately continues to the next configured mroute state limiter. Configuring an explicit deny statement in an ACL can be more efficient than forcing the mroute to fall through an ACL (by means of the implicit **deny any** statement at the end of the ACL).

Examples

The following example shows the configuration of per interface mroute state limiters. In this example, a service provider uses per interface mroute state limiters to provide a multicast Call Admission Control (CAC) in a network environment where all the multicast flows utilize the same amount of bandwidth. The service provider configures three mroute state limits on Gigabit Ethernet interface 0/0 to provide the multicast CAC needed to provision an interface for Standard Definition (SD) channel bundles being offered to subscribers:

- An mroute state limit of 75 for the SD channels that match acl-basic.
- An mroute state limit of 25 for the SD channels that match acl-premium.
- An mroute state limit of 25 for the SD channels that match acl-gold.

```
interface GigabitEthernet0/0
description --- Interface towards the DSLAM ---
.
.
.
ip multicast limit out acl-basic 75
ip multicast limit out acl-premium 75
ip multicast limit out acl-gold 25
```

Related Commands

Command	Description
clear ip multicast limit	Resets the exceeded counter for per interface mroute state limiters.
debug ip mrouting limits	Displays debugging information about configured per interface mroute state limiters and bandwidth-based multicast CAC policies.
ip multicast limit cost	Applies costs to mroute state limiters.
show ip multicast limit	Displays statistics about configured per interface mroute state limiters.

ip multicast limit cost

To apply a cost to mroutes that match per interface mroute state limiters, use the **ip multicast limit cost** command in global configuration mode. To restore the default cost for mroutes being limited by per interface mroute state limiters, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **limit cost** *access-list cost-multiplier*

no ip multicast [**vrf** *vrf-name*] **limit cost** *access-list cost-multiplier*

Syntax Description

vrf *vrf-name*	(Optional) Specifies that the cost be applied only to mroutes associated with the Multicast Virtual Private Network (VPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
access-list	Extended or standard access control list (ACL) name or number that defines the mroutes for which to apply a cost.
cost-multiplier	Cost value applied to mroutes that match the corresponding ACL. The range is from 0 to 2147483647.

Command Default

If no **ip multicast limit cost** commands are configured or if an mroute that is being limited by a per interface mroute state limiter does not match any of the ACLs applied to **ip multicast limit cost** command configurations, a cost of 1 is applied to the mroutes being limited.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use this command to apply a cost to mroutes that match per interface mroute state limiters (configured with the **ip multicast limit** command in interface configuration mode). This command is primarily used to provide bandwidth-based Call Admission Control (CAC) in network environments where multicast flows utilize different amounts of bandwidth. Accordingly, when this command is configured, the configuration is usually referred to as a bandwidth-based multicast CAC policy.

ACLs are used with this command to define the IP multicast traffic for which to apply a cost. Standard ACLs can be used to define the (*, G) state. Extended ACLs can be used to define the (S, G) state. Extended ACLs also can be used to define the (*, G) state, by specifying 0.0.0.0 for the source address and source wildcard—referred to as (0, G)—in the permit or deny statements that compose the extended access list.

Bandwidth-based CAC policies are used with per interface mroute state limiters. Bandwidth-based CAC policies provide the capability to define costs (globally or per MVRF instance) to be applied to mroutes that are being limited by an mroute state limiter. The *cost-multiplier* argument is used to specify the cost to apply to mroutes that match the ACL specified for the *access-list* argument.

Mechanics of the Bandwidth-Based Multicast CAC Policies

- Once an mroute matches an ACL configured for a per interface mroute state limiter, the Cisco IOS software performs a top-down search from the global or per MVRF list of configured bandwidth-based multicast CAC policies to determine if a cost should be applied to the mroute.
- A cost is applied to the first bandwidth-based CAC policy that matches the mroute. A match is found when the ACL applied to the bandwidth-based CAC policy permits the mroute state.
- The counter for the mroute state limiter either adds or subtracts the cost configured for the *cost-multiplier* argument. If no costs are configured or if the mroute does not match any of the configured bandwidth-based CAC polices, the default cost of 1 is used.

Tips for Configuring Bandwidth-Based CAC Policies for IP Multicast

- To ensure that a particular cost applies to all mroutes being limited, you can configure a bandwidth-based CAC policy whose ACL contains a **permit any** statement. Configuring a bandwidth-based CAC policy in this manner effectively ensures that the default cost is not applied to any mroutes being limited.
- Configuring a bandwidth-based CAC policy with a cost of 0 for the *cost-multiplier* argument can be used to skip the accounting of certain mroutes (for example, to prevent Auto-RP groups or a specific multicast channel from being accounted).
- An explicit deny statement for a specific mroute in an ACL can be used to specify the state that will not match the ACL (thus, preventing the ACL from being accounted). If an mroute matches a deny statement, the search immediately continues to the next configured bandwidth-based CAC policy. Configuring an explicit deny statement in an ACL can be more efficient than forcing the mroute to fall through an ACL (by means of the implicit **deny any** statement at the end of the ACL).

Examples

The following example shows a bandwidth-based multicast CAC policy configuration. In this example, a service provider uses per interface mroute state limiters with bandwidth-based multicast CAC policies to provision Gigabit Ethernet interface 0/0 for the fair sharing of bandwidth required between three content providers.

```
!
interface GigabitEthernet0/0
 ip multicast limit out acl-CP1-channels 250000
 ip multicast limit out acl-CP2-channels 250000
 ip multicast limit out acl-CP3-channels 250000
!
!
ip multicast limit cost acl-MP2SD-channels 4000
ip multicast limit cost acl-MP2HD-channels 18000
ip multicast limit cost acl-MP4SD-channels 1600
ip multicast limit cost acl-MP4HD-channels 6000
!
.
.
.
!
interface GigabitEthernet0/0
 ip multicast limit out acl-CP1-channels 250000
 ip multicast limit out acl-CP2-channels 250000
 ip multicast limit out acl-CP3-channels 250000
!
```

Related Commands

Command	Description
ip multicast limit	Configures per interface mroute state limiters.

ip multicast mrinfo-filter

To filter multicast router information (mrinfo) request packets, use the **ip multicast mrinfo-filter** command in global configuration mode. To remove the filter on mrinfo requests, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **mrinfo-filter** *access-list*

no ip multicast [**vrf** *vrf-name*] **mrinfo-filter**

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
access-list	IP standard numbered or named access list that determines which networks or hosts can query the local multicast router with the **mrinfo** command.

Defaults

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **ip multicast mrinfo-filter** command filters the mrinfo request packets from all of the sources permitted by the specified access list. That is, if the access list permits a source, that source's mrinfo requests are filtered. For all sources that the access list explicitly or implicitly denies, the mrinfo requests are allowed to proceed.

Examples

The following example shows how to filter mrinfo request packets from all hosts on network 192.168.1.0:

```
ip multicast mrinfo-filter 4
access-list 4 permit 192.178.1.0 0.0.0.255
```

Related Commands

Command	Description
mrinfo	Queries a multicast router about which neighboring multicast routers are peering with it.

ip multicast multipath

To enable load splitting of IP multicast traffic over Equal Cost Multipath (ECMP), use the **ip multicast multipath** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **multipath** [**s-g-hash** {**basic** | **next-hop-based**}]

no ip multicast [**vrf** *vrf-name*] **multipath** [**s-g-hash** {**basic** | **next-hop-based**}]

Syntax Description

vrf *vrf-name*	(Optional) Enables ECMP multicast load splitting for IP multicast traffic associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
s-g-hash	(Optional) Enables ECMP multicast load splitting based on source and group address or on source, group, and next-hop address. If you specify the optional **s-g-hash** keyword for load splitting IP multicast traffic, you must select the algorithm used to calculate the equal-cost paths by specifying one of the following keywords: • **basic**—Enables a simple hash based on source and group address. This algorithm is referred to as the basic S-G-hash algorithm. • **next-hop-based**—Enables a more complex hash based on source, group, and next-hop address. This algorithm is referred to as the next-hop-based S-G-hash algorithm.

Command Default

If multiple equal-cost paths exist, multicast traffic will not be load split across those paths.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(8)T	This command was introduced.
12.0(5)S	This command was integrated into Cisco IOS Release 12.0(5)S.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was implemented on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified. The **s-g-hash**, **basic**, and **next-hop-based** keywords were added in support of the IP Multicast Load Splitting—Equal Cost Multipath (ECMP) Using S, G and Next Hop feature.

Release	Modification
15.0(1)M	This command was modified. The **s-g-hash**, **basic**, and **next-hop-based** keywords were added in support of the IP Multicast Load Splitting—Equal Cost Multipath (ECMP) Using S, G and Next Hop feature.
15.0(1)S	This command was integrated into Cisco IOS Release15.0(1)S.

Usage Guidelines

Use the **ip multicast multipath** command to enable load splitting of IP multicast traffic across multiple equal-cost paths.

If two or more equal-cost paths from a source are available, unicast traffic will be load split across those paths. However, by default, multicast traffic is not load split across multiple equal-cost paths. In general, multicast traffic flows down from the reverse path forwarding (RPF) neighbor. According to the Protocol Independent Multicast (PIM) specifications, this neighbor must have the highest IP address if more than one neighbor has the same metric.

Configuring load splitting with the **ip multicast multipath** command causes the system to load split multicast traffic across multiple equal-cost paths based on source address using the S-hash algorithm. When the **ip multicast multipath** command is configured and multiple equal-cost paths exist, the path in which multicast traffic will travel is selected based on the source IP address. Multicast traffic from different sources will be load split across the different equal-cost paths. Load splitting will not occur across equal-cost paths for multicast traffic from the same source sent to different multicast groups.

Note The **ip multicast multipath** command load splits the traffic but does not *load balance* the traffic. Traffic from a source will use only one path, even if the traffic far outweighs traffic from other sources.

If the **ip multicast multipath** command is configured with the **s-g-hash** keyword and multiple equal-cost paths exist, load splitting will occur across equal-cost paths based on source and group address or on source, group, and next-hop address. If you specify the optional **s-g-hash** keyword for load splitting IP multicast traffic, you must select the algorithm used to calculate the equal-cost paths by specifying one of the following keywords:

- **basic**—Enables a simple hash based on source and group address. The basic S-G-hash algorithm is predictable because no randomization is used in calculating the hash value. The basic S-G-hash algorithm, however, is subject to polarization because for a given source and group, the same hash is always picked irrespective of the router the hash is being calculated on.
- **next-hop-based**—Enables a more complex hash based on source, group, and next-hop address. The next-hop-based S-G-hash algorithm is predictable because no randomization is used in coming up with the hash value. Unlike the S-hash and basic S-G-hash algorithms, the next-hop-based hash mechanism is not subject to polarization.

Examples

The following example shows how to enable ECMP multicast load splitting on a router based on source address using the S-hash algorithm:

```
ip multicast multipath
```

The following example shows how to enable ECMP multicast load splitting on a router based on source and group address using the basic S-G-hash algorithm:

```
ip multicast multipath s-g-hash basic
```

The following example shows how to enable ECMP multicast load splitting on a router based on source, group, and next-hop address using the next-hop-based S-G-hash algorithm:

```
ip multicast multipath s-g-hash next-hop-based
```

ip multicast rate-limit

Note Effective with Cisco IOS Release 15.0(1)M and Cisco IOS Release 12.2(33)SRE, the **ip multicast rate-limit** command is not available in Cisco IOS software.

To control the rate at which a sender from the source list can send to a multicast group in the group list, use the **ip multicast rate-limit** command in interface configuration mode. To remove the control, use the **no** form of this command.

ip multicast rate-limit {**in** | **out**} [**video** | **whiteboard**] [**group-list** *access-list*] [**source-list** *access-list*] *kbps*

no ip multicast rate-limit {**in** | **out**} [**video** | **whiteboard**] [**group-list** *access-list*] [**source-list** *access-list*] *kbps*

Syntax Description

in	Accepts only packets at the rate of the value for the *kbps* argument or slower on the interface.
out	Sends only a maximum of the value for the *kbps* argument on the interface.
video	(Optional) Performs rate limiting based on the User Datagram Protocol (UDP) port number used by video traffic. Video traffic is identified by consulting the Session Announcement Protocol (SAP) cache.
whiteboard	(Optional) Performs rate limiting based on the UDP port number used by whiteboard traffic. Whiteboard traffic is identified by consulting the SAP cache.
group-list *access-list*	(Optional) Specifies the access list number or name that controls which multicast groups are subject to the rate limit.
source-list *access-list*	(Optional) Specifies the access list number or name that controls which senders are subject to the rate limit.
kbps	Transmission rate (in kbps). Any packets sent at greater than this value are discarded. The default value is 0, meaning that no traffic is permitted. Therefore, set this to a positive value.

Defaults

If this command is not configured, there is no rate limit.
If this command is configured, the *kbps* value defaults to 0, meaning that no traffic is permitted.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was removed.
12.2(33)SRE	This command was removed.

Usage Guidelines

If a router receives a packet the user has sent over the limit, the packet is dropped; otherwise, it is forwarded.

For the **video** or **whiteboard** keyword to work, the **ip sap listen** command must be enabled so that the port number can be obtained from the SAP cache. If the **ip sap listen** command is not enabled, or the group address is not in the SAP cache, no rate-limiting is done for the group.

Examples

In the following example, packets to any group from sources in network 172.16.0.0 will have their packets rate-limited to 64 kbps:

```
interface serial 0
 ip multicast rate-limit out group-list 1 source-list 2 64
access-list 1 permit 0.0.0.0 255.255.255.255
access-list 2 permit 172.16.0.0 0.0.255.255
```

Related Commands

Command	Description
ip sap listen	Enables the Cisco IOS software to listen to session directory advertisements.

ip multicast redundancy routeflush maxtime

To configure an additional timeout period before stale forwarding plane multicast routing (mroute) information is flushed following a Route Processor (RP) switchover, use the **ip multicast redundancy routeflush maxtime** command in global configuration mode. To restore the default with respect to the command, use the **no** form of this command.

ip multicast redundancy routeflush maxtime *seconds*

no ip multicast redundancy routeflush maxtime

Syntax Description

seconds	Timeout period, in seconds. The range is from 0 to 3600.

Command Default

The default nonstop forwarding (NSF) route flush time is 30 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SRE	This command was introduced.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

Use the **ip multicast redundancy routeflush maxtime** command to configure an additional timeout period before stale forwarding plane mroute information is flushed. This timeout period is added on to the default nonstop forwarding (NSF) route flush time as a delay between the downloading of refreshed multicast control plane route information to the forwarding plane and the flushing of "stale" NSF forwarding plane information retained from a stateful switchover (SSO) before the RP switchover.

Caution It is not recommended that you configure this additional delay unless it is specifically required for your topology because it could increase the risk of routing loops during NSF.

Note You would need to invoke this command only if you have a routing protocol that requires additional time to populate routing information after the signaling of unicast routing convergence (for example, Border Gateway Protocol [BGP] in a configuration with a large number of VPN routing and forwarding [VRF] instances). The need to configure this timeout period may be determined during predeployment SSO stress testing.

Use the **show ip multicast redundancy state** command to display the current redundancy state for IP multicast. The output from this command can be used to confirm the NSF state flush timeout period being used.

Examples

The following example shows how to configure an additional timeout period of 900 seconds (15 minutes) before stale forwarding plane mroute information is flushed:

```
Router(config)# ip multicast redundancy routeflush maxtime 900
```

Related Commands

Command	Description
show ip multicast redundancy state	Displays information about the current redundancy state for IP multicast.

ip multicast route-limit

To limit the number of multicast routes (mroutes) that can be added to a multicast routing table, use the **ip multicast route-limit** command in global configuration mode. To disable this configuration, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **route-limit** *limit* [*threshold*]

no ip multicast [**vrf** *vrf-name*] **route-limit** *limit* [*threshold*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
limit	The number of mroutes that can be added. The range is from 1 to 2147483647. The default is 2147483647.
threshold	(Optional) The number of mroutes that cause a warning message to occur. The threshold value must not exceed the limit value.

Defaults

limit: 2147483647

Command Modes

Global configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **ip multicast route-limit** command limits the number of multicast routes that can be added to a router and generates an error message when the limit is exceeded. If the user sets the *threshold* argument, a threshold error message is generated when the threshold is exceeded, and the message continues to occur until the number of mroutes reaches the limit set by the *limit* argument.

The mroute warning threshold must not exceed the mroute limit.

Examples

The following example shows how to set the mroute limit to 200,000 and the threshold to 20,000 mroutes for a VRF instance named test:

```
ip multicast vrf test route-limit 200000 20000
```

ip multicast rpf backoff

To configure the intervals at which Protocol Independent Multicast (PIM) Reverse Path Forwarding (RPF) failover will be triggered by changes in the routing tables, use the **ip multicast rpf backoff** command in global configuration mode. To set the triggered RPF check to the default values, use the **no** form of this command.

ip multicast rpf backoff *minimum maximum* [**disable**]

no ip multicast rpf backoff *minimum maximum* [**disable**]

Syntax Description

minimum	The minimum configured backoff interval. The backoff interval is reset to the number of milliseconds (ms) configured by the *minimum* argument if a backoff interval has expired without any routing changes. The default is 500 milliseconds (ms).
maximum	The maximum amount of time, in milliseconds, allowed for a backoff interval. The maximum length of time that is allowed is 5000 ms. The default is 5000 ms.
disable	(Optional) Turns off the triggered RPF check function.

Command Default

This command is enabled by default.
minimum: 500 ms.
maximum: 5000 ms.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In an unstable unicast routing environment that uses triggered RPF checks, the environment could be constantly triggering RPF checks, which places a burden on the resources of the router. To avoid this problem, use the **ip multicast rpf backoff** command to prevent a second triggered RPF check from occurring for the length of time configured. That is, the PIM "backs off" from another triggered RPF check for a minimum amount of milliseconds as configured by the user.

If the backoff period expires without further routing table changes, PIM then scans for routing changes and accordingly establishes multicast RPF changes. However, if more routing changes occur during the backoff period, PIM doubles the backoff period to avoid overloading the router with PIM RPF changes while the routing table is still converging.

Note We recommend that users keep the default values for this command. The default values allow subsecond RPF failover.

The *maximum* argument is used to configure the maximum backoff interval. The backoff time is reset to the time configured by the *minimum* argument if an entire backoff interval has expired without routing changes.

The *maximum* argument default allows the RPF change behavior to be backward-compatible, allowing a 5-second RPF check interval in case of frequent route changes and a 500-ms RPF check interval in stable networks with only unplanned routing changes. Before the introduction of the **ip multicast rpf backoff** command, PIM polled the routing tables for changes every 5 seconds.

You likely need not change the defaults of the **ip multicast rpf backoff** command unless you have frequent route changes in your router (for example, on a dial-in router). Changing the defaults can allow you to reduce the maximum RPF check interval for faster availability of IP multicast on newly established routes or to increase the maximum RPF check interval to reduce the CPU load caused by the RPF check.

Examples

The following example shows how to set the minimum backoff interval to 100 ms and the maximum backoff interval to 2500 ms:

```
ip multicast rpf backoff 100 2500
```

ip multicast rpf interval

To modify the intervals at which periodic Reverse Path Forwarding (RPF) checks occur, use the **ip multicast rpf interval** command in global configuration mode. To return to the default interval, use the **no** form of this command.

ip multicast rpf interval *seconds* [**list** *access-list* | **route-map** *route-map*]

no ip multicast rpf interval *seconds* [**list** *access-list* | **route-map** *route-map*]

Syntax Description

seconds	The number of seconds at which the interval is configured. The default is 10 seconds.
list *access-list*	(Optional) Defines the interval of periodic RPF checks for an access list.
route-map *route-map*	(Optional) Defines the interval of periodic RPF checks for a route map.

Command Default

This command is enabled by default.
seconds: 10

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can configure multiple instances of this command by using an access list or a route map.

Note We recommend that users keep the default values for this command. The default values allow subsecond RPF failover.

Examples

The following example shows how to set the periodic RPF check interval to 10 seconds:

```
ip multicast rpf interval 10
```

The following example shows how to set the periodic RPF check interval for groups that are defined by access list 10 to 3 seconds:

```
ip multicast rpf interval 3 list 10
```

The following example shows how to set the periodic RPF check interval for groups that are defined by the route map named map to 2 seconds:

```
ip multicast rpf interval 2 route-map map
```

Related Commands

Command	Description
ip igmp query-interval	Configures the frequency at which the Cisco IOS software sends IGMP host hello messages.

ip multicast rpf mofrr

To enable a Provider Edge (PE) router to perform Reverse Path Forwarding (RPF) lookups using multicast only fast re-route (MoFRR) on an IP address of the exit router in the global table or a specific VPN, use the **ip multicast rpf mofrr** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **rpf mofrr** {*access-list-number* | *access-list-name*} [**sticky**]

no ip multicast [**vrf** *vrf-name*] **rpf mofrr** {*access-list-number* | *access-list-name*} [**sticky**]

Syntax Description

vrf *vrf-name*	(Optional) Enables a PE router to perform an RPF lookup using MoFRR on the exit router for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
access-list-name	Name of the IP access list or object group access control list (OGACL). Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
access-list-number	Number of the access control list (ACL). MoFRR is enabled for the mroute matching the ACL. • An extended IP access list is in the range 100 to 199 or 2000 to 2699. **Note** MoFRR accepts extended ACLs only. It does not accept standard ACLs.
sticky	(Optional) Ensures that the primary RPF does not change even if a better primary comes along. It changes only if for some reason the current primary RPF is unreachable. The **sticky** keyword ensures that there is no RPF flapping happening on mroutes if the unicast routes are fluctuating for some reason.

Command Default

The RPF MoFRR functionality is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Use the **ip multicast rpf mofrr** command to enable a PE router to perform RPF lookups using MoFRR on an IP address of the exit router in the global table or a specific VPN. MoFRR uses standard Protocol Independent Multicast (PIM) join messages to set up a primary and a secondary multicast forwarding path by establishing a primary and a secondary RPF interface on each router that receives a PIM join

message. Data is received from both the primary and backup paths. If the router detects a forwarding error in the primary path, it switches RPF to the secondary path and immediately has packets available to forward out to each outgoing interface.

MoFRR accepts extended ACLs only. It does not accept standard ACLs.

Examples

The following example shows how to enable a PE router to perform RPF lookups using MoFRR for the mroute matching the ACL numbered 150:

```
ip multicast rpf mofrr 150
```

Related Commands

Command	Description
show ip mroute	Displays information about the multicast routing (mroute) table.
show ip rpf	Displays the information that IP multicast routing uses to perform the RPF check for a multicast source.

ip multicast rpf proxy vector

To enable a provider edge (PE) router to perform a Reverse Path Forwarding (RPF) check on an IP address of the exit router in the global table or a specific VPN, use the **ip multicast rpf proxy vector** command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **rpf proxy** [**rd**] [**disable**] **vector**

no ip multicast [**vrf** *vrf-name*] **rpf proxy** [**rd**] [**disable**] **vector**

Syntax Description

vrf *vrf-name*	(Optional) Enables a PE router to perform an RPF check on the exit router for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument. **Note** The **rd** keyword is required if the **vrf** keyword and *vrf-name* argument are entered.
rd	(Optional) Enables the route distinguisher (RD) vector in MVPN inter-AS Option B deployments. **Note** In an Option B deployment, you must enter the **ip multicast rpf proxy** command with the **rd** keyword for MVPN inter-AS support. The **rd** keyword is not required for MVPN inter-AS support Option C deployments.
disable	(Optional) Rejects the Protocol Independent Multicast (PIM) proxy and attribute RPF information.
vector	Enables the Border Gateway Protocol (BGP) next-hop as vector in PIM join messages.

Command Default

The RPF Vector functionality is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **ip multicast rpf proxy vector** command to enable a PE router to perform an RPF check on an IP address of the exit router in the global table or a specified VPN.

Use the **rd** keyword to configure PE routers to include the RD value of the VPN associated with the PIM RPF Vector encoding inserted into PIM join and prune messages. Because ASBRs in MVPN Option B deployments change the next hop of the originating PE router for a given MDT group, including the RD value in the PIM RPF Vector encoding enables the ASBR to perform a lookup on the RD value for a prefix, which, in turn, enables the ASBR to identify which VPN the RPF Vector is intended for.

RPF Vector Functionality

Normally, in an MVPN environment, PIM sends join messages containing the IP address of upstream PE routers that are sources of a given Multicast Distribution Tree (MDT) group. To be able to perform RPF checks, however, provider (P) routers must have IPv4 reachability to source PE routers in remote autonomous systems. This behavior is not the case with inter-AS Options B and C (defined in RFC 4364) because the autonomous systems do not exchange any of their Interior Gateway Protocol (IGP) routes, including those of their local PE routers. However, P routers do have reachability to the BGP next hop of the BGP MDT update received with the BGP MDT Subaddress Family Identifier (SAFI) updates at the PE routers. Therefore, if the PE routers add the remote PE router IP address (as received within the BGP MDT SAFI) and the BGP next-hop address of this address within the PIM join, the P routers can perform an RPF check on the BGP next-hop address rather than the original PE router address, which, in turn, allows the P router to forward the join toward the Autonomous System Border Router (ASBR) that injected the MDT SAFI updates for a remote autonomous system. This functionality is generally referred to as the *PIM RPF Vector*; the actual vector that is inserted into PIM joins is referred to as the *RPF Vector* or the *Proxy Vector*. The PIM RPF Vector, therefore, enables P routers to determine the exit ASBR to a source PE router in a remote autonomous system. Having received the join that contains a RPF Vector, an ASBR can then determine that the next-hop address is in fact itself and can perform an RPF check based on the originating PE router address carried in the PIM join.

RPF Vector Configuration Guidelines

When configured on PE routers using the **ip multicast rpf proxy vector** command, the RPF Vector is encoded as a part of the source address in PIM join and prune messages. The RPF Vector is the IGP next hop for PIM RPF neighbor in PIM join and prune messages, which is typically the exit ASBR router to a prefix in a remote autonomous system.

When enabling the RPF Vector on PE routers in Option B deployments, the following form of the **ip multicast rpf proxy vector** command should be used:

ip multicast vrf *vrf-name* **rpf proxy rd vector**

This form of the command enables an PE router to perform RPF checks on an IP address of the exit router for a specific VPN. The **rd** keyword is used in this form of the command to configure PE routers to include the RD value of the VPN associated with the PIM RPF Vector encoding inserted into PIM join and prune messages. Because ASBRs in Option B deployments change the next hop of the originating PE router for a given MDT group, including the RD value in the PIM RPF Vector encoding enables the ASBR to perform a lookup on the RD value for a prefix, which, in turn, enables the ASBR to identify which VPN the RPF Vector is intended for.

When enabling the RPF Vector on PE routers in Option C deployments, the following form of the **ip multicast rpf proxy vector** command should be used:

ip multicast rpf proxy vector

This form of the command enables the PE router to perform RPF checks on an IP address of the exit router in the global table.

RPF Vector Verification

Use the **show ip pim neighbor** command to verify that a PIM neighbor supports the RPF Vector functionality. The P flag in the output of the **show ip pim neighbor** command indicates that a PIM neighbor has announced (through PIM hello messages) its capability to handle RPF Vectors in PIM join

messages. All Cisco IOS versions that support the PIM RPF Vector feature announce this PIM hello option. An RPF Vector is only included in PIM messages when all PIM neighbors on an RPF interface support it.

Examples

The following example shows how to enable a PE router to perform RPF checks on the IP address of the exit router in the global table:

```
ip multicast rpf proxy vector
```

Related Commands

Command	Description
show ip pim neighbor	Displays information about PIM neighbors.

ip multicast rpf select

To configure Reverse Path Forwarding (RPF) lookups originating in a receiver Multicast VPN (MVPN) routing and forwarding (MVRF) instance or in the global routing table to be performed in a source MVRF instance or in the global routing table based on group address, use the **ip multicast rpf select** command. To disable the functionality, use the **no** form of the command.

ip multicast [**vrf** *receiver-vrf-name*] **rpf select** {**global** | **vrf** *source-vrf-name*} **group-list** *access-list*

no ip multicast [**vrf** *receiver-vrf-name*] **rpf select** {**global** | **vrf** *source-vrf-name*} **group-list** *access-list*

Syntax Description

vrf *receiver-vrf-name*	(Optional) Applies a group-based VRF selection policy to RPF lookups originating in the MVRF specified for the *receiver-vrf-name* argument. If the optional **vrf** keyword and *receiver-vrf-name* argument are not specified, the group-based VRF selection policy applies to RPF lookups originating in the global table.
global	Specifies that the RPF lookup for groups matching the access control list (ACL) specified for the **group-list** keyword and *access-list* argument be performed in the global routing table.
vrf *source-vrf-name*	Specifies that the RPF lookups for groups matching the ACL specified with the **group-list** keyword and *access-list* argument be performed in the VRF specified for the *vrf-name* argument.
group-list *access-list*	Specifies the ACL to be applied to the group-based VRF selection policy.

Command Default

No group-based VRF selection policies are configured.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **ip multicast rpf select** command to configure group-based VRF selection policies. By defining group-based VRF selection policies, you can configure the RPF lookups originating in a receiver MVRF or in the global routing table to be performed in a source MVRF or in the global routing table based on group address. ACLs are used to define the groups to be applied to a group-based VRF selection policy.

Use the **show ip rpf select** command after configuring group-based VRF selection policies to display group-to-VRF mapping information.

Use the **show ip rpf** command to display how IP multicast does RPF.

Examples

The following example shows how to use a group-based VRF selection policy to configure the RPF lookup for groups that match ACL 1 to be performed in VPN-A instead of the global table:

```
ip multicast rpf select vrf VPN-A group-list 1
!
.
.
.
!
access-list 1 permit 239.0.0.0 0.255.255.255
!
```

Related Commands

Command	Description
show ip rpf	Displays how IP multicast routing does RPF.
show ip rpf select	Displays group-to-VRF mapping information.

ip multicast rpf select topology

To associate a multicast topology with a multicast group with a specific mroute entry, use the **ip multicast rpf select topology** command in global configuration mode. To disable the functionality, use the **no** form of this command.

ip multicast rpf select topology {**multicast** | **unicast**} *topology-name access-list-number*

no ip multicast rpf select topology {**multicast** | **unicast**} *topology-name access-list-number*

Syntax Description

multicast	Associates a multicast topology with an (S,G) mroute entry.
unicast	Associates a unicast topology with an (S,G) mroute entry.
topology-name	Name of the topology instance.
access-list-number	Number of the access list.

Command Default

The topology is not associated with an (S,G) mroute entry.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The **ip multicast rpf select topology** command associates a multicast topology with an (S,G) mroute entry. One (S,G) mroute entry can be associated with multiple topologies. During RPF lookup, PIM MT-ID will be used (smaller ID has higher priority) to select a topology.

One access list could be associated with multiple (S,G) mroute entries. The sequence number in the access list is used to determine the order of (S,G) mroute entry lookup within the access list.

One topology can be associated with only one access list.

Examples

The following example shows how to associate a multicast topology with an (S,G) mroute entry:

```
ip multicast rpf select topology multicast topology live-A 111
```

Related Commands

Command	Description
debug ip multicast topology	Enables debugging output for IP multicast stream topology creation events, deletion events, and IP multicast stream ACL matching events.
ip multicast topology	Configures topology selection for multicast streams.
show ip multicast topology	Displays IP multicast topology information.

ip multicast topology

To configure topology selection for multicast streams, use the **ip multicast topology** command in global configuration mode. To disable the functionality, use the **no** form of this command.

ip multicast topology {**multicast** | **unicast**} *topology-name* **tid** *topology-number*

no ip multicast topology {**multicast** | **unicast**} *topology-name* **tid** *topology-number*

Syntax Description

multicast	Configures a multicast topology instance.
unicast	Configures a unicast topology instance.
topology-name	Name of the topology instance.
tid *topology-number*	Specifies the number of the topology identifier.

Command Default

All multicast streams are associated with the multicast base topology.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The **ip multicast topology** command configures topology selection for multicast streams, which is usually only required for first hop and last hop routers (and may not be required for transit routers in between). The stream, specified by an extended IP access list, can be source based, group based, or a combination of both. The sequence number in the access list will decide the order of the (S,G) mroute entries.

Examples

The following example shows how to configure topology selection for multicast streams:

```
ip multicast topology multicast live-A 111
```

Related Commands

Command	Description
debug ip multicast topology	Enables debugging output for IP multicast stream topology creation events, deletion events, and IP multicast stream ACL matching events.
ip multicast rpf select topology	Associates a multicast topology with a multicast group with a specific mroute entry.
show ip multicast topology	Displays IP multicast topology information.

ip multicast ttl-threshold

Note Effective with Cisco IOS Release 15.0(1)M and Cisco IOS Release 12.2(33)SRE, the **ip multicast ttl-threshold** command is not available in Cisco IOS software.

To configure the time-to-live (TTL) threshold of multicast packets being forwarded out an interface, use the **ip multicast ttl-threshold** command in interface configuration mode. To return to the default TTL threshold, use the **no** form of this command.

ip multicast ttl-threshold *ttl-value*

no ip multicast ttl-threshold *ttl-value*

Syntax Description

ttl-value	Time-to-live value, in hops. It can be a value from 0 to 255. The default value is 0, which means that all multicast packets are forwarded out the interface.

Defaults

The default TTL value is 0, which means that all multicast packets are forwarded out the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was removed.
12.2(33)SRE	This command was removed.

Usage Guidelines

Only multicast packets with a TTL value greater than the threshold are forwarded out the interface.

You should configure the TTL threshold only on border routers. Conversely, routers on which you configure a TTL threshold value automatically become border routers.

This command replaces the **ip multicast-threshold** command.

Examples

The following example sets the TTL threshold on a border router to 200, which is a very high value. In this example multicast packets must have a TTL greater than 200 in order to be forwarded out this interface. Multicast applications generally set this value well below 200. Therefore, setting a value of 200 means that no packets will be forwarded out the interface.

```
interface tunnel 0
 ip multicast ttl-threshold 200
```

ip multicast use-functional

To enable the mapping of IP multicast addresses to the Token Ring functional address 0xc000.0004.0000, use the **ip multicast use-functional** command in interface configuration mode. To disable the function, use the **no** form of this command.

ip multicast use-functional

no ip multicast use-functional

Syntax Description

This command has no arguments or keywords.

Defaults

IP multicast address are mapped to the MAC-layer address 0xFFFF.FFFF.FFFF.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is accepted only on a Token Ring interface.

Neighboring devices on the Token Ring on which this feature is used should also use the same functional address for IP multicast traffic.

Because there are a limited number of Token Ring functional addresses, other protocols may be assigned to the Token Ring functional address 0xc000.0004.0000. Therefore, not every frame sent to the functional address is necessarily an IP multicast frame.

Examples

The following example configures any IP multicast packets going out Token Ring interface 0 to be mapped to MAC address 0xc000.0004.0000:

```
interface token 0
 ip address 10.0.0.0 255.255.255.0
 ip pim dense-mode
 ip multicast use-functional
```

ip multicast-routing

To enable IP multicast routing, use the **ip multicast-routing** command in global configuration mode. To disable IP multicast routing, use the **no** form of this command.

ip multicast-routing [**vrf** *vrf-name*] [**distributed**]

no ip multicast-routing [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Enables IP multicast routing for the Multicast Virtual Private Network (VPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
distributed	(Optional) Enables Multicast Distributed Switching (MDS).

Command Default

IP multicast routing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
11.2(11)GS	The **distributed** keyword was added.
12.0(5)T	The effect of this command was modified. If IP multicast Multilayer Switching (MLS) is enabled, using the **no** form of this command now disables IP multicast routing on the Multicast MultiLayer Switching (MMLS) route processor (RP) and purges all multicast MLS cache entries on the MMLS-SE.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.2S	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

When IP multicast routing is disabled, the Cisco IOS software does not forward any multicast packets.

Note For IP multicast, after enabling IP multicast routing, PIM must be configured on all interfaces. Disabling IP multicast routing does not remove PIM; PIM still must be explicitly removed from the interface configurations.

Examples

The following example shows how to enable IP multicast routing:

```
Router(config)# ip multicast-routing
```

The following example shows how to enable IP multicast routing on a specific VRF:

```
Router(config)# ip multicast-routing vrf vrf1
```

The following example shows how to disable IP multicast routing:

```
Router(config)# no ip multicast-routing
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.

ip pgm host

Note Support for the PGM Host feature has been removed. Use of this command is not recommended.

To enable Pragmatic General Multicast (PGM) Host, use the **ip pgm host** command in global configuration mode. To disable PGM Host and close all open PGM Host traffic sessions, use the **no** form of this command.

ip pgm host [**source-interface** {*interface-type interface-number*} | *connection-parameter*]

no ip pgm host

Syntax Description

source-interface *interface-type interface-number*	(Optional) Specifies the interface type and number on which to run PGM Host.
connection-parameter	(Optional) Configures advanced PGM Host connection parameters. The optional configuration parameters should be configured only by experts in PGM technology. See Table 1 for a comprehensive list of the optional connection parameters and their definitions.

Defaults

PGM Host is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Using the **ip pgm host** command without a keyword or an argument enables PGM Host on the router and configures the router to source PGM packets through a virtual host interface.

Specifying a physical or logical interface type (for example, an Ethernet, serial, or loopback interface) with the **ip pgm host source-interface** command configures the router to source PGM packets out of the physical or logical interface.

Note You must first enable PGM Host globally on the router using the **ip pgm host** command before sourcing PGM packets out of a physical or logical interface using the **ip pgm host source-interface** command.

Sourcing PGM packets through a virtual host interface enables the router to send and receive PGM packets through any router interface. The virtual host interface also serves as the interface to the multicast applications that reside at the PGM network layer.

Sourcing IP multicast traffic out a specific physical or logical interface configures the router to send PGM packets out that interface only and to receive packets on any router interface.

When both PGM Host and Router Assist are enabled on the router, the router can process received PGM packets as a virtual PGM Host, originate PGM packets and serve as its own first hop PGM network element, and forward received PGM packets. Refer to the "Configuring PGM Host and Router Assist" chapter of the *Cisco IOS IP Configuration Guide* for more information about PGM Router Assist.

Table 1 lists the available parameters for the *connection-parameter* argument. The parameters should be configured only by experts in PGM technology. Use the **no ip pgm host** *connection-parameter* command to return a parameter to its default value.

Table 1 ip pgm host Connection Parameters

Parameter	Definition
ihb-max *milliseconds*	(Optional) Sets the source path message (SPM) interheartbeat timer maximum. The default is 10000 milliseconds (ms).
ihb-min *milliseconds*	(Optional) Sets the SPM interheartbeat timer minimum. The default is 1000 ms.
join *milliseconds*	(Optional) Sets the amount of time the PGM Host waits, when running in router mode, for client requests. The default is 0 ms.
nak-gen-ivl *milliseconds*	(Optional) Sets the amount of time the PGM Host waits for a PGM negative acknowledgment (NAK) data packet. The default is 60000 ms.
nak-rb-ivl *milliseconds*	(Optional) Sets the amount of time the PGM Host waits before sending a PGM NAK data packet. The default is 500 ms.
nak-rdata-ivl *milliseconds*	(Optional) Sets the amount of time the PGM Host waits for a re-sent PGM NAK (NAK RDATA) data packet. The default is 2000 ms.
nak-rpt-ivl *milliseconds*	(Optional) Sets the amount of time the PGM Host waits for a PGM NAK confirmation (NAK NCF) data packet. The default is 2000 ms.
ncf-max *packets-per-second*	(Optional) Sets the maximum number of PGM NAK confirmation data packets (NAK NCFs) the PGM Host sends per second. The default is infinite.
rx-buffer-mgmt {**full** | **minimum**}	(Optional) Sets the type of receive data buffers (full or minimum) for the PGM Host. The default is minimum.
spm-ambient-ivl *milliseconds*	(Optional) Sets the amount of time the PGM Host waits for a PGM source path message (SPM) ambient data packet. The default is 6000 ms.

Table 1 ip pgm host Connection Parameters (continued)

Parameter	Definition
spm-rpt-ivl *milliseconds*	(Optional) Sets the amount of time the PGM Host waits for a PGM SPM repeat data packet. The default is 3000 ms.
stream-type {**apdu** | **byte**}	(Optional) Sets the data stream type (apdu or byte) for the PGM Host. The default is apdu.
tpdu-size *number*	(Optional) Sets the size of the source transport data unit (TPDU) for the PGM Host. The available range is 41 through 16384 bytes. The default is 1400 bytes.
ttl *number*	(Optional) Sets the time-to-live (TTL) value on the PGM Host for sent multicast data packets. The default is 255 hops. The TTL value for a packet is decremented by 1 as the packet passes through a router.
tx-buffer-mgmt {**keep** | **return**}	(Optional) Sets the type of transmit data buffers (keep or return) for the PGM Host. The default is return.
tx-adv-method {**data** | **time**}	(Optional) Sets the type of advanced transmit window method (data or time) for the PGM Host. The default is time.
txw-adv-secs *milliseconds*	(Optional) Sets the size of the advanced transmit window for the PGM Host. The default is 6000 ms.
txw-adv-timeout-max *milliseconds*	(Optional) Sets the time after which a transmit window will be advanced regardless of observed NAKs.
txw-rte *bytes-per-second*	(Optional) Sets the data transmit rate for the PGM Host. The default is 16384 bytes per second.
txw-secs *milliseconds*	(Optional) Sets the data transmit window size for the PGM Host. The default is 30000 ms.
txw-timeout-max *milliseconds*	(Optional) Sets the amount of time the PGM Host waits for data packets, even if the PGM Host receives PGM NAK data packets. The default is 3600000 ms.

Examples

The following example enables PGM Host (both the source and receiver part of the PGM network layer) globally on the router and configures the router to source PGM packets through a virtual host interface:

```
ip pgm host
```

The following example enables PGM Host globally on the router and configures the router to source PGM packets out of physical Ethernet interface 0/1:

```
ip pgm host
ip pgm host source-interface ethernet 0/1
```

Related Commands

Command	Description
clear ip pgm host	Resets PGM Host connections to their default values and clears traffic statistics.
ip pgm router	Enables PGM Router Assist and thereby allows PGM to operate more efficiently on the router.
show ip pgm host defaults	Displays the default values for PGM Host traffic.
show ip pgm host sessions	Displays open PGM Host traffic sessions.
show ip pgm host traffic	Displays PGM Host traffic statistics.

ip pgm router

To enable Pragmatic General Multicast (PGM) Router Assist and thereby allow PGM to operate more efficiently on the router, use the **ip pgm router** command in interface configuration mode. To disable PGM Router Assist for the interface, use the **no** form of this command.

ip pgm router

no ip pgm router

Syntax Description

This command has no arguments or keywords.

Defaults

PGM Router Assist is disabled for the interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is highly recommended for optimal deployment of PGM Reliable Transport Protocol on a host.

Examples

In the following example, PGM Router Assist is configured on Ethernet interfaces 0 and 1:

```
ip multicast-routing
interface ethernet 0
 ip pim sparse-dense-mode
 ip pgm router
interface ethernet 1
 ip pim sparse-dense-mode
 ip pgm router
```

Related Commands

Command	Description
clear ip pgm router	Clears PGM traffic statistics.
ip pgm host	Enables PGM Host.
show ip pgm router	Displays PGM Reliable Transport Protocol state and statistics.

ip pim

To enable Protocol Independent Multicast (PIM) on an interface, use the **ip pim** command in interface configuration mode. To disable PIM on the interface, use the **no** form of this command.

ip pim {**dense-mode** [**proxy-register** {**list** *access-list* | **route-map** *map-name*}] | **passive** | **sparse-mode** | **sparse-dense-mode** }

no ip pim {**dense-mode** [**proxy-register** {**list** *access-list* | **route-map** *map-name*}] | **passive** | **sparse-mode** | **sparse-dense-mode** }

Syntax Description

dense-mode	Enables dense mode of operation.
proxy-register	(Optional) Enables proxy registering on the interface of a designated router (DR) (leading toward the bordering dense mode region) for multicast traffic from sources not connected to the DR.
list *access-list*	(Optional) Defines the extended access list number or name.
route-map *map-name*	(Optional) Defines the route map.
passive	Enables passive mode of operation
sparse-mode	Enables sparse mode of operation.
sparse-dense-mode	Treats the interface in either sparse mode or dense mode of operation, depending on which mode the multicast group operates in.

Defaults

IP multicast routing is disabled on all interfaces.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
10.0	This command was introduced.
11.1	The **sparse-dense-mode** keyword was added.
12.0S	The following keywords and arguments were added: • **proxy-register** • **list** *access-list* • **route-map** *map-name*
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRE	This command was modified. The **passive** keyword was added.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Enabling PIM on an interface also enables Internet Group Management Protocol (IGMP) operation on that interface. An interface can be configured to be in dense mode, passive mode, sparse mode, or sparse-dense mode. The mode describes how the Cisco IOS software populates its multicast routing table and how the software forwards multicast packets it receives from its directly connected LANs. Dense mode interfaces are always added to the table when the multicast routing table is populated. Sparse mode interfaces are added to the table only when periodic join messages are received from downstream routers, or there is a directly connected member on the interface.

Dense Mode

Initially, a dense mode interface forwards multicast packets until the router determines that there are group members or downstream routers, or until a prune message is received from a downstream router. Then, the dense mode interface periodically forwards multicast packets out the interface until the same conditions occur. Dense mode assumes that multicast group members are present. Dense mode routers never send a join message. They do send prune messages as soon as they determine they have no members or downstream PIM routers. A dense mode interface is subject to multicast flooding by default.

Dense Mode with Proxy Registering

For a router in a PIM sparse mode (PIM-SM) domain configured to operate in sparse mode or sparse-dense mode, the **ip pim dense-mode proxy-register** command must be configured on the interface leading toward the bordering dense mode region. This configuration will enable the router to register traffic from the dense mode region with the rendezvous point (RP) in the sparse mode domain.

Prior to Cisco IOS Release 12.0 S, an RP needed to be running on the border router leading toward a dense mode region so that the RP could learn about traffic from sources in the dense mode region.

This command requires an extended access list or route map argument specifying which traffic the router needs to register with the RP. This command applies only to sources reachable through a PIM router. Cisco IOS software will always register traffic from remote sources if it arrives on a dense mode interface and if the Reverse Path Forwarding (RPF) neighbor leading toward the source is a Distance Vector Multicast Routing Protocol (DVMRP) but not a PIM router. This functionality has existed since Cisco IOS Release 10.0 and cannot be modified (restricted) with an access list or route map.

Passive Mode

An interface configured with passive mode does not pass or forward PIM control plane traffic; it passes or forwards only IGMP traffic. If passive mode is configured on an interface enabled for IP multicast, the router will not send PIM messages on the interface nor will it accept PIM messages from other routers on this interface. The router acts as the only PIM router on the network and works as the designated router (DR) and the designated forwarder (DF) for all Bidirectional PIM group ranges.

The **ip pim neighbor-filter** command has no effect and is superseded by the **ip pim passive** command when both commands are configured on the same interface.

Do not use the **ip pim passive** command on LANs that have more than one IP multicast router connected to them, because all routers with this command become DR and DF, resulting in duplicate traffic (PIM-SM, PIM-DM, PIM-SSM) or looping traffic (Bidir-PIM). To limit PIM messages to and from valid routers on LANs with more than one router, use the **ip pim neighbor-filter** command

Sparse Mode

A sparse mode interface is used for multicast forwarding only if a join message is received from a downstream router or if group members are directly connected to the interface. Sparse mode assumes that no other multicast group members are present. When sparse mode routers want to join the shared path, they periodically send join messages toward the RP. When sparse mode routers want to join the source path, they periodically send join messages toward the source; they also send periodic prune messages toward the RP to prune the shared path.

Sparse-Dense Mode

An alternative to choosing just dense mode or just sparse mode is to run PIM in a single region in sparse mode for some groups and dense mode for other groups.

In sparse-dense mode, if the group is in dense mode, the interface will be treated as dense mode. If the group is in sparse mode, the interface will be treated in sparse mode. The group is "sparse" if the router knows about an RP for that group.

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

- Members or DVMRP neighbors are on the interface.
- Any of the PIM neighbors on the interface have not pruned for the group.

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

- Members or DVMRP neighbors are on the interface.
- A PIM neighbor on the interface has received an explicit join message.

Examples

The following example shows how to enable PIM-SM on tunnel interface 0 and set the address of the RP router to 226.0.0.8:

```
ip pim rp-address 226.0.0.8
interface tunnel 0
  ip pim sparse-mode
```

The following example shows how to enable PIM dense mode (PIM-DM) on Ethernet interface 1:

```
interface ethernet 1
  ip pim dense-mode
```

The following example shows how to enable PIM sparse-dense mode on Ethernet interface 1:

```
interface ethernet 1
  ip pim sparse-dense-mode
```

The following example shows how to register the multicast traffic for any source and any multicast group:

```
interface ethernet 0
  ip address 172.16.0.0 255.255.255.0
  description Ethernet interface towards the PIM sparse-mode domain
  ip pim sparse-dense-mode
!
interface ethernet 1
  ip address 192.44.81.5 255.255.255.0
  description Ethernet interface towards the PIM dens-mode region
  ip pim dense-mode proxy-register list 100
!
access-list 100 permit ip any any
```

Related Commands

Command	Description
ip multicast-routing	Enables IP multicast routing or multicast distributed switching.
ip pim neighbor-filter	Filters PIM messages.

Command	Description
ip pim rp-address	Configures the address of a PIM RP for a particular group.
show ip pim interface	Displays information about interfaces configured for PIM.

ip pim accept-register

To configure a candidate rendezvous point (RP) router to filter Protocol Independent Multicast (PIM) register messages, use the **ip pim accept-register** command in global configuration mode. To remove the PIM register filter, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **accept-register** {**list** *access-list* | **route-map** *map-name*}

no ip pim [**vrf** *vrf-name*] **accept-register** {**list** *access-list* | **route-map** *map-name*}

Syntax Description

vrf *vrf-name*	(Optional) Configures a PIM register filter on candidate RPs for (S, G) traffic associated with the multicast Virtual Private Network (VPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
list *access-list*	Specifies an extended access list number or name that defines the (S, G) traffic in PIM register messages to be permitted or denied.
route-map *map-name*	Specifies a route map that defines the (S, G) traffic in PIM register messages to be permitted or denied.

Command Default

No PIM register filters are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to prevent unauthorized sources from registering with the RP. If an unauthorized source sends a register message to the RP, the RP will immediately send back a register-stop message.

The access list or route map provided for the **ip pim accept-register** command should only filter on IP source addresses and IP destination addresses. Filtering on other fields (for example, IP protocol or UDP port number) will not be effective and may cause undesired traffic to be forwarded from the RP down the shared tree to multicast group members. If more complex filtering is desired, use the **ip multicast boundary** command instead.

Note If the RP is also the first hop designated router (DR) for directly connected sources, PIM register packets will not be filtered using the **ip pim accept-register** command. For this case, use the **ip multicast boundary** command to filter the directly connected source traffic.

Examples

The following example shows how to permit register packets for source address 172.16.10.1 sending to the SSM group range (232.0.0.0/8). All other PIM register messages not matching the extended access list (ssm-range) are denied. These statements should be configured on all candidate RPs because candidate RPs will receive PIM registers from first hop routers.

```
ip pim accept-register list ssm-range
ip access-list extended ssm-range
 permit ip 172.16.10.1 0.0.0.255 232.0.0.0 0.255.255.255
```

Related Commands

Command	Description
ip multicast boundary	Configures an administratively scoped IPv4 multicast boundary.

ip pim accept-rp

To configure a router to accept join or prune messages destined for a specified rendezvous point (RP) and for a specific list of groups, use the **ip pim accept-rp** command in global configuration mode. To remove that check, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **accept-rp** {*rp-address* | **auto-rp**} [*access-list*]

no ip pim [**vrf** *vrf-name*] **accept-rp** {*rp-address* | **auto-rp**} [*access-list*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
rp-address	RP address of the RP allowed to send join messages to groups in the range specified by the group access list.
auto-rp	Accepts join and register messages only for RPs that are in the Auto-RP cache.
access-list	(Optional) Access list number or name that defines which groups are subject to the check.

Defaults

The command is disabled, so all join messages and prune messages are processed.

Command Modes

Global configuration

Command History

Release	Modification
10.2	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command causes the router to accept only (*, G) join messages destined for the specified RP address. Additionally, the group address must be in the range specified by the access list.

When the *rp-address* argument is one of the addresses of the system, the system will be the RP only for the specified group range specified by the access list. When the group address is not in the group range, the RP will not accept join or register messages and will respond immediately to register messages with register-stop messages.

Examples

The following example shows how to configure the router to accept join or prune messages destined for the RP at address 172.17.1.1 for the multicast group 224.2.2.2:

```
ip pim accept-rp 172.17.1.1 3
access-list 3 permit 224.2.2.2
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.

ip pim autorp listener

To cause IP multicast traffic for the two Auto-RP groups 224.0.1.39 and 224.0.1.40 to be Protocol Independent Multicast (PIM) dense mode flooded across interfaces operating in PIM sparse mode, use the **ip pim autorp listener** command in global configuration mode. To disable this feature, use the **no** form of this command.

ip pim autorp listener

no ip pim autorp listener

Syntax Description

This command has no arguments or keywords.

Defaults

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(7)	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **ip pim autorp listener** command with interfaces configured for PIM sparse mode operation in order to establish a network configuration where Auto-RP operates in PIM dense mode and multicast traffic can operate in sparse mode, bidirectional mode, or Source Specific Multicast (SSM) mode.

Examples

The following example enables IP multicast routing and the Auto-RP listener feature on a router. It also configures the router as a candidate RP for the multicast groups 239.254.2.0 through 239.254.2.255.

```
ip multicast-routing
ip pim autorp listener

ip pim send-rp-announce Loopback0 scope 16 group-list 1
ip pim send-rp-discovery Loopback1 scope 16
access-list 1 permit 239.254.2.0 0.0.0.255
```

ip pim bidir-enable

To enable bidirectional Protocol Independent Multicast (bidir-PIM), use the **ip pim bidir-enable** command in global configuration mode. To disable bidir-PIM, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **bidir-enable**

no ip pim [**vrf** *vrf-name*] **bidir-enable**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Defaults

The command is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(18)ST	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2	This command was integrated into Cisco IOS Release 12.2.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Bidir-PIM is disabled by default to ensure complete backward compatibility when upgrading a router to Cisco IOS Release 12.0(18)ST or a later release.

When bidir-PIM is disabled, the router will behave similarly to a router without bidir-PIM support. The following conditions will apply:

- PIM hello messages sent by the router will not contain the bidirectional mode option.
- The router will not send designated forwarder (DF) election messages and will ignore DF election messages it receives.
- The **ip pim rp-address, ip pim send-rp-announce**, and **ip pim rp-candidate** global configuration commands will be treated as follows:
  - If these commands are configured when bidir-PIM is disabled, bidirectional mode will not be a configuration option.

  - If these commands are configured with the bidirectional mode option when bidir-PIM is enabled and then bidir-PIM is disabled, these commands will be removed from the command-line interface (CLI). In this situation, these commands must be configured again with the bidirectional mode option when bidir-PIM is reenabled.

- The **df** keyword for the **show ip pim interface** user EXEC or privileged EXEC command and **debug ip pim** privileged EXEC command is not supported.

Examples

The following example shows how to configure a rendezvous point (RP) for both sparse mode and bidirectional mode groups: 224/8 and 227/8 are bidirectional groups, 226/8 is sparse mode, and 225/8 is dense mode. The RP must be configured to use different IP addresses for the sparse mode and bidirectional mode operations. Two loopback interfaces are used to allow this configuration. The addresses of these loopback interfaces must be routed throughout the PIM domain such that the other routers in the PIM domain can receive Auto-RP announcements and communicate with the RP.

```
ip multicast-routing
ip pim bidir-enable
!
interface loopback 0
description One Loopback adddress for this routers Bidir Mode RP function
ip address 10.0.1.1 255.255.255.0
 ip pim sparse-dense-mode
!
interface loopback 1
 description One Loopback adddress for this routers Sparse Mode RP function
 ip address 10.0.2.1 255.255.255.0
 ip pim sparse-dense-mode

ip pim send-rp-announce Loopback0 scope 10 group-list 45 bidir
ip pim send-rp-announce Loopback1 scope 10 group-list 46
ip pim send-rp-discovery scope 10

access-list 45 permit 224.0.0.0 0.255.255.255
access-list 45 permit 227.0.0.0 0.255.255.255
access-list 45 deny   225.0.0.0 0.255.255.255

access-list 46 permit 226.0.0.0 0.255.255.255
```

Related Commands

Command	Description
debug ip pim	Displays PIM packets received and sent, and to display PIM-related events.
ip pim rp-address	Configures the address of a PIM RP for a particular group.
ip pim rp-candidate	Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR.
ip pm send-rp-announce	Uses Auto-RP to configure for which groups the router is willing to act as RP.

ip pim bidir-neighbor-filter

To configure an access list (ACL) to specify which bidirectionally capable (bidir-capable) neighbors will participate in the designated forwarder (DF) election, use the **ip pim bidir-neighbor-filter** command in interface configuration mode. To allow all neighbors to participate in DF election, use the **no** form of this command.

ip pim bidir-neighbor-filter *acl-name*

no ip pim bidir-neighbor-filter *acl-name*

Syntax Description

acl-name	Specified ACL.

Defaults

All routers are considered to be bidirectional (bidir) capable.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.2(10)S	This command was introduced.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Normally, DF election only occurs on those interfaces on which all Protocol Independent Multicast (PIM) neighbors are bidir capable. To allow for a smoother transition from a sparse-mode only network to a hybrid bidir-/sparse-mode network, the **ip pim bidir-neighbor-filter** command enables you to specify what routers should be participating on the DF election, while still allowing all routers to participate in the sparse-mode domain.

Bidirectional PIM allows multicast routers to keep reduced state information. All of the multicast routers in a segment must be bidirectionally enabled in order for bidir to elect a DF. Because routers in a segment are not always bidir-enabled, a mechanism is necessary to allow these routers to elect a DF from those routers on a segment that are bidir-enabled.

Multicast boundaries on the nonbidir routers are defined to prevent PIM messages and data for the bidir groups to leak in or out of the bidir subset cloud. Meanwhile, the bidir routers can elect a DF from among themselves even when there are nonbidir routers in the segment.

The **ip pim bidir-neighbor-filter** command allows the use of an ACL to specify which neighbors will participate in the DF election, allowing bidir deployment in the necessary routers without having to upgrade all of the routers in the segment.

Default behavior is that all routers are considered to be bidir-capable. Therefore, if one neighbor does not support bidir, the DF election will not occur.

When the **ip pim bidir-neighbor-filter** command is enabled, the routers that are permitted by the ACL are considered to be bidir-capable. Therefore:

- If a permitted neighbor does not support bidir, the DF election will not occur.
- If a denied neighbor does not support bidir, DF election still occurs among all other routers on the segment.

Examples

In the following example, the neighbor at address 10.4.0.3 is considered to be bidir-capable:

```
Router# show ip pim neighbor ethernet 3/3

PIM Neighbor Table
Neighbor          Interface                Uptime/Expires    Ver   DR
Address
Prio/Mode
10.4.0.4          Ethernet3/3              00:01:52/00:01:20 v2    1 / DR B
10.4.0.3          Ethernet3/3              00:01:52/00:01:20 v2    1 / B

Router# show access-lists 50

Standard IP access list 50
    10 permit 10.4.0.4 (3 matches)
    20 deny   10.4.0.3 (7 matches)
```

The **ip pim bidir-neighbor-filter 50** command sets conditions for DF election through use of ACL 50.

```
Router(config) interface ethernet 3/3
Router(config-if)# ip pim bidir-neighbor-filter 50
```

The following example shows the neighbor router at address 10.4.0.4 is now permitted to participate in DF election, and the neighbor router at address 10.4.0.3 is now denied access to DF election:

```
Router# show run interface ethernet 3/3

Building configuration...

Current configuration :210 bytes
!
interface Ethernet3/3
 ip address 10.4.0.2 255.255.0.0
 no ip redirects
 no ip proxy-arp
 ip pim bidir-neighbor-filter 50
 ip pim sparse-dense-mode
 no ip route-cache cef
 no ip route-cache
 duplex half
 end

Router# show ip pim neighbor ethernet 3/3

PIM Neighbor Table
Neighbor          Interface                Uptime/Expires    Ver   DR
Address
```

```
Prio/Mode
10.4.0.4          Ethernet3/3             00:04:03/00:01:39 v2    1 / DR B
10.4.0.3          Ethernet3/3             00:04:03/00:01:38 v2    1 /
```

ip pim bidir-offer-interval

To configure the Protocol Independent Multicast (PIM) bidirectionally capable designated forwarder (DF) election offer message interval time, use the **ip pim bidir-offer-interval** command in global configuration mode. To disable the message interval configuration, use the **no** form of this command.

ip pim bidir-offer-interval *seconds* [**msec**]

no ip pim bidir-offer-interval *seconds* [**msec**]

Syntax Description

seconds	Interval time, in seconds. The valid range is from 1 to 20000.
msec	(Optional) Specifies interval in milliseconds (ms).

Command Default

The default value for interval time is 100 ms.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following examples shows how to set the message interval time to 22 seconds:

```
Router# configure terminal
Router(config)# ip pim bidir-offer-interval 22
```

Related Commands

Command	Description
ip pim bidir-neighbor-filter	Configures an ACL to specify which bidirectionally capable neighbors will participate in the designated forwarder election.
ip pim bidir-offer-limit	Configures the PIM bidirectionally capable number of unanswered offers before it changes as the DF.

ip pim bidir-offer-limit

To configure the Protocol Independent Multicast (PIM) bidirectionally capable number of unanswered offers before it changes as the designated forwarder (DF), use the **ip pim bidir-offer-limit** command in global configuration mode. To remove the limit, use the **no** form of this command.

ip pim bidir-offer-limit *number*

no ip pim bidir-offer-limit *number*

Syntax Description

number	Limit of unanswered offers. The valid range is 4 to 100.

Command Default

The default value is three unanswered offers.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following examples shows how to set the unanswered offer limit to 75:

```
Router# configure terminal
Router(config)# ip pim bidir-offer-limit 75
```

Related Commands

Command	Description
ip pim bidir-neighbor-filter	Configures an ACL to specify which bidirectionally capable neighbors will participate in the designated forwarder election.
ip pim bidir-offer-interval	Configures the PIM bidirectionally capable DF election offer message interval time.

ip pim border

The **ip pim border** command is replaced by the **ip pim bsr-border** command. See the description of the **ip pim bsr-border** command for more information.

ip pim bsr-border

To prevent bootstrap router (BSR) messages from being sent or received through an interface, use the **ip pim bsr-border** command in interface configuration mode. To disable this configuration, use the **no** form of this command.

ip pim bsr-border

no ip pim bsr-border

Syntax Description

This command has no arguments or keywords.

Defaults

The command is disabled.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
11.3 T	The **ip pim border** command was introduced.
12.0(8)	The **ip pim border** command was replaced by the **ip pim bsr-border** command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

When this command is configured on an interface, no Protocol Independent Multicast (PIM) Version 2 BSR messages will be sent or received through the interface. Configure an interface bordering another PIM domain with this command to avoid BSR messages from being exchanged between the two domains. BSR messages should not be exchanged between different domains, because routers in one domain may elect rendezvous points (RPs) in the other domain, resulting in protocol malfunction or loss of isolation between the domains.

Note This command does not set up multicast boundaries. It sets up only a PIM domain BSR message border.

Examples

The following example configures the interface to be the PIM domain border:

```
interface ethernet 1
ip pim bsr-border
```

Related Commands

Command	Description
ip multicast boundary	Configures an administratively scoped boundary.
ip pim bsr-candidate	Configures the router to announce its candidacy as a BSR.

ip pim bsr-candidate

To configure a router to announce its candidacy as a bootstrap router (BSR), use the **ip pim bsr-candidate** command in global configuration mode. To remove this router as a candidate BSR, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority*]]

no ip pim [**vrf** *vrf-name*] **bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority*]]

Syntax Description

vrf *vrf-name*	(Optional) Configures the router to announce its candidacy as a BSR for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
interface-type interface-number	Interface type and number on this router from which the BSR address is derived. This address is sent in BSR messages. **Note** This interface must be enabled for Protocol Independent Multicast (PIM) using the **ip pim** command.
hash-mask-length	(Optional) Length of a mask (32 bits maximum) that is to be ANDed with the group address before the PIMv2 hash function is called. All groups with the same seed hash correspond to the same rendezvous point (RP). For example, if this value is 24, only the first 24 bits of the group addresses matter. The hash mask length allows one RP to be used for multiple groups. The default hash mask length is 0.
priority	(Optional) Priority of the candidate BSR (C-BSR). The range is from 0 to 255. The default priority is 0. The C-BSR with the highest priority value is preferred. **Note** The Cisco IOS and Cisco IOS XE implementation of PIM BSR uses the value 0 as the default priority for candidate BSRs. This implementation predates RFC 5059, which specifies that 64 be used as the default priority value. The Cisco IOS and Cisco IOS XE implementation, thus, deviates from RFC 5059. To comply with the default priority value specified in the RFC, you must explicitly set the priority value to 64.

Command Default

The router is not configured to announce itself as a candidate BSR.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3T	This command was introduced.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.

Release	Modification
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was implemented on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command configures the router to send BSR messages to all its PIM neighbors, with the address of the designated interface as the BSR address.

Note The interface specified for this command must be enabled for Protocol Independent Multicast (PIM) using the **ip pim** command.

This command should be configured on backbone routers that have good connectivity to all parts of the PIM domain.

The BSR mechanism is specified in RFC 2362. Candidate RP (C-RP) routers unicast C-RP advertisement packets to the BSR. The BSR then aggregates these advertisements in BSR messages, which it regularly multicasts with a TTL of 1 to the ALL-PIM-ROUTERS group address, 224.0.0.13. The multicasting of these messages is handled by hop-by-hop RPF flooding; so no preexisting IP multicast routing setup is required (unlike with AutoRP). In addition, the BSR does not preselect the designated RP for a particular group range (unlike AutoRP); instead, each router that receives BSR messages will elect RPs for group ranges based on the information in the BSR messages.

Note Cisco routers always accept and process BSR messages. There is no command to disable this function.

Cisco routers perform the following steps to determine which C-RP is used for a group:

1. A longest match lookup is performed on the group prefix that is announced by the BSR C-RPs.
2. If more than one BSR-learned C-RP are found by the longest match lookup, the C-RP with the lowest priority (configured with the **ip pim rp-candidate** command) is preferred.
3. If more than one BSR-learned C-RP have the same priority, the BSR hash function is used to select the RP for a group.
4. If more than one BSR-learned C-RP return the same hash value derived from the BSR hash function., the BSR C-RP with the highest IP address is preferred.

Examples

The following example shows how to configure the IP address of the router on Gigabit Ethernet interface 0/0 to be a BSR C-RP with a hash mask length of 0 and a priority of 192:

```
ip pim bsr-candidate Gigabit Ethernet 0/0 0 192
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.
ip pim rp-candidate	Configures the router to advertise itself to the BSR as a PIMv2 C-RP.
show ip pim bsr-router	Displays information about a BSR.

ip pim dm-fallback

To enable Protocol Independent Multicast (PIM) dense mode (DM) fallback, use the **ip pim dm-fallback** command in global configuration mode. To prevent PIM dense mode fallback, use the **no** form of this command.

ip pim dm-fallback

no ip pim dm-fallback

Syntax Description

This command has no arguments or keywords.

Command Default

PIM dense mode fallback is enabled for all interfaces on the router that are configured with either the **ip pim dense-mode** or **ip pim sparse-dense-mode** commands.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

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

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

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

Use the **no ip pim dm-fallback** command to disable PIM-DM flooding on sparse-dense interfaces.

Cause and Effect of Dense Mode Fallback

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

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

Effects of Preventing Dense Mode Fallback

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

With the introduction of PIM-DM fallback prevention, the PIM-DM fallback behavior has been changed to prevent dense mode flooding. By default, if all of the interfaces are configured to operate in PIM sparse mode (using the **ip pim sparse-mode** command), there is no need to configure the **no ip pim dm-fallback** command (that is, the PIM-DM fallback behavior is enabled by default). If any interfaces are not configured using the **ip pim sparse-mode** command (for example, using the **ip pim sparse-dense-mode** command), then the PIM-DM fallback behavior can be explicit disabled using the **no ip pim dm-fallback** command.

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

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

Examples

The following example shows how to disable PIM-DM fallback:

```
no ip pim dm-fallback
```

Related Commands

Command	Description
ip pim dense-mode	Enables PIM dense mode on the interface.
ip pim sparse-mode	Enables PIM sparse mode on the interface.
ip pim sparse-dense-mode	Enables PIM to operate in sparse or dense mode, depending on the group.

ip pim dr-priority

To set the priority for which a router is elected as the designated router (DR), use the **ip pim dr-priority** command in interface configuration mode. To disable this function, use the **no** form of this command.

ip pim dr-priority *priority-value*

no ip pim dr-priority *priority-value*

Syntax Description

priority-value	Value in the range from 0 to 4294967294 used to determine the priority of the router to be selected as the DR.

Defaults

The command is disabled.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.1(2)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

When a DR is a candidate for election, the following conditions apply:

- The router with the highest priority value configured on an interface will be elected as the DR. If this priority value is the same on multiple routers, then the router with the highest IP address configured on an interface will be elected as the DR.
- If a router does not advertise a priority value in its hello messages, the router is regarded as having the highest priority and will be elected as the DR. If there are multiple routers with this priority status, then the router with the highest IP address configured on an interface will be elected as the DR.

Examples

The following example sets the DR priority value of the Ethernet0 interface to 200:

```
interface Ethernet0
  ip address 10.0.1.2 255.255.255.0
  ip pim dr-priority 200
```

ip pim log-neighbor-changes

To log the Protocol Independent Multicast (PIM) neighboring up or down status and the designated router changes, use the **ip pim log-neighbor-changes** command in global configuration mode. To disable the configured parameters, use the **no** form of this command.

ip pim log-neighbor-changes

no ip pim log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

The PIM status changes are logged in.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

This command enables syslog messages that help to generate a list of neighbor state changes.

Examples

The following examples shows how to disable the logging of the neighboring changes:

```
Router# configure terminal
Router(config)# no ip pim log-neighbor-changes
```

Related Commands

Command	Description
ip pim dr-priority	Sets the priority for which a router is elected as the designated router.

ip pim minimum-vc-rate

To configure the minimum traffic rate to keep virtual circuits (VCs) from being idled, use the **ip pim minimum-vc-rate** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip pim minimum-vc-rate *pps*

no ip pim minimum-vc-rate

Syntax Description

pps	Rate, in packets per second, below which a VC is eligible for idling. The default value is 0, which means all VCs are eligible for idling. The range is from 0 to 4294967295.

Defaults

The default rate is 0 pps, which indicates all VCs are eligible for idling.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command applies to an ATM interface only and also requires IP Protocol Independent Multicast sparse mode (PIM-SM).

An idling policy uses the **ip pim vc-count** *number* command to limit the number of VCs created by PIM. When the router stays at or below this number, no idling policy is in effect. When the next VC to be opened will exceed the number, an idling policy is exercised. Any virtual circuits with a traffic rate lower than the **ip pim minimum-vc-rate** command are subject to the idling policy.

Examples

The following example configures a minimum rate of 2500 pps over a VC, below which the VC is eligible for idling:

```
ip pim minimum-vc-rate 2500
```

Related Commands

Command	Description
ip pim vc-count	Changes the maximum number of VCs that PIM can open.

ip pim multipoint-signalling

To enable Protocol Independent Multicast (PIM) to open ATM multipoint switched virtual circuits (VCs) for each multicast group that a receiver joins, use the **ip pim multipoint-signalling** command in interface configuration mode. To disable the feature, use the **no** form of this command.

ip pim multipoint-signalling

no ip pim multipoint-signalling

Syntax Description

This command has no arguments or keywords.

Defaults

The command is disabled.
All multicast traffic goes to the static map multipoint VC as long as the **atm multipoint-signalling** command is configured.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is accepted only on an ATM interface. It allows optimal multicast trees to be built down to ATM switch granularity. This command can enhance router performance and link utilization because packets are not replicated and sent multiple times over the ATM interface.

Examples

The following example enables PIM to open ATM multipoint switched VCs for each multicast group that is joined:

```
ip pim multipoint-signalling
```

Related Commands

Command	Description
atm multipoint-signalling	Enables point-to-multipoint signaling to the ATM switch.
ip pim minimum-vc-rate	Configures the minimum traffic rate to keep VCs from being idled.
ip pim vc-count	Changes the maximum number of VCs that PIM can open.
show ip pim vc	Displays ATM virtual circuit status information for multipoint VCs opened by PIM.

ip pim nbma-mode

To configure a multiaccess WAN interface to be in nonbroadcast multiaccess (NBMA) mode, use the **ip pim nbma-mode** command in interface configuration mode. To disable this function, use the **no** form of this command.

ip pim nbma-mode

no ip pim nbma-mode

Syntax Description

This command has no arguments or keywords.

Defaults

The command is disabled.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Use this command on Frame Relay, Switched Multimegabit Data Service (SMDS), or ATM only, especially when these media do not have native multicast available. Do not use this command on multicast-capable LANs such as Ethernet or FDDI.

When this command is configured, each Protocol Independent Multicast (PIM) join message is tracked in the outgoing interface list of a multicast routing table entry. Therefore, only PIM WAN neighbors that have joined for the group will get packets sent as data-link unicasts. This command should only be used when the **ip pim sparse-mode** command is configured on the interface. This command is not recommended for LANs that have natural multicast capabilities.

Examples

The following example configures an interface to be in NBMA mode:

```
ip pim nbma-mode
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.

ip pim neighbor-filter

To prevent a router from participating in Protocol Independent Multicast (PIM) (for example, to configure stub multicast routing), use the **ip pim neighbor-filter** command in interface configuration mode. To remove the restriction, use the **no** form of this command.

ip pim neighbor-filter *access-list*

no ip pim neighbor-filter *access-list*

Syntax Description

access-list	Number or name of a standard IP access list that denies PIM packets from a source.

Defaults

The command is disabled.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Examples

The following example enables stub multicast routing on Router A, which has an outgoing interface with IP address 10.0.0.1. Router B is a central router with an incoming interface with address 10.0.0.2. Access list 1 filters PIM messages from the source (stub Router A).

Router A Configuration

```
ip multicast-routing
ip pim dense-mode
ip igmp helper-address 10.0.0.2
```

Router B Configuration

```
ip multicast-routing
 ip pim dense-mode : or ip pim sparse-mode
 ip pim neighbor-filter 1
access-list 1 deny 10.0.0.1
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
ip igmp helper-address	Causes the system to forward all IGMP host reports and leave messages received on the interface to the specified IP address.

ip pim passive

To configure an interface to operate in Protocol Independent Multicast (PIM) passive mode, use the **ip pim passive** command in interface configuration mode. To disable PIM passive mode operation on an interface, use the **no** form of this command.

ip pim passive

no ip pim passive

Syntax Description

This command has no arguments or keywords.

Command Default

PIM passive mode operation is disabled.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.2(37)SE	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

If the **ip pim passive** command is configured on an interface enabled for IP multicast, the router will operate this interface in PIM passive mode, which means that the router will not send PIM messages on the interface nor will it accept PIM messages from other routers across this interface. The router will instead consider that it is the only PIM router on the network and thus act as the Designated Router (DR) and also as the Designated Forwarder (DF) for all bidirectional PIM (bidir-PIM) group ranges. Operations of the Interior Gateway Management Protocol (IGMP) are unaffected by this command.

Note Do not use the **ip pim passive** command on LANs that have more than one multicast router connected to them because all routers with this command configured will consider themselves to be DR/DF, resulting in duplicate traffic (for PIM sparse mode [PIM-SM], PIM dense mode [PIM-DM], and Source Specific Multicast [PIM-SSM]) or even in looping traffic (for bidir-PIM). Instead, use the **ip pim neighbor-filter** command to limit PIM messages to and from valid routers on LANs with more than one router.

Note The **ip pim passive** and **ip pim neighbor-filter** commands can be used together on an interface. If both commands are configured, the **ip pim passive** command will take precedence over the **ip pim neighbor-filter** command.

Use the **show ip pim interface** command to confirm the mode that PIM interfaces are operating in.

Examples

The following example shows how to configure an interface to operate in PIM passive mode. In this example, a stub router is configured to support multicast stub routing. VLAN interface 100 is configured to operate in PIM passive mode.

```
ip multicast-routing
!
interface Vlan100
  ip pim sparse-mode
  ip igmp helper-address 172.16.32.1
  ip pim passive
!
interface GigabitEthernet1/0
  ip pim sparse-mode
!
ip pim ssm default
```

Related Commands

Command	Description
ip pim neighbor-filter	Prevents a router from participating in PIM (for example, to configure multicast stub routing).
show ip pim interface	Displays information about interfaces configured for PIM.

ip pim query-interval

To configure the frequency of Protocol Independent Multicast (PIM) query (hello) messages, use the **ip pim query-interval** command in interface configuration mode. To return to the default interval, use the **no** form of this command.

ip pim query-interval *period* [**msec**]

no ip pim query-interval

Syntax Description

period	The number of seconds or milliseconds (ms) that can be configured for the PIM hello (query) interval. The range is from 1 to 65535.
msec	(Optional) Specifies that the interval configured for the *period* argument be interpreted in milliseconds. If the **msec** keyword is not used along with the *period* argument, the interval range is assumed to be in seconds.

Command Default

PIM hello (query) messages are sent every 30 seconds.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	The **msec** keyword was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Use this command to configure the frequency of PIM neighbor discovery messages. By default these messages are sent once every 30 seconds. In PIM Version 1 (PIMv1), these messages are referred to as PIM query messages; in PIM Version 2 (PIMv2), these messages are referred to as PIM hello messages. By default, routers run PIMv2 and send PIM hello messages. A router will change (auto-fallback) to PIMv1 and will send PIM query messages if it detects a neighboring router that only supports PIMv1. As soon as that neighboring PIMv1 router is removed from the network, the router will revert to PIMv2.

Note A router can be configured to exclusively use PIMv1 on an interface with the **ip pim version 1** command.

Note In PIM version 2, PIM hello messages also contain a variety of options that allow PIM routers on the network to learn about the capabilities of PIM neighbors. For more information about these capabilities, see the **show ip pim neighbor** command page.

PIM neighbor discovery messages are used to determine which router on a network is acting as the Designated Router (DR) for PIM sparse mode (PIM-SM) and Source Specific Multicast (SSM). The DR is responsible for joining PIM-SM and SSM groups receiving multicast traffic from sources requested by receivers (hosts). In addition, in PIM-SM, the DR is also responsible for registering local sources with the RP. If the DR fails, a backup router will become the DR and then forward traffic for local receivers and register local sources.

The *period* argument is used to specify the PIM hello (query) interval. The interval determines the frequency at which PIM hello (query) messages are sent.

Note When an interfaces enabled for PIM comes up, a PIM hello (query) message is sent immediately. In some cases, the initial PIM hello (query) message may be lost**.**If the first PIM hello (query) does not get sent when an interface initially comes up, another one will be sent 3 seconds later regardless of the PIM hello (query) interval to ensure that there are no initialization delays.

The configured PIM hello interval also determines the holdtime used by a PIM router. The Cisco IOS software calculates the holdtime as follows:

3 * the interval specified for the *period* argument

By default, PIM routers announce the holdtime in PIM hello (query) messages.If the holdtime expires and another router has not received another hello (query) message from this router, it will timeout the PIM neighbor. If the timed out router was the DR, the timeout will trigger DR election. By default, the DR-failover interval occurs after 90 seconds (after the default holdtime expires for a DR). To reduce DR-failover time in redundant networks, a lower value for the *period* argument can be configured on all routers. The minimum DR-failover time that can be configured (in seconds) is 3 seconds (when the *period* argument is set to 1 second). The DR-failover time can be reduced to less than 3 seconds if the **msecs** keyword is specified. When the **msecs** keyword is used with the **ip pim query-interval** command, the value specified for the *period* argument is interpreted as a value in milliseconds (instead of seconds). By enabling a router to send PIM hello messages more often, this functionality allows the router to discover unresponsive neighbors more quickly. As a result, the router can implement failover or recovery procedures more efficiently

Note If IGMP Version 1 is being used on a network, then the DR is also the IGMP querier; if at least IGMP version 2 is being used, then the router with the lowest IP address becomes the IGMP querier.

Examples

The following example shows how to set the PIM hello interval to 45 seconds:

```
interface FastEthernet0/1
 ip pim query-interval 45
```

The following example shows how to set the PIM hello interval to 100 milliseconds:

```
interface FastEthernet0/1
 ip pim query-interval 100 msec
```

Related Commands

Command	Description
show ip pim neighbor	Displays information about PIM neighbors discovered by PIMv1 router query messages or PIMv2 hello messages

ip pim register-rate-limit

To rate limit Protocol Independent Multicast sparse mode (PIM-SM) register packets based on either packets per second or bits per second, use the **ip pim register-rate-limit** command in global configuration mode. To disable this limit, use the **no** form of this command.

Cisco IOS Releases Prior to Releases 12.2(33)SRE and 15.0(1)M

ip pim [**vrf** *vrf-name*] **register-rate-limit** *packets-per-second*

no ip pim [**vrf** *vrf-name*] **register-rate-limit**

Cisco IOS Releases 12.2(33)SRE, 15.0(1)M, and Cisco IOS XE Release 2.1, and Subsequent 12.2SR, 15.0 Mainline, T Releases, and Cisco IOS XE Releases

ip pim [**vrf** *vrf-name*] **register-rate-limit** *bits-per-second*

no ip pim [**vrf** *vrf-name*] **register-rate-limit**

Syntax Description

vrf *vrf-name*	(Optional) Rate limits PIM-SM register packets associated with the Multicast Virtual Private Network (MVPN) virtual routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
packets-per-second	Maximum number of register packets sent per second by the router. The range is from 1 to 65535 seconds. By default, a maximum rate is not set.
bits-per-second	Maximum number of register bits sent per second. The range is from 8000 to 2000000000 bits. By default, a maximum rate is not set.

Command Default

No rate limit is set for PIM-SM register packets.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3T	This command was introduced.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was implemented on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was modified. The value that can be supplied for the rate limit for PIM-SM register packets was changed from a value in packets per second to a value of a bits per second on a per-RP basis.

Release	Modification
15.0(1)M	This command was modified. The value that can be supplied for the rate limit for PIM-SM register packets was changed from a value in packets per second to a value of bits per second on a per-RP basis.
12.2(33)SRE	This command was modified. The value that can be supplied for the rate limit for PIM-SM register packets was changed from a value in packets per second to a value of bits per second on a per-RP basis.

Usage Guidelines

Use this command to rate limit the PIM-SM register packets based on either packets per second or bits per second. Enabling this command will limit the load on the DR and RP at the expense of dropping those register packets that exceed the set limit. Receivers may experience data packet loss within the first second in which register packets are sent from bursty sources.

Setting a value for the *packets-per-second* argument using the **ip pim register-rate-limit** command sets rate limiting on all PIM-SM registers.

Setting a value for the *bits-per-second* argument using the **ip pim register-rate-limit** command sets rate limiting on PIM-SM registers on a per-RP basis.

If the **ip pim** command is configured with the **dense-mode** and **proxy-register** keywords, you must set a limit on the maximum number of PIM-SM register packets sent because of the potentially large number of sources from the dense mode area that may send data into the sparse mode region (and thus need registering in the border router).

This command applies only to sparse mode (S, G) multicast routing entries.

Examples

The following example shows how to configure the **ip pim register-rate-limit** command with a maximum rate of two register packets per second:

```
ip pim register-rate-limit 2
```

The following examples shows how to configure the **ip pim register-rate-limit** command with a maximum rate of 8000 bits per second:

```
ip pim register-rate-limit 8000
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.

ip pim register-source

To configure the IP source address of a register message to an interface address other than the outgoing interface address of the designated router (DR) leading toward the rendezvous point (RP), use the **ip pim register-source** command in global configuration mode. To disable this configuration, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **register-source** *interface-type interface-number*

no ip pim [**vrf** *vrf-name*] **register-source**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
interface-type interface-number	Interface type and interface number that identify the IP source address of a register message.

Defaults

By default, the IP address of the outgoing interface of the DR leading toward the RP is used as the IP source address of a register message.

Command Modes

Global configuration

Command History

Release	Modification
12.0(8)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is required only when the IP source address of a register message is not a uniquely routed address to which the RP can send packets. This situation may occur if the source address is filtered such that packets sent to it will not be forwarded or if the source address is not unique to the network. In these cases, the replies sent from the RP to the source address will fail to reach the DR, resulting in Protocol Independent Multicast sparse mode (PIM-SM) protocol failures.

If no IP source address is configured or if the configured source address is not in service, the IP address of the outgoing interface of the DR leading toward the RP is used as the IP source address of the register message. Therefore, we recommend using a loopback interface with an IP address that is uniquely routed throughout the PIM-SM domain.

Examples

The following example shows how to configure the IP source address of the register message to the loopback 3 interface of a DR:

```
ip pim register-source loopback 3
```

ip pim rp-address

To statically configure the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for multicast groups, use the **ip pim rp-address** command in global configuration mode. To remove an RP address, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **rp-address** *rp-address* [*access-list*] [**override**] [**bidir**]

no ip pim [**vrf** *vrf-name*] **rp-address** *rp-address* [*access-list*] [**override**] [**bidir**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies that the static group-to-RP mapping be associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
rp-address	IP address of the RP to be used for the static group-to-RP mapping. This is a unicast IP address in four-part dotted-decimal notation.
access-list	(Optional) Number or name of a standard access list that defines the multicast groups to be statically mapped to the RP. **Note** If no access list is defined, the RP will map to all multicast groups, 224/4.
override	(Optional) Specifies that if dynamic and static group-to-RP mappings are used together and there is an RP address conflict, the RP address configured for a static group-to-RP mapping will take precedence. **Note** If the **override** keyword is not specified and there is RP address conflict, dynamic group-to-RP mappings will take precedence over static group-to-RP mappings.
bidir	(Optional) Specifies that the static group-to-RP mapping be applied to a bidir-PIM RP. If the command is configured without the **bidir** keyword, the groups will operate in sparse mode. **Note** The **bidir** keyword is available as an optional keyword only if bidir-PIM has been enabled (using the **ip pim bidir-enable** command).

Command Default

No PIM static group-to-RP mappings are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.2	This command was introduced.
11.1	The **override** keyword was added.
12.1(2)T	The **bidir** keyword was added.

Release	Modification
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

In the Cisco IOS implementation of PIM, each multicast group individually operates in one of the following modes: dense mode, sparse mode, or bidirectional mode. Groups in sparse mode (PIM-SM) or bidirectional mode (bidir-PIM) use RPs to connect sources and receivers. All routers in a PIM domain need to have a consistent configuration for the mode and RP addresses of the multicast groups.

The Cisco IOS software learns the mode and RP addresses of multicast groups through the following three mechanisms: static group-to-RP mapping configurations, Auto-RP, and bootstrap router (BSR). By default, groups will operate in dense mode. No commands explicitly define groups to operate in dense mode.

Use the **ip pim rp-address** command to statically define the RP address for PIM-SM or bidir-PIM groups (an **ip pim rp-address** command configuration is referred to as a static group-to-RP mapping).

You can configure a single RP for more than one group using an access list. If no access list is specified, the static RP will map to all multicast groups, 224/4.

You can configure multiple RPs, but only one RP per group range.

If multiple **ip pim rp-address** commands are configured, the following rules apply:

- Highest RP IP address selected regardless of reachability: If a multicast group is matched by the access list of more than one configured **ip pim rp-address** command, then the RP for the group is determined by the RP with the highest RP address configured.
- One RP address per command: If multiple **ip pim rp-address** commands are configured, each static group-to-RP mapping must be configured with a unique RP address (if not, it will be overwritten).This restriction also means that only one RP address can be used to provide RP functions for either sparse mode or bidirectional mode groups. If you want to configure static group-to-RP mappings for both bidirectional and sparse mode, the RP addresses must be unique for each mode.
- One access list per command: If multiple **ip pim rp-address** commands are configured, only one access list can be configured per static group-to-RP mapping. An access list cannot be reused with other static group-to-RP mappings configured on a router.

If dynamic and static group-to-RP mappings are used together, the following rule applies to a multicast group: Dynamic group-to-RP mappings take precedence over static group-to-RP mappings—unless the **override** keyword is used.

Examples

The following example shows how to set the PIM RP address to 192.168.0.1 for all multicast groups (224/4) and defines all groups to operate in sparse mode:

```
ip pim rp-address 192.168.0.1
```

The following example shows how to set the bidir-PIM RP address to 172.16.0.2 for the multicast range 239/8.

```
access list 10 239.0.0.0 0.255.255.255
ip pim rp-address 172.16.0.2 10 bidir
```

Note The RP address used for static group-to-RP mappings must be unique. You cannot use the same RP address for both bidir-PIM and PIM-SM groups.

ip pim rp-announce-filter

To filter incoming rendezvous point (RP) announcement messages sent from candidate RPs (C-RPs) to the RP mapping agent, use the **ip pim rp-announce-filter** command in global configuration mode. To remove the filter, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **rp-announce-filter** {**group-list** *access-list* | **rp-list** *access-list* [**group-list** *access-list*]}

no ip pim [**vrf** *vrf-name*] **rp-announce-filter** {**group-list** *access-list* | **rp-list** *access-list* [**group-list** *access-list*]}

Syntax Description

vrf *vrf-name*	(Optional) Specifies that the filter be applied to incoming RP messages sent from C-RPs associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
group-list *access-list*	Specifies the number or name of a standard access list that defines the multicast groups to be permitted or denied from RP announcements sent by C-RPs to the RP mapping agent.
rp-list *access-list*	Specifies the number or name of a standard access list that defines the IP addresses of C-RPs whose RP announcements are to be permitted or denied by the RP mapping agent.

Command Default

All RP announcements are accepted by the RP mapping agent.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **ip pim rp-announce-filter** command to filter incoming Auto-RP announcement messages sent from C-RPs to RP mapping agents. This command should only be configured on RP mapping agents.

Auto-RP provides a means to distribute group-to-RP mappings within a multicast network without having to manually configure static RPs on every router. To accomplish this distribution, Auto-RP uses the following mechanisms:

- C-RPs send RP announcements to multicast group 224.0.1.39.
- RP mapping agents receive the RP announcements from C-RPs and determine which C-RP should be the RP for any given group (or groups) based on the highest IP address. RP mapping agents then distribute that information to all multicast routers by means of RP discovery messages, which are sent to the Auto-RP multicast group address 224.0.1.40.
- The sending of both RP announcements and RP discovery messages occurs every 60 seconds by default with a holdtime of 180 seconds. If no RP is found, each router then searches locally for a static RP mapping. If no static RP mapping is configured, the router defaults to dense mode.

The **ip pim rp-announce filter** command allows you to configure policies on an RP mapping agent that define the C-RPs whose RP announcements are to be filtered (ignored) by the mapping agent. You can use this command to configure the mapping agent to filter RP announcement messages from specific or unknown routers by permitting or denying specific C-RPs .You can also filter RP announcement messages from an candidate RP for specific group prefixes, thereby restricting that router to be the C-RP for only the ranges not filtered on the RP mapping agent.

Caution If you use more than one RP-mapping agent, you must configure the same filters on all mapping agents to avoid inconsistencies in Auto-RP operations.

Caution An improperly configured **ip pim rp-announce-filter** command may result in RP announcements being ignored. In addition, the **ip pim rp-announce-filter** command should only be configured on the mapping agent; if not, the command will fail because non-mapping agents do not listen to group 224.0.1.39 and do not know how to distribute the necessary group-to-RP mappings.

Use the **rp-list** keyword and *access-list* argument to specify the standard access list that defines the IP addresses of C-RPs whose RP announcements are to be permitted or denied on the RP mapping agent. Use the **group-list** keyword and *access-list* argument to specify the standard access list that defines the multicast groups to be permitted or denied from RP announcements sent by C-RPs to the RP mapping agent. RP announcement messages received that match the access list specified for **rp-list** keyword and access list specified for the **group-list** keyword are filtered by the RP mapping agent.

If a C-RP list is not specified (using the **rp-list** keyword and *access-list* argument), the command will permit all C-RPs. If a group list is not specified (using the **group-list** keyword and *access-list* argument), the command will deny all groups.

If no **ip pim rp-announce-filter** commands are configured, a router enabled to be an RP mapping agent (using the **ip pim send-rp-discovery** command) will accept all RP announcements for all groups from all C-RPs. Configure one or more **ip pim rp-announce-filter** commands on RP mapping agents to filter unwanted RP messages.

Examples

The following example shows how to configure the router to accept RP announcements from the C-RPs defined in access list 1 for the group range defined in access list 2:

```
ip pim rp-announce-filter rp-list 1 group-list 2
access-list 1 permit 10.0.0.1
access-list 1 permit 10.0.0.2
access-list 2 permit 224.0.0.0 15.255.255.255
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.
ip pim send-rp-discovery	Configures the router to be an RP mapping agent.

ip pim rp-candidate

To configure a router to advertise itself to the bootstrap router (BSR) as a Protocol Independent Multicast (PIM) Version 2 (PIMv2) candidate rendezvous point (C-RP), use the **ip pim rp-candidate** command in global configuration mode. To remove this router as a C-RP, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **rp-candidate** *interface-type interface-number* [**bidir**] [**group-list** *access-list*] [**interval** *seconds*] [**priority** *value*]

no ip pim [**vrf** *vrf-name*] **rp-candidate**

Syntax Description

vrf *vrf-name*	(Optional) Configures the router to advertise itself to the BSR as PIMv2 C-RP for the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
interface-type interface-number	IP address associated with this interface type and number to be advertised as a C-RP address.
bidir	(Optional) Indicates that the multicast groups specified by the *access-list* argument are to operate in bidirectional mode. If the command is configured without this option, the groups specified will operate in PIM sparse mode.
group-list *access-list*	(Optional) Specifies the standard IP access list number or name that defines the group prefixes that are advertised in association with the RP address. The access list name cannot contain a space or quotation mark, and it must begin with an alphabetic character to avoid confusion with numbered access lists.
interval *seconds*	(Optional) Specifies the C-RP advertisement interval, in seconds. The range is from 1 to 16383. The default value is 60.
priority *value*	(Optional) Specifies the priority of the C-RP. Range is from 0 to 255. The default priority value is 0. The BSR C-RP with the lowest priority value is preferred. **Note** The Cisco IOS and Cisco IOS XE implementation of PIM BSR uses the value 0 as the default priority for candidate RPs. This implementation predates the draft-ietf-pim-sm-bsr IETF draft, the first IETF draft to specify 192 as the default priority value. The Cisco IOS and Cisco IOS XE implementation, thus, deviates from the IETF draft. To comply with the default priority value specified in the draft, you must explicitly set the priority value to 192.

Command Default

The router is not configured to announce itself to the BSR as a PIMv2 C-RP.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3T	This command was introduced.
12.1(2)T	This command was modified. The **bidir** keyword was added.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was implemented on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to configure the router to send PIMv2 messages that advertise itself as a candidate RP to the BSR.

This command should be configured on backbone routers that have good connectivity to all parts of the PIM domain.

The IP address associated with the interface specified for the *interface-type* and *interface-number* arguments will be advertised as the C-RP address.

Note The interface specified for this command must be enabled for Protocol Independent Multicast (PIM) using the **ip pim** command.

If the optional **group-list** keyword and *access-list* argument are configured, the group prefixes defined by the standard IP access list will also be advertised in association with the RP address.

Use this command with the optional **bidir** keyword when you want bidirectional forwarding and you are using the PIM Version 2 BSR mechanism to distribute group-to-RP mappings. Other options are as follows:

- If you are using Auto-RP to distribute group-to-RP mappings, use the **bidir** keyword with the **ip pim send-rp-announce** command.
- If you are not distributing group-to-RP mappings using either Auto-RP or the PIMv2 BSR mechanism, use the **bidir** keyword with the **ip pim rp-address** command.

When the **interval** keyword is specified, the C-RP advertisement interval is set to a value specified by the *seconds* argument. The default interval is 60 seconds. Reducing this interval to a time of less than 60 seconds can reduce the time required to fail over to a secondary RP at the expense of generating more PIMv2 messages.

When the **priority** keyword is specified, the router will announce itself to be a C-RP with the priority specified for the *value* argument. For more information about the BSR selection process, see the **ip pim bsr-candidate** command page.

Examples

The following example shows how to configure the router to advertise itself as a C-RP to the BSR in its PIM domain. The standard access list number 4 specifies the group prefix associated with the RP that has the address identified by Gigabit Ethernet interface 0/0. That RP is responsible for the groups with the prefix 239.

```
ip pim rp-candidate Gigabit Ethernet 0/0 group-list 4
access-list 4 permit 239.0.0.0 0.255.255.255
```

Related Commands

Command	Description
ip pim	Enables PIM on an interface.
ip pim bsr-candidate	Configures the router to announce its candidacy as a BSR.
ip pim rp-address	Configures the address of a PIM RP for a particular group.
ip pim rp-announce-filter	Filters incoming Auto-RP announcement messages coming from the RP.
ip pim send-rp-announce	Uses Auto-RP to configure for which groups the router is willing to act as RP.

ip pim send-rp-announce

To use Auto-RP to configure groups for which the router will act as a rendezvous point (RP), use the **ip pim send-rp-announce** command in global configuration mode. To unconfigure this router as an RP, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **send-rp-announce** {*interface-type interface-number* | *ip-address*} **scope** *ttl-value* [**group-list** *access-list*] [**interval** *seconds*] [**bidir**]

no ip pim [**vrf** *vrf-name*] **send-rp-announce** {*interface-type interface-number* | *ip-address*}

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
interface-type interface-number	Interface type and number that is used to define the RP address. No space is required between the values.
ip-address	IP address of the RP for the group. The IP address must be a directly connected address. If the command is configured with this argument, the RP-announce message will be sourced by the interface to which this IP address is connected (that is, the source address in the IP header of the RP-announce message is the IP address of that interface).
scope *ttl-value*	Specifies the time-to-live (TTL) value that limits the number of Auto-RP announcements.
group-list *access-list*	(Optional) Specifies the standard IP access list number or name that defines the group prefixes that are advertised in association with the RP 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 interval between RP announcements in seconds. The total holdtime of the RP announcements is automatically set to three times the value of the interval. The default interval is 60 seconds.
bidir	(Optional) Indicates that the multicast groups specified by the *access-list* argument are to operate in bidirectional mode. If the command is configured without this keyword, the groups specified will operate in Protocol Independent Multicast sparse mode (PIM-SM).

Defaults

Auto-RP is disabled.
seconds: 60

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.1(2)T	This command was modified. The following keywords and argument were added: • **interval** *seconds* • **bidir**
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.4(5)	This command was modified. The *ip-address* argument was added.
12.3(17)	This command was modified. The *ip-address* argument was added.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRE	This command was modified. The *ip-address* argument was added.

Usage Guidelines

Enter this command on the router that you want to be an RP. When you are using Auto-RP to distribute group-to-RP mappings, this command causes the router to send 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 RP for the groups in the range described by the access list.

Use this command with the **bidir** keyword when you want bidirectional forwarding and you are using Auto-RP to distribute group-to-RP mappings. Other options are as follows:

- If you are using the PIM Version 2 bootstrap router (PIMv2 BSR) mechanism to distribute group-to-RP mappings, use the **bidir** keyword with the **ip pim rp-candidate** command.
- If you are not distributing group-to-RP mappings using either Auto-RP or the PIMv2 BSR mechanism, use the **bidir** keyword with the **ip pim rp-address** command.

Examples

The following example shows how to configure the router to send RP announcements out all Protocol Independent Multicast (PIM)-enabled interfaces for a maximum of 31 hops. The IP address by which the router wants to be identified as RP is the IP address associated with Ethernet interface 0. Access list 5 describes the groups for which this router serves as RP.

```
ip pim send-rp-announce ethernet0 scope 31 group-list 5
access-list 5 permit 224.0.0.0 15.255.255.255
```

Related Commands

Command	Description
access-list (IP standard)	Defines a standard IP access list.

Command	Description
ip pim rp-address	Configures the address of a PIM RP for a particular group.
ip pim rp-candidate	Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR.

ip pim send-rp-discovery

To configure the router to be a rendezvous point (RP) mapping agent, use the **ip pim send-rp-discovery** command in global configuration mode. To deconfigure the router from functioning as the RP mapping agent, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **send-rp-discovery** [*interface-type interface-number*] **scope** *ttl-value* [**interval** *seconds*]

no ip pim [**vrf** *vrf-name*] **send-rp-discovery**

Syntax Description

vrf *vrf-name*	(Optional) Configures the router to be an RP mapping agent for the specified Multicast Virtual Private Network (VPN) routing and forwarding (MVRF) instance.
interface-type interface-number	(Optional) Interface type and number that is to be used as the source address of the RP mapping agent.
scope *ttl-value*	Specifies the time-to-live (TTL) value for Auto-RP discovery messages. The range is from 1 to 255.
interval *seconds*	(Optional) Specifies the interval at which Auto-RP discovery messages are sent. The range is from 1 to 16383. **Note** By default, Auto-RP discovery messages are sent at an interval of 60 seconds or when the RP mapping agent detects changes.

Command Default

The router is not configured to be an RP mapping agent.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(8)	The **interval** keyword and *seconds* argument were added.
12.4(9)T	The **interval** keyword and *seconds* argument were added.
12.2(33)SRB	The **interval** keyword and *seconds* argument were added.
12.2(18)SXF11	The **interval** keyword and *seconds* argument were added.

Usage Guidelines

Use the **ip pim send-rp-discovery** command to configure the router to be an RP mapping agent. An RP mapping agent receives Auto-RP announcement messages, which it stores in its local group-to-RP mapping cache. The RP mapping agent uses the information contained in the Auto-RP announcement messages to elect the RP. The RP mapping agent elects the candidate RP with the highest IP address as the RP for a group range.

The required **scope** keyword and *ttl-value* argument are used to specify the TTL value in the IP header of Auto-RP discovery messages.

Note For the **scope** keyword and *ttl-value* argument, specify a TTL large enough to cover your Protocol Independent Multicast (PIM) domain.

The optional **interval** keyword and *seconds* argument are used to specify the interval at which Auto-RP discovery messages are sent. By default, Auto-RP discovery messages are sent at an interval of 60 seconds or when the RP mapping agent detects changes.

Note Lowering the interval at which Auto-RP discovery messages are sent from the default value of 60 seconds results in more frequent floodings of the group-to-RP mappings. In some network environments, the disadvantages of lowering the interval (more control packet overhead) may outweigh the advantages (more frequent group-to-RP mapping updates).

When Auto-RP is used, the following events occur:

1. The RP mapping agent listens for Auto-RP announcement messages sent by candidate RPs to the well-known group address CISCO-RP-ANNOUNCE (224.0.1.39).
2. The RP mapping agents stores the information learned from Auto-RP announcement messages in its local group-to-RP mapping cache.
3. The RP mapping agents elects the candidate RP with the highest IP address as the RP and announces the RP in the Auto-RP discovery messages that it sends out.
4. The Auto-RP discovery messages that the RP mapping agent sends to the well-known group CISCO-RP-DISCOVERY (224.0.1.40), which Cisco routers join by default, contains the elected RP learned from the RP mapping agent's group-to-RP mapping cache.
5. PIM designated routers listen for the Auto-RP discovery messages sent to 224.0.1.40 to learn the RP and store the information about the RP in their local group-to-RP mapping caches.

Use the **show ip pim rp** command with the **mapping** keyword to display all the group-to-RP mappings that the router has learned from Auto-RP.

Examples

The following example shows how to configure a router to be an RP mapping agent. In this example, the RP mapping agent is configured to use loopback 0 as the source address for Auto-RP messages. The Auto-RP discovery messages sent by the RP mapping agent are configured to be sent out at an interval of 50 seconds with a TTL of 20 hops.

```
ip pim send-rp-discovery loopback 0 scope 20 interval 50
```

Related Commands

Command	Description
show ip pim rp	Displays active RPs that are cached with associated multicast routing entries.

ip pim snooping (global configuration)

To enable Protocol Independent Multicast (PIM) snooping globally, use the **ip pim snooping** command in global configuration mode. To disable PIM snooping globally, use the **no** form of this command.

ip pim snooping

no ip pim snooping

Syntax Description

This command has no arguments or keywords.

Defaults

PIM snooping is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(17a)SX	This command was introduced.
12.2(17d)SXB	This command was implemented on Catalyst 6500 series switches and Cisco 7600 Internet routers with a Supervisor Engine 2.
12.2(18)SXF2	This command was implemented on Catalyst 6500 series switches and Cisco 7600 Internet routers with a Supervisor Engine 32.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

PIM snooping is not supported on groups that use the reserved MAC address range, for example, 0100.5e00.00xx, as an alias.

When you disable PIM snooping globally, PIM snooping is disabled on all VLANs.

Examples

This example shows how to enable PIM snooping globally:

```
ip pim snooping
```

This example shows how to disable PIM snooping globally:

```
no ip pim snooping
```

Related Commands

Command	Description
show ip pim snooping	Displays information about IP PIM snooping.

ip pim snooping (interface configuration)

To enable Protocol Independent Multicast (PIM) snooping on an interface, use the **ip pim snooping** command in interface configuration mode. To disable PIM snooping on an interface, use the **no** form of this command.

ip pim snooping

no ip pim snooping

Syntax Description

This command has no arguments or keywords.

Defaults

PIM snooping is disabled on an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(17a)SX	This command was introduced.
12.2(17d)SXB	This command was implemented on Catalyst 6500 series switches and Cisco 7600 Internet routers with a Supervisor Engine 2.
12.2(18)SXF2	This command was implemented on Catalyst 6500 series switches and Cisco 7600 Internet routers with a Supervisor Engine 32.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

PIM snooping is not supported on groups that use the reserved MAC address range, for example, 0100.5e00.00xx, as an alias.

You must enable PIM snooping globally before enabling PIM snooping on an interface. To enable PIM snooping globally, use the **ip pim snooping** command in global configuration mode. When you disable PIM snooping globally, PIM snooping is disabled on all VLANs.

You can enable PIM snooping on VLAN interfaces only.

Examples

This example shows how to enable PIM snooping on a VLAN interface:

```
interface vlan 101
 ip pim snooping
```

This example shows how to disable PIM snooping on a VLAN interface:

```
interface vlan 101
 no ip pim snooping
```

Related Commands

Command	Description
ip pim snooping (global configuration)	Enables PIM snooping globally.
show ip pim snooping	Displays information about IP PIM snooping.

ip pim snooping dr-flood

To enable flooding of the packets to the designated router, use the **ip pim snooping dr-flood** command in global configuration mode. To disable the flooding of the packets to the designated router, use the **no** form of this command.

ip pim snooping dr-flood

no ip pim snooping dr-flood

Syntax Description

This command has no arguments or keywords.

Defaults

The flooding of packets to the designated router is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXF	This command was introduced.
12.2(18)SXF2	This command implemented on Catalyst 6500 series switches and Cisco 7600 Internet routers with a Supervisor Engine 2 or Supervisor Engine 32.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

PIM snooping is not supported on groups that use the reserved MAC address range, for example, 0100.5e00.00xx, as an alias.

Enter the **no ip pim snooping dr-flood** command only on switches that have no designated routers attached.

The designated router is programmed automatically in the (S,G) O-list.

Examples

The following example shows how to enable flooding of the packets to the designated router:

```
ip pim snooping dr-flood
```

The following example shows how to disable flooding of the packets to the designated router:

```
no ip pim snooping dr-flood
```

Related Commands

Command	Description
show ip pim snooping	Displays information about IP PIM snooping.

ip pim snooping suppress sgr-prune

To enable suppression of SGR-prune packets to the designated router, use the **ip pim snooping suppress sgr-prune** command in global configuration mode. To disable the suppression of the packets to the designated router, use the **no** form of this command.

ip pim snooping suppress sgr-prune

no ip pim snooping suppress sgr-prune

Syntax Description

This command has no arguments or keywords.

Command Default

The suppression of packets to the designated router is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)ZY	This command was introduced.
12.2(18)SXF	This command was introduced.

Usage Guidelines

If a shared tree and SPT diverge in a VLAN on your switch router, and you have PIM snooping configured, then duplicate multicast packets may be delivered in your network. PIM snooping may stop the prune message sent by the receiver from reaching the upstream switch router in the shared tree, which causes more than one upstream switch router to forward the multicast traffic. This situation causes duplicate multicast packets to be delivered to the receivers. The sending of duplicate multicast packets only lasts a couple of seconds because the PIM-ASSERT mechanism is initiated and stops the extraneous flow. However, the cycle repeats itself when the next prune message is sent. To stop this situation from occurring, enter the **no ip pim snooping suppress sgr-prune** command.

Examples

The following example shows how to enable suppression of the SGR-prune packets to the designated router:

```
Router(config)# ip pim snooping suppress sgr-prune
```

Related Commands

Command	Description
show ip pim snooping	Displays information about IP PIM snooping.

ip pim sparse sg-expiry-timer

To adjust the (S, G) expiry timer interval for Protocol Independent Multicast sparse mode (PIM-SM) (S, G) multicast routes (mroutes), use the **ip pim sparse sg-expiry-timer** command in global configuration mode. To restore the default setting with respect to this command, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **sparse sg-expiry-timer** *seconds* [**sg-list** *access-list*]

no ip pim [**vrf** *vrf-name*] **sparse sg-expiry-timer**

Syntax Description

vrf *vrf-name*	(Optional) Configures the expiry timer for PIM-SM (S, G) mroute entries associated with the Multicast Virtual Private Network (VPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
seconds	Duration of the expiry timer interval, in seconds. The range is from 181 (3 minutes 1 second) to 57600 (16 hours).
sg-list *access-list*	(Optional) Specifies that the time value for the expiry timer be applied only to the (S, G) mroute entries that match the extended access list specified for the *access-list* argument.

Command Default

The expiry timer interval for PIM-SM (S, G) mroute entries is set to 180 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXE5	This command was introduced.
12.2(18)SXF4	This command was integrated into Cisco IOS Release 12.2(18)SXF4.
12.2(35)SE	This command was integrated into Cisco IOS Release 12.2(35)SE.
12.2(25)SEE2	This command was integrated into Cisco IOS Release 12.2(25)SEE2.
15.0(1)M	This command was integrated into a release before Cisco IOS Release 15.0(1)M

Usage Guidelines

Use the **ip pim sparse sg-expire-timer** command to adjust the expiry timer interval for PIM-SM (S, G) mroute entries to a time value greater than the default expiry timer interval of 180 seconds. This command can be used to lock down the shortest-path tree (SPT) for intermittent sources in PIM-SM network environments, such as sources in trading floor environments that sporadically send financial data streams to multicast groups during trading floor hours.

When a source stops sending traffic to a multicast group, the corresponding (S, G) mroute entry eventually times out and the (S, G) entry is removed. When the source resumes sending traffic to the group, the (S, G) entry is rebuilt. During the short time interval before the (S, G) entry is rebuilt, the traffic is forwarded on the (*, G) forwarding entry. There is a small window of time before the (S, G)

entry is completely built in which packets may be dropped. The **ip pim sparse sg-expiry-timer** command can be used to maintain the (S, G) entry so that it will not be removed and the stream will not potentially suffer packet loss.

Note The **ip pim sparse sg-expire-timer** command only applies to PIM-SM (S, G) mroute entries and, thus, does not apply to PIM-SM (*, G) mroute entries.

Examples

The following example shows how to adjust the expiry timer interval to 36000 seconds (10 hours) for PIM-SM (S, G) entries that match the extended access list named test_acl.

```
ip pim sparse sg-expiry-timer 36000 sg-list test_acl
!
ip access-list extended test-acl
 permit ip any host 234.1.1.1
```

ip pim spt-threshold

Command	Description
ip pim spt-threshold	Configures when a PIM leaf router should join the shortest path source tree for the specified group.

To configure when a Protocol Independent Multicast (PIM) leaf router should join the shortest path source tree for the specified group, use the **ip pim spt-threshold** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **spt-threshold** {*kbps* | **infinity**} [**group-list** *access-list*]

no ip pim [**vrf** *vrf-name*] **spt-threshold** {*kbps* | **infinity**} [**group-list** *access-list*]

Cisco IOS T-Train Release

ip pim [**vrf** *vrf-name*] **spt-threshold** {**0** | **infinity**} [**group-list** *access-list*]

no ip pim [**vrf** *vrf-name*] **spt-threshold** {**0** | **infinity**} [**group-list** *access-list*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
kbps	Traffic rate; valid values are from 0 to 4294967 kbps.
infinity	Causes all sources for the specified group to use the shared tree.
group-list *access-list*	(Optional) Specifies the groups to which the threshold applies. Must be an IP standard access list number or name. If the value is 0, the threshold applies to all groups.
0	Specifies to always switch to the source tree.

Defaults

When this command is not used, the PIM leaf router joins the shortest path tree immediately after the first packet arrives from a new source.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If a source sends at a rate greater than or equal to traffic rate (the *kbps* value), a PIM join message is triggered toward the source to construct a source tree.

If the **infinity** keyword is specified, all sources for the specified group will use the shared tree. Specifying a **group-list** *access-list* indicates the groups to which the threshold applies.

If the traffic rate from the source drops below the threshold traffic rate, the leaf router will switch back to the shared tree and send a prune message toward the source.

Examples

The following example shows how to set a threshold of 4 kbps. If the traffic rate exceeds this threshold, the traffic to a group from a source causes the router to switch to the shortest path tree to that source.

```
Router# configure terminal
Router(config)# ip pim spt-threshold 4
```

Related Commands

Command	Description
ip pim bidir-neighbor-filter	Configures an ACL to specify which bidirectionally capable neighbors will participate in the designated forwarder election.

ip pim ssm

To define the Source Specific Multicast (SSM) range of IP multicast addresses, use the **ip pim ssm** command in global configuration mode. To disable the SSM range, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **ssm** {**default** | **range** *access-list*}

no ip pim [**vrf** *vrf-name*] **ssm** {**default** | **range** *access-list*}

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
default	Defines the SSM range access list to 232/8.
range *access-list*	Specifies the standard IP access list number or name defining the SSM range.

Defaults

The command is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When an SSM range of IP multicast addresses is defined by the **ip pim ssm** command, no Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages will be accepted or originated in the SSM range.

Examples

The following example shows how to configure SSM service for the IP address range defined by access list 4:

```
access-list 4 permit 224.2.151.141
ip pim ssm range 4
```

Related Commands

Command	Description
ip igmp v3lite	Enables the acceptance and processing of IGMP v3lite membership reports on an interface.
ip urd	Enables interception of TCP packets sent to the reserved URD port 659 on an interface and processing of URD channel subscription reports.

ip pim state-refresh disable

To disable the processing and forwarding of PIM dense mode state refresh control messages on a Protocol Independent Multicast (PIM) router, use the **ip pim state-refresh disable** command in global configuration mode. To reenable the processing and forwarding of PIM dense mode state refresh control messages, use the **no** form of this command.

ip pim [**vrf** *vrf-name*] **state-refresh disable**

no ip pim [**vrf** *vrf-name*] **state-refresh disable**

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Defaults

The processing and forwarding of PIM dense mode state refresh control messages is enabled on PIM routers that are running a Cisco IOS software release that supports the PIM dense mode state refresh feature.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Configuring this command removes PIM dense mode state refresh information from PIM hello messages.

Examples

The following example shows how to disable the periodic forwarding of the PIM dense mode state refresh control message down a source-based IP multicast distribution tree:

```
ip pim state-refresh disable
```

Related Commands

Command	Description
ip pim state-refresh origination-interval	Configures the origination of and the interval for the PIM dense mode state refresh control messages on a PIM router.
show ip pim interface	Displays information about interfaces configured for PIM.
show ip pim neighbor	Lists the PIM neighbors discovered by the Cisco IOS software.

ip pim state-refresh origination-interval

To configure the origination of and the interval for PIM dense mode state refresh control messages on a Protocol Independent Multicast (PIM) router, use the **ip pim state-refresh origination-interval** command in interface configuration mode. To stop the origination of the PIM dense mode state refresh control message, use the **no** form of this command.

ip pim state-refresh origination-interval [*interval*]

no ip pim state-refresh origination-interval [*interval*]

Syntax Description

interval	(Optional) The number of seconds between PIM dense mode state refresh control messages. The default is 60 seconds. The available interval range is from 4 to 100 seconds.

Defaults

PIM dense mode state refresh control message origination is disabled. By default, all PIM routers that are running a Cisco IOS software release that supports PIM dense mode state refresh process and forward PIM dense mode state refresh control messages.

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

Configure this command on the interfaces of the first hop, PIM dense mode routers that are directly connected to sources for PIM-DM multicast groups.

By default, the processing and forwarding of PIM dense mode state refresh control messages is enabled on PIM routers that are running a Cisco IOS software release that supports PIM dense mode state refresh.

Examples

The following example configures the origination of the state refresh control message on Ethernet interface 0 of a PIM dense mode router with an interval of 80 seconds:

```
interface ethernet 0
 ip pim state-refresh origination-interval 80
```

Related Commands

Command	Description
ip pim state-refresh disable	Disables the processing and forwarding of PIM dense mode state refresh feature control messages on a PIM router.
show ip pim interface	Displays information about interfaces configured for PIM.
show ip pim neighbor	Lists the PIM neighbors discovered by the Cisco IOS software.

ip pim v1-rp-reachability

To send Protocol Independent Multicast version 1 (PIMv1) rendezvous point (RP) reachability packets, use the **ip pim v1-rp-reachability** command in global configuration mode. To stop the packets, use the **no** form of this command.

ip pim v1-rp-reachability

no ip pim v1-rp-reachability

Syntax Description

This command has no arguments or keywords.

Command Default

The command is enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example shows how to set the PIMV1 RP reachability packets:

```
Router# configure terminal
Router(config)# ip pim v1-rp-reachability
```

Related Commands

Command	Description
ip pim bidir-neighbor-filter	Configures an ACL to specify which bidirectionally capable neighbors will participate in the designated forwarder election.

ip pim vc-count

To change the maximum number of virtual circuits (VCs) that Protocol Independent Multicast (PIM) can open, use the **ip pim vc-count** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip pim vc-count *number*

no ip pim vc-count

Syntax Description

number	Maximum number of VCs that PIM can open. The default is 200 VCs. The range is from 1 to 65535.

Defaults

200 VCs per ATM interface or subinterface

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example allows PIM to open a maximum of 250 VCs:

```
ip pim vc-count 250
```

Related Commands

Command	Description
ip pim minimum-vc-rate	Configures the minimum traffic rate to keep VCs from being idled.
ip pim multipoint-signalling	Enables PIM to open ATM multipoint switched VCs for each multicast group that a receiver joins.
ip pim	Enables PIM on an interface.
show ip pim vc	Displays ATM VCs status information for multipoint VCs opened by PIM.

ip pim version

To configure the Protocol Independent Multicast (PIM) version of the interface, use the **ip pim version** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip pim version [**1** | **2**]

no ip pim version

Syntax Description

1	(Optional) Configures PIM Version 1.
2	(Optional) Configures PIM Version 2.

Defaults

Version 2

Command Modes

Interface configuration (config-if)
Virtual network interface (config-if-vnet)

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.2S	This command was modified. Support was added for this command in virtual network interface configuration mode.

Usage Guidelines

An interface in Version 2 mode automatically downgrades to Version 1 mode if that interface has a PIM Version 1 neighbor. The interface returns to Version 2 mode after all Version 1 neighbors disappear (that is, they are shut down or upgraded).

Examples

The following example configures the interface to operate in PIM Version 1 mode:

```
interface ethernet 0
 ip address 10.0.0.0 255.0.0.0
 ip pim sparse-dense-mode
 ip pim version 1
```

ip rgmp

To enable the Router-Port Group Management Protocol (RGMP) on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces, use the **ip rgmp** command in interface configuration mode. To disable RGMP on the interfaces, use the **no** form of this command.

ip rgmp

no ip rgmp

Syntax Description

This command has no arguments or keywords.

Defaults

RGMP is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(10)S	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

RGMP is supported only on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces.

Before you enable RGMP, the following features must be enabled on your router:

- IP routing
- IP multicast
- PIM in sparse mode, sparse-dense mode, source specific mode, or bidirectional mode

If your router is in a bidirectional group, make sure to enable RGMP only on interfaces that do not function as a designated forwarder (DF). If you enable RGMP on an interface that functions as a DF, the interface will not forward multicast packets up the bidirectional shared tree to the rendezvous point (RP).

The following features must be enabled on your switch:

- IP multicast
- IGMP snooping

Examples

The following example enables RGMP on Ethernet interface 1/0:

```
interface ethernet 1/0
 ip rgmp
```

Related Commands

Command	Description
debug ip rgmp	Logs debug messages sent by an RGMP-enabled router.
show ip igmp interface	Displays multicast-related information about an interface.

ip sap cache-timeout

To limit how long a Session Announcement Protocol (SAP) cache entry stays active in the cache, use the **ip sap cache-timeout** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip sap cache-timeout *minutes*

no ip sap cache-timeout

Syntax Description

minutes	Time (in minutes) that a SAP cache entry is active in the cache.

Defaults

By default, session announcements remain for 1440 minutes (24 hours) in the cache.

Command Modes

Global configuration

Command History

Release	Modification
11.2	The **ip sdr cache-timeout** command was introduced.
12.2	The **ip sdr cache-timeout** command was replaced by the **ip sap cache-timeout** command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This 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.

Examples

The following example causes SAP cache entries to remain in the cache for 30 minutes:

```
ip sap cache-timeout 30
```

Related Commands

Command	Description
clear ip sap	Deletes a SAP cache entry or the entire SAP cache.
show ip sap	Displays the SAP cache.

ip sap listen

To enable the Cisco IOS software to listen to session directory announcements, use the **ip sap listen** command in interface configuration mode. To disable the function, use the **no** form of this command.

ip sap listen

no ip sap listen

Syntax Description

This command has no arguments or keywords.

Defaults

The command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	The **ip sdr listen** command was introduced.
12.2	The **ip sdr listen** command was replaced by the **ip sap listen** command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Cisco IOS software can receive and store Session Description Protocol (SDP) and Session Announcement Protocol (SAP) session announcements. When the **ip sap listen** command is configured on an interface, the well-known session directory groups on that interface can receive and store session announcements. The announcements can be displayed with the **show ip sap** command. The **ip multicast rate-limit** command uses stored session announcements. To configure the period of time after which received announcements will expire, use the **ip sap cache-timeout** command.

When the **no ip multicast routing** command is configured, announcements are only stored if they are received on an interface configured with the **ip sap listen** command. When a system is configured as a multicast router, it is sufficient to configure the **ip sap listen** command on only a single multicast-enabled interface. The well-known session directory groups are handled as local joined groups after the **ip sap listen** command is first configured (see the L flag of the **show ip mroute** command). This configuration causes announcements received from all multicast-enabled interfaces to be routed and stored within the system.

Examples

The following example shows how to enable a router to listen to session directory announcements:

```
ip routing
interface loopback 0
 ip address 10.0.0.51 255.255.255.0
 ip pim sparse-dense mode
 ip sap listen
```

Related Commands

Command	Description
clear ip sap	Deletes a SAP cache entry or the entire SAP cache.
ip multicast rate-limit	Controls the rate a sender from the source list can send to a multicast group in the group list.
ip multicast-routing	Enables IP multicast routing or multicast distributed switching.
ip sap cache-timeout	Limits how long a SAP cache entry stays active in the cache.
show ip mroute	Displays the contents of the IP mroute routing table.
show ip sap	Displays the SAP cache.

ip sdr cache-timeout

The **ip sdr cache-timeout** command is replaced by the **ip sap cache-timeout** command. See the description of the **ip sap cache-timeout** command for more information.

ip sdr listen

The **ip sdr listen** command is replaced by the **ip sap listen** command. See the description of the **ip sap listen** command for more information.

ip service reflect

To match and rewrite multicast packets routed onto a Vif1 interface, use the **ip service reflect** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ip service reflect *input-interface* **destination** *destination-address* **to** *new-destination-address* **mask-len** *number* **source** *new-source-address*

no ip service reflect *input-interface* **destination** *destination-address* **to** *new-destination-address* **mask-len** *number* **source** *new-source-address*

Syntax Description

input-interface	Interface type and number.
destination	Identifies packets with the specified destination address.
destination-address	Destination IP address in the packets, in A.B.C.D format.
to	Modifies the destination IP address in reflected packets to a new IP address.
new-destination-address	New destination address to be used, in A.B.C.D format.
mask-len *number*	Specifies the mask length of the destination address to match. The *number* argument is a value from 0 to 32.
source	Modifies the source address in reflected packets.The source address must be on the same subnet as the Vif1 interface.
new-source-address	New source address to be used, in A.B.C.D format.

Command Default

The multicast service reflection feature is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Use the **ip service reflect** command to match and rewrite multicast packets routed onto a Vif1 interface.

The matched and rewritten packet is sent back into Cisco multicast packet routing, where it is handled like any other packet arriving from an interface.

More than one multicast service reflection operation can be configured to match the same packet, allowing you to replicate the same received traffic to multiple destination addresses.

Examples

The following example shows how to translate any multicast packet with a destination address of 239.1.1.0/24 to a destination of 239.2.2.0/24 with a new source address of 10.1.1.2. For example, a packet with a source and destination of (10.10.10.10, 239.1.1.15) would be translated to (10.1.1.2, 239.2.2.15).

```
Router(config)# interface Vif1
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# ip pim sparse-mode
Router(config-if)# ip service reflect Ethernet 0/0 destination 239.1.1.0 to 239.2.2.0
mask-len 24 source 10.1.1.2
Router(config-if)# ip igmp static-group 239.1.1.0
Router(config-if)# ip igmp static-group 239.1.1.1
```

ip urd

To enable interception of TCP packets sent to the reserved URL Rendezvous Directory (URD) port 465 on an interface and processing of URD channel subscription reports, use the **ip urd** command in interface configuration mode. To disable URD on an interface, use the **no** form of this command.

ip urd [**proxy**]

no ip urd [**proxy**]

Syntax Description

proxy	(Optional) Allows an interface to accept URL requests from any TCP connection sent to that interface. If the **proxy** keyword is not configured, the interface will accept URL requests from TCP connections only if the requests originated from directly connected hosts. The **proxy** option must be enabled on an interface if it is unnumbered or if it has downstream routers configured with Internet Group Management Protocol (IGMP) proxy routing. To prevent users on the backbone from creating URD state on your router, do not enable the **proxy** option on a backbone interface of your router.

Defaults

The command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To use this command, you must first define a Source Specific Multicast (SSM) range of IP addresses using the **ip pim ssm** global configuration command. When URD is enabled, it is supported in the SSM range of addresses only. We recommend that you not enable URD on backbone interfaces, but only on interfaces connecting to hosts.

URD functionality is available for multicast process switching, fast switching, and distributed fast-switching paths.

Examples

The following example shows how to configure URD on Ethernet interface 3/3:

```
interface ethernet 3/3
 ip urd
```

Related Commands

Command	Description
ip pim ssm	Defines the SSM range of IP multicast addresses.

manager

To specify the interface that is to act as the Manager for Multicast Routing Monitor (MRM), and to specify the multicast group address the Test Receiver will listen to, use the **manager** command in MRM manager configuration mode. To remove the Manager or group address, use the **no** form of this command.

manager *interface-type interface-number* **group** *ip-address*

no manager *interface-type interface-number* **group** *ip-address*

Syntax Description

interface-type interface-number	Interface type and number of the Manager. The IP address associated with this interface is the source address of the Manager.
group *ip-address*	Specifies the IP multicast group address that the Test Receiver will listen to.

Command Default

There is no MRM Manager configured.

Command Modes

MRM manager configuration (config-mrm-manager)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command identifies the interface that acts as the Manager, and therefore is required in order to run MRM.

Examples

The following example shows how to configure Ethernet interface 0 as the Manager and the Test Receiver to listen to multicast group 239.1.1.1:

```
ip mrm manager test1
 manager ethernet 0 group 239.1.1.1
```

Related Commands

Command	Description
beacon (multicast routing monitor)	Changes the frequency, duration, or scope of beacon messages that the Manager sends to Test Senders and Test Receivers during an MRM test.
ip mrm accept-manager	Configures a Test Sender or Test Receiver to accept requests only from Managers that pass an access list.
show ip mrm manager	Displays test information for MRM.

mdt data

To specify a range of addresses to be used in the data multicast distribution tree (MDT) pool, use the **mdt data** command in VRF configuration or VRF address family configuration mode. To disable this function, use the **no** form of this command.

mdt data {*group-address-range wildcard-bits* [**threshold** *kb/s*] [**list** *access-list*] | **mpls mldp** *number-of-data-mdts*}

no mdt data {*group-address-range wildcard-bits* [**threshold** *kb/s*] [**list** *access-list*] | **mpls mldp** *number-of-data-mdts*}

Syntax Description

group-address-range	Multicast group address range. The range is from 224.0.0.1 to 239.255.255.255.
wildcard-bits	Wildcard bits to be applied to the multicast group address range.
threshold *kb/s*	(Optional) Defines the bandwidth threshold value in kilobits per second (kb/s). The range is from 1 to 4294967.
list *access-list*	(Optional) Limits the creation of the data MDT to the particular (S,G) Multicast Virtual Private Network (MVPN) entries defined in the access list specified for the *access-list* argument.
mpls mldp *number-of-data-mdts*	Specifies the number of data MDTs created using Multicast Label Distribution Protocol (MLDP) Label Switched Path (LSP).

Command Default

A data MDT pool is not configured.

Command Modes

VRF address family configuration (config-vrf-af)
VRF configuration (config-vrf)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was added on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
15.0(1)S	This command was modified. The keywords **mpls mldp** were added.

Usage Guidelines

A data MDT can include a maximum of 256 multicast groups per MVPN. Multicast groups used to create the data MDT are dynamically chosen from a pool of configured IP addresses.

Use the **mdt data** command to specify a range of addresses to be used in the data MDT pool. Because these are multicast group addresses (Class D addresses), there is no concept of a subnet; therefore, you can use all addresses in the mask (wildcard) range. The threshold is specified in kb/s. Using the optional **list** keyword and *access-list* argument, you can define the (S, G) MVPN entries to be used in a data MDT pool, which would further limit the creation of a data MDT pool to the particular (S, G) MVPN entries defined in the access list specified for the *access-list* argument.

You can access the **mdt data** command by using the **ip vrf** global configuration command. You can also access the **mdt data** command by using the **vrf definition** global configuration command followed by the **address-family ipv4** VRF configuration command.

Examples

The following example shows how to configure the range of group addresses for the MDT data pool. In this example, the mask 0.0.0.15 allows the range 239.192.20.32 to 239.192.20.47 to be used as the address pool. In addition, a threshold of 1 kb/s has been set, which means that if a multicast stream exceeds 1 kb/s, then a data MDT is created.

```
ip vrf vrf1
 rd 10:27
 route-target export 10:27
 route-target import 10:27
 mdt default 232.0.0.1
 mdt data 232.0.1.0 0.0.0.255 threshold 500 list 101
!
.
.
.
!
ip pim ssm default
ip pim vrf vrf1 accept-rp auto-rp
!
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address family configuration mode.
mdt default	Configures a default MDT group for a VPN VRF.
mdt preference	Specifies a preference for a particular MDT type.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

mdt default

To configure a default multicast distribution tree (MDT) group for a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **mdt default** command in VRF configuration or VRF address family configuration mode. To disable this function, use the **no** form of this command.

mdt default {*group-address* | **mpls mldp** *root-address*}

no mdt default {*group-address* | **mpls mldp** *root-address*}

Syntax Description

group-address	IP address of the default MDT group. This address serves as an identifier for the community in that provider edge (PE) routers configured with the same group address become members of the group, allowing them to receive packets sent by each other.
mpls mldp *root-address*	Specifies the multipoint-to-multipoint (MP2MP) Label Switched Path (LSP) root address of the default MDT group, which was created using Multicast Label Distribution Protocol (MLDP) LSP.

Defaults

The command is disabled.

Command Modes

VRF address family configuration (config-vrf-af)
VRF configuration (config-vrf)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
15.0(1)S	This command was modified. The **mpls mldp** keywords were added.

Usage Guidelines

The default MDT group must be the same group configured on all PE routers that belong to the same VPN.

If Source Specific Multicast (SSM) is used as the protocol for the default MDT, the source IP address will be the address used to source the Border Gateway Protocol (BGP) sessions.

A tunnel interface is created as a result of this command. By default, the destination address of the tunnel header is the *group-address* argument.

You can access the **mdt default** command by using the **ip vrf** global configuration command. You can also access the **mdt default** command by using the **vrf definition** global configuration command followed by the **address-family ipv4** VRF configuration command.

Examples

In the following example, Protocol Independent Multicast (PIM) SSM is configured in the backbone. Therefore, the default and data MDT groups are configured within the SSM range of IP addresses. Inside the VPN, PIM sparse mode (PIM-SM) is configured and only Auto-RP announcements are accepted.

```
!
ip vrf vrf1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 mdt default 232.0.0.1
 mdt data 232.0.1.0 0.0.0.255 threshold 500 list 101
!
.
.
.
!
ip pim ssm default
ip pim vrf vrf1 accept-rp auto-rp
!
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address family configuration mode.
mdt data	Configures the multicast group address range for data MDT groups.
mdt preference	Specifies a preference for a particular MDT type.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

mdt log-reuse

To enable the recording of data multicast distribution tree (MDT) reuse, use the **mdt log-reuse** command in VRF configuration mode. To disable this function, use the **no** form of this command.

mdt log-reuse

no mdt log-reuse

Syntax Description

This command has no arguments or keywords.

Defaults

The command is disabled.

Command Modes

VRF configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **mdt log-reuse** command generates a syslog message whenever a data MDT is reused.

Examples

The following example shows how to enable MDT log reuse:

```
mdt log-reuse
```

Related Commands

Command	Description
mdt data	Configures the multicast group address range for data MDT groups.
mdt default	Configures a default MDT group for a VPN VRF.

mdt preference

To specify a preference for a particular multicast distribution tree (MDT) type, use the **mdt preference** command in VRF configuration or VRF address family configuration mode. To disable this function, use the **no** form of this command.

mdt preference {**mldp** | **pim**}

no mdt preference {**mldp** | **pim**}

Syntax Description

mldp	Specifies the creation of MDTs using Multicast Label Distribution Protocol (MLDP).
pim	Specifies the creation of MDTs using Protocol Independent Multicast (PIM).

Command Default

MDTs are created using PIM.

Command Modes

VRF address family configuration (config-vrf-af)
VRF configuration (config-vrf)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

In order to support the Multicast Virtual Private Network (MVPN) migration strategy, MLDP MDTs can be configured in conjunction with PIM MDTs. In order to influence the path selection in the mroute table, this command can be used to specify a preference for a certain tree type. If the command is not configured, PIM is preferred to MLDP. The order in which the keywords **pim** and **mldp** are entered gives the preference. The keyword entered first has the higher preference.

You can also access the **mdt preference** command by using the **vrf definition** global configuration command followed by the **address-family ipv4** VRF configuration command.

Examples

The following example shows how to specify the creation of MDTs using MLDP:

```
ip vrf vrf1
 mdt preference mldp
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address family configuration mode.
mdt data	Configures the multicast group address range for data MDT groups.

Command	Description
mdt default	Configures a default MDT group for a VPN VRF.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

mls ip multicast (global configuration)

Note Effective with Cisco IOS Release 12.2(33)SRE, the **mls ip multicast(global configuration)** command is not available in Cisco IOS software.

To enable MLS IP and configure the hardware switching globally, use the **mls ip multicast** command in global configuration mode. To disable MLS IP, use the **no** form of this command.

mls ip multicast [**capability**]

mls ip multicast [**vrf** *name*] [**connected | egress local | mfd | refresh-state | shared-tree-mfd | syslog | threshold** *ppsec*]

no mls ip multicast [**vrf**]

Syntax Description

capability	(Optional) Exports the information about the egress capability from the switch processor to the route processor.
vrf *name*	(Optional) Specifies the VRF name.
connected	(Optional) Installs the interface/mask entries for bridging directly connected sources to the internal router.
egress local	(Optional) Populates the multicast expansion table with local Layer 3-routed interfaces.
mfd	(Optional) Enables complete hardware switching.
refresh-state	(Optional) Refreshes the expiration time of the (S,G) entry or the (*,G) entry with NULL OIF.
shared-tree-mfd	(Optional) Enables the complete shortcut for (*,G) flows.
syslog	(Optional) Enables the display of multicast related syslog messages on console.
threshold *ppsec*	(Optional) Sets the minimum traffic rate; below this rate, the flow is software-switched instead of hardware-switched. Valid values are from 10 to 10000 seconds.

Defaults

The defaults are as follows:

- Multicast is disabled.
- Hardware switching is allowed for all eligible multicast routes.
- **connected** is enabled.
- **egress local** is disabled.
- **mfd** is enabled.
- **refresh-state** is enabled.
- **shared-tree-mfd** is enabled.
- **syslog** is disabled.

Command Modes Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command was changed to include the **capability** keyword.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXF	This command was changed to include the **egress local** keywords.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	Support for the syslog feature was added.
12.2(33)SRE	This command was removed.

Usage Guidelines

Note After you enter the **mls ip multicast egress local** command, you must perform a system reset for the configuration to take effect.

Egress multicast replication is not supported on systems that are configured with a Supervisor Engine 32.

When entering the **mls ip multicast egress local** command, ensure that IPv6 multicast is not enabled. Since the egress multicast replication performance enhancement feature cannot separately turn on or turn off IPv4 and IPv6, you cannot have IPv4 and IPv6 multicast enabled when this feature is turned on.

These optional keywords are supported only on systems that are configured with a Supervisor Engine 720 with a PFC3:

- **threshold**
- **connected**
- **refresh-state**
- **shared-tree-mfd**
- **mfd**

The **threshold** *ppsec* optional keyword and argument do not impact flows that are already populated in the hardware cache.

The expiration time refresh is updated when flow statistics are received (indicating that the traffic is received from the RPF interface).

Examples This example shows how to enable the MLS IP shortcuts:

```
Router(config)# mls ip multicast
```

This example shows how to enable the hardware switching on a specific multicast route:

```
Router(config)# mls ip multicast vrf test1
```

This example shows how to export the information about egress capability from the switch processor to the route processor:

```
Router(config)# mls ip multicast capability
```

This example shows how to populate the multicast expansion table with local Layer 3-routed interfaces:

```
Router(config)# mls ip multicast egress local
```

Related Commands

Command	Description
mls rp ip (global configuration mode)	Enables external systems to establish IP shortcuts to the MSFC.
show mls ip multicast	Displays the MLS IP information.

mls ip multicast (interface configuration)

To enable MLS IP shortcuts on the interface, use the **mls ip multicast** command in interface configuration mode. To disable MLS IP shortcuts on the interface, use the **no** form of this command.

mls ip multicast

no mls ip multicast

Syntax Description

This command has no arguments or keywords.

Defaults

Multicast is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to enable the MLS IP shortcuts:

```
Router(config-if)# mls ip multicast
```

Related Commands

Command	Description
show mls ip multicast	Displays the MLS IP information.

mls ip multicast bidir gm-scan-interval

To set the RPF scan interval for the Bidir rendevous point, use the **mls ip multicast bidir gm-scan-interval** command in global configuration mode. To disable the RPF scan interval for the Bidir rendevous point, use the **no** form of this command.

mls ip multicast bidir gm-scan-interval *interval*

no mls ip multicast bidir gm-scan-interval

Syntax Description

interval	RPF scan interval for the Bidir rendevous point; valid values are from 1 to 1000 seconds.

Defaults

10 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

When you set the RPF scan interval for the Bidir rendevous point, you set the time that the periodic scan timer updates the RPF in the DF table for all Bidir rendevous points in the hardware.

Examples

This example shows how to set the RPF scan interval for the Bidir rendevous point:

```
Router(config)# mls ip multicast bidir gm-scan-interval 30
```

Related Commands

Command	Description
show mls ip multicast bidir	Displays the Bidir hardware-switched entries.

mls ip multicast connected

To enable the downloading of directly connected subnets globally, use the **mls ip multicast connected** command in global configuration mode. To disable the downloading of directly connected subnets globally, use the **no** form of this command.

mls ip multicast connected

no mls ip multicast connected

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Do not create directly connected subnets for the following cases:

- To make more room available in the FIB TCAM
- The switch is the first-hop router for a source
- The entries are for Bidir, SSM, and DM mode groups

In these cases, if you enable the downloading of directly connected subnets, the directly connected source hits the MMLS (*,G) entry and is switched using the MMLS (*,G) entry. The registers are not sent to the route processor (in the case of PIM-SM), and the (S,G) state is not created on the first hop (in the case of PIM-DM).

The subnet entry is installed in the TCAM entries with a shorter mask to catch directly connected sources before they hit such entries. You can punt traffic from directly connected sources to the MSFC. Once the MSFC sees this traffic, it can install an MMLS (S,G) entry for this source, which gets installed before the subnet entry in the TCAM. New packets from this source are now switched with the (S,G) entry.

Examples

This example shows how to enable the downloading of directly connected subnets:

```
Router(config)# mls ip multicast connected
```

Related Commands

Command	Description
mls ip multicast (global configuration)	Enables MLS IP and configures the hardware switching globally.
show mls ip multicast	Displays the MLS IP information.

mls ip multicast consistency-check

To enable and configure the hardware-shortcut consistency checker, use the **mls ip multicast consistency-check** command in global configuration mode. To disable the consistency checkers, use the **no** form of this command.

mls ip multicast consistency-check [auto-repair | error-message | **settle-time** *seconds* | **type** [**rp-sp** [**table** | **vrf**] | **scan-mroute** [**count** *count-number*] | **settle-time** *seconds* | **period** *seconds*]

no mls ip multicast consistency-check

Syntax Description

auto-repair	(Optional) Specifies the automatic repair for the consistency checker.
error-message	(Optional) Specifies the error message for the consistency checker.
settle-time *seconds*	(Optional) Specifies the settle time for the consistency checker; valid values are from 2 to 3600 seconds.
type rp-sp	(Optional) Specifies the type of consistency check as a MLSM route switch processor.
table	(Optional) Specifies the VRF multicast table to check. Valid values are 0 to 65535.
vrf	(Optional) Specifies the VPN routing/forwarding instance to check.
type scan-mroute	(Optional) Specifies the type of consistency check as a scan check of the mroute table.
count *count-number*	(Optional) Specifies the maximum number of prefixes to check per scan; valid values are from 2 to 500.
period *seconds*	(Optional) Specifies the period between scans; valid values are from 2 to 3600 seconds.

Defaults

The defaults are as follows:

- Consistency check is enabled.
- **count** *count-number* is 20.
- **period** *seconds* is 2 seconds.
- **settle-time** *seconds* is 60 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The consistency checker scans the mroute table and assures that the multicast-hardware entries are consistent with the mroute table. Whenever an inconsistency is detected, the inconsistency is automatically corrected.

To display the inconsistency error, use the **show mls ip multicast consistency-check** command.

Examples

This example shows how to enable the hardware-shortcut consistency checker:

```
Router(config)# mls ip multicast consistency-check
```

This example shows how to enable the hardware-shortcut consistency checker and configure the scan check of the mroute table:

```
Router(config)# mls ip multicast consistency-check type scan-mroute count 20 period 35
```

This example shows how to enable the hardware-shortcut consistency checker and specify the period between scans:

```
Router(config)# mls ip multicast consistency-check type scan-mroute period 35
```

Related Commands

Command	Description
show mls ip multicast consistency-check	Displays the MLS IP information.

mls ip multicast flow-stat-timer

To set the time interval between two consecutive batches of flow-statistics messages from the switch processor to the route processor, use the **mls ip multicast flow-stat-timer** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mls ip multicast flow-stat-timer *num*

no mls ip multicast flow-stat-timer

Syntax Description

num	Time interval between two consecutive batches of flow-statistics messages from the switch processor to the route processor.

Defaults

25 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to configure the time interval between two consecutive batches of flow-statistics messages from the switch processor to the route processor:

```
Router(config)# mls ip multicast flow-stat-timer 10
```

Related Commands

Command	Description
show mls ip multicast	Displays the MLS IP information.

mls ip multicast non-rpf aging

To enable rate-limiting of non-RPF traffic, use the **mls ip multicast non-rpf aging** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mls ip multicast non-rpf aging {**global** | **fast**} *time*

no mls ip multicast non-rpf aging {**global** | **fast**}

Syntax Description

global *time*	Specifies the global aging time interval. Valid values are 1 to 180; by default the time is set to 20 seconds.
fast *time*	Specifies the fast aging time interval. Valid values are 2 to 10; by default the time is set to 2 seconds.

Defaults

The fast aging time default is 2 seconds and the global aging time default is 20 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced for the Supervisor Engine 720.

Usage Guidelines

You should not configure ACL-based filtering of RPF failures.

Examples

This example shows how to enable rate-limiting of non-RPF traffic:

```
Router(config)# mls ip multicast non-rpf aging global 90
```

This example shows how to display the multicast configuration of the router:

```
Router# show running | incl mls ip multicast
mls ip multicast non-rpf aging global 90
mls ip multicast non-rpf aging fast 4
Router#
```

Related Commands

Command	Description
show mls ip multicast	Displays the MLS IP information.

mls ip multicast replication-mode

To enable and specify the replication mode, use the **mls ip multicast replication-mode** command in global configuration mode. To restore the system to automatic detection mode, use the **no** form of this command.

mls ip multicast replication-mode {**egress** | **ingress**}

no mls ip multicast replication-mode {**egress** | **ingress**}

Syntax Description

egress	Forces the system to the egress mode of replication.
ingress	Forces the system to the ingress mode of replication.

Defaults

The Supervisor Engine 720 automatically detects the replication mode based on the module types that are installed in the system. If all modules are capable of egress replication, the system uses egress-replication mode. If the supervisor engine detects the modules that are not capable of egress replication, the replication mode automatically switches to ingress replication.

If the system is functioning in the automatic-detection egress mode, and you install a module that cannot perform egress replication, the following occurs:

- The Cisco 7600 series router reverts to ingress mode.
- A system log is generated.
- A system reload occurs to revert to the old configuration.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXF	Thic command was changed to support the **egress** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Note During the change from egress- to ingress-replication mode, traffic interruptions may occur because the shortcuts are purged and reinstalled. To avoid interruptions in traffic forwarding, enter the **mls ip multicast replication-mode ingress** command.

If you enter the **no mls ip multicast replication-mode egress** command, only the forced-egress mode resets and not the forced-ingress mode.

If you enter the **no mls ip multicast replication-mode ingress** command, only the forced-ingress mode resets and not the forced-egress mode.

Examples

This example shows how to enable the ingress-replication mode:

```
Router(config)# mls ip multicast replication-mode ingress
```

This example shows how to enable the egress-replication mode:

```
Router(config)# mls ip multicast replication-mode egress
```

This example shows how to disable the current egress-replication mode and return to automatic detection mode:

```
Router(config)# no mls ip multicast replication-mode egress
```

Related Commands

Command	Description
show mls ip multicast capability	Displays the MLS IP information.

mls ip multicast sso

To configure the stateful switchover (SSO) parameters, use the **mls ip multicast sso** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mls ip multicast sso {**convergence-time** *time* | **leak** {**interval** *seconds* | **percent** *percentage*}}

no mls ip multicast sso {**convergence-time** *time* | **leak** {**interval** *seconds* | **percent** *percentage*}}

Syntax Description

convergence-time *time*	Specifies the maximum time to wait for protocol convergence; valid values are from 0 to 3600 seconds.
leak interval *seconds*	Specifies the packet-leak interval; valid values are from 0 to 3600 seconds.
leak percent *percentage*	Specifies the percentage of multicast packets leaked to the router during switchover so that protocol convergence can take place; valid values are from 1 to 100 percent.

Command Default

The defaults are as follows:

- **convergence-time** *time*—20 seconds
- **leak** *interval*—60 seconds
- **leak** *percentage*—10 percent

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to set the maximum time to wait for protocol convergence to 300 seconds:

```
Router(config)# mls ip multicast sso convergence-time 300
Router(config)#
```

This example shows how to set the packet-leak interval to 200 seconds:

```
Router(config)# mls ip multicast sso leak interval 200
Router(config)#
```

This example shows how to set the packet-leak percentage to 55 percent:

```
Router(config)# mls ip multicast sso leak percent 55
Router(config)#
```

Related Commands

Command	Description
show mls ip multicast sso	Displays information about multicast high-availability SSO.

mls ip multicast stub

To enable the support for non-RPF traffic drops for PIM sparse-mode stub networks, use the **mls ip multicast stub** command in interface configuration mode. To disable support for non-RPF traffic drops for PIM sparse-mode stub networks, use the **no** form of this command.

mls ip multicast stub

no mls ip multicast stub

Syntax Description

This command has no arguments or keywords.

Defaults

Multicast is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you enable the ACL-based method of filtering RPF failures by entering the **mls ip multicast stub** command on the redundant router, the following ACLs automatically download to the PFC and are applied to the interface that you specify:

- access-list 100 permit ip A.B.C.0 0.0.0.255 any
- access-list 100 permit ip A.B.D.0 0.0.0.255 any
- access-list 100 permit ip any 224.0.0.0 0.0.0.255
- access-list 100 permit ip any 224.0.1.0 0.0.0.255
- access-list 100 deny ip any 224.0.0.0 15.255.255.255

The ACLs filter the RPF failures and drop them in the hardware so that they are not forwarded to the router.

Use the ACL-based method of filtering the RPF failures only in sparse-mode stub networks where there are no downstream routers. For dense-mode groups, the RPF failure packets have to be seen on the router for the PIM-assert mechanism to function properly. Use CEF-or NetFlow-based rate limiting to rate limit the RPF failures in dense-mode networks and sparse-mode transit networks.

Examples

This example shows how to enable the support for the non-RPF traffic drops for the PIM sparse-mode stub networks:

```
Router(config-if)# mls ip multicast stub
```

Related Commands

Command	Description
show mls ip multicast	Displays the MLS IP information.

mls ip multicast threshold

To configure a threshold rate for installing hardware shortcuts, use the **mls ip multicast threshold** command in global configuration mode. To deconfigure the threshold rate, use the **no** form of this command.

mls ip multicast threshold *pps*

no mls ip multicast threshold

Syntax Description

pps	Threshold in packets per seconds. Valid values are from 10 to 10000.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to prevent creation of MLS entries for short-lived multicast flows such as join requests.

If multicast traffic drops below the configured multicast rate threshold, all multicast traffic is routed by the MSFC.

This command does not affect already installed routes. For example, if you enter this command and the shortcuts are already installed, the shortcuts are not removed if they are disqualified. To apply the threshold to existing routes, clear the route and let it reestablish.

Examples

This example shows how to configure the IP MLS threshold to 10 packets per second:

```
Router(config)# mls ip multicast threshold 10
```

Related Commands

Command	Description
mls rp ip (global configuration)	Enables external systems to establish IP shortcuts to the MSFC.
show mls ip multicast	Displays the MLS IP information.

mode bypass

To enable Virtual Multipoint Interfaces (VMI) to support multicast traffic, use the **mode bypass** command in interface configuration mode. To return the interface to the default mode of aggregate, use the **no** form of this command.

mode [aggregate | bypass]

no mode bypass

Syntax Description

aggregate	Sets the mode to aggregate. All virtual-access interfaces created by PPPoE sessions are logically aggregated under the VMI.
bypass	Sets the mode to bypass.

Command Default

No mode

Command Modes

Interface configuration

Command History

Release	Modification
12.4(15)XF	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T to support multicast traffic on Virtual Multipoint Interfaces (VMIs).

Usage Guidelines

Use the mode bypass command when you need to support multicast traffic in router-to-radio configurations.

Aggregate Mode

The default mode for operation of the VMI is **aggregate** mode. In aggregate mode, all of the virtual-access interfaces created by PPPoE sessions are logically aggregated under the VMI. As such, applications above Layer 2, such as, EIGRP and OSPFv3, should be defined on the VMI interface only. Packets sent to the VMI will be correctly forwarded to the correct virtual-access interface.

Bypass Mode

Using **bypass** mode is recommended for multicast applications.

In **bypass** mode, the virtual-access interfaces are directly exposed to applications running above Layer2. In bypass mode, definition of a VMI is still required because the VMI will continue to manage presentation of cross-layer signals, such as, neighbor up, neighbor down, and metrics. However, applications will still be aware on the actual underlying virtual-access interfaces and send packets to them directly.

Using **bypass** mode can cause databases in the applications to be larger because knowledge of more interfaces are required for normal operation.

After you enter the **mode bypass** command, Cisco recommends that you copy the running configuration to NVRAM. because the default mode of operation for VMI is to logically aggregate the virtual-access interfaces.

Examples

The following example sets the interface mode to bypass:

```
Router# enable
Router# configure terminal
Router(config)# interface vmi1
Router(config-if)# mode bypass
```

Related Commands

Command	Description
interface vmi	Creates a VMI interface.

mpls mldp forwarding recursive

To enable Multicast Label Distribution Protocol (MLDP) recursive forwarding over a point-to-multipoint (P2MP) Label Switched Path (LSP), use the **mpls mldp forwarding recursive** command in global configuration mode. To disable MLDP recursive forwarding over a P2MP LSP, use the **no** form of this command.

mpls mldp forwarding recursive

no mpls mldp forwarding recursive

Syntax Description

This command has no arguments or keywords.

Command Default

MLDP recursive forwarding is enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

MLDP has two ways to resolve the next-hop that is used for forwarding labeled packets. Without this command enabled, MLDP resolves the outgoing interface based on the next hop to the downstream label switched router (LSR). If this command is enabled, the outgoing interface is resolved by Multicast Forwarding Information (MFI) using point-to-point (P2P) LSPs. The MLDP uses recursive forwarding over a P2P LSP. This means that a P2P LSP for the next hop needs to be available in the MFI. This configuration needs to be enabled to make MLDP Fast Re-route (FRR) backup over a traffic engineering (TE) tunnel possible.

Examples

The following example shows how to enable MLDP recursive forwarding on routers configured with MLDP P2MP functionality:

```
Router(config)# mpls mldp forwarding recursive
```

Related Commands

Command	Description
show mpls mldp database	Displays MLDP information.

mpls mldp logging notifications

To enable Multicast Label Distribution Protocol (MLDP) system log notifications, use the **mpls mldp logging notifications** command in global configuration mode. To disable this function, use the **no** form of this command.

mpls mldp logging notifications

no mpls mldp logging notifications

Syntax Description

This command has no arguments or keywords.

Command Default

MLDP logging notifications are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

Use the **mpls mldp logging notifications** command to generate syslog messages when internal errors occur in MLDP.

Examples

The following example shows how to enable MLDP logging notifications:

```
Router(config)# mpls mldp logging notifications
```

Related Commands

Command	Description
show mpls mldp database	Displays MLDP information.

mpls mldp path

To configure Multicast Label Distribution Protocol (MLDP) path options, use the **mpls mldp path** command in global configuration mode. To disable this configuration, use the **no** form of this command.

mpls mldp path {**multipath** {**downstream** | **upstream**} | **traffic-eng**}

no mpls mldp path {**multipath** {**downstream** | **upstream**} | **traffic-eng**}

Syntax Description

multipath downstream	Enables MLDP multipath for downstream Label Distribution Protocol (LDP) neighbors.
multipath upstream	Enables MLDP multipath for upstream LDP neighbors.
traffic-eng	Allows MLDP to use Traffic Engineering (TE) tunnels.

Command Default

MLDP path options are not configured on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

If there are multiple downstream paths available to reach an LDP peer, load balancing of the branches of the LSPs over these paths occurs.

The assignment of the downstream paths to the label switched paths (LSPs) is done in a circular way. If this command is disabled, the path with the highest next-hop IP address is used to reach an LDP peer.

If there are multiple paths available to reach the root of a multiprotocol LSP, an algorithm based on the Forwarding Equivalence Class (FEC) length of the LSP is used to determine the path. If this command is disabled, the path with the highest next-hop IP address is used to reach the root.

If point-to-point MPLS TE tunnels are present in the unicast routing table, and LDP sessions exist with the destinations, then MLDP will consider TE tunnels as valid paths towards an mLDP neighbor. This command is disabled by default. If this command is not enabled and TE tunnels are present in the unicast routing table then the Interior Gateway Protocol (IGP) command **mpls traffic-eng multicast-intact** must be used to preserve the non-TE tunnel routes for use with MLDP path selection

Examples

The following example shows how to enable load balancing of different LSPs over the paths available to reach a downstream LDP peer:

```
Router(config)# mpls mldp path multicast downstream
```

Related Commands

Command	Description
show mpls mldp database	Displays MLDP information.

mrinfo

To query which neighboring multicast routers are acting as peers with the local router, use the **mrinfo** command in user EXEC or privileged EXEC mode.

mrinfo vrf *route-name* [*source-address* | *interface*] [*host-name* | *host-address*]

Syntax Description

vrf *route-name*	Specifies the VPN routing or forwarding instance.
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.
interface	(Optional) Source interface used on mrinfo requests. If omitted, the source is based on the outbound interface for the destination.
host-name | *host-address*	(Optional) The Domain Name System (DNS) name or IP address of the multicast router to query. If omitted, the router queries itself.

Defaults

The command is disabled.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **vrf** and *route-name* keyword and argument pair was added.

Usage Guidelines

The **mrinfo** command is the original tool of the multicast backbone (MBONE) to determine which neighboring multicast routers are peering with a multicast router. Cisco routers have supported responding to mrinfo requests since Cisco IOS Release 10.2.

You can query a multicast router using the **mrinfo** command. The output format is identical to the multicast routed version of the Distance Vector Multicast Routing Protocol (DVMRP). (The mrouted software is the UNIX software that implements DVMRP.)

Examples

The following is sample output from the **mrinfo** command:

```
Router# mrinfo vrf 192.0.1.0
```

```
192.31.7.37 (barrnet-gw.cisco.com) [version cisco 11.1] [flags: PMSA]:
  192.31.7.37 -> 192.31.7.34 (sj-wall-2.cisco.com) [1/0/pim]
  192.31.7.37 -> 192.31.7.47 (dirtylab-gw-2.cisco.com) [1/0/pim]
  192.31.7.37 -> 192.31.7.44 (dirtylab-gw-1.cisco.com) [1/0/pim]
```

The flags indicate the following:

- P: prune-capable
- M: mtrace-capable
- S: Simple Network Management Protocol (SNMP)-capable
- A: Auto-Rendezvous Point (RP)-capable

mrm

To start or stop a Multicast Routing Monitor (MRM) test, use the **mrm** command in privileged EXEC mode.

mrm *test-name* {**start** | **stop**}

Syntax Description

test-name	Name of the MRM test to start or stop.
start	Starts the MRM test specified for the *test-name* argument.
stop	Stops the MRM test specified for the *test-name* argument.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must use this command to run an MRM test. When the test runs, the Test Sender sends User Datagram Protocol (UDP) or UDP/Real-Time Transport Protocol (RTP) packets (depending on the **senders** command) to the Test Receiver.

Examples

The following example shows how to start an MRM test. In this example, the MRM test named test1 is started.

```
Router# mrm test1 start
```

Related Commands

Command	Description
ip mrm manager	Identifies an MRM test and enters the mode in which you specify the test parameters.
senders	Configures Test Sender parameters used in MRM.
show ip mrm status-report	Displays the status reports in the MRM status report cache.

mstat

To display IP multicast packet rate and loss information, use the **mstat** command in user EXEC or privileged EXEC mode.

mstat {**vrf** *route-name* {*source-name* | *source-address*} | {*source-name* | *source-address*} [*destination-name* | *destination-address*] [*group-name* | *group-address*]}

Syntax Description

vrf *route-name*	Specifies the VPN routing or forwarding instance.
source-name | *source-address*	Domain Name System (DNS) name or the IP address of the multicast-capable source.
destination-name | *destination-address*	(Optional) DNS name or address of the destination. If omitted, the command uses the system at which the command is typed.
group-name | *group-address*	(Optional) DNS name or multicast address of the group to be displayed. Default address is 224.2.0.1 (the group used for multicast backbone [MBONE] Audio).

Defaults

The command is disabled.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **vrf** *route-name* keyword and argument pair was added.

Usage Guidelines

If no arguments are entered, the router will interactively prompt you for them.

This command is a form of UNIX mtrace that reports packet rate and loss information.

Examples

The following is sample output from the **mstat** command in user EXEC mode:

```
Router> mstat lwei-home-ss2 172.16.0.1 224.0.255.255

Type escape sequence to abort.
Mtrace from 172.16.0.0 to 172.16.0.10 via group 224.0.255.255
>From source (lwei-home-ss2.cisco.com) to destination (lwei-ss20.cisco.com)
Waiting to accumulate statistics......
Results after 10 seconds:
```

```
  Source          Response Dest    Packet Statistics For    Only For Traffic
172.16.0.0        172.16.0.10 All Multicast Traffic     From 172.16.0.0
     |         __/  rtt 48   ms   Lost/Sent = Pct  Rate     To 224.0.255.255
     v        /     hop 48   ms   ---------------------     --------------------
172.16.0.1        lwei-cisco-isdn.cisco.com
     |      ^      ttl   1
     v      |      hop 31   ms    0/12 = 0%      1 pps    0/1 = --%  0 pps
172.16.0.2
172.16.0.3        eng-frmt12-pri.cisco.com
     |      ^      ttl   2
     v      |      hop -17  ms    -735/12 = --%      1 pps    0/1 = --%  0 pps
172.16.0.4
172.16.0.5        eng-cc-4.cisco.com
     |      ^      ttl   3
     v      |      hop -21  ms    -678/23 = --%      2 pps    0/1 = --%  0 pps
172.16.0.6
172.16.0.7        eng-ios-2.cisco.com
     |      ^      ttl   4
     v      |      hop 5    ms    605/639 = 95%      63 pps    1/1 = --%  0 pps
172.16.0.8
172.16.0.9        eng-ios-f-5.cisco.com
     |       \__   ttl   5
     v          \  hop 0    ms        4         0 pps           0    0 pps
172.16.0.0        172.16.0.10
  Receiver        Query Source
```

Table 2 describes the significant fields shown in the display.

Table 2 mstat Field Descriptions

Field	Description
Source	Traffic source of packet.
Response Dest	Place where the router sends the results of the **mstat** command.
ttl	Number of hops required from the traffic source to the current hop.
hop	Number of milliseconds of delay.
Only For Traffic From	0 packets dropped out of 2 packets received. If, for example, –2/2 was indicated, then there are 2 extra packets, which could indicate a loop condition.

Related Commands

Command	Description
mtrace	Traces the path from a source to a destination branch for a multicast distribution tree.

mtrace

To trace the path from a source to a destination branch for a multicast distribution tree, use the **mtrace** command in user EXEC or privileged EXEC mode.

mtrace {**vrf** *route-name* {*source-name* | *source-address*} [*destination-name* | *destination-address*] [*group-name* | *group-address*] [*trace-time*] | {*source-name* | *source-address*} [*destination-name* | *destination-address*] [*group-name* | *group-address*] [*trace-time*]}

Syntax Description

vrf *route-name*	Specifies the VPN routing or forwarding instance.
source-name | *source-address*	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.
destination-name | *destination-address*	(Optional) DNS name or address of the unicast destination. If omitted, the mtrace starts from the system at which the command is typed.
group-name | *group-address*	(Optional) DNS name or multicast address of the group to be traced. Default address is 224.2.0.1 (the group used for multicast backbone [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.
trace-time	(Optional) The duration for which the multicast trace request must remain active. The range is from 1 to 255 router hops.

Defaults

The command is disabled.

Command Modes

User EXEC (<)
Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **vrf** *route-name* keyword and argument pair was added.

Usage Guidelines

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 then follows the multicast path from the destination to the source by passing the mtrace request packet via 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 will interactively prompt 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 in user EXEC mode:

```
Router> mtrace 172.16.0.0 172.16.0.10 239.254.254.254

Type escape sequence to abort.
Mtrace from 172.16.0.0 to 172.16.0.10 via group 239.254.254.254
From source (?) to destination (?)
Querying full reverse path...
 0  172.16.0.10
-1  172.16.0.8 PIM  thresh^ 0  0 ms
-2  172.16.0.6 PIM  thresh^ 0  2 ms
-3  172.16.0.5 PIM  thresh^ 0  894 ms
-4  172.16.0.3 PIM  thresh^ 0  893 ms
-5  172.16.0.2 PIM  thresh^ 0  894 ms
-6  172.16.0.1 PIM  thresh^ 0  893 ms
```

Table 3 describes the significant fields shown in the display.

Table 3 mtrace Field Descriptions

Field	Description
Mtrace from 172.16.0.0 to 172.16.0.10 via group 239.254.254.254	Name and address of the source, destination, and group for which routes are being traced.
-3 172.16.0.5	Hops away from the destination (–3) and address of the intermediate router.
PIM thresh^ 0	Multicast protocol in use on this hop, and time-to-live (TTL) threshold.
893 ms	Time taken for the trace to be forwarded between hops.

Related Commands

Command	Description
mstat	Displays IP multicast packet rate and loss information.

receivers

To establish Test Receivers for Multicast Routing Monitor (MRM) tests or modify the parameters of Test Receivers, use the **receivers** command in MRM manager configuration mode. To restore the default values, use the **no** form of this command.

Form of the Command to Establish Test Receivers

receivers *access-list* **sender-list** *access-list* [*packet-delay*]

no receivers *access-list*

Form of the Command to Modify the Parameters of Test Receivers

receivers *access-list* [**window** *seconds*] [**report-delay** *seconds*] [**loss** *percentage*] [**no-join**] [**monitor** | **poll**]

no receivers *access-list*

Syntax Description

access-list	IP named or numbered access list that establishes the Test Receivers. Only these Test Receivers are subject to the other keywords and arguments specified in this command.
sender-list *access-list*	Specifies the sources that the Test Receiver should monitor. If the named or numbered access list matches any access list specified in the **senders** command, the associated **packet-delay** *milliseconds* keyword and argument of that **senders** command are used in this command. Otherwise, the *packet-delay* argument is required in this **receivers** command.
packet-delay	(Optional) Specifies the delay between test packets (in milliseconds). The range is from 50 to 10000. If the **sender-list** access list matches any access list specified in a **senders** command, the associated **packet-delay** *milliseconds* keyword and argument of that **senders** command are used in this command. Otherwise, the *packet-delay* argument is required in this **receivers** command.
window *seconds*	(Optional) Specifies the duration (in seconds) of a test period. This is a sliding window of time in which the packet count is collected, so that the loss percentage can be calculated. The range is from 1 to 10. The default is 5 seconds.
report-delay *seconds*	(Optional) Specifies the delay (in seconds) between status reports. The delay prevents multiple Test Receivers from sending status reports to the Manager at the same time for the same failure. This value is relevant only if there are multiple Test Receivers. The range is from 1 to 60. The default is 1 second.
loss *percentage*	(Optional) Specifies the threshold percentage of packet loss required before a status report is triggered. The range is from 0 to 100. The default is 0 percent, which means that a status report is sent for any packet loss. (This value is not applied to packet duplication; a fault report is sent for any duplicated packets.) Loss percentage calculation is explained in the "Usage Guidelines" section of this command.

no-join	(Optional) Specifies that the Test Receiver does not join the monitored group. The default is that the Test Receiver joins the monitored group.
monitor | **poll**	(Optional) Specifies whether the Test Receiver monitors the test group or polls for receiver statistics. The **monitor** keyword means the Test Receiver reports only if the test criteria are met. The **poll** keyword means the Test Receiver sends status reports regularly, whether test criteria are met or not. The default is the behavior set with the **monitor** keyword.

Command Default

No Test Receivers are configured for MRM tests.

Command Modes

MRM manager configuration (config-mrm-manager)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is required for MRM to work; the **receivers** *access-list* and **sender-list** *access-list* keyword-argument pairs must be specified.

Note The Cisco IOS CLI parser accepts the command entered without the required **sender-list** *access-list* keyword-argument pair. This keyword-argument pair, however, is not optional. For an MRM test to work, you must specify the sources that the Test Receiver should monitor using the **sender-list** keyword and *access-list* argument.

Optionally, you can use the **receivers** command to modify the parameters for Test Receivers.

Loss percentage is calculated based on the **packet-delay** value of the **senders** command, which defaults to 200 milliseconds, or 5 packets per second. If the **window** keyword defaults to 5 seconds, then the Test Receiver expects 5 packets per second for 5 seconds = 25 packets. If the Test Receiver receives only 15 packets, then 25 – 15 = 10 lost packets. Lost packets divided by packets expected equals loss percentage; 10/25 equals a loss percentage of 40 percent.

Examples

The following example shows how to establish a Test Receiver for an MRM test:

```
ip mrm manager test1
 manager Ethernet0/0 group 239.1.1.1
 senders 1
 receivers 2 sender-list 1
!
access-list 1 permit 10.1.1.2
```

```
access-list 2 permit 10.1.4.2
!
```

Related Commands

Command	Description
senders	Establishes Test Senders for MRM.

router-guard ip multicast

To enable the router guard for switch ports that are connected to multicast routers, use the **router-guard ip multicast** command in interface configuration mode. To disable the router guard on switch ports that are connected to multicast routers, use the **no** form of this command.

router-guard ip multicast [**vlan** *vlan-id*]

no router-guard ip multicast [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id*	(Optional) Specifies the Layer 2 VLAN identification.

Command Default

The router guard for switch ports that are connected to multicast routers is disabled by default.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

You can enter the **vlan** *vlan-id* keyword and argument if the port is a trunk port.

You cannot enter a range or multiple VLANs in a single command.

For the router guard to work on switch ports, you must enter the **router-guard ip multicast switchports** global configuration command command before entering the **router-guard ip multicast** interface configuration command.

Examples

This example shows how to enable the router guard on an interface:

```
Router(config-if)# router-guard ip multicast
```

This example shows how to disable router guard on an interface:

```
Router(config-if)# no router-guard ip multicast vlan 100
```

Related Commands

Command	Description
clear router-guard ip multicast statistics	Clears the router guard statistical information.
router-guard ip multicast switchports	Enables or disables the router guard on all switch ports.

router-guard ip multicast switchports

To enable the router guard on all switch ports, use the **router-guard ip multicast switchports** command in global configuration mode. To disable the router guard on all switch ports, use the **no** form of this command.

router-guard ip multicast switchports

no router-guard ip multicast switchports

Syntax Description

This command has no arguments or keywords.

Command Default

The router guard is disabled on all switch ports.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

If received on a port that has router guard enabled, the following packet types are discarded and the statistics are updated indicating that packets are being dropped by the router guard:

- Internet Group Management Protocol (IGMP) query messages
- IPv4 Peripheral Interface Manager version 2 messages
- IGMP PIM messages (PIMv1)
- IGMP Distance Vector Multicast Routing Protocol (DVMRP) messages
- Router-port Group Management Protocol (RGMP)messages
- Cisco Group Multicast Protocol (CGMP)messages

Examples

This example shows how to enable the router guard on all switch ports:

```
Router(config)# router-guard ip multicast switchports
```

This example shows how to disable the router guard on all switch ports:

```
Router(config)# no router-guard ip multicast switchports
```

Related Commands

Command	Description
clear router-guard ip multicast statistics	Clears the router guard statistical information.
router-guard ip multicast	Enables or disables the router guard for switch ports that are connected to multicast routers.
show router-guard	Displays the router guard status and configuration information.

senders

To configure Test Sender parameters used for a Multicast Routing Monitor (MRM) test, use the **senders** command in MRM manager configuration mode. To restore the default settings, use the **no** form of this command.

senders *access-list* [**packet-delay** *milliseconds*] [**rtp** | **udp**] [**target-only** | **all-multicasts** | **all-test-senders**] [*proxy-src*]

no senders *access-list*

Syntax Description

access-list	IP named or numbered access list that defines which Test Senders are involved in the test and which Test Senders these parameters apply to.
packet-delay *milliseconds*	(Optional) Specifies the delay between test packets (in milliseconds). The range is from 50 to 10000. The default is 200 milliseconds, which results in 5 packets per second.
rtp | **udp**	(Optional) Specifies the encapsulation of test packets, either Real-Time Transport Protocol (RTP)-encapsulated or User Datagram Protocol (UDP)-encapsulated. By default, test packets are RTP-encapsulated.
target-only	(Optional) Specifies that test packets are sent out on the targeted interface only (that is, the interface with the IP address that is specified in the Test Sender request target field). By default, test packets are sent out on all interfaces that are enabled with IP multicast.
all-multicasts	(Optional) Specifies that the test packets are sent out on all interfaces that are enabled with IP multicast. This is the default method for sending test packets.
all-test-senders	(Optional) Specifies that test packets are sent out on all interfaces that have test-sender mode enabled. By default, test packets are sent out on all interfaces that are enabled with IP multicast.
proxy-src	(Optional) Source IP address for which the Test Sender will proxy test packets. Enter an address if you want to test, for a specific source, whether the multicast distribution tree is working.

Command Default

No test senders are configured to be involved in MRM tests.

Command Modes

MRM manager configuration (config-mrm-manager)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to specify which Test Senders are involved in the test and are affected by these parameters.

Examples

The following example shows how to configure a Test Sender for an MRM test:

```
ip mrm manager test1
 manager Ethernet0/0 group 239.1.1.1
 senders 1
 receivers 2 sender-list 1
!
access-list 1 permit 10.1.1.2
access-list 2 permit 10.1.4.2
```

Related Commands

Command	Description
receivers	Establishes Test Receivers for MRM.

show ip dvmrp route

Note The **show ip dvmrp route** command is not available in 12.2(33)SRB, 15.0(1)M, and later 12.2SR, 15.0M, and T releases.

To display the contents of the Distance Vector Multicast Routing Protocol (DVMRP) routing table, use the **show ip dvmrp route** command in user EXEC or privileged EXEC mode.

show ip dvmrp route [**address** *hostname* | **interface** *type number*] [**poison**]

Syntax Description

address	(Optional) Displays information about the specified DVMRP route.
hostname	(Optional) IP name or IP address.
interface	(Optional) Displays information about the specified interface from the DVMRP routing table.
type	(Optional) Interface type.
number	(Optional) Interface or subinterface number.
poison	(Optional) Displays information about DVMRP routes that have been poisoned.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA and the **poison** keyword was added.
12.2(33)SRB	This command was removed. It is not available in Cisco IOS Release 12.2(33)SRB and later Cisco IOS 12.2SR releases.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was removed.

Usage Guidelines

Use the **show ip dvmrp route** EXEC command to show the contents of the DVMRP routing table.

Examples

The following example shows output of the **show ip dvmrp route** command:

```
Router# show ip dvmrp route

DVMRP Routing Table - 1 entry
172.16.0.0/16 [100/11] uptime 07:55:50, expires 00:02:52
    via 192.168.0.0, Tunnel3
```

Table 4 describes the significant fields shown in the display.

Table 4 show ip dvmrp route Field Descriptions

Field	Description
1 entry	Number of entries in the DMVRP routing table.
172.16.0.0/16	Source network.
[100/11]	Administrative distance/metric.
uptime	How long (in hours, minutes, and seconds) that the route has been in the DVMRP routing table.
expires	How long (in hours, minutes, and seconds) until the entry is removed from the DVMRP routing table.
via 192.168.0.0	Next hop router to the source network.
Tunnel3	Interface to the source network.

show ip igmp groups

To display the multicast groups with receivers that are directly connected to the router and that were learned through Internet Group Management Protocol (IGMP), use the **show ip igmp groups** command in user EXEC or privileged EXEC mode.

show ip igmp [**vrf** *vrf-name*] **groups** [*group-name* | *group-address* | *interface-type interface-number*] [**detail**]

Syntax Description

vrf *vrf-name*	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance and indicates the name assigned to the VRF.
group-name	(Optional) Name of the multicast group, as defined in the Domain Name System (DNS) hosts table.
group-address	(Optional) Address of the multicast group. This is a multicast IP address in four-part, dotted-decimal notation.
interface-type interface-number	(Optional) Interface type and Interface number.
detail	(Optional) Provides a detailed description of the sources known through IGMP Version 3 (IGMPv3), IGMPv3lite, or URL Rendezvous Directory (URD).

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.1(3)T	Fields were added to the output of this command to support the Source Specific Multicast (SSM) feature.
12.1(5)T	The **detail** keyword was added.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(2)T	A field was added to the output of this command to support the SSM mapping feature.
12.2(18)S	A field was added to the output of this command to support the SSM mapping feature.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you omit all optional arguments and keywords, the **show ip igmp groups** command displays by group address, interface type, and interface number all directly connected multicast groups.

Examples

The following is sample output from the **show ip igmp groups** command:

```
Router# show ip igmp groups

IGMP Connected Group Membership
Group Address     Interface         Uptime      Expires     Last Reporter
239.255.255.254   Ethernet3/1       1w0d        00:02:19    172.21.200.159
224.0.1.40        Ethernet3/1       1w0d        00:02:15    172.21.200.1
224.0.1.40        Ethernet3/3       1w0d        never       172.16.214.251
224.0.1.1         Ethernet3/1       1w0d        00:02:11    172.21.200.11
224.9.9.2         Ethernet3/1       1w0d        00:02:10    172.21.200.155
232.1.1.1         Ethernet3/1       5d21h       stopped     172.21.200.206
```

The following is sample output from the **show ip igmp groups** command with the *group-address* argument and **detail** keyword:

```
Router# show ip igmp groups 192.168.1.1 detail

Interface:      Ethernet3/2
Group:          192.168.1.1
Uptime:         01:58:28
Group mode:     INCLUDE
Last reporter:  10.0.119.133
CSR Grp Exp:    00:02:38
Group source list: (C - Cisco Src Report, U - URD, R - Remote
                    S- Static, M - SSM Mapping)
  Source Address   Uptime    v3 Exp    CSR Exp   Fwd  Flags
  172.16.214.1     01:58:28  stopped   00:02:31  Yes  C
```

Table 5 describes the significant fields shown in the displays.

Table 5 show ip igmp groups Field Descriptions

Field	Description
Group Address	Address of the multicast group.
Interface	Interface through which the group is reachable.
Uptime	Time in weeks, days, hours, minutes, and seconds that this multicast group has been known.
Expires	Time in weeks, days, hours, minutes, and seconds until the entry expires. If an entry expires, then the entry (for a short period) shows "now" before it is removed. "never" indicates that the entry will not time out, because a local receiver is on this router for this entry. "stopped" indicates that timing out of this entry is not determined by this expire timer. If the router is in INCLUDE mode for a group, then the whole group entry times out after the last source entry has timed out (unless the mode is changed to EXCLUDE mode before it times out).
Last Reporter	Last host to report being a member of the multicast group. Both IGMP v3lite and URD require a v2-report.
Group mode:	Either INCLUDE or EXCLUDE. The group mode is based on the type of membership reports that are received on the interface for the group. In the output for the **show ip igmp groups detail** command, the EXCLUDE mode also shows the Expires: field for the group entry (not shown in the output).

Table 5 show ip igmp groups Field Descriptions (continued)

Field	Description
CSR Grp Exp	Shown for multicast groups in the SSM range. It indicates the time (in hours, minutes, and seconds) since the last received group membership report was received. Cisco IOS software needs to use these reports for the operation of URD and IGMP v3lite, but they do not indicate group membership by themselves.
Group source list:	Details of which sources have been requested by the multicast group.
Source Address	IP address of the source.
Uptime	Time since the source state was created.
v3 Exp	Time in hours, minutes, and seconds until the membership for the source times out according to IGMP operations. “stopped” displays if no member uses IGMPv3 (but only IGMP v3lite or URD).
CSR Exp	Time in hours, minutes, and seconds until the membership for the source times out according to IGMP v3lite or URD reports. “stopped” displays if members use only IGMPv3.
Fwd	Status of whether the router is forwarding multicast traffic due to this entry.
Flags	Information about the entry. The Remote flag indicates that an IGMPv3 report has been received by this source. The C flag indicates that an IGMP v3lite or URD report was received by this source. The U flag indicates that a URD report was received for this source.

Related Commands

Command	Description
ip igmp query-interval	Configures the frequency at which the Cisco IOS software sends IGMP host query messages.
ip igmp ssm-map enable	Enables SSM mapping for groups in a configured SSM range.
show ip igmp ssm-mapping	Displays information about SSM mapping or displays the sources that SSM mapping uses for a particular group.

show ip igmp interface

To display multicast-related information about an interface, use the **show ip igmp interface** command in user EXEC or privileged EXEC mode.

show ip igmp [**vrf** *vrf-name*] **interface** [*interface-type interface-number*]

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
interface-type	(Optional) Interface type.
interface-number	(Optional) Interface number.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

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

This command also displays information about dynamically learned Distance Vector Multicast Routing Protocol (DVMRP) routers on the interface.

Examples

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

```
Router# show ip igmp interface

Ethernet0 is up, line protocol is up
  Internet address is 192.168.37.6, subnet mask is 255.255.255.0
  IGMP is enabled on interface
  IGMP query interval is 60 seconds
  Inbound IGMP access group is not set
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 192.168.37.33
  No multicast groups joined
```

```
Ethernet1 is up, line protocol is up
  Internet address is 192.168.36.129, subnet mask is 255.255.255.0
  IGMP is enabled on interface
  IGMP query interval is 60 seconds
  Inbound IGMP access group is not set
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  Multicast designated router (DR) is 192.168.36.131
  Multicast groups joined: 225.2.2.2 226.2.2.2
Tunnel0 is up, line protocol is up
  Internet address is 10.1.37.2, subnet mask is 255.255.0.0
  IGMP is enabled on interface
  IGMP query interval is 60 seconds
  Inbound IGMP access group is not set
  Multicast routing is enabled on interface
  Multicast TTL threshold is 0
  No multicast groups joined
```

Table 6 describes the significant fields shown in the display.

Table 6 show ip igmp interface Field Descriptions

Field	Description
Ethernet0 is up, line protocol is up	Interface type, number, and status.
Internet address is..., subnet mask is...	Internet address of the interface and subnet mask being applied to the interface, as specified with the **ip address** command.
IGMP is enabled on interface	Indicates whether IGMP has been enabled on the interface with the **ip pim** command.
IGMP query interval is 60 seconds	Interval at which the Cisco IOS software sends Protocol Independent Multicast (PIM) router query messages, as specified with the **ip igmp query-interval** command.
Inbound IGMP access group is not set	Indicates whether an IGMP access group has been configured with the **ip igmp access-group** command.
Multicast routing is enabled on interface	Indicates whether multicast routing has been enabled on the interface with the **ip pim** command.
Multicast TTL threshold is 0	Packet time-to-live threshold, as specified with the **ip multicast ttl-threshold** command.
Multicast designated router (DR) is...	IP address of the designated router for this LAN segment (subnet).
No multicast groups joined	Indicates whether this interface is a member of any multicast groups and, if so, lists the IP addresses of the groups.

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip igmp access-group	Controls the multicast groups that hosts on the subnet serviced by an interface can join.
ip igmp query-interval	Configures the frequency at which the Cisco IOS software sends IGMP host query messages.

Command	Description
ip multicast ttl-threshold	Configures the TTL threshold of packets being forwarded out an interface.
ip pim	Enables PIM on an interface.

show ip igmp membership

To display Internet Group Management Protocol (IGMP) membership information for multicast groups and (S, G) channels, use the **show ip igmp membership** command in user EXEC or privileged EXEC mode.

show ip igmp membership [*group-address* | *group-name*] [**tracked**] [**all**]

Syntax Description

group-address	(Optional) The IP address of the multicast group for which to display IGMP membership information.
group-name	(Optional) The name of the multicast group, as defined in the Domain Name System (DNS) hosts table, for which to display IGMP membership information.
tracked	(Optional) Displays the multicast groups with the explicit tracking feature enabled.
all	(Optional) Displays the detailed information about the multicast groups with and without the explicit tracking feature enabled.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(19)S	This command was introduced.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to display IGMP membership information for multicast groups and (S, G) channels. This command allows you to display detailed information about multicast group and channel membership and explicit tracking.

Examples

The following is sample output from the **show ip igmp membership** user EXEC command. Each entry in the output shows the aggregate membership information (indicated by the A flag) for a particular multicast group or channel from the IGMP cache. If the entry is prepended with a forward slash ("/") flag, the entry is a filtering entry that is blocking the data forwarding of the multicast group or channel.

```
Router> show ip igmp membership

Flags:A  - aggregate, T - tracked
       L  - Local, S - static, V - virtual, R - Reported through v3
       I - v3lite, D - Urd, M - SSM (S,G) channel
       1,2,3 - The version of IGMP, the group is in
Channel/Group-Flags:
       / - Filtering entry (Exclude mode (S,G), Include mode (*,G))
Reporter:
       <ip-address> - last reporter if group is not explicitly tracked
       <n>/<m>      - <n> reporter in include mode,<m> reporter in exclude

 Channel/Group                 Reporter        Uptime   Exp.  Flags  Interface
 *,224.0.1.40                  10.10.0.1       00:01:34 02:41 2LA   Et2/0
 *,239.1.1.1                   2/0             00:00:10 stop  3AT    Et2/0
```

The following is sample output from the **show ip igmp membership** user EXEC command with the multicast group address 239.1.1.1 and the **tracked** keyword specified:

```
Router> show ip igmp membership 239.1.1.1 tracked

Flags:A  - aggregate, T - tracked
       L  - Local, S - static, V - virtual, R - Reported through v3
       I - v3lite, D - Urd, M - SSM (S,G) channel
       1,2,3 - The version of IGMP, the group is in
Channel/Group-Flags:
       / - Filtering entry (Exclude mode (S,G), Include mode (*,G))
Reporter:
       <ip-address> - last reporter if group is not explicitly tracked
       <n>/<m>      - <n> reporter in include mode,<m> reporter in exclude

 Channel/Group                 Reporter        Uptime   Exp.  Flags  Interface
 *,239.1.1.1                   2/0             00:00:11 stop  3AT    Et2/0
 10.30.0.100,239.1.1.1         10.10.0.10      00:00:11 02:48 RT     Et2/0
 10.30.0.101,239.1.1.1         10.10.0.20      00:00:03 02:56 RT     Et2/0
 10.30.0.101,239.1.1.1         10.10.0.10      00:00:11 02:48 RT     Et2/0
 10.30.0.102,239.1.1.1         10.10.0.20      00:00:03 02:56 RT     Et2/0
```

Table 7 describes the significant fields shown in the displays.

Table 7 show ip igmp membership Field Descriptions

Field	Description
Channel/Group	(S, G) channel or multicast group filtering entry.
Reporter	Displays information about the hosts reporting membership with the (S, G) channel or multicast group entry.
Uptime	The Uptime timer is how long (in hours, minutes, and seconds) the entry has been known.
Exp.	The Exp. timer is how long (in minutes and seconds) until the entry expires.

Table 7 show ip igmp membership Field Descriptions (continued)

Field	Description
Flags	Provides information about the entry: • A—aggregate. Indicates that the aggregate information for the (S, G) channel or multicast group is being displayed. • T—tracked—Indicates that the multicast group is configured with the explicit tracking feature. • L—local. Indicates that the router itself is interested in receiving the traffic for this multicast group or channel. In order for the application to receive this traffic, the packets are sent to the process level of the router. When the **ip igmp join-group** command is configured for a multicast group, the L flag is set. • S—static. Indicates that the multicast group or channel is forwarded on the interface. When the **ip igmp static-group** command is configured on the interface, the S flag is set. • V—virtual. Indicates that service such as Hoot and Holler is running on the router requesting the traffic for the multicast group or channel. These services can process IP multicast traffic in the fast switching path. The L flag will not be set by these applications.
	• R—reported through v3. Indicates that an IGMP Version 3 (IGMPv3) report was received for this entry. • I—v3lite. Indicates that an IGMP Version 3 lite (IGMP v3lite) report was received for this entry. • D—URD. Indicates that a URL Rendezvous Directory (URD) report was received for this entry. • M—SSM (S, G) channel. Indicates that the multicast group address is in the Source Specific Multicast (SSM) range. • 1, 2, 3—The version of IGMP. The version of IGMP that the multicast group is running.
Interface	Interface type and number.

Related Commands

Command	Description
ip igmp explicit-tracking	Enables explicit tracking of hosts, groups, and channels for IGMP Version 3.
ip igmp version	Configures the version of IGMP that the router uses.
show ip igmp groups	Displays the multicast groups with receivers that are directly connected to the router and that were learned through IGMP.

show ip igmp snooping

To display the Internet Group Management Protocol (IGMP) snooping configuration of a device, use the **show ip igmp snooping** command in user EXEC or privileged EXEC mode.

show ip igmp snooping [**groups** [**count** | **vlan** *vlan-id* [*ip-address* | **count**]] | **mrouter** [**vlan** *vlan-id*] **querier** | **vlan** *vlan-id*]

Syntax Description

groups	(Optional) Displays group information.
count	(Optional) Displays the number of multicast groups learned by IGMP snooping.
vlan *vlan-id*	(Optional) Specifies a VLAN. Valid values are 1 to 1001. If this keyword is not configured, information is displayed for all VLANs.
ip-address	(Optional) Displays information about the specified group.
count	(Optional) Displays group count inside a VLAN.
mrouter	(Optional) Displays information about dynamically learned and manually configured multicast router ports.
querier	(Optional) Displays IGMP querier information.
vlan *vlan-id*	(Optional) Specifies a VLAN. Valid values are 1 to 1001. If this keyword is not configured, information is displayed for all VLANs.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC on Cisco 870 series Integrated Services Routers (ISRs). The **groups** and **querier** keywords were added.
12.4(15)T	The **groups** and **count** keywords were added on the Cisco 87x and the Cisco 1800 series Integrated Services Routers (ISRs) and on EtherSwitch high-speed WAN interface cards (HWICs) and EtherSwitch network modules running on the Cisco 1841, 2800, and 3800 series ISRs.

Usage Guidelines

You can also use the **show mac-address-table multicast** command to display entries in the MAC address table for a VLAN that has IGMP snooping enabled.

Examples

The following is sample output from the **show ip igmp snooping** command:

```
Router# show ip igmp snooping

Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping              : Enabled
IGMPv3 snooping (minimal)  : Enabled
Report suppression         : Enabled
TCN solicit query          : Disabled
TCN flood query count      : 2
Last Member Query Interval : 1000

Vlan 1:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Enabled
Explicit host tracking               : Enabled
Multicast router learning mode       : pim-dvmrp
Last Member Query Interval           : 1000
CGMP interoperability mode           : IGMP_ONLY

Vlan 11:
--------
IGMP snooping                        : Enabled
IGMPv2 immediate leave               : Disabled
Explicit host tracking               : Enabled
Multicast router learning mode       : pim-dvmrp
Last Member Query Interval           : 1000
CGMP interoperability mode           : IGMP_ONLY
```

The information in the output display is self-explanatory.

The following is sample output from the **show ip igmp snooping** command using the **vlan** keyword:

```
Router# show ip igmp snooping vlan 1

vlan 1
----------
  IGMP snooping is globally enabled
  IGMP snooping is enabled on this Vlan
  IGMP snooping immediate-leave is enabled on this Vlan
  IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
```

The information in the output display is self-explanatory.

The following is sample output from the **show ip igmp snooping** command using the **mrouter** keyword:

Note In this example, Fa0/3 is a dynamically learned router port, and Fa0/2 is a configured static router port.

```
Router# show ip igmp snooping mrouter vlan 1

Vlan    ports
----    -----
   1    Fa0/2(static), Fa0/3(dynamic)
```

The information in the output display is self-explanatory.

The following is sample output from the **show ip igmp snooping** command using the **groups** keyword:

```
Router #show ip igmp snooping groups
Vlan      Group           Version     Port List
------------------------------------------------------------
1         192.168.1.2      v2          Fa0/1/0
11        192.168.1.2      v2          Fa0/1/1
```

The information in the output display is self-explanatory.

The following is sample output from the **show ip igmp snooping groups** command with the **count** keyword specified:

```
Router# show ip igmp snooping groups count

Total number of groups:   2
```

The information in the output is self-explanatory.

Related Commands

Command	Description
ip igmp snooping	Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN.
ip igmp snooping vlan	Enables IGMP snooping on the VLAN interface.
ip igmp snooping vlan immediate-leave	Enables IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
show mac-address-table multicast	Displays the Layer 2 multicast entries for a VLAN.

show ip igmp snooping explicit-tracking

To display the information about the explicit host-tracking status for IGMPv3 hosts, use the **show ip igmp snooping explicit-tracking** command in user EXEC or privileged EXEC mode.

show ip igmp snooping explicit-tracking vlan *vlan-id*

Syntax Description

vlan *vlan-id*	Specifies the VLAN to display.

Defaults

If you do not specify a VLAN, information for VLAN 1 is displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

:This example shows how to display the information about the explicit host-tracking status for all IGMPv2 and IGMPv3 hosts:

```
Router# show ip igmp snooping explicit-tracking
Current number of entries: 3 Configured DB size limit: 32000
VLAN 1
Source/Group Interface Reporter Filter_mode
-------------------------------------------------------------------------------
VLAN 2
Source/Group Interface Reporter Filter_mode
-------------------------------------------------------------------------------
VLAN 6
Source/Group Interface Reporter Filter_mode
-------------------------------------------------------------------------------
VLAN 7
Source/Group Interface Reporter Filter_mode
-------------------------------------------------------------------------------
VLAN 10
Source/Group Interface Reporter Filter_mode
-------------------------------------------------------------------------------
0.0.0.0/224.0.1.40 Vl10: 11.10.0.2 EXCLUDE
:
Router#
```

:This example shows how to display the information about the explicit host-tracking status for IGMPv2 and IGMPv3 hosts:

```
Router# show ip igmp snooping explicit-tracking vlan 25

Source/Group          Interface   Reporter     Filter_mode
------------------------------------------------------------------------
10.1.1.1/226.2.2.2    Vl25:1/2    10.27.2.3    INCLUDE
10.2.2.2/226.2.2.2    Vl25:1/2    10.27.2.3    INCLUDE
Router#
```

Related Commands

Command	Description
ip igmp snooping explicit-tracking	Enables explicit host tracking.

show ip igmp snooping filter

To display the Internet Group Management Protocol (IGMP) filtering rules, use the **show ip igmp snooping filter** command in privileged EXEC mode.

show ip igmp snooping filter interface *type mod/port* [**statistics**]

Syntax Description

interface *type*	Interface type; possible valid values are **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel** *num*, and **vlan** *vlan-id*.
mod/port	Module and port number
statistics	(Optional) Displays IGMP filtering statistics.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

IGMP filtering allows you to configure filters on a per-port basis, a per-switch virtual interface (SVI) basis, or both.

The *mod/port* is not supported when you enter the **vlan** *vlan-id* keyword and argument.

IGMP filtering is supported for IPv4 only.

IGMP filters is not supported on routed ports.

If the port is in the shutdown state, the system cannot determine if the port is in trunk mode or access mode, and you will not be able to display the filter status by entering the **show ip igmp snooping filter** command. In this case, you can enter the **show running-config interface** command to display the configuration.

IGMP filtering statistics are maintained for the following only:

- A specific switch port in an SVI.
- A specific VLAN in a trunk.

Examples

The following example displays the default filters configured on the SVI:

```
Router# show ip igmp snooping filter interface vlan 20

Access-Group: Channel1-Acl
Groups/Channels Limit: 100 (Exception List: Channel6-Acl)
IGMP Minimum-Version: Not Configured
Router#
```

The following example displays the output on a switch port that is in access mode:

```
Router# show ip igmp snooping filter interface gigabitethernet3/48

Access-Group: Channel4-Acl
Groups/Channels Limit: 10 (Exception List: Channel3-Acl)
Router#
```

The following example displays the filters configured for all switch ports in access mode under this SVI:

```
Router# show ip igmp snooping filter interface vlan 20 detail
VLAN20 :

Access-Group: Not Configured
Groups/Channels Limit: Not Configured
VLAN20 :
Access-Group: Channel4-ACL
Groups/Channels Limit: 10 (Exception-list: Channel3-Acl)
Router#
```

The following example displays the default trunk port filters:

```
Router# show ip igmp snooping filter interface gigabitethernet3/46

Access-Group: Channel1-Acl
Groups/Channels Limit: 10 (Exception List: Channel3-Acl)
Router#
```

The following example displays the per-VLAN filters for all VLANs on this trunk:

```
Router# show ip igmp snooping filter interface gigabitethernet3/46 detail

Vlan 10 :
Access-Group: Not Configured
Groups/Channels Limit: Not Configured
Vlan 20 :
Access-Group: Not Configured
Groups/Channels Limit: 8 (Exception List: Channel4-Acl)
Router#
```

The following example displays the output on a trunk port for a specific VLAN:

```
Router# show ip igmp snooping filter interface gigabitethernet3/46 vlan 20

Access-Group: Not Configured
Groups/Channels Limit: 8 (Exception List: Channel4-Acl)
Router#
```

The following example displays the statistics for each switch port in access mode under the SVI:

```
Router# show ip igmp snooping filter interface vlan 20 statistics

GigabitEthernet3/47 :
IGMP Filters are not configured
GigabitEthernet3/48 :
Access-group denied : 0
Limit denied : 2
Limit status : 0 active out of 2 max
Minimum-version denied : 0
```

Table 8 describes the significant fields shown in the displays.

Table 8 show ip igmp snooping Field Descriptions

Field	Description
Access-Group: Channel1-Acl	Name of the access group.
Groups/Channels Limit: 100 (Exception List: Channel6-Acl)	Number of IGMP groups or channels allowed on an interface is set to 100, with the exception of group Channel1-Acl.
IGMP Minimum-Version: Not Configured	Minimum version not configured (**ip igmp snooping minimum-version** command).
IGMP Filters are not configured	Filtering on the IGMP protocol is disabled.
Access-group denied : 0	Number of access groups denied.
Limit denied : 2	
Limit status : 0 active out of 2 max	Number of active groups.
Minimum-version denied : 0	

Related Commands

Command	Description
ip igmp snooping access-group	Configures an IGMP group access group.
ip igmp snooping limit	Limits the number of IGMP groups or channels allowed on an interface.
ip igmp snooping minimum-version	Filters on the IGMP protocol.

show ip igmp snooping mrouter

Note The documentation for this command has been integrated into the documentation for the **show ip igmp snooping** command. Please see the **show ip igmp snooping** command for complete and up-to-date information about displaying information for dynamically learned and manually configured multicast router ports.

To display information on dynamically learned and manually configured multicast router ports, use the **show ip igmp snooping mrouter** command in privileged EXEC mode.

show ip igmp snooping mrouter [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN. Valid values are 1 to 1001.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5.2)WC(1)	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can also use the **show mac-address-table multicast** command to display entries in the MAC address table for a VLAN that has Internet Group Management Protocol (IGMP) snooping enabled.

Examples

The following is sample output from the **show ip igmp snooping mrouter vlan 1** command:

Note In this example, Fa0/3 is a dynamically learned router port, and Fa0/2 is a configured static router port.

```
Router# show ip igmp snooping mrouter vlan 1

Vlan    ports
----    -----
   1    Fa0/2(static), Fa0/3(dynamic)
```

Related commands

Command	Description
ip igmp snooping	Globally enables IGMP snooping. IGMP snooping must be globally enabled in order to be enabled on a VLAN.
ip igmp snooping vlan	Enables IGMP snooping on the VLAN interface.
ip igmp snooping vlan immediate-leave	Enables IGMP Immediate-Leave processing.
ip igmp snooping vlan mrouter	Configures a Layer 2 port as a multicast router port.
show mac-address-table multicast	Displays the Layer 2 multicast entries for a VLAN.

show ip igmp snooping rate-limit

To display the information about the IGMP-snooping rate limit, use the **show ip igmp snooping rate-limit** command in user EXEC or privileged EXEC mode.

show ip igmp snooping rate-limit [**statistics** | **vlan** *vlan-id*]

Syntax Description

statistics	(Optional) Displays IGMP-snooping statistics.
vlan *vlan-id*	(Optional) Specifies a VLAN; valid values are from 1 to 4094.

Defaults

This command has no default settings.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the Supervisor Engine 720.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to display the statistics for IGMP-snooping rate limiting:

```
Router# show ip igmp snooping rate-limit statistics

Max IGMP messages incoming rate : Not configured
Vlan   Incoming rate  Rate-limiting ON  Disable count  Time to Enable
-----+---------------+-----------------+---------------+---------------+
222   1000            No                0
111   5999            Yes               3              185
```

This example shows how to display IGMP-snooping rate-limit information for a specific VLAN:

```
Router# show ip igmp snooping rate-limit vlan 19

Max IGMP messages incoming rate : 200 pps
Vlan       Incoming IGMP rate (in pps)
--------+---------------------------------
19       200
```

Related Commands

Command	Description
ip igmp snooping rate	Sets the rate limit for IGMP-snooping packets.

show ip igmp snooping statistics

To display IGMPv3 statistics, use the **show ip igmp snooping statistics** command in user EXEC or privileged EXEC mode.

show ip igmp snooping statistics [**interface** *type* [*number*]} | **port-channel** *number* | **vlan** *vlan-id*]

Syntax Description

interface type	(Optional) Displays IGMP statistics for the specified interface type; possible valid values are **ethernet**, **fastethernet**, and **gigabitethernet**.
number	(Optional) Multicast-related statistics for the specified module and port; see the "Usage Guidelines" section for valid values.
port-channel *number*	(Optional) Displays multicast-related statistics for the specified port-channel; valid values are from 1 to 282.
vlan *vlan-id*	(Optional) Displays multicast-related statistics for the specified VLAN; valid values for *vlan-id* are from 1 to 4094.

Defaults

This command has no default settings.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The **show ip igmp snooping statistics** command displays the following statistics:

- List of ports that are members of a group
- Filter mode
- Reporter-address behind the port
- Additional information (such as the last-join and last-leave collected since the previous time that a **clear ip igmp snooping statistics** command was issued)

The *number* argument designates the module and port number. Valid values for *number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The **port-channel** *number* values from 257 to 282 are supported on the CSM and the FWSM only.

The #hosts behind the VLAN is displayed only if you define the max-hosts policy on the specified VLAN and enable the log policy for the specified VLAN.

Examples

This example shows how to display IGMPv3 statistics:

```
Router# show ip igmp snooping statistics interface FastEthernet5/1

IGMP Snooping statistics
Service-policy: Policy1policy tied with this interface
#Channels: 3
#hosts : 3
Query Rx: 2901 GS Query Rx: 0 V3 Query Tot Rx: 0
Join Rx: 8686 Leave Rx: 0 V3 Report Rx: 2300
Join Rx from router ports: 8684 Leave Rx from router ports: 0
Total Rx: 11587
Channel/Group         Interface  Reporter    Uptime     Last-Join  Last-Leave
10.7.20.1,239.1.1.1   F5/1       10.5.20.1   00:12:00   1:10:00    -
10.7.30.1,239.1.1.1   F5/1       10.5.30.1   00:50:10   1:10:02    0:30:02
10.7.40.1,239.1.1.1   F5/1       10.5.40.1   00:10:10   1:10:03    -
```

Table 9 describes the fields that are shown in the example.

Table 9 show ip igmp snooping statistics Field Descriptions

Field	Description
Service-policy: Policy1	Policy tied to this interface.
#Channels: 3	Number of channels behind the specified interface.
#hosts	Number of hosts behind the specified interface. This field is displayed only if max-hosts policy is used.

Related Commands

Command	Description
clear ip igmp snooping statistics	Clears the IGMP-snooping statistics.

show ip igmp ssm-mapping

To display information about Source Specific Multicast (SSM) mapping or to display the sources that SSM mapping uses for a particular group, use the **show ip igmp ssm-mapping** command in user EXEC or privileged EXEC mode.

show ip igmp [**vrf** *vrf-name*] **ssm-mapping** [*group-address*]

Syntax Description

vrf	(Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
group-address	(Optional) Address of the group about which to display SSM mapping information.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18) SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to display the sources that SSM mapping is using for a particular group, or would use for a group if SSM mapping were configured. If no SSM mapping is known for the specified group, and Domain Name System (DNS)-based SSM mapping is enabled, this command sends out a DNS query for the group. The DNS query initiates DNS-based SSM mapping for this group. If no SSM mapping group is specified by the *group-address* argument, this command displays the configured SSM mapping state.

Use the **vrf** *vrf-name* keyword and argument to displays SSM mapping information for a particular VRF.

Examples

The following example shows how to display information about the configured SSM mapping state:

```
Router# show ip igmp ssm-mapping

SSM Mapping  : Enabled
DNS Lookup   : Enabled
Mcast domain : ssm-map.cisco.com
Name servers : 10.0.0.0
               10.0.0.1
```

Table 10 describes the significant fields shown in the display.

Table 10 show ip igmp ssm-mapping Field Descriptions

Field	Description
SSM Mapping : Enabled	The SSM Mapping feature is enabled.
DNS Lookup : Enabled	DNS-based SSM mapping is enabled.
Mcast domain : ssm-map.cisco.com	Multicast domain.
Name servers : 10.0.0.0 10.0.0.1	Addresses of the configured named servers.

The following example shows how to display information about the configured DNS-based SSM mapping:

```
Router# show ip igmp ssm-mapping 232.1.1.4

Group address: 232.1.1.4
Database     : DNS
DNS name     : 4.1.1.232.ssm-map.cisco.com
Expire time  : 860000
Source list  : 172.16.8.5
             :172.16.8.6
```

Table 11 describes the significant fields shown in the display.

Table 11 show ip igmp ssm-mapping Field Descriptions

Field	Description
Group address: 232.1.1.4	The router has mapped group 232.1.1.4.
Database : DNS	Group mapping is performed via DNS.
DNS name : 4.1.1.232.ssm-map.cisco.com	Name of the DNS that performs group mapping.
Expire time : 860000	Cache time of the DNS registration record on the DNS server, in milliseconds.
Source list : 172.16.8.5 :172.16.8.6	The group address is mapped via DNS to these source addresses.

The following example shows how to display information about the configured static SSM mapping:

```
Router# show ip igmp ssm-mapping 232.1.1.4

Group address: 232.1.1.4
Database     : Static
Source list  : 172.16.8.5
             : 172.16.8.6
```

Table 12 describes the significant fields shown in the display.

Table 12 show ip igmp ssm-mapping Field Descriptions

Field	Description
Group address: 232.1.1.4	The address of the group with SSM mapping to the router.
Database : Static	Static SSM mapping is configured.
Source list : 172.16.8.5 : 172.16.8.6	Source addresses configured for static SSM mapping.

The following is sample output from the **show ip igmp ssm-mapping** command when no SSM mappings can be found:

```
Router# show ip igmp ssm-mapping 232.1.1.4

Can't resolve %i to source-mapping
```

Related Commands

Command	Description
ip igmp ssm-map enable	Enables SSM mapping for groups in a configured SSM range.
show ip igmp group	Displays the multicast groups with receivers that are directly connected to the router and that were learned through IGMP.

show ip igmp static-group class-map

To display the contents of Internet Group Management Protocol (IGMP) static group class map configurations and the interfaces using class maps, use the **show ip igmp static-group class-map** command in user EXEC or privileged EXEC mode.

show ip igmp static-group class-map [**interface** [*type number*]]

Syntax Description

interface	(Optional) Filters the output to display only the interfaces using class maps.
type number	(Optional) Interface type and number entered to filter the output to display only the class map attached to a particular interface.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(18)SXF5	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Use this command to display the contents of IGMP static group class map configurations and the interfaces using class maps.

Use this command with the optional **interface** keyword to filter the output to display only the interfaces using class maps.

Use this command with the optional **interface** keyword and *type number* arguments to filter the output to display only the class map attached to a particular interface.

Examples

The following is sample output from the **show ip igmp static-group class-map** command. The output is self-explanatory:

```
Router# show ip igmp static-group class-map

Class-map static1
  Group address range 228.8.8.7 to 228.8.8.9
  Group address 232.8.8.7, source address 10.1.1.10
  Interfaces using the classmap:
    Loopback0

Class-map static
  Group address range 232.7.7.7 to 232.7.7.9, source address 10.1.1.10
  Group address 227.7.7.7
  Group address range 227.7.7.7 to 227.7.7.9
  Group address 232.7.7.7, source address 10.1.1.10
  Interfaces using the classmap:
    Ethernet3/1
```

The following is sample output from the **show ip igmp static-group** command with the **interface** keyword. The output is self-explanatory.

```
Router# show ip igmp static-group class-map interface

Loopback0
  Class-map attached: static1

Ethernet3/1
  Class-map attached: static
```

The following is sample output from the **show ip igmp static-group** command with the **interface** keyword and *type number* arguments. The output is self-explanatory.

```
Router# show ip igmp static-group class-map interface Ethernet 3/1

Ethernet3/1
  Class-map attached: static
```

Related Commands

Command	Description
class-map type multicast-flows	Enters multicast-flows class-map configuration mode to create or modify IGMP static group class maps.
group (multicast-flows)	Defines the group entries to be associated with a IGMP static group class map.
ip igmp static-group	Configures static group membership entries on an interface.

show ip igmp udlr

To display unidirectional link routing (UDLR) information for directly connected multicast groups on interfaces that have a unidirectional link (UDL) helper address configured, use the **show ip igmp udlr** command in user EXEC or privileged EXEC mode.

show ip igmp udlr [*group-name* | *group-address* | *interface-type interface-number*]

Syntax Description

group-name | *group-address*	(Optional) Name or address of the multicast group for which to show UDLR information.
interface-type interface-number	(Optional) Interface type and number for which to show UDLR information.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(17d)SXB1	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command displays which groups are being forwarded and received over the UDL.

On the upstream router, this command shows which interface is a UDL interface and which IP multicast groups are being forwarded out that interface. The UDL Reporter is the IP address of the downstream interface on the receiving router. If there is more than one downstream router, this field shows which downstream router forwarded the IGMP host report to the upstream router over the ground-based network. This report is forwarded over the UDL so that all downstream routers know which groups have already been requested by other downstream routers and additional IGMP host reports are suppressed.

On the downstream router, this command (in the Interface field) shows which local interface received an IGMP host report (from a directly connected host for a specific group). The UDL Reporter is the IP address of the router that had forwarded the IGMP host report to the upstream router over the ground-based network. The UDL Interfaces column shows the interface on which IP multicast packets are being received.

Examples

The following is sample output of the **show ip igmp udlr** command on an upstream router:

```
upstream-rtr# show ip igmp udlr

IGMP UDLR Status, UDL Interfaces: Serial0
Group Address    Interface            UDL Reporter     Reporter Expires
224.2.127.254    Serial0              10.0.0.2         00:02:12
224.0.1.40       Serial0              10.0.0.2         00:02:11
225.7.7.7        Serial0              10.0.0.2         00:02:15
```

The following is sample output of the **show ip igmp udlr** command on a downstream router:

```
downstream-rtr# show ip igmp udlr

IGMP UDLR Status, UDL Interfaces: Serial0
Group Address    Interface            UDL Reporter     Reporter Expires
224.2.127.254    Serial0              10.0.0.2         00:02:49
224.0.1.40       Serial0              10.0.0.2         00:02:48
225.7.7.7        Serial0              10.0.0.2         00:02:52
```

Table 13 describes the significant fields shown in the first display.

Table 13 show ip igmp udlr Field Descriptions

Field	Description
Group Address	All groups helpered by the UDL Reporter on the interface.
Interface	Interface type and number to which the group is connected.
UDL Reporter	IP address of the router on the UDL network that is IGMP helpering for the group.
Reporter Expires	How soon the UDL Reporter will become inactive, in hours:minutes:seconds. This can occur under the following conditions: • The UDL Reporter has become nonoperational. • The link or network to the reporter has become nonoperational. • The group member attached to the UDL Reporter has left the group.

show ip mcache

Note Effective with Cisco IOS Release 12.2(33)SRE, the **show ip mcache** command is not available in Cisco IOS software.

To display the contents of the IP fast-switching cache, use the **show ip mcache** command in user EXEC or privileged EXEC mode.

show ip mcache [**vrf** *vrf-name*] [*group-address* | *group-name*] [*source-address* | *source-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the contents of the IP fast-switching cache associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
group-address | *group-name*	(Optional) The address or name of the group for which to display the fast-switching cache. Can be either a Class D IP address or a Domain Name System (DNS) name.
source-address | *source-name*	(Optional) The specified source address or name for which to display a single multicast cache entry. Can be either a unicast IP address or a DNS name.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was implemented on the Supervisor Engine 720 only.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)M	This command was removed.
12.2(33)SRE	This command was removed.

Examples

The following is sample output from the **show ip mcache** privileged EXEC command when multicast distributed switching (MDS) is in effect:

```
Router# show ip mcache

IP Multicast Fast-Switching Cache
(*, 239.2.3.4), Fddi3/0/0, Last used: mds
  Tunnel3         MAC Header: 5000602F9C150000603E473F60AAAA030000000800 (Fddi3/0/0)
  Tunnel0         MAC Header: 5000602F9C150000603E473F60AAAA030000000800 (Fddi3/0/0)
  Tunnel1         MAC Header: 5000602F9C150000603E473F60AAAA030000000800 (Fddi3/0/0)
```

Table 14 describes the significant fields shown in the display.

Table 14 show ip mcache Field Descriptions

Field	Description
*	Source address or source wildcard (*).
239.2.3.4	Destination address.
Fddi	Incoming or expected interface on which the packet should be received.
Last used:	Latest time the entry was accessed for a packet that was successfully fast switched. The word “Semi-fast” indicates that the first part of the outgoing interface list is fast switched and the rest of the list is process level switched.
Tunnel0 MAC Header:	Outgoing interface list and respective MAC header that is used when rewriting the packet for output. If the interface is a tunnel, the MAC header will show the real next hop MAC header and then, in parentheses, the real interface name.

show ip mfib

To display the forwarding entries and interfaces in the IPv4 Multicast Forwarding Information Base (MFIB), use the **show ip mfib** command in user EXEC or privileged EXEC mode.

show ip mfib [**vrf** {*vrf-name* | *****}] [**all** | **linkscope** | *group-address/mask* | *group-address* [*source-address*] | *source-address group-address*] [**verbose**]

Syntax Description

vrf {*vrf-name* | *****}	(Optional) Displays forwarding entries and interfaces in the IPv4 MFIB associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances. After specifying the optional **vrf** keyword, you must specify either: • *vrf-name*—Name of an MVRF. Displays forwarding entries and interfaces in the IPv4 MFIB associated with the MVRF specified for the *vrf-name* argument. • *****—Displays a summary of traffic statistics from the IPv4 MFIB for sources and groups associated with all tables (all MVRF tables and the global table).
all	(Optional) Displays forwarding entries and interfaces in the IPv4 MFIB for both linkscope (reserved) and non-linkscope (non-reserved) groups.
linkscope	(Optional) Displays forwarding entries and interfaces in the IPv4 MFIB for linkscope (reserved) groups.
group-address/mask	(Optional) Multicast group address followed by a forward slash (**/**) and group mask, in dotted decimal notation, which is referred to as a (*, G/mask) entry.
group-address	(Optional) Multicast group address.
source-address	(Optional) Multicast source address.
verbose	(Optional) Includes hardware-related IPv4 MFIB flags and Cisco Express Forwarding (CEF)-related adjacency information.

Command Default

If no optional keywords or arguments are entered, forwarding entries and interfaces in the IPv4 MFIB associated with nonlinkscope multicast groups are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **show ip mfib** command to display IPv4 MFIB forwarding entries and interfaces.

A forwarding entry in the IPv4 MFIB has flags that determine the default forwarding and signaling behavior to use for packets matching the entry. The entry also has per-interface flags that further specify the forwarding behavior for packets received or forwarded on specific interfaces.

Note For a description of the significant MFIB and Multicast Routing Information Base (MRIB) forwarding entries and interface flags, see the "Multicast Forwarding Information Base Overview" module.

Examples

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

```
Router# show ip mfib 232.1.1.1

 (192.168.1.2,232.1.1.1) Flags:
   SW Forwarding: 3786/10/28/2, Other: 0/0/0
   Serial1/0 Flags: A
   Ethernet0/0 Flags: F NS
     Pkts: 3786/0
```

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

```
Router# show ip mfib
Entry Flags:    C - Directly Connected, S - Signal, IA - Inherit A flag,
                XO - Data Rate Above Threshold, K - Keepalive
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
                A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward
Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   FS Pkt Count/PS Pkt Count
Default
 (*,224.0.0.0/4) Flags: C HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: 0/0/0
 (*,224.0.1.40) Flags: C HW
   SW Forwarding: 0/0/0/0, Other: 0/0/0
   HW Forwarding:   0/0/0/0, Other: 0/0/0
   GigabitEthernet0/0/0 Flags: F IC NS
     Pkts: 0/0
```

Table 15 describes the significant fields shown in the displays.

Table 15 show ip mfib Field Descriptions

Field	Description
SW Forwarding:	Statistics on the packets that are received from and forwarded out of at least one interface (packet count/packets per second/average packet size/kbits per second).
Other:	Statistics on received packets. These counters include statistics about the packets received and forwarded and packets received but not forwarded.
Pkts	Total number of packets received and forwarded since the creation of the multicast forwarding state to which this counter applies.

show ip mfib active

To display information from the IPv4 Multicast Forwarding Information Base (MFIB) about the rate at which active multicast sources are sending to multicast groups, use the **show ip mfib active** command in user EXEC or privileged EXEC mode.

show ip mfib [**vrf** {*vrf-name* | *}] [**all** | **linkscope** | *group-address/mask* | *group-address* [*source-address*] | *source-address group-address*] **active** [*kbps*]

Syntax Description

vrf {*vrf-name* | *}	(Optional) Displays the rate at which active multicast sources are sending to multicast groups associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances. After specifying the optional **vrf** keyword, you must specify either: • *vrf-name*—Name of an MVRF. Displays the rate at which active multicast sources are sending to multicast groups associated with the MVRF specified for the *vrf-name* argument. • *—Displays the rate at which active multicast sources are sending to multicast groups for all tables (all MVRF tables and the global table).
all	(Optional) Displays the rate at which active multicast sources are sending to both linkscope (reserved) and nonlinkscope (nonreserved) groups.
linkscope	(Optional) Displays the rate at which active multicast sources are sending to linkscope (reserved) groups.
group-address/mask	(Optional) Multicast group address followed by a forward slash (/) and group mask, in dotted decimal notation, which is referred to as a (*, G/mask) entry.
group-address	(Optional) Multicast group address.
source-address	(Optional) Multicast source address.
kbps	(Optional) Kilobits per second (kbps).

Command Default

If no optional keywords or arguments are entered, all active sources sending to nonlinkscope multicast groups at a rate greater than or less than 4 kbps are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **show ip mfib active** command to display active multicast streams forwarding at a rate greater than or equal to the value specified for the optional *kbps* argument. If no value is specified for the optional *kbps* argument, this command will display all active sources sending to nonlinkscope (nonreserved) multicast groups at a rate greater than or equal to 4 kbps.

Note In some cases, you may need to specify a sufficiently low value for the *kbps* argument to ensure that low data rate streams are displayed (multicast streams sending traffic at a rate less than 4 kbps).

Examples

The following sample output from the **show ip mfib active** command displays the active multicast sources that are sending traffic to nonlinkscope multicast groups at a rate greater than or equal to 1 kbps on a router participating in a multicast network.

```
Router# show ip mfib active 1

Active Multicast Sources - sending >= 1 kbps
Default
Group: 239.1.1.1
  Source: 192.168.1.2,
   SW Rate: 10 pps/2 kbps(1sec), 2 kbps(last 121 sec)
```

Table 16 describes the significant fields shown in the display.

Table 16 show ip mfib active Field Descriptions

Field	Description
Active Multicast Sources - sending >=	Active multicast sources sending traffic at a rate greater than or equal to the value specified after the equal (=) sign, in kbps.
Group:	Multicast group address.
Source:	Multicast source address.
SW Rate:	Rate at which active sources are sending traffic to multicast groups.

show ip mfib count

To display summary traffic statistics from the IPv4 Multicast Forwarding Information Base (MFIB) about multicast sources and groups, use the **show ip mfib count** command in user EXEC or privileged EXEC mode.

show ip mfib [**vrf** {*vrf-name* | *}] [**all** | **linkscope** | *group-address/mask* | *group-address* [*source-address*] | *source-address group-address*] **count**

Syntax Description

vrf {*vrf-name* | *}	(Optional) Displays a summary of traffic statistics from the IPv4 MFIB about multicast sources and groups associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances. After specifying the optional **vrf** keyword, you must specify either: • *vrf-name*—Name of an MVRF. Displays a summary of traffic statistics from the IPv4 MFIB for sources and groups associated with the MVRF specified for the *vrf-name* argument. • *—Displays a summary of traffic statistics from the IPv4 MFIB for sources and groups associated with all tables (all MVRF tables and the global table).
all	(Optional) Displays a summary of traffic statistics from the IPv4 MFIB about multicast sources sending to both linkscope (reserved) and nonlinkscope (nonreserved) groups.
linkscope	(Optional) Displays a summary of traffic statistics from the IPv4 MFIB about multicast sources sending to linkscope (reserved) groups.
group-address/mask	(Optional) Multicast group address followed by a forward slash (/) and group mask, in dotted decimal notation, referred to as a (*, G/mask) entry.
group-address	(Optional) Multicast group address.
source-address	(Optional) Multicast source address.

Command Default

If no optional keywords or arguments are entered, a summary of traffic statistics from the IPv4 MFIB about multicast sources sending traffic to nonreserved (nonlinkscope) multicast groups is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
Cisco IOS Release 15.1(1)S	This command was modified. New counters were added to the output to show (*,G/m) and the total number of unique groups in the database.

Usage Guidelines

Use the **show ip mfib count** command to display a summary of traffic statistics from the IPv4 MFIB about multicast sources and groups, including number of packets, packets per second, average packet size, and kilobytes per second.

Examples

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

```
Router# show ip mfib count

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:      Total/RPF failed/Other drops(OIF-null, rate-limit etc)
Default
 11 routes, 6 (*,G)s, 3 (*,G/m)s
Group: 224.0.0.0/4
  RP-tree,
   SW Forwarding: 0/0/0/0, Other: 0/0/0
Group: 224.0.1.40
  RP-tree,
   SW Forwarding: 0/0/0/0, Other: 0/0/0
Group: 232.0.0.0/8
  RP-tree,
   SW Forwarding: 0/0/0/0, Other: 0/0/0
Group: 232.1.1.1
  Source: 10.1.1.1,
   SW Forwarding: 0/0/0/0, Other: 0/0/0
  Totals - Source count: 1, Packet count: 0
Group: 232.1.1.2
  Source: 10.1.1.1,
   SW Forwarding: 0/0/0/0, Other: 0/0/0
  Totals - Source count: 1, Packet count: 25044

Groups: 3, 0.66 average sources per group
```

Table 17 describes the significant fields shown in the display.

Table 17 show ip mfib count Field Descriptions

Field	Description
Forwarding Counts	Statistics on the packets that are received and forwarded out an interface. This section tracks the following statistics: • Pkt Count/—Total number of packets received and forwarded since the multicast forwarding state to which this counter applies was created. • Pkts per second/—Number of packets received and forwarded per second. • Avg Pkt Size/ —Total number of bytes divided by the total number of packets for this multicast forwarding state. There is no direct display for the total number of bytes. You can calculate the total number of bytes by multiplying the average packet size by the packet count. • Kilobits per second—Bytes per second divided by packets per second divided by 1000.

Table 17 show ip mfib count Field Descriptions (continued)

Field	Description
Other counts	Statistics on the received packets. These counters include statistics about the packets received and forwarded and packets received but not forwarded. This section tracks the following statistics: • Total/—Total number of packets received. • RPF failed/—Number of packets not forwarded due to a failed Reverse Path Forwarding (RPF) or acceptance check (when bidirectional Protocol Independent Multicast (PIM) is configured). • Other drops(OIF-null, rate-limit etc)—Number of packets not forwarded for reasons other than an RPF failure or acceptance check (such as the outgoing interface [OIF] list was empty or because the packets were discarded because of a configuration that was enabled).
Default	Summary information about all the routes and groups in the MFIB database. This section tracks the following statistics: • routes—Total number of routes in the MFIB database. • (*,G)s—Total number of (*, G) entries in the MFIB database. • (*,G/m)s—Total number of groups that have a specific mask in the MFIB database.
Group:	Summary information about counters for (*, G) and the range of (S, G) states for one particular group G. The following RP-tree: and Source: output fields contain information about the individual states belonging to this group. **Note** For Source Specific Multicast (PIM-SSM) range groups, the Group: displays are statistical. All SSM range (S, G) states are individual, unrelated SSM channels.
RP-tree:	Counters for the (*, G) state of this group G. These counters are displayed only for groups that have a forwarding mode that do not forward packets on the shared tree. These (*, G) groups are bidirectional PIM and PIM sparse mode (PIM-SM) groups. There are no RP-tree displays for PIM SSM range groups.
SW Forwarding:	Statistics on the packets that are received from and forwarded to at least one interface.
Other:	Statistics on received packets. These counters include statistics about the packets received and forwarded and packets received but not forwarded.
Totals -	This section tracks the following statistics: • Source count—Total number of multicast sources sending to multicast groups in the IPv4 MFIB. • Packet count—Total number of packets received and forwarded. This count is cumulative for all sources in the source count.
Groups	The total number of unique groups in the MFIB database, and the average number of sources per group.

show ip mfib interface

To display IPv4 Multicast Forwarding Information Base (MFIB)-related information about interfaces and their forwarding status, use the **show ip mfib interface** command in user EXEC or privileged EXEC mode.

show ip mfib interface [**control** | **data**] [*type number*]

Syntax Description

control	(Optional) Displays interfaces in the IPv4 MFIB, and any associated control information.
data	(Optional) Displays IPv4 MFIB forwarding information about interfaces.
type number	(Optional) Interface type and number.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Examples

The following is sample output from the **show ip mfib interface** command:

```
Router# show ip mfib interface

IPv4 Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
    Initialization State: MFIB Init Running
    Total signalling packets queued: 0
    Process Status: may enable - 3 - pid 202
    Tables 1/1/0 (active/mrib/io)
MFIB interface             status    CEF-based output
                                    [configured,available]
Ethernet0/0                up      [yes       ,yes      ]
Ethernet0/1                down    [yes       ,no       ]
Ethernet0/2                down    [yes       ,no       ]
Ethernet0/3                down    [yes       ,no       ]
Ethernet1/0                up      [yes       ,yes      ]
Ethernet1/1                down    [yes       ,no       ]
Ethernet1/2                down    [yes       ,no       ]
Ethernet1/3                down    [yes       ,no       ]
Serial2/0                  down    [yes       ,no       ]
Serial2/1                  down    [yes       ,no       ]
Serial2/2                  down    [yes       ,no       ]
Serial2/3                  down    [yes       ,no       ]
Serial3/0                  down    [yes       ,no       ]
Serial3/1                  down    [yes       ,no       ]
Serial3/2                  down    [yes       ,no       ]
Serial3/3                  down    [yes       ,no       ]
Loopback0                  up      [yes       ,yes      ]
Tunnel0                    up      [yes       ,yes      ]
```

Table 18 describes the significant fields shown in the display.

Table 18 show ip mfib interface Field Descriptions

Field	Description
IPv4 Multicast Forwarding (MFIB) status:	Displays the status of interfaces in the IPv4 MFIB.
Configuration Status	IPv4 MFIB configuration status on the interface.
Initialization State	Intialization state of the IPv4 MFIB.
MFIB interface	Lists available interfaces for which to display IPv4 MFIB status.
status	Status of the interface.
CEF-based output	Provides information about the status of Cisco Express Forwarding on the MFIB interface. This section tracks whether Cisco Express Forwarding has been configured and whether it is available on the interface.

The following is sample output from the **show ip mfib interface control** command:

```
Router# show ip mfib interface control

                                                MFIB Forwarding
MFIB interface                    IP   PIM     Process        CEF
                                             (Conf/Oper)  (Conf/Oper)
Ethernet0/0                       up   on     yes  yes     yes  yes
Ethernet0/1                       off  off    yes  no      yes  no
Ethernet0/2                       off  off    yes  no      yes  no
Ethernet0/3                       off  off    yes  no      yes  no
Ethernet1/0                       up   on     yes  yes     yes  yes
Ethernet1/1                       off  off    yes  no      yes  no
Ethernet1/2                       off  off    yes  no      yes  no
Ethernet1/3                       off  off    yes  no      yes  no
Serial2/0                         off  off    yes  no      yes  no
Serial2/1                         off  off    yes  no      yes  no
Serial2/2                         off  off    yes  no      yes  no
Serial2/3                         off  off    yes  no      yes  no
Serial3/0                         off  off    yes  no      yes  no
Serial3/1                         off  off    yes  no      yes  no
Serial3/2                         off  off    yes  no      yes  no
Serial3/3                         off  off    yes  no      yes  no
Loopback0                         up   on     yes  yes     yes  yes
Tunnel0                           up   reg    yes  out     yes  out
```

Table 19 describes the significant fields shown in the display.

Table 19 show ip mfib interface control Field Descriptions

Field	Description
MFIB interface	Lists available interfaces for which to display IPv4 MFIB status.
IP	Displays the status of IP on the available interfaces.
PIM	Displays the status of PIM on the available interfaces.

Table 19 show ip mfib interface control Field Descriptions (continued)

Field	Description
Process	Displays the configuration and operational status of the IPv4 MFIB on the available interfaces.
CEF	Displays the configuration and operational status of CEF on the available interfaces.

The following is sample output from the **show ip mfib interface data** command:

```
Router# show ip mfib interface data

                                                   MFIB Forwarding
MFIB interface                          Type    Process         CEF
                                                          (Active/Available)
 Ethernet0/0                            None    yes        yes    yes
 Ethernet1/0                            None    yes        yes    yes
 Loopback0                              None    yes        yes    yes
 Tunnel0                                None    out        out    out
```

Table 20 describes the significant fields shown in the display.

Table 20 show ip mfib interface data Field Descriptions

Field	Description
MFIB interface	Lists available interfaces for which to display IPv4 MFIB forwarding status.
Type	Next hop type value (for example, IPv4, IPv6, LSM, LSM NBMA, MDTv4, MDTv6, None, v4Dec, and v6Dec).
Process	Displays the status of the IPv4 MFIB process.
CEF	Displays the status of Cisco Express Forwarding (whether it is active and available) for IPv4 MFIB interfaces.

show ip mfib route

To display the forwarding entries and interfaces in the IPv4 Multicast Forwarding Information Base (MFIB) without packet header information and forwarding counters, use the **show ip mfib route** command in user EXEC or privileged EXEC mode.

show ip mfib [**vrf** {*vrf-name* | *}] **route** [**all** | **linkscope** | *group-address/mask* | *group-address* [*source-address*] | *source-address group-address*] [**detail** | **internal**]

Syntax Description

vrf {*vrf-name* | *}	(Optional) Displays the forwarding entries and interfaces in the IPv4 MFIB associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances. After specifying the optional **vrf** keyword, you must specify either: • *vrf-name*—Name of an MVRF. Displays the forwarding entries and interfaces in the IPv4 MFIB associated with the MVRF specified for the *vrf-name* argument. • *—Displays the forwarding entries and interfaces in the IPv4 MFIB associated with all tables (all MVRF tables and the global table).
all	(Optional) Displays the forwarding entries and interfaces in the IPv4 MFIB for both linkscope (reserved) and nonlinkscope (nonreserved) groups.
linkscope	(Optional) Displays the forwarding entries and interfaces in the IPv4 MFIB for linkscope (reserved) groups.
group-address/mask	(Optional) Multicast group address followed by a forward slash (/) and group mask, in dotted decimal notation (referred to as a (*, G/mask) entry).
group-address	(Optional) Multicast group address.
source-address	(Optional) Multicast source address.
detail	(Optional) For use by Cisco technical support. Displays detailed information about the routes in the IPv4 MFIB.
internal	(Optional) For use by Cisco technical support. Displays the internal data structures for the routes in the IPv4 MFIB.

Command Default

If no optional keywords or arguments are entered, forwarding entries and interfaces in the IPv4 MFIB associated with nonlinkscope multicast groups are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **show ip mfib route** command to display the forwarding entries and interfaces in the IPv4 MFIB. Unlike the **show ip mfib** command, the output from this command does not display packet header information and IPv4 MFIB packet and forwarding counters.

Note For a description of the significant MFIB and Multicast Routing Information Base (MRIB) forwarding entries and interface flags, see the "Multicast Forwarding Information Base (MFIB) Overview" module.

Examples

The following is sample output from the **show ip mfib route** command:

```
Router# show ip mfib route

Default
 (*,224.0.0.0/4) C
 (*,224.0.1.39) C
   Loopback0 NS
   GigabitEthernet1/0/0 F NS
   GigabitEthernet0/0/0 NS
 (192.168.6.6,224.0.1.39)
   GigabitEthernet1/0/0 A NS
 (*,224.0.1.40) C
   Loopback0 F IC NS
   GigabitEthernet1/0/0 F NS
 (192.168.6.6,224.0.1.40)
   Loopback0 F IC NS
   GigabitEthernet1/0/0 A
 (*,232.0.0.0/8)
 (*,239.1.1.1) C
   GigabitEthernet1/0/0 A
 (192.168.1.2,239.1.1.1)
   GigabitEthernet1/0/0 F NS
   GigabitEthernet0/0/0 A
```

Related Commands

Command	Description
show ip mfib	Displays the forwarding entries and interfaces in the IPv4 MFIB.

show ip mfib status

To display the general IPv4 Multicast Forwarding Information Base (MFIB) configuration and operational status, use the **show ip mfib status** command in user EXEC or privileged EXEC mode.

show ip mfib status

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **show ip mfib status** command to find such information as whether the IPv4 MFIB is enabled and running.

Examples

The following is sample output from the **show ip mfib status** command:

```
Router# show ip mfib status

IPv4 Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
    Initialization State: MFIB Init Running
    Total signalling packets queued: 0
    Process Status: may enable - 3 - pid 202
    Tables 1/1/0 (active/mrib/io)
```

show ip mfib summary

To display summary information about the number of IPv4 Multicast Forwarding Information Base (MFIB) entries (including linkscope groups) and interfaces, use the **show ip mfib summary** command in user EXEC or privileged EXEC mode.

show ip mfib [**vrf** {*vrf-name* | *}] **summary** [**detail** | **internal**]

Syntax Description

vrf {*vrf-name* | *}	(Optional) Displays summary information about the number of IPv4 MFIB entries and interfaces associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances. After specifying the optional **vrf** keyword, you must specify either: • *vrf-name*—Name of an MVRF. Displays summary information about the number of IPv4 MFIB entries and interfaces associated with the MVRF specified for the *vrf-name* argument. • *—Displays summary information about the number of IPv4 MFIB entries and interfaces associated with all tables (all MVRF tables and the global table).
detail	(Optional) For use by Cisco technical support. Displays more detailed information about the IPv4 MFIB entries and interfaces in the summary of the IPv4 MFIB.
internal	(Optional) For use by Cisco technical support. Displays internal data structures associated with IPv4 MFIB entries and interfaces in the summary of the IPv4 MFIB.

Command Default

If no optional keywords or arguments are entered, this command displays summary information about the number of IPv4 MFIB entries and interfaces from the global table.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

The **show ip mfib summary** command shows the IPv4 multicast routing table in abbreviated form. The command displays only the number of IPv4 MFIB entries, the number of (*, G), (S, G), and (*, G/m) entries, and the number of IPv4 MFIB interfaces.

The **show ip mfib summary** command counts all entries, including linkscope entries.

Examples

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

```
Router# show ip mfib summary

Default
 15 prefixes (15/0/0 fwd/non-fwd/deleted)
 28 ioitems (28/0/0 fwd/non-fwd/deleted)
 Forwarding prefixes: [3 (S,G), 9 (*,G), 3 (*,G/m)]
 Table id 0x0, instance 0x4B23B54
 Database: epoch 0
```

Table 21 describes the significant fields shown in the display.

Table 21 show ip mfib summary Field Descriptions

Field	Description
15 prefixes (15/0/0 fwd/non-fwd/deleted)	Number of prefixes in the IPv4 MFIB and a summary of the status of the prefixes (forwarded/nonforwarded/deleted), including linkscope prefixes.
28 ioitems (28/0/0 fwd/non-fwd/deleted)	Number of interfaces in the IPv4 MFIB.
Forwarding prefixes: [3 (S,G), 9 (*,G), 3 (*,G/m)]	Total number of (S, G), (*, G), and (*, G/m) prefixes in the IPv4 MFIB.

show ip mpacket

Note Effective with Cisco IOS Release 15.0(1)M and Cisco IOS Release 12.2(33)SRE, the **show ip mpacket** is not available in Cisco IOS software.

To display the contents of the circular cache-header buffer, use the **show ip mpacket** command in privileged EXEC mode.

show ip mpacket [**vrf** *vrf-name*] [*group-address* | *group-name*] [*source-address* | *source-name*] [**quality**] [**detail**] [**read-only**]

Syntax Description

vrf *vrf-name*	(Optional) Displays the contents of the circular cache-header buffer associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
group-address | *group-name*	(Optional) The specified group address or group name for which matching cache headers are displayed.
source-address | *source-name*	(Optional) The specified source address or source name for which matching cache headers are displayed.
quality	(Optional) Displays Real-Time Transport Protocol (RTP) data quality.
detail	(Optional) Displays summary information and displays the rest of the IP header fields on an additional line, plus the first 8 bytes after the IP header (usually the User Datagram Protocol [UDP] port numbers).
read-only	(Optional) Specifies that the circular buffer will not be cleared of the IP multicast packet headers.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.1	This command was introduced.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was implemented on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **quality** and **read-only** keywords were added.
15.0(1)M	This command was removed.
12.2(33)SRE	This command was removed.

Usage Guidelines

This command is applicable only when the **ip multicast cache-headers** command is in effect.

Each time this command is entered, a new buffer is allocated. The summary display (when the **detail** keyword is omitted) shows the IP packet identifier, time-to-live (TTL) value, source and destination IP addresses, and a local time stamp when the packet was received.

All the arguments and keywords can be used in the same command in any combination.

Examples

The following is sample output from the **show ip mpacket** command for the group named smallgroup:

```
Router# show ip mpacket smallgroup

IP Multicast Header Cache - entry count:6, next index: 7
Key: id/ttl timestamp (name) source group

D782/117 206416.908 (company1.example.com) 192.168.228.10 224.5.6.7
7302/113 206417.908 (example.edu) 172.16.2.17 224.5.6.7
6CB2/114 206417.412 (company2.example.com) 172.16.19.40 224.5.6.7
D782/117 206417.868 (company1.example.com) 192.168.228.10 224.5.6.7
E2E9/123 206418.488 (example.com) 239.1.8.10 224.5.6.7
1CA7/127 206418.544 (company4.example.com) 192.168.6.10 224.5.6.7
```

Table 22 describes the significant fields shown in the display.

Table 22 show ip mpacket Field Descriptions

Field	Description
entry count	Number of packets cached (one packet for each line in the display). The cache has lines numbered from 0 to 1024.
next index	The index for the next element in the cache.
id	Identification number of the IP packet.
ttl	Current TTL of the packet.
timestamp	Time-stamp sequence number of the packet.
(name)	Domain Name System (DNS) name of the source sending to the group. Name appears in parentheses.
source	IP address of the source sending to the group.
group	Multicast group address to which the packet is sent. In this example, the group address is the group name smallgroup.

Related Commands

Command	Description
ip multicast cache-headers	Allocates a circular buffer to store IP multicast packet headers that the router receives.

show ip mr proxy

To list the Reverse Path Forwarding (RPF) vector proxies received on a multicast router discovered by the Cisco IOS software, use the **show ip mr proxy** command in user EXEC or privileged EXEC mode.

show ip mr [*group*] **proxy**

Syntax Description

group	(Optional) Multicast routing group.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(30)S	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to determine if an RPF vector proxy is received on a core router.

Examples

The following is sample output from the **show ip mr proxy** command:

```
Router# show ip mr proxy

Proxy Table
Proxy        Assigner      Origin   Uptime/Expire
10.0.0.1     10.0.2.2      PIM      00:02:16/00:02:14
```

Table 23 describes the fields shown in the display.

Table 23 show ip mr proxy Field Descriptions

Field	Description
Proxy	Proxy value.
Assigner	IP address of the router assigning the proxy vector.
Origin	Protocol origin.
Uptime/Expires	Uptime shows how long (in hours:minutes:seconds) the entry has been in the table. Expires shows how long (in hours:minutes:seconds or in milliseconds) until the entry will be removed from the IP multicast routing table.

Related Commands

Command	Description
show ip pim interface	Displays information about interfaces configured for PIM.
show ip pim neighbor	Displays information about PIM neighbors.

show ip mrib client

To display information about the clients of the IPv4 Multicast Routing Information Base (MRIB), use the **show ip mrib client** command in user EXEC or privileged EXEC mode.

show ip mrib [**vrf** *vrf-name*] **client** [**filter**] [**name** *client-name* [**:***connection-id*]]

Syntax Description

vrf *vrf-name*	(Optional) Displays information about clients of the IPv4 MRIB associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
filter	(Optional) Displays information about the IPv4 MRIB flags each client owns and the flags each client is interested in.
name *client-name*	(Optional) Displays the name an IPv4 MRIB client. **Note** The names of the MRIB clients that can be specified for the *client-name* argument can be found by entering the **show ip mrib client** command with no optional keywords or arguments.
:*connection-id*	(Optional) The connection ID associated with the IPv4 MRIB client. The colon is required. **Note** The connection ID is typically the Process ID (PID) value associated with the MRIB client.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use the **show ip mrib client** command to display information about the clients of the IPv4 MRIB. When this command is entered with the optional **filter** keyword, the output will display additional information, including the IPv4 MRIB flags each clients owns and the flags each client is interested in.

Note For a description of the significant MFIB and MRIB forwarding entries and interface flags, see the "Multicast Forwarding Information Base (MFIB) Overview" module.

Examples

The following is sample output from the **show ip mrib client** command:

```
Router# show ip mrib client

IP MRIB client-connections
MRIB Trans for MVRF #0     table:199    (connection id 1)
IPv4_mfib(0x5474934):7.196       (connection id 2)
```

The following is sample output from the **show ip mrib client** command with the **filter** and **name** keywords and *client-name* and **:***connection-id* arguments:

```
Router# show ip mrib client filter name IPv4_mfib(0x5474934):7.196

IP MRIB client-connections
IPv4_mfib(0x5474934):7.196      (connection id 2)
  interest filter:
    entry attributes:  S C IA K ET DDE
    interface attributes:  A DP F IC NS SP
    groups:
      include 0.0.0.0/0
    interfaces:
      include All
  ownership filter:
    groups:
      include 0.0.0.0/0
    interfaces:
      include All
```

show ip mrib route

To display the routes in the IPv4 Multicast Routing Information Base (MRIB) table, use the **show ip mrib route** command in user EXEC or privileged EXEC mode.

show ip mrib [**vrf** *vrf-name*] **route** [**reserved** | [*source-address* | *] [*group-address*[*/mask*]]]

Syntax Description

vrf *vrf-name*	(Optional) Displays routes in the IPv4 MRIB associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
reserved	(Optional) Displays routes in the IPv4 MRIB associated with linkscope groups.
source-address	(Optional) Multicast source address.
*	(Optional) Displays shared tree entries in the IPv4 MRIB.
group-address	(Optional) Multicast group address.
group-address/mask	(Optional) Multicast group address followed by a forward slash (/) and group mask, in dotted decimal notation, which is referred to as a (*, G/mask) entry.

Command Default

If this command is entered without the optional **reserved** keyword, the output displays only routes in the IPv4 MRIB associated with nonreserved (nonlinkscope) groups.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use the **show ip mrib route c**ommand to display the IPv4 MRIB table. All entries are created by various clients of the IPv4 MRIB, such as, Protocol Independent Multicast (PIM) and the IPv4 MFIB. The flags on each entry or interface act as a communication mechanism between the various clients of the IPv4 MRIB.

Note For a description of the significant MFIB and MRIB forwarding entries and interface flags, see the "Multicast Forwarding Information Base (MFIB) Overview" module.

Examples

The following is sample output from the **show ip mrib route** command:

```
Router# show ip mrib route

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, D - Drop
    ET - Data Rate Exceeds Threshold,K - Keepalive,DDE - Data Driven Event
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
    LD - Local Disinterest, MD - mCAC Denied

(*,224.0.0.0/4) Flags: C

(*,224.0.1.39) RPF nbr: 0.0.0.0 Flags: C
  Ethernet1/0 Flags: F NS
  Ethernet0/0 Flags: NS
  Loopback0 Flags: NS

(*,224.0.1.40) RPF nbr: 0.0.0.0 Flags: C
  Ethernet1/0 Flags: F NS
  Loopback0 Flags: F IC NS

(*,232.0.0.0/8) Flags:

(192.168.6.6,224.0.1.39) RPF nbr: 192.168.123.2 Flags:
  Ethernet1/0 Flags: A NS

(192.168.6.6,224.0.1.40) RPF nbr: 192.168.123.2 Flags:
  Ethernet1/0 Flags: A
  Loopback0 Flags: F IC NS
```

show ip mrib route summary

To display the total number of routes and interfaces in the IPv4 Multicast Routing Information Base (MRIB), use the **show ip mrib route summary** command in user EXEC or privileged EXEC mode.

show ip mrib [**vrf** *vrf-name*] **route summary**

Syntax Description

vrf *vrf-name*	(Optional) Displays the total number of routes and interfaces in the IPv4 MRIB associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use the **show ip mrib summary** command to display the total number of routes and interfaces in the IPv4 Multicast Routing Information Base (MRIB).

Note The total number of routes and interfaces displayed in the output includes routes and interfaces associated with both reserved (linkscope) and nonreserved multicast groups.

Examples

The following is sample out from the **show ip mrib summary** command:

```
Router# show ip mrib summary

MRIB Route-DB Summary
  No. of (*,G) routes = 11
  No. of (S,G) routes = 2
  No. of Route x Interfaces (RxI) = 25
```

show ip mrm interface

To display Multicast Routing Monitor (MRM) information related to interfaces, use the **show ip mrm interface** command in user EXEC or privileged EXEC mode.

show ip mrm interface [*type number*]

Syntax Description

type number	(Optional) Interface type and number for which to display MRM interface information.

Command Default

If no interface is specified for the *type* and *number* arguments, information about all interfaces participating in MRM is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to display which interfaces are participating in MRM, in which roles, and whether the interfaces are up or down.

Examples

The following is sample output from the **show ip mrm interface** command:

```
Router# show ip mrm interface

Interface           Address         Mode                Status
Ethernet0           10.0.0.1        Test-Sender         Up
Ethernet1           10.0.0.10       Test-Receiver       Up
```

Table 24 describes the fields shown in the display.

Table 24 show ip mrm interface Field Descriptions

Field	Description
Interface	List of interfaces on this router that serve as a Test Sender or Test Receiver.
Address	IP address of the interface.

Table 24 show ip mrm interface Field Descriptions

Field	Description
Mode	Role that the interface plays in MRM, either Test Sender or Test Receiver.
Status	Status of the interface.

Related Commands

Command	Description
ip mrm	Configures an interface to operate as a Test Sender or Test Receiver, or both, for MRM.

show ip mrm manager

To display information about a Multicast Routing Monitor (MRM) test, use the **show ip mrm manager** command in user EXEC or privileged EXEC mode.

show ip mrm manager [*test-name*]

Syntax Description

test-name	(Optional) Name of the MRM test for which to display information.

Command Default

If no test name is specified for the *test-name* argument, information about all Managers is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to display status information and the parameters configured for an MRM test.

Examples

The following is sample output from the **show ip mrm manager** command executed at two different times:

```
Router# show ip mrm manager test

Manager:test/10.0.0.0 is running, expire:1d00h
  Beacon interval/holdtime/ttl:60/86400/32
  Group:239.1.2.3, UDP port test-packet/status-report:16384/65535
  Test senders:
    10.0.0.1 /Ack
  Test receivers:
    10.0.0.2 /Ack

Router# show ip mrm manager test

Manager:test/10.0.0.0 is not running
  Beacon interval/holdtime/ttl:60/86400/32
  Group:239.1.2.3, UDP port test-packet/status-report:16384/65535
  Test senders:
    10.0.0.1
  Test receivers:
    10.0.0.2
```

Table 25 describes the fields shown in the display.

Table 25 show ip mrm manager Field Descriptions

Field	Description
Manager	Status of the test.
Beacon interval/holdtime/ttl	The interval at which beacon messages are sent (Beacon interval), the duration of the test period (holdtime), and the time-to-live value of beacon messages. **Note** Beacon parameters are controlled with the **beacon** command. By default, beacon messages are sent at an interval of 60 seconds; the duration of the test period is 86400 seconds (1 day); and the time-to-live of beacon messages is 32 hops.
Group	IP multicast group that the Test Receiver will listen to, as configured by the **manager** command.
UDP port test-packet/status-report	User Datagram Protocol (UDP) port number to which test packets are sent by a Test Sender and status reports are sent by a Test Receiver. **Note** The UDP port numbers to which test packets are sent by a Test Sender and status reports are sent by a Test Receiver are controlled with the **udp-port** command. By default, the Test Sender uses UDP port number 16834 to send test packets, and the Test Receiver uses UDP port number 65535 to send status reports.
Test senders	IP address of Test Senders.
Test receivers	IP address of Test Receivers.

Related Commands

Command	Description
beacon	Changes the frequency, duration, or scope of beacon messages that the Manager sends to the Test Sender and Test Receiver.
ip mrm manager	Specifies the name of an MRM test to be created or modified, and enters MRM manager configuration mode.
manager	Specifies that an interface is the Manager for MRM, and specifies the multicast group address the Test Receiver will listen to.
udp-port	Changes the UDP port numbers to which the Test Sender sends test packets or the Test Receiver sends status reports.

show ip mrm status-report

To display the status reports in the Multicast Routing Monitor (MRM) status report cache, use the **show ip mrm status-report** command in user EXEC or privileged EXEC mode.

show ip mrm status-report [*ip-address*]

Syntax Description

ip-address	(Optional) IP address of a Test Receiver for which to display status reports.

Command Default

If no IP address is specified for the optional *ip-address* argument, all status reports in the MRM status report cache are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show ip mrm status-report** command during your MRM test period to learn if any errors are reported. The Manager immediately displays error reports and sends error reports, if any, to the circular status report cache. The cache holds up to 1024 lines, with one line for each error report.

No errors reported indicates that the Test Receiver is receiving test packets without loss or duplicates from the Test Sender.

Use the **show ip mrm status-report** command with the optional *ip-address* argument to restrict the output to display only status reports sent by the Test Receiver at the specified IP address. If no IP address is specified for the optional *ip-address* argument, all status reports in the MRM status report cache are displayed.

Use the **clear ip mrm status-report** command to clear the MRM status report cache.

Examples

The following is sample output from the **show ip mrm status-report** command:

```
Router# show ip mrm status-report

IP MRM status report cache:
Timestamp        Manager         Test Receiver   Pkt Loss/Dup (%)      Ehsr
*Apr 20 07:36:08 10.0.0.0        10.0.0.1        5            (20%)    0
```

```
*Apr 20 07:36:09 10.0.0.0        10.0.0.1        10          (40%)    0
*Apr 20 07:36:10 10.0.0.0        10.0.0.1        15          (60%)    0
```

Table 26 describes the fields shown in the display.

Table 26 show ip mrm status-report Field Descriptions

Field	Description
Timestamp	Time when the status report arrived in the cache. Month and date, hours:minutes:seconds.
Manager	IP address of the Manager.
Test Receiver	IP address of the Test Receiver.
Pkt Loss/Dup	Number of packets lost or duplicated.
(%)	Percentage of packets lost or duplicated. Loss percentage is calculated based on the **packet-delay** value of the **senders** command, which defaults to 200 milliseconds (or 5 packets per second). If the default for the **window** keyword (5 seconds) is not changed, then the Test Receiver expects 5 packets per second for 5 seconds = 25 packets. If the Test Receiver receives only 15 packets, then 25 – 15 = 10 lost packets. Lost packets divided by packets expected equals loss percentage; 10/25 equals a loss percentage of 40 percent. A negative percentage indicates duplicate packets were received. If the packet loss reaches 100 percent, the Test Receiver will not send periodic reports until the packet loss decreases to less than 100 percent.
Ehsr	Extended highest sequence number received from Real-Time Transport Protocol (RTP).

Related Commands

Command	Description
clear ip mrm status-report	Clears the MRM status report cache.

show ip mroute

To display the contents of the multicast routing (mroute) table, use the **show ip mroute** command in user EXEC or privileged EXEC mode.

show ip mroute [**vrf** *vrf-name*] [[**active** [*kbps*] [**interface** *type number*] | **bidirectional** | **count** [**terse**] | **dense** | **interface** *type number* | **proxy** | **pruned** | **sparse** | **ssm** | **static** | **summary**] | [*group-address* [*source-address*]] [**count** [**terse**] | **interface** *type number* | **proxy** | **pruned** | **summary**] | [*source-address group-address*] [**count** [**terse**] | **interface** *type number* | **proxy** | **pruned** | **summary**] | [*group-address*] **active** [*kbps*] [**interface** *type number* | **verbose**]]

Syntax Description

vrf *vrf-name*	(Optional) Filters the output to display only the contents of the mroute table that pertain to the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
active *kbps*	(Optional) Displays the rate that active sources are sending to multicast groups, in kilobits per second (kbps). Active sources are those sending at the *kbps* value or higher. The range is from 1 to 4294967295. The *kbps* default is 4 kbps.
interface *type number*	(Optional) Filters the output to display only mroute table information related to the interface specified for the *type number* arguments.
bidirectional	(Optional) Filters the output to display only information about bidirectional routes in the mroute table.
count	(Optional) Displays statistics about the group and source, including number of packets, packets per second, average packet size, and bytes per second.
terse	(Optional) Filters the output to display a subset of mroute statistics, excluding source and group statistics for each mroute entry in the mroute table.
dense	(Optional) Filters the output to display only information about dense mode routes in the mroute table.
proxy	(Optional) Displays information about Reverse Path Forwarding (RPF) vector proxies received on a multicast router.
pruned	(Optional) Filters the output to display only information about pruned routes in the mroute table.
sparse	(Optional) Filters the output to display only information about sparse mode routes in the mroute table.
ssm	(Optional) Filters the output to display only the Source Specific Multicast (SSM) routes in the mroute table.
static	(Optional) Filters the output to display only the static routes in the mroute table.
summary	(Optional) Filters the output to display a one-line, abbreviated summary of each entry in the mroute table.
group-address	(Optional) IP address or Domain Name System (DNS) name of a multicast group.
source-address	(Optional) IP address or DNS name of a multicast source.
verbose	(Optional) Displays additional information.

Command Default

If you omit all optional arguments and keywords, the **show ip mroute** command displays all entries in the mroute table.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(5)T	This command was modified. The H flag for multicast multilayer switching (MMLS) was added in the output display.
12.1(3)T	This command was modified. The U, s, and I flags for SSM were introduced.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.0(30)S	This command was modified. The **proxy** keyword and the v and V flags were added for the Multicast VPN Inter-AS Support feature.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S. The **vrf** keyword and *vrf-name* argument were added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.3	This command was modified. The Z, Y, and y flags were introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.4(6)T	This command was modified. The **terse** keyword was added.
12.4(7)	This command was modified. The **terse** keyword was added.
12.2(18)SXF2	This command was modified. The **terse** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The **terse** keyword was added. The **proxy** keyword and the v and V flags were added for the Multicast VPN Inter-AS Support feature.
12.2(31)SB2	This command was modified. The E flag for the Multicast VPN Extranet Support feature was introduced. The **proxy** keyword and the v and V flags were added for the Multicast VPN Inter-AS Support feature. The **terse** keyword was added.
12.2(33)SXH	This command was modified. The **proxy** keyword and the v and V flags were added for the Multicast VPN Inter-AS Support feature.
12.2(33)SRC	This command was modified. The E flag for the Multicast VPN Extranet Support feature was introduced.
12.2(33)SRE	This command was modified. The **verbose** keyword was added.
12.4(20)T	This command was modified. The **proxy** keyword and the v and V flags were added for the Multicast VPN Inter-AS Support feature.
15.0(1)M	This command was modified. The E flag for the Multicast VPN Extranet Support feature was introduced.

Release	Modification
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.
Cisco IOS XE Release 3.2S	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

Use the **show ip mroute** command to display information about mroute entries in the mroute table. The Cisco IOS software populates the multicast routing table by creating (S, G) entries from (*, G) entries. The asterisk (*) refers to all source addresses, the "S" refers to a single source address, and the "G" is the destination multicast group address. In creating (S, G) entries, the software uses the best path to that destination group found in the unicast routing table (that is, through RPF).

Use the **clear ip mroute** command to delete entries from the mroute table.

Examples

The following is sample output from the **show ip mroute** command for a router operating in sparse mode:

```
Router# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.0.255.3), uptime 5:29:15, RP is 192.168.37.2, flags: SC
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Sparse, 5:29:15/0:02:57

(192.168.46.0/24, 224.0.255.3), uptime 5:29:15, expires 0:02:59, flags: C
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1
  Outgoing interface list:
    Ethernet0, Forward/Sparse, 5:29:15/0:02:57
```

The following is sample output from the **show ip mroute** command with the IP multicast group address 232.6.6.6 specified:

```
Router# show ip mroute 232.6.6.6

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Outgoing interface flags:H - Hardware switched
Timers:Uptime/Expires
Interface state:Interface, Next-Hop or VCD, State/Mode

(*, 232.6.6.6), 00:01:20/00:02:59, RP 224.0.0.0, flags:sSJP
  Incoming interface:Null, RPF nbr 224.0.0.0
  Outgoing interface list:Null
```

```
(10.2.2.2, 232.6.6.6), 00:01:20/00:02:59, flags:CTI
  Incoming interface:Ethernet3/3, RPF nbr 224.0.0.0
  Outgoing interface list:
    Ethernet3/1, Forward/Sparse-Dense, 00:00:36/00:02:35
```

The following is sample output from the **show ip mroute** command for a router operating in dense mode. This output displays the contents of the IP multicast routing table for the multicast group named cbone-audio.

```
Router# show ip mroute cbone-audio

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.0.255.1), uptime 0:57:31, expires 0:02:59, RP is 224.0.0.0, flags: DC
  Incoming interface: Null, RPF neighbor 224.0.0.0, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Dense, 0:57:31/0:02:52
    Tunnel0, Forward/Dense, 0:56:55/0:01:28

(192.168.37.100, 224.0.255.1), uptime 20:20:00, expires 0:02:55, flags: C
  Incoming interface: Tunnel0, RPF neighbor 10.20.37.33, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Dense, 20:20:00/0:02:52
```

The following is sample output from the **show ip mroute** command that shows the virtual circuit descriptor (VCD) value, because an ATM interface with Protocol Independent Multicast (PIM) multipoint signaling is enabled:

```
Router# show ip mroute 224.1.1.1

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 224.1.1.1), 00:03:57/00:02:54, RP 172.16.0.0, flags: SJ
  Incoming interface: Null, RPF nbr 224.0.0.0224.0.0.0
  Outgoing interface list:
    ATM0/0, VCD 14, Forward/Sparse, 00:03:57/00:02:53
```

The following is sample output from the **show ip mroute** command with the **summary** keyword:

```
Router# show ip mroute summary

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
```

```
       U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel,
       Y - Joined MDT-data group, y - Sending to MDT-data group
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.255.255.255), 2d16h/00:02:30, RP 172.16.10.13, flags: SJPC

(*, 224.2.127.253), 00:58:18/00:02:00, RP 172.16.10.13, flags: SJC

(*, 224.1.127.255), 00:58:21/00:02:03, RP 172.16.10.13, flags: SJC

(*, 224.2.127.254), 2d16h/00:00:00, RP 172.16.10.13, flags: SJCL
  (172.16.160.67, 224.2.127.254), 00:02:46/00:00:12, flags: CLJT
  (172.16.244.217, 224.2.127.254), 00:02:15/00:00:40, flags: CLJT
  (172.16.8.33, 224.2.127.254), 00:00:25/00:02:32, flags: CLJT
  (172.16.2.62, 224.2.127.254), 00:00:51/00:02:03, flags: CLJT
  (172.16.8.3, 224.2.127.254), 00:00:26/00:02:33, flags: CLJT
  (172.16.60.189, 224.2.127.254), 00:03:47/00:00:46, flags: CLJT
```

The following is sample output from the **show ip mroute** command with the **active** keyword:

```
Router# show ip mroute active 4

Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
   Source: 192.168.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)

Group: 224.2.207.215, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

Table 27 describes the significant fields shown in the displays.

Table 27 show ip mroute Field Descriptions

Field	Description
Flags:	Provides information about the entry. • D—Dense. Entry is operating in dense mode. • S—Sparse. Entry is operating in sparse mode. • B—Bidir Group. Indicates that a multicast group is operating in bidirectional mode. • s—SSM Group. Indicates that a multicast group is within the SSM range of IP addresses. This flag is reset if the SSM range changes. • C—Connected. A member of the multicast group is present on the directly connected interface.

Table 27 show ip mroute Field Descriptions (continued)

Field	Description
Flags: (continued)	• L—Local. The router itself is a member of the multicast group. Groups are joined locally by the **ip igmp join-group** command (for the configured group), the **ip sap listen** command (for the well-known session directory groups), and rendezvous point (RP) mapping (for the well-known groups 224.0.1.39 and 224.0.1.40). Locally joined groups are not fast switched. • P—Pruned. Route has been pruned. The Cisco IOS software keeps this information so that a downstream member can join the source. • R—RP-bit set. Indicates that the (S, G) entry is pointing toward the RP. This flag typically indicates a prune state along the shared tree for a particular source. • F—Register flag. Indicates that the software is registering for a multicast source. • T—SPT-bit set. Indicates that packets have been received on the shortest path source tree. • J—Join SPT. For (*, G) entries, indicates that the rate of traffic flowing down the shared tree is exceeding the SPT-Threshold set for the group. (The default SPT-Threshold setting is 0 kbps.) When the J - Join shortest path tree (SPT) flag is set, the next (S, G) packet received down the shared tree triggers an (S, G) join in the direction of the source, thereby causing the router to join the source tree. For (S, G) entries, indicates that the entry was created because the SPT-Threshold for the group was exceeded. When the J - Join SPT flag is set for (S, G) entries, the router monitors the traffic rate on the source tree and attempts to switch back to the shared tree for this source if the traffic rate on the source tree falls below the SPT-Threshold of the group for more than 1 minute.

Table 27 show ip mroute Field Descriptions (continued)

Field	Description
Flags: (continued)	**Note** The router measures the traffic rate on the shared tree and compares the measured rate to the SPT-Threshold of the group once every second. If the traffic rate exceeds the SPT-Threshold, the J - Join SPT flag is set on the (*, G) entry until the next measurement of the traffic rate. The flag is cleared when the next packet arrives on the shared tree and a new measurement interval is started. If the default SPT-Threshold value of 0 kbps is used for the group, the J - Join SPT flag is always set on (*, G) entries and is never cleared. When the default SPT-Threshold value is used, the router immediately switches to the shortest path source tree when traffic from a new source is received. • M—MSDP created entry. Indicates that a (*, G) entry was learned through a Multicast Source Discovery Protocol (MSDP) peer. This flag is applicable only for an RP running MSDP. • E—Extranet source mroute entry. Indicates that a (*, G) or (S, G) entry in the VRF routing table is a source Multicast VRF (MVRF) entry and has extranet receiver MVRF entries linked to it. • X—Proxy Join Timer Running. Indicates that the proxy join timer is running. This flag is set only for (S, G) entries of an RP or "turnaround" router. A "turnaround" router is located at the intersection of a shared path (*, G) tree and the shortest path from the source to the RP. • A—Candidate for MSDP Advertisement. Indicates that an (S, G) entry was advertised through an MSDP peer. This flag is applicable only for an RP running MSDP. • U—URD. Indicates that a URL Rendezvous Directory (URD) channel subscription report was received for the (S, G) entry. • I—Received Source Specific Host Report. Indicates that an (S, G) entry was created by an (S, G) report. This (S, G) report could have been created by Internet Group Management Protocol Version 3 (IGMPv3), URD, or IGMP v3lite. This flag is set only on the designated router (DR). • Z—Multicast Tunnel. Indicates that this entry is an IP multicast group that belongs to the Multicast Distribution Tree (MDT) tunnel. All packets received for this IP multicast state are sent to the MDT tunnel for decapsulation. • Y—Joined MDT-data group. Indicates that the traffic was received through an MDT tunnel that was set up specifically for this source and group. This flag is set in Virtual Private Network (VPN) mroute tables only.

Table 27 show ip mroute Field Descriptions (continued)

Field	Description
Flags: (continued)	• y—Sending to MDT-data group. Indicates that the traffic was sent through an MDT tunnel that was set up specifically for this source and group. This flag is set in VPN mroute tables only.
Outgoing interface flags:	Provides information about the entry. • H—Hardware switched. Indicates that a multicast Multilayer Switching (MMLS) forwarding path has been established for this entry.
Timers:Uptime/Expires	"Uptime" indicates per interface how long (in hours, minutes, and seconds) the entry has been in the IP multicast routing table. "Expires" indicates per interface how long (in hours, minutes, and seconds) until the entry will be removed from the IP multicast routing table.
Interface state:	Indicates the state of the incoming or outgoing interface. • Interface. Indicates the type and number of the interface listed in the incoming or outgoing interface list. • Next-Hop or VCD. "Next-hop" specifies the IP address of the downstream neighbor. "VCD" specifies the virtual circuit descriptor number. "VCD0" means the group is using the static map virtual circuit. • State/Mode. "State" indicates that packets will either be forwarded, pruned, or null on the interface depending on whether there are restrictions due to access lists or a time-to-live (TTL) threshold. "Mode" indicates whether the interface is operating in dense, sparse, or sparse-dense mode.
(*, 224.0.255.1) and (192.168.37.100, 224.0.255.1)	Entry in the IP multicast routing table. The entry consists of the IP address of the source followed by the IP address of the multicast group. An asterisk (*) in place of the source router indicates all sources. Entries in the first format are referred to as (*, G) or "star comma G" entries. Entries in the second format are referred to as (S, G) or "S comma G" entries. (*, G) entries are used to build (S, G) entries.
RP	Address of the RP router. For routers and access servers operating in sparse mode, this address is always 224.0.0.0.
flags:	Information about the entry.
Incoming interface:	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.

Table 27 show ip mroute Field Descriptions (continued)

Field	Description
RPF neighbor or RPF nbr	IP address of the upstream router to the source. Tunneling indicates that this router is sending data to the RP encapsulated in register packets. The hexadecimal number in parentheses indicates to which RP it is registering. Each bit indicates a different RP if multiple RPs per group are used. If an asterisk (*) appears after the IP address in this field, the RPF neighbor has been learned through an assert.
Outgoing interface list:	Interfaces through which packets will be forwarded. When the **ip pim nbma-mode** command is enabled on the interface, the IP address of the Protocol Independent Multicast (PIM) neighbor is also displayed.

The following is sample output from the **show ip mroute** command with the **count** keyword:

```
Router# show ip mroute count

IP Multicast Statistics
4045 routes using 2280688 bytes of memory
41 groups, 97.65 average sources per group
Forwarding Counts:Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second
Other counts:Total/RPF failed/Other drops(OIF-null, rate-limit etc)

Group:239.0.18.1, Source count:200, Packets forwarded:348232, Packets received:348551
  RP-tree:Forwarding:12/0/218/0, Other:12/0/0
  Source:10.1.1.1/32, Forwarding:1763/1/776/9, Other:1764/0/1
  Source:10.1.1.2/32, Forwarding:1763/1/777/9, Other:1764/0/1
  Source:10.1.1.3/32, Forwarding:1763/1/783/10, Other:1764/0/1
  Source:10.1.1.4/32, Forwarding:1762/1/789/10, Other:1763/0/1
  Source:10.1.1.5/32, Forwarding:1762/1/768/10, Other:1763/0/1
  Source:10.1.1.6/32, Forwarding:1793/1/778/10, Other:1794/0/1
  Source:10.1.1.7/32, Forwarding:1793/1/763/10, Other:1794/0/1
  Source:10.1.1.8/32, Forwarding:1793/1/785/10, Other:1794/0/1
  Source:10.1.1.9/32, Forwarding:1793/1/764/9, Other:1794/0/1
  Source:10.1.1.10/32, Forwarding:1791/1/774/10, Other:1792/0/1
  Source:10.1.2.1/32, Forwarding:1689/1/780/10, Other:1691/0/2
  Source:10.1.2.2/32, Forwarding:1689/1/782/10, Other:1691/0/2
  Source:10.1.2.3/32, Forwarding:1689/1/776/9, Other:1691/0/2
.
.
.

Group:239.0.18.132, Source count:0, Packets forwarded:8810, Packets received:8810
  RP-tree:Forwarding:8810/7/780/49, Other:8810/0/0

Group:239.0.17.132, Source count:0, Packets forwarded:704491, Packets received:704491
  RP-tree:Forwarding:704491/639/782/4009, Other:704491/0/0

Group:239.0.17.133, Source count:0, Packets forwarded:704441, Packets received:704441
  RP-tree:Forwarding:704441/639/782/3988, Other:704441/0/0

Group:239.0.18.133, Source count:0, Packets forwarded:8810, Packets received:8810
  RP-tree:Forwarding:8810/8/786/49, Other:8810/0/0

Group:239.0.18.193, Source count:0, Packets forwarded:0, Packets received:0

Group:239.0.17.193, Source count:0, Packets forwarded:0, Packets received:0

Group:239.0.18.134, Source count:0, Packets forwarded:8803, Packets received:8803
  RP-tree:Forwarding:8803/8/774/49, Other:8803/0/0
```

Note The RP-tree field is displayed only for non-SSM groups that have a (*, G) entry and a positive packet received count.

The following is sample output from the **show ip mroute** command with the **count** and **terse** keywords:

```
Router# show ip mroute count terse

IP Multicast Statistics
4 routes using 2610 bytes of memory
3 groups, 0.33 average sources per group
```

Table 28 describes the significant fields shown in the displays.

Table 28 show ip mroute count Field Descriptions

Field	Description
Group:	Summary statistics for traffic on an IP multicast group G. This row is displayed only for non-SSM groups.
Forwarding Counts:	Statistics on the packets that are received and forwarded to at least one interface. **Note** There is no specific command to clear only the forwarding counters; you can clear only the actual multicast forwarding state with the **clear ip mroute** command. Issuing this command will cause interruption of traffic forwarding.
Pkt Count/	Total number of packets received and forwarded since the multicast forwarding state to which this counter applies was created.
Pkts per second/	Number of packets received and forwarded per second. On an IP multicast fast-switching platform, this number is the number of packets during the last second. Other platforms may use a different approach to calculate this number. Please refer to the platform documentation for more information.
Avg Pkt Size/	Total number of bytes divided by the total number of packets for this multicast forwarding state. There is no direct display for the total number of bytes. You can calculate the total number of bytes by multiplying the average packet size by the packet count.
Kilobits per second	Bytes per second divided by packets per second divided by 1000. On an IP multicast fast-switching platform, the number of packets per second is the number of packets during the last second. Other platforms may use a different approach to calculate this number. Please refer to the platform documentation for more information.
Other counts:	Statistics on the received packets. These counters include statistics about the packets received and forwarded and packets received but not forwarded.
Total/	Total number of packets received.
RPF failed/	Number of packets not forwarded due to a failed RPF or acceptance check (when bidir-PIM is configured).

Table 28 show ip mroute count Field Descriptions (continued)

Field	Description
Other drops (OIF-null, rate-limit etc)	Number of packets not forwarded for reasons other than an RPF or acceptance check (such as the OIF list was empty or because the packets were discarded because of a configuration, such as **ip multicast rate-limit**, was enabled).
Group:	Summary information about counters for (*, G) and the range of (S, G) states for one particular group G. The following RP-tree: and Source: output fields contain information about the individual states belonging to this group. **Note** For SSM range groups, the groups displayed after the Group output field are statistical. All SSM range (S, G) states are individual, unrelated SSM channels.
Source count:	Number of (S, G) states for this group G. Individual (S, G) counters are detailed in the output field rows.
Packets forwarded:	The sum of the packets detailed in the Forwarding Counts fields for this IP multicast group G. This field is the sum of the RP-tree and all Source fields for this group G.
Packets received:	The sum of packets detailed in the Other counts fields for this IP multicast group G. This field is the sum of the Other counts and Pkt Count fields of the RP-tree and Source rows for this group G.
RP-tree:	Counters for the (*, G) state of this group G. These counters are displayed only for groups that have a forwarding mode that does not forward packets on the shared tree. These (*, G) groups are bidir-PIM and PIM sparse mode (PIM-SM) groups. There are no RP-tree displays for PIM dense mode (PIM-DM) and SSM range groups.
Source:	Counters for an individual (S, G) state of this group G. There are no (S, G) states for bidir-PIM groups.

Related Commands

Command	Description
clear ip mroute	Deletes entries from the mroute table.

show ip msdp count

To display the number of sources and groups originated in Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages and the number of SA messages from an MSDP peer in the SA cache, use the **show ip msdp count** command in user EXEC or privileged EXEC mode.

show ip msdp [**vrf** *vrf-name*] **count** [*as-number*]

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
as-number	(Optional) The number of sources and groups originated in SA messages from the specified autonomous system number.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(7)	This command was modified to display information about the number of SA messages from each MSDP peer in the SA cache.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720 only.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **ip msdp cache-sa-state** command must be configured for this command to have any output.

Examples

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

```
Router# show ip msdp count

SA State per Peer Counters, <Peer>: <# SA learned>
 224.135.250.116: 24
 172.16.240.253: 3964
 172.16.253.19: 10
 172.16.170.110: 11
```

```
SA State per ASN Counters, <asn>: <# sources>/<# groups>
 Total entries: 4009
 ?: 192/98, 9: 1/1, 14: 107/57, 17: 7/5
 18: 4/3, 25: 23/17, 26: 39/27, 27: 2/2
 32: 19/7, 38: 2/1, 52: 4/4, 57: 1/1
 68: 4/4, 73: 12/8, 81: 19/1, 87: 9/6
 .
 .
 .
```

Table 29 describes the significant fields shown in the display.

Table 29 show ip msdp count Field Descriptions

Field	Description
224.135.250.116: 24	MSDP peer with IP address 224.135.250.116: 24 SA messages from the MSDP peer in the SA cache.
Total entries	Total number of SA entries in the SA cache.
9: 1/1	Autonomous system 9: 1 source/1 group.

Related Commands

Command	Description
ip msdp cache-sa-state	Enables the router to create SA state.

show ip msdp peer

To display detailed information about Multicast Source Discovery Protocol (MSDP) peers, use the **show ip msdp peer** command in user EXEC or privileged EXEC mode.

show ip msdp [**vrf** *vrf-name*] **peer** [*peer-address* | *peer-name*] [**accepted-sas** | **advertised-sas**]

Syntax Description

vrf *vrf-name*	(Optional) Displays information about MSDP peers associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
peer-address | *peer-name*	(Optional) Domain Name System (DNS) name or IP address of the MSDP peer for which information is displayed.
accepted-sas	(Optional) Displays information about Source-Active (SA) messages received by the MSDP peer.
advertised-sas	(Optional) Displays information about SA messages advertised to the MSDP peer.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(7)	This command was modified. The output was modified to display information about the Source Active (SA) message limit configured using the **ip msdp sa-limit** command.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	This command was implemented on the Supervisor Engine 720 only.
12.4(2)T	This command was modified. The output was modified to display whether an MSDP peer has message digest 5 (MD5) password authentication enabled.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Examples

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

```
Router# show ip msdp peer 224.135.250.116

MSDP Peer 224.135.250.116 (rtp5-rp1.cisco.com), AS 109 (configured AS)
Description:
 Connection status:
   State: Up, Resets: 9, Connection source: Loopback2 (228.69.199.17)
   Uptime(Downtime): 1d10h, Messages sent/received: 436765/429062
   Output messages discarded: 0
   Connection and counters cleared 1w2d     ago
 SA Filtering:
   Input (S,G) filter: none, route-map: none
   Input RP filter: none, route-map: none
   Output (S,G) filter: none, route-map: none
   Output RP filter: none, route-map: none
 SA-Requests:
   Input filter: none
   Sending SA-Requests to peer: disabled
 Peer ttl threshold: 0
 SAs learned from this peer: 32, SAs limit: 500
 Input queue size: 0, Output queue size: 0
```

Table 30 describes the significant fields shown in the display.

Table 30 show ip msdp peer Field Descriptions

Field	Description
MSDP Peer	IP address of the MSDP peer.
AS	Autonomous system to which the MSDP peer belongs.
State:	State of the MSDP peer.
Connection source:	Interface used to obtain the IP address for the TCP local connection address.
Uptime (Downtime):	Days and hours the MSDP peer is up or down. If the time is less than 24 hours, it is shown in terms of hours:minutes:seconds.
Messages sent/received:	Number of SA messages sent to the MSDP peer/number of SA messages received from the MSDP peer.
SA Filtering:	Information regarding access list filtering of SA input and output, if any.
SA-Requests:	Information regarding access list filtering of SA requests, if any.
SAs learned from this peer:	Number of SA messages from the MSDP peer in the SA cache.
SAs limit:	SA message limit for this MSDP peer.

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

show ip msdp rpf-peer

To display the unique Multicast Source Discovery Protocol (MSDP) peer information from which a router will accept Source-Active (SA) messages originating from the specified rendezvous point (RP), use the **show ip msdp rpf-peer** command in user EXEC or privileged EXEC mode.

show ip msdp [**vrf** *vrf-name*] **rpf-peer** *rp-address*

Syntax Description

vrf *vrf-name*	(Optional) Displays MSDP information about a peer from which the router will accept SA messages that originated from an RP associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
rp-address	Address of the rendezvous point (RP).

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.0(27)S	This command was integrated into Cisco IOS Release 12.0(27)S.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use this command when you need MSDP information about a peer from which the router will accept SA messages that originated from an RP. The **ip msdp rfc-3618 rpf-rules** command must be configured for the **show ip msdp rpf-peer** command to generate output.

Examples

The following is sample output for the **show ip msdp rpf-peer** command:

```
Router# show ip msdp rpf-peer 10.0.0.0

RPF peer information for ? (25.8.8.8)
RPF peer: ? (2.2.2.3)
RPF route/mask: 0.0.0.0/0
RPF rule: Peer is IGP next hop of best route
RPF type: unicast (rip)
```

Table 31 describes the significant fields shown in the display.

Table 31 show ip msdp rpf Field Descriptions

Field	Description
RPF peer information for	Reverse Path Forwarding (RPF) peer address for the specified RP address. The question mark (?) indicates that the system does not find a name for that particular address.
RPF peer:	Peer address from which this device would accept MSDP SAs originated by the specified RP address. The question mark (?) indicates that the system does not find a name for that particular address.
RPF route/mask:	Network and mask of the RP address that the system determines from the route lookups that it used to choose the RPF peer.
RPF rule:	Rule used to determine the RPF peer for the specified RP address.
RPF type:	Route lookup or protocol used to choose the RPF peer for the specified RP address.

Related Commands

Command	Description
ip msdp rpf rfc3618	Enables IETF RFC 3618-compliant MSDP peer-RPF forwarding rules.

show ip msdp sa-cache

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

show ip msdp [**vrf** *vrf-name*] **sa-cache** [*group-address* | *source-address* | *group-name* | *source-name*] [*group-address* | *source-address* | *group-name* | *source-name*] [*as-number*] [**rejected-sa** [**detail**] [**read-only**]]

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
group-address | *source-address* | *group-name* | *source-name*	(Optional) Group address, source address, group name, or source name of the group or source about which (S, G) state information is displayed. If two addresses or names are specified, an (S, G) entry corresponding to those addresses is displayed. If only one group address is specified, all sources for that group are displayed. If no options are specified, the entire Source-Active (SA) cache is displayed.
as-number	(Optional) Autonomous system (AS) number from which the SA message originated.
rejected-sa	(Optional) Displays the most recently received and rejected MSDP SA messages.
detail	(Optional) Displays detailed information about the IP address of the MSDP peer that sent the SA message and the reason that the SA message was rejected.
read-only	(Optional) Checkpoints the rejected SA cache. Once checkpointed, the rejected SA cache is emptied.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

By default, (S,G) state is cached.

Rejected SA messages are cached only if the **ip msdp cache-rejected-sa** command is configured.

Use the **show ip msdp sa-cache** with the optional **rejected-sa** keyword to display SA messages stored in the rejected SA cache. When the **detail** keyword is added to the command string, the output includes the IP address of the MSDP peer router that sent the SA message and the reason that the SA message was rejected.

When the optional **read-only** keyword is added to the command string, the router checkpoints the rejected SA cache, which ensures that a consistent snapshot of the rejected SA cache is displayed in the output. After being checkpointed, the rejected SA cache is cleared.

Note Checkpointing the rejected SA cache requires that the router make a second copy of the rejected SA cache, which could cause the command to fail if the router is low on memory.

When the optional **read-only** keyword is not added to the command string, the router displays rejected MSDP SA messages out of the active rejected SA cache, which could result in inconsistent display output if rejected SA message entries are overwritten by rejected SA message entries that are captured as the output is being processed for display.

Examples

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

```
Router# show ip msdp sa-cache

MSDP Source-Active Cache - 2398 entries
(172.16.41.33, 238.105.148.0), RP 172.16.3.111, MBGP/AS 704, 2d10h/00:05:33
(172.16.112.8, 224.2.0.1), RP 192.168.200.65, MBGP/AS 10888, 00:03:21/00:02:38
(172.16.10.13, 227.37.32.1), RP 192.168.3.92, MBGP/AS 704, 05:22:20/00:03:32
(172.16.66.18, 233.0.0.1), RP 192.168.3.111, MBGP/AS 704, 2d10h/00:05:35
(172.16.66.148, 233.0.0.1), RP 192.168.3.111, MBGP/AS 704, 2d10h/00:05:35
(172.16.10.13, 227.37.32.2), RP 192.168.3.92, MBGP/AS 704, 00:44:30/00:01:31
(172.16.70.203, 224.2.236.2), RP 192.168.253.7, MBGP/AS 3582, 02:34:16/00:05:49
(172.18.42.104, 236.195.56.2), RP 192.168.3.92, MBGP/AS 704, 04:21:13/00:05:22
(172.16.10.13, 227.37.32.3), RP 192.168.3.92, MBGP/AS 704, 00:44:30/00:02:31
(172.18.15.43, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 6d09h/00:05:35
(172.18.15.111, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 16:18:08/00:05:35
(172.18.21.45, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 16:18:08/00:05:35
(172.18.15.75, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 08:40:52/00:05:35
(172.18.15.100, 224.0.92.3), RP 192.168.200.65, MBGP/AS 10888, 08:40:52/00:05:35
(172.16.10.13, 227.37.32.6), RP 192.168.3.92, MBGP/AS 704, 00:45:30/00:05:31
(172.18.41.33, 224.247.228.10), RP 192.168.3.111, MBGP/AS 704, 2d10h/00:05:35
(172.18.222.210, 224.2.224.13), RP 192.168.3.92, MBGP/AS 704, 01:51:53/00:05:22
(172.18.41.33, 229.231.124.13), RP 192.168.3.111, MBGP/AS 704, 2d10h/00:05:33
(172.18.32.138, 224.2.200.23), RP 192.168.253.7, MBGP/AS 3582, 21:33:40/00:05:49
(172.18.75.244, 224.2.200.23), RP 192.168.253.7, MBGP/AS 3582, 21:33:40/00:05:49
```

Table 32 describes the significant fields shown in the display.

Table 32 show ip msdp sa-cache Field Descriptions

Field	Description
(172.16.41.33, 238.105.148.0)	Indicates that the first address (source) is sending to the second address (group).
RP 172.16.3.111	IP address of the Rendezvous point (RP) where the SA message originated.
MBGP/AS 704	Indicates that the RP from which the SA message originated is in AS 704 according to multiprotocol Border Gateway Protocol (BGP).
2d10h/00:05:33	The route has been cached for 2 days and 10 hours. If no SA message is received in 5 minutes and 33 seconds, the route will be removed from the SA cache.

The following is sample output from the **show ip msdp sa-cache** command with the **rejected**, **detail**, and **read-only** keywords specified:

```
Router# show ip msdp sa-cache rejected detail read-only

MSDP Rejected SA Cache
 35 rejected SAs received over 02:50:01, cache size: 50 entries
 Timestamp (source, group)
 2832.248, (10.10.10.4, 227.7.7.12), RP: 10.10.10.4, Peer: 10.10.10.4,
     Reason: sa-limit-exceeded
 2915.232, (10.10.10.8, 224.1.1.1), RP: 10.11.11.11, Peer: 10.10.10.8,
     Reason: in-filter
 3509.584, (10.12.12.2, 225.5.5.5), RP: 10.15.15.1, Peer: 10.12.12.2,
            Reason: rpf-fail
 .
 .
 .
```

Table 33 describes the significant fields shown in the display.

Table 33 show ip msdp sa-cache rejected detail read-only Field Descriptions

Field	Description
35 rejected SAs received over 02:50:01	The number of rejected SA message entries received in the length of time indicated in HH:MM:SS.
cache size:	Indicates the size of the rejected SA cache. This field is controlled by the **ip msdp rejected-sa-cache** command. If the rejected SA cache overflows, entries are overwritten, starting from the first entry.
Timestamp	Indicates the router uptime in *seconds.milliseconds.*
(source, group)	The (S, G) information advertised in the rejected SA message.
RP:	Indicates the IP address of the Rendezvous Point (RP) that originated the SA message.

Table 33 show ip msdp sa-cache rejected detail read-only Field Descriptions (continued)

Field	Description
Peer:	Indicates the IP address of the MSDP peer that sent the rejected SA message.
Reason:	Indicates the reason that the router rejected the SA message. The possible reasons are as follows: • autorp-group—Indicates that the SA message was rejected because it included one of the two AutoRP groups (224.0.1.39 and 224.0.1.40). • in-filter—Indicates that the SA message was rejected because it was filtered by a configured incoming filter list (configured by the **ip msdp sa-filter in** command). • no-memory—Indicates that the SA message was rejected because the router ran out of memory while allocating storage for the MSDP SA message. • rpf-fail—Indicates that the SA message was rejected because it failed the Reverse Path Forwarding (RPF) check. • rp-filter—Indicates that the SA message was rejected because it was filtered by a configured incoming RP filter list (configured by the **ip msdp sa-filter in** command). • sa-limit-exceeded—Indicates that the SA message was rejected because the maximum number of SA cache entries (controlled by the **ip msdp sa-limit** command) was already exhausted when the SA message was received. • ssm-range—Indicates that the SA message was rejected because it indicated a group in the SSM range.

Related Commands

Command	Description
clear ip msdp sa-cache	Clears MSDP SA cache entries.
ip msdp cache-sa-state	Enables the router to create SA state.

show ip msdp summary

To display Multicast Source Discovery Protocol (MSDP) peer status, use the **show ip msdp summary** command in user EXEC or privileged EXEC mode.

show ip msdp [**vrf** *vrf-name*] **summary**

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.1(7)	This command was modified to display information about the number of Source-Active (SA) messages from each MSDP peer in the SA cache.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720 only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Examples

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

```
Router# show ip msdp summary

MSDP Peer Status Summary
Peer Address     AS    State    Uptime/  Reset SA    Peer Name
                                Downtime Count Count
224.135.250.116  109   Up       1d10h    9     111   rtp5-rp1
*172.20.240.253 1239  Up       14:24:00 5     4010  sl-rp-stk
172.16.253.19    109   Up       12:36:17 5     10    shinjuku-rp1
172.16.170.110   109   Up       1d11h    9     12    ams-rp1
```

Table 34 describes the significant fields shown in the display.

Table 34 show ip msdp summary Field Descriptions

Field	Description
Peer Address	IP address of the MSDP peer.
AS	Autonomous system to which the MSDP peer belongs.

Table 34 show ip msdp summary Field Descriptions (continued)

Field	Description
State	State of the MSDP peer.
Uptime/Downtime	Days and hours the MSDP peer is up or down, per state shown in the previous column. If the time is less than 24 hours, it is shown in terms of hours:minutes:seconds.
SA Count	Number of SA messages from this MSDP peer in the SA cache.
Peer Name	Name of the MSDP peer.

show ip multicast

To display information about IP multicast global configuration parameters, use the **show ip multicast** command in user EXEC or privileged EXEC mode.

show ip multicast [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Restricts the output to displaying IP multicast global configuration parameters associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified by the *vrf-name* argument.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)ZW	This command was integrated into Cisco IOS Release 12.2(33)ZW.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show ip multicast** command. The output is self-explanatory.

```
Router# show ip multicast

   Multicast Routing: enabled
   Multicast Multipath: disabled
   Multicast Route limit: No limit
   Multicast Triggered RPF check: enabled
   Multicast Fallback group mode: Dense
```

Table 35 describes the fields shown in the display.

Table 35 show ip multicast Field Descriptions

Field	Description
Multicast routing:	Indicates whether multicast routing has been enabled or disabled (using the **ip multicast-routing** command).
Multicast multipath:	Indicates whether multicast load splitting has been enabled or disabled (using the **ip multicast multipath** command) and displays what hash algorithm is configured for load splitting IP multicast traffic (when multicast load splitting has been enabled).
Multicast Route limit:	Displays the limit configured for the **ip multicast route-limit** command.

Table 35 show ip multicast Field Descriptions (continued)

Field	Description
Multicast Triggered RPF check:	Indicates whether RPF triggered RPF checks have been enabled (the default) or disabled (using the **no ip multicast rpf backoff** command)
Multicast Fallback group mode:	Indicates the multicast fallback group mode (dense or sparse) in use (configured with the **ip pim dm-fallback** command). The default is dense mode.

Related Commands

Command	Description
ip multicast-routing	Enables IP multicast routing.
ip multicast multipath	Enables load splitting of IP multicast traffic over ECMP.
ip multicast route-limit	Limits the number of mroutes that can be added to a multicast routing table.
ip multicast rpf backoff	Configures the intervals at which PIM RPF failover will be triggered by changes in the routing tables.
ip pim dm-fallback	Enables PIM-DM fallback.

show ip multicast interface

To display information about IP multicast interface configuration parameters and packet counters, use the **show ip multicast interface** command in user EXEC or privileged EXEC mode.

show ip multicast [**vrf** *vrf-name*] **interface** [*type number*]

Syntax Description

vrf *vrf-name*	(Optional) Restricts the output to displaying information about multicast-enabled interfaces associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified by the *vrf-name* argument.
type number	(Optional) Interface type and number for which to display IP multicast interface-specific configuration paratemeters and packets counters.

Command Default

If no optional arguments and keywords are specified, this command will display IP multicast configuration parameters and packet counters for all multicast-enabled interfaces.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)ZW	This command was integrated into Cisco IOS Release 12.2(33)ZW.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show ip multicast interface** command with *type number* arguments:

```
Router# show ip multicast interface fastethernet 1/0

FastEthernet1/0 is up, line protocol is up
  Internet address is 10.1.1.1/24
  Multicast routing: enabled
  Multicast switching: fast
  Multicast packets in/out: 0/0
  Multicast boundary: test       (in/out)
  Multicast Tagswitching: disabled
  Multicast TTL threshold: 0
  Multicast Tagswitching: disabled
```

Table 36 describes the fields shown in the display.

Table 36 show ip multicast interface Field Descriptions

Field	Description
<interface type> <interface number> is	Indicates the state of the multicast-enabled interface (up or down).
line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
IP address is	IP address configured for the interface (using the ip address command)
Multicast routing:	Indicates whether multicast routing (Protocol Independent Multicast [PIM]) has been enabled or disabled on the interface (using the **ip pim** command).
Multicast switching:	Indicates the type of multicast switching operating on the interface (as configured with the **ip mroute-cache** command). **Note** In Cisco IOS Releases that support the IPv4 MFIB, the **ip mroute-cache** command has been removed and this field will always display "fast" in the output.
Multicast packets in/out:	Displays multicast packet counters. **Note** These counters are also displayed in the output of the **show ip pim interface** command.
Multicast boundary:	Indicates the multicast boundary configured on an interface (using the **ip multicast boundary** command). **Note** If no IP multicast boundaries are configured on the interface, this field will not be displayed in the output.
Multicast TTL threshold:	Indicates the time-to-live (TTL) threshold of multicast packets being forwarded out an interface (as configured with the **ip multicast ttl-threshold** command). **Note** This field is obsolete in Cisco IOS Releases that support the IPv4 MFIB. For those releases, the **ip multicast ttl-threshold** command has been removed and this field will always "0" in the output.
Multicast Tagswitching:	This field is obsolete. It will always display "Disabled" in the output.

Related Commands

Command	Description
ip pim	Enables PIM on an interface.
ip mroute-cache	Configures IP multicast fast or distributed switching on interface.
ip multicast boundary	Configures an administratively scoped IPv4 multicast boundary on an interface.

Command	Description
ip multicast ttl-threshold	Configures the TTL threshold of multicast packets being forwarded out an interface.
show ip pim interface	Displays information about interfaces configured for PIM.

show ip multicast redundancy state

To display information about the current redundancy state for IP multicast, use the **show ip multicast redundancy state** command in user EXEC or privileged EXEC mode.

Syntax for the Catalyst 6500 Series Switch in Cisco IOS Release 12.2(33)SXI and Later Releases

show ip multicast redundancy state

Syntax for the Cisco 7600 Series Router in Cisco IOS Release 12.2(33)SRE and Later Releases
Syntax for the Cisco 7600 Series Router and Cisco 10000 Series Router in Cisco IOS Release 15.0(1)S and Later Releases

show ip multicast redundancy state [**verbose**]

Syntax Description

verbose	(Optional) Displays additional information about the In Service Software Upgrade (ISSU) negotiation status for each defined IP multicast synchronization message type.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
12.2(33)SRE	This command was modified. The **verbose** keyword was added, and new output fields were added to display ISSU status information.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

Use this command to display the current IP multicast redundancy state of the Route Processors (RPs). The output displays information about the current multicast redundancy state of the RPs and the current synchronization state of the standby RP.

Examples

The following is sample output from the **show ip multicast redundancy state** command from a Catalyst 6500 series switch running Cisco IOS Release 12.2(33)SXI:

```
Router# show ip multicast redundancy state

Multicast Redundancy state:   SSO
Sync message epoch:           0
Sync message sequence number: 11
Stale NSF state flush timeout: 30000 ms
Current sync state: Synched
```

Table 37 describes the fields shown in the display.

Table 37 show ip multicast redundancy state Field Descriptions

Field	Description
Multicast Redundancy state:	Indicates the current redundancy state of the RPs.
Sync message epoch:	Internal qualifier for the synchronization message sequence number.
Sync message sequence number:	Internal sequence number assigned to a synchronization message within a synchronization message epoch.
Stale NSF state flush timeout:	Indicates the nonstop forwarding (NSF) state flush timeout period. **Note** In the event of an RP switchover, this timeout period occurs after unicast and multicast reconvergence. The timeout period is the delay between the downloading of refreshed multicast control plane route information to the forwarding plane and the flushing of stale NSF forwarding plane information that was retained from before the RP switchover. The default timeout period is 30,000 milliseconds (ms). Use the **ip multicast redundancy routeflush maxtime** command to configure an additional timeout period before stale forwarding plane multicast routing (mroute) information is flushed.
Current sync state:	Current synchronization state of the standby RP.

The following is sample output from the **show ip multicast redundancy state** command from a Cisco 7600 series router running Cisco IOS Release 12.2(33)SRE:

```
Router# show ip multicast redundancy state

Multicast IPv4 Redundancy Mode:   SSO
Multicast IPv6 Redundancy Mode:   Not enabled
Multicast IPv4 HA state machine status: Idle
Multicast IPv6 HA state machine status: Idle
Sync message epoch:           0
Sync message sequence number: 21
Stale NSF state flush timeout: 30000 ms
Current sync state: Synched
Multicast ISSU Client Status:
  PIM MIC client            ISSU compatible
  MRIB MIC client           ISSU compatible
  MFIB IPv4 MIC client      ISSU compatible
  MFIB IPv6 MIC client      No ISSU result reported
  PLATFORM IPv4 MIC client  Unregistered - ignored
  PLATFORM IPv6 MIC client  Unregistered - ignored
  IPv4 SSO supported for:   PIM, MRIB, MFIBV4
  IPv6 SSO blocked by:      MFIBV6
```

The following is sample output from the **show ip multicast redundancy state** command with the **verbose** keyword from a Cisco 7600 series router running Cisco IOS Release 12.2(33)SRE:

```
Router# show ip multicast redundancy state verbose

Multicast IPv4 Redundancy Mode:   SSO
Multicast IPv6 Redundancy Mode:   Not enabled
Multicast IPv4 HA state machine status: Idle
Multicast IPv6 HA state machine status: Idle
Sync message epoch:           0
Sync message sequence number: 21
Stale NSF state flush timeout: 30000 ms
Current sync state: Synched
Multicast ISSU Client Status:
  PIM MIC client            ISSU compatible
  MRIB MIC client           ISSU compatible
  MFIB IPv4 MIC client      ISSU compatible
  MFIB IPv6 MIC client      No ISSU result reported
  PLATFORM IPv4 MIC client  Unregistered - ignored
  PLATFORM IPv6 MIC client  Unregistered - ignored
  IPv4 SSO supported for:   PIM, MRIB, MFIBV4
  IPv6 SSO blocked by:      MFIBV6

Multicast ISSU sync message status

SYNC_RP_MAPPING               : Compatible
SYNC_RP_ROUTE                 : Compatible
SYNC_BSR                      : Compatible
SYNC_AUTORP_DISCOV_IDB        : Compatible
SYNC_MDB                      : Compatible
SYNC_MIDB                     : Compatible
SYNC_MSDP                     : Compatible
SYNC_RPDF                     : Compatible
SYNC_MDT_TUNNEL               : Compatible
SYNC_REG_TUNNEL               : Compatible
SYNC_MCAC_RSV                 : Compatible
SYNC_MDT_DATA_RCV             : Compatible
SYNC_MDT_DATA_SND             : Compatible
SYNC_MDT_DATA_RCV_DECAP       : Compatible
SYNC_LSP_VIF                  : Compatible
```

Table 38 describes the significant fields shown in the display.

Table 38 show ip multicast redundancy state Field Descriptions

Field	Description
Multicast IPv4 Redundancy Mode:	Indicates the current redundancy mode in operation for IPv4 multicast.
Multicast IPv6 Redundancy Mode:	Indicates the current redundancy mode in operation for IPv6 multicast.
Multicast IPv4 HA state machine status:	Provides the status of IPv4 high availability (HA) state machine events. **Note** This status is displayed only on the active RP. Possible state machine status values are as follows: • DDE replaying • Flush pending • Idle • Not enabled • NSF hold-off extending • Unicast converging Following an RP switchover, the multicast NSF HA state machine is enabled under the following conditions: • The system is configured to be in stateful switchover (SSO) mode. • All registered IPv4 multicast software components (Protocol Independent Multicast [PIM], Multicast Routing Information Base [MRIB], Multicast Forwarding Information Base [MFIB], and, on applicable router types, the platform multicast driver software) have successfully completed ISSU negotiation with their peer on the "old" active RP before the RP switchover occurred. • Multicast routing is configured for the default multicast routing table or for one or more nondefault multicast routing tables (for example, VPN routing and forwarding [VRF] instances). If the multicast IPv4 HA state machine is not enabled, the state machine status displayed is "Not enabled."

Table 38 show ip multicast redundancy state Field Descriptions (continued)

Field	Description
	If the multicast IPv4 HA state machine is enabled, the state machine status progresses through the following states after a switchover occurs: • Unicast converging—Indicates that this RP is gathering updated multicast and unicast routing information from neighboring routers and hosts for one or more IPv4 multicast routing tables. This phase of the state machine must complete before the next phase, data driven events (DDE) replay, can begin. • DDE replaying—Indicates that this RP is incorporating synched MFIB state information for multicast (S,G) routes that were created before the switchover by DDEs into the multicast routing table. This information is being incorporated for one or more IPv4 multicast routing tables. Multicast routes learned via DDEs cannot be learned from neighboring PIM routers or hosts and are, instead, synched by the MFIB during steady state operation in order to enable data flow continuity through an SSO switchover. DDEs comprise one of the two following types: – Initial start of data flow from a directly connected data source (host) that is detected on a “first hop” router. – Shortest path tree (SPT) switchover at a “last hop” router that is triggered by multicast data packets received via a (*, G) multicast route from a given source “S” and sent to an Internet Group Management Protocol (IGMP) host that has requested reception of packets from a multicast group address “G.” • NSF hold-off extending—Indicates that after completion of DDE replay, an additional NSF hold-off delay was requested by the platform multicast driver software for one or more IPv4 multicast routing tables. The hold-off period will continue until it is either released by the platform multicast driver software or until the maximum allowable hold-off time has elapsed. This phase of the HA state machine is optional and occurs only when required for correct serialization of platform multicast driver software databases during initial postswitchover processing.

Table 38 show ip multicast redundancy state Field Descriptions (continued)

Field	Description
	• Flush pending—Indicates that the multicast HA state machine is waiting for the hold-off period to flush "stale" multicast data plane forwarding state. After the hold-time period ends (the period when the current converged multicast routing control plane state is downloaded to the multicast data plane software and hardware), a "flush" is performed to delete any multicast forwarding state that was previously stored in the data plane (through synching from the "old" active RP during steady state operation) that has not been "refreshed" by matching state from the reconverged post failover routing information in the multicast control plane. A fixed time delay is observed between the termination of the hold-off period and the flushing of stale multicast data plane forwarding state. • Idle—Indicates that the multicast HA state machine has completed its progression through all state machine phases for all IPv4 multicast routing tables. Following the flushing of stale multicast data plane state, normal multicast route and forwarding state maintenance has resumed.
Multicast IPv6 HA state machine status:	Provides the status of IPv6 HA state machine events. **Note** This status is displayed only on the active RP. The field descriptions for the IPv6 HA state machine are nearly the same as for the IPv4 HA state machine; therefore, you can apply the field descriptions from the IPv4 HA state machine, substituting IPv6 for IPv4. The one exception is that the conditions for enabling the IPv6 HA state machine are slightly different (because the Multicast VPN feature is not supported for the IPv6 address family). The conditions required for enabling the IPv6 multicast HA state machine are, therefore, as follows: • The system is configured to be in SSO mode • All registered IPv6 multicast software components (PIM, MRIB, MFIB, and, on applicable router types, the platform multicast driver software) have successfully completed ISSU negotiation with their peer on the "old" active RP before the RP switchover occurred. • Multicast routing is configured for the IPv6 multicast address family.
Sync message epoch:	Internal qualifier for the synchronization message sequence number.
Sync message sequence number:	Internal sequence number assigned to a synchronization message within a synchronization message epoch.

Table 38 show ip multicast redundancy state Field Descriptions (continued)

Field	Description
Stale NSF state flush timeout:	Indicates the NSF state flush timeout period. **Note** In the event of an RP switchover, this timeout period occurs after unicast and multicast reconvergence. The timeout period is the delay between the downloading of refreshed multicast control plane route information to the forwarding plane and the flushing of stale NSF forwarding plane information that was retained from before the RP switchover. The default timeout period is 30,000 ms. Use the **ip multicast redundancy routeflush maxtime** command to configure an additional timeout period before stale forwarding plane mroute information is flushed.
Current sync state:	Current synchronization state of the standby RP.
Multicast ISSU Client Status:	Provides status on the various ISSU clients. Multicast requires participation from multiple software components, each of which require their own communication channel to the standby RP. ISSU client status tracks ISSU negotiation state for each of these components.
Multicast ISSU sync message status:	Provides the status of ISSU synchronization messages. For each type of internal multicast forwarding database, ISSU requires agreement from the active and standby peers on which message version will be used. These outputs show that the negotiation completion status for each of the synched database types.

Related Commands

Command	Description
debug ip multicast redundancy	Displays information about IP multicast redundancy events.
ip multicast redundancy routeflush maxtime	Configures an additional timeout period before stale forwarding plane mroute information is flushed following an RP switchover.
show ip multicast redundancy statistics	Displays IP multicast redundancy statistics.

show ip multicast redundancy statistics

To display IP multicast redundancy statistics, use the **show ip multicast redundancy statistics** command in user EXEC or privileged EXEC mode.

show ip multicast redundancy statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

Use the **show ip multicast redundancy statistics** command to display IP multicast redundancy statistics. The output displays the following information:

- A summary statistic showing the current number of synchronization messages awaiting transmission from the active Route Processor (RP) to the standby RP. (This count is summed across all synchronization database types.)
- A summary statistic showing the current number of synchronization messages that have been sent from the active RP to the standby RP, but for which the active RP has not yet received acknowledg ment from the standby for successful reception. (This count is summed across all synchronization database types.)
- The last two statistics, displaying the count of messages awaiting transmission or acknowledgement, provide a way to measure the load on the internal synchronization message sending mechanism.

Use the **clear ip multicast redundancy statistics** command to reset IP multicast redundancy statistics.

Examples

The following is sample output from the **show ip multicast redundancy statistics** command:

```
mcast-iouha-1# show ip multicast redundancy statistics
Multicast Redundancy Statistics

Sync Type              Updates       Syncs        Sync failures

RP mapping              0            0            0
Bidir. RP route info    0            0            0
Bootstrap cache         0            0            0
Autorp discovery IDB    0            0            0
RPDF                    0            0            0
MDT tunnel              0            0            0
PIM register tunnel     0            0            0
```

```
MCAC Reservation        0            0            0
Data MDT receive        0            0            0
Data MDT send           0            0            0
Data MDT receive decap  0            0            0
Lspvif                  0            0            0

Requests Awaiting Sync Msg Transmission: 0
Requests Awaiting Sync Msg Acknowledgement: 0
```

Table 39 describes the significant fields shown in the display.

Table 39 show ip multicast redundancy statistics Field Descriptions

Field	Description
Sync Type	Displays statistics about the internal multicast forwarding databases that are synchronized between the active and standby RP. The following internal multicast forwarding databases are synchronized between the active and standby RPs: • RP mapping—Internal database that stores group-to-RP mapping information. • Bidirectional (bidir) RP route info—Internal database that stores bidir-Protocol Independent Multicast (PIM) RP route information. • Bootstrap cache—Internal database that stores bootstrap router (BSR) candidate information. • AutoRP discovery IDB—Internal database that stores the identity of the interface chosen on the active RP for use as the source interface for AutoRP discovery messages. • RPDF—Internal database that stores bidir-PIM designated forwarder (DF) information. • MDT tunnel—Internal database that stores MVPN Multicast Distribution Tree (MDT) tunnel information. • PIM register tunnel—Internal database that stores Protocol Independent Multicast (PIM) register tunnel information. • MCAC Reservation—Internal database that stores the identity of IPv6 (S, G) multicast routes for which a multicast Call Admission Control (MCAC) cost is currently accrued for each interface on the active RP. Retention of this information on the standby RP enables that RP, on becoming the new active RP during an RP switchover, to reserve MCAC bandwidth for these multicast routes during the initial post switchover multicast state reconvergence period, which, therefore, enables continuity of these multicast data streams through an RP switchover.

Table 39 show ip multicast redundancy statistics Field Descriptions (continued)

Field	Description
Updates	Tracks the number of updates that required standby RP synchronization for each of the internal multicast forwarding databases. If the number of updates displayed under the "Updates" column for an internal multicast forwarding database matches the number of synchronizations displayed under the "Syncs" column, it can be inferred that the standby RP is currently synchronized. **Note** Over time, however, the number of updates for a given multicast forwarding database is expected to exceed the number of synchronizations. In normal operating conditions, this disparity is usually due to update bundling: when several updates are sent simultaneously (or within a relatively short period of time), the Cisco IOS software will bundle the updates when synchronizing data on the standby RP. **Note** If the number of updates exceeds the number of synchronizations because of a synchronization failure, then the number displayed under "Sync failures" will also increment.
Syncs	Number of times that the data for a given internal multicast forwarding database has been synchronized on the standby RP.

Table 39 show ip multicast redundancy statistics Field Descriptions (continued)

Field	Description
Sync failures	Number of times that synchronization of data for a given internal multicast forwarding database failed on the standby RP. **Tip** The **show ip multicast redundancy state** command can be used to determine the synchronization state after a synchronization failure. When the standby RP has been resynchronized after a failure, the current state shown in the "Current sync state" field will display "Synched." **Note** An alternative way to determine whether the standby RP has been resynchronized is to examine the "Requests Awaiting Sync Msg Transmission" and the "Requests Awaiting Sync Msg Acknowledgement" fields. The value displayed for these fields will normally be zero (except in situations where the system is under heavy load). In the event of a synchronization failure, the number of synchronization message requests for updates awaiting transmission and acknowledgment will begin accumulating in the queue; the values displayed for those fields, thus, will increment accordingly. After the standby RP recovers from the failure and resynchronizes, the value displayed for those fields will return to zero.
Requests Awaiting Sync Msg Transmission:	Synchronization message requests that are in the queue for transmission from the active RP to the standby RP.
Requests Awaiting Sync Msg Acknowledgement:	Synchronization message requests that are in transit awaiting acknowledgment from the standby RP.

Table 39 show ip multicast redundancy statistics Field Descriptions (continued)

Field	Description
Average Sync Wait Time =	Displays the average time, in milliseconds (ms), that a synchronization message request for an update waits in the queue before being sent to the standby RP. **Note** Both this field and the "Average Sync Ack Time =" field can be interpreted as a measure of how heavy the load is on the synchronization message sending mechanism. The average wait time for a synchronization message request in the queue will generally be short (even on a heavily loaded system). On a lightly loaded system, the value displayed for this field may even appear as 0 ms (when the wait time is less than half of a millisecond, the system will round down to zero).
Average Sync Ack Time =	Displays the average round-trip time of synchronization message requests for updates, in milliseconds (ms). The average for the round-trip time is based on the time between when messages are sent to the standby RP for acknowledgment to the time at which the active RP receives acknowledgments from the standby RP for those messages. **Note** The average time that is displayed for this field will always be higher than the average time displayed for the "Average Sync Wait Time" field; however—even on a heavily loaded system—the average time displayed for this field will generally be short.

Related Commands

Command	Description
clear ip multicast redundancy statistics	Resets IP multicast redundancy statistics.
debug ip multicast redundancy	Displays information about IP multicast redundancy events.

show ip multicast rpf tracked

Note The **show ip multicast rpf tracked** command is not available in Cisco IOS Release 15.0(1)S2 and later Cisco IOS 15.0S releases.

To display IP multicast Return Path Forwarding (RPF) tracked information, use the **show ip multicast rpf tracked** command in user EXEC or privileged EXEC mode.

show ip multicast rpf tracked

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
15.0(1)S2	This command was removed. It is not available in Cisco IOS Release 15.0(1)S2 and later Cisco IOS 15.0S releases.

Examples

The following is sample output from the **show ip multicast rpf tracked** command.

```
Router# show ip multicast rpf tracked

RPF interface: Ethernet0
  RPF neighbor: ? (10.0.10.2)
  RPF route/mask: 10.0.33.0/16
  RPF type: unicast (eigrp 1)
  RPF recursion count: 0
```

Related Commands

Command	Description
debug ip multicast rpf tracked	Displays information about IP multicast rpf tracked events.

show ip multicast topology

To display multicast topology information, use the **show ip multicast topology** command in user EXEC or privileged EXEC mode.

show ip multicast topology [{**multicast** | **unicast**} *topology-name*]

Syntax Description

multicast *topology-name*	(Optional) Displays information about the specified multicast topology instance.
unicast *topology-name*	(Optional) Displays information about the specified unicast topology instance.

Command Default

Information about all topology instances is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

This command displays topology information for multicast streams that are configured to support the Multicast Live-Live feature. This feature delivers two multicast streams with the same content over diverse paths in the network. This functionality reduces packet loss due to network failures on any one of the paths.

Examples

The following is sample output from the **show ip multicast topology** command:

```
Router# show ip multicast topology multicast live-A

Topology: ipv4 multicast live-A
TID: 1
 Extended IP ACL: 101
Associated VPN VRF is IPv4 default
```

Table 40 describes the fields shown in the display.

Table 40 show ip multicast topology Field Descriptions

Field	Description
Topology	The multicast data stream topology instance whose information is being displayed.
TID	The identity of the topology instance.

Table 40 show ip multicast topology Field Descriptions (continued)

Field	Description
Extended IP ACL	The IP access list that is associated with the topology instance.
Associated VPN VRF	The Virtual Private Network (VPN) Virtual Routing and Forwarding (VRF) instance that is associated with the topology instance.

Related Commands

Command	Description
debug ip multicast topology	Enables debugging output for IP multicast stream topology creation events, deletion events, and IP multicast stream ACL matching events.
ip multicast rpf select topology	Associates a multicast topology with a multicast group with a specific mroute entry.
ip multicast topology	Configures topology selection for multicast streams.

show ip pgm host defaults

Note Support for the PGM Host feature has been removed. Use of this command is not recommended.

To display the default values for Pragmatic General Multicast (PGM) Host traffic, use the **show ip pgm host defaults** command in user EXEC or privileged EXEC mode.

show ip pgm host defaults

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.1(1)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The default values displayed in the **show ip pgm host defaults** command output are applied to every new host connection that is opened.

Examples

The following is sample output from the **show ip pgm host defaults** user EXEC command:

```
Router> show ip pgm host defaults

Source Session Default Values :

    spm-ambient-ivl (6000), txw-adv-secs (6000)
    txw-adv-timeout-max (3600000), txw-rte (16384), txw-secs (30000)
    ncf-max (infinite), spm-rpt-ivl (3000), ihb-min (1000)
    ihb-max (10000), join (0), tpdu-size (16384)
    txw-adv-method (time), tx-buffer-mgmt (return)

Receiver Session Default Values :

    nak-gen-ivl (60000), nak-rb-ivl (500), nak-rdata-ivl (2000)
    nak-rpt-ivl (2000), rx-buffer-mgmt (minimum), rx-local-retrans (none)

Common Default Values:
```

```
    stream-type (apdu), ttl (255)

Address used to source packets:(10.1.1.1)
```

Table 41 describes the fields and default values in the sample output.

Table 41 show ip pgm host defaults Field Descriptions

Field	Description
Source Session Default Values	Displays the values for source-specific PGM Host traffic defaults.
spm-ambient-ivl (6000)	Amount of time, in milliseconds, the PGM Host waits for a PGM source path message (SPM) ambient data packet. The default is 6000 ms.
txw-adv-secs (6000)	Amount of time, in milliseconds, of the advanced transmit window for the PGM Host. The default is 6000 ms.
txw-adv-timeout-max (3600000)	Amount of time, in milliseconds, the PGM Host waits for data packets, even if the PGM Host receives PGM NAK data packets. The default is 3600000 ms.
txw-rte (16384)	The data transmit rate, in bytes-per-second, for the PGM Host. The default is 16384 bytes per second.
txw-secs (30000)	Data transmit window size, in milliseconds, for the PGM Host. The default is 30000 ms.
ncf-max (infinite)	Maximum number of PGM NAK confirmation data packets (NAK NCFs), in packets per second, the PGM Host sends per second. The default is infinite.
spm-rpt-ivl (3000)	Amount of time, in milliseconds, the PGM Host waits for a PGM SPM repeat data packet. The default is 3000 ms.
ihb-min (1000)	SPM interheartbeat timer minimum, in milliseconds. The default is 1000 ms.
ihb-max (10000)	SPM interheartbeat timer maximum, in milliseconds. The default is 10000 milliseconds (ms).
join (0)	Amount of time, in milliseconds, the PGM Host waits, when running in router mode, for client requests. The default is 0 ms.
tpdu-size (16384)	Size of the source transport data unit (TPDU) for the PGM Host. The available range is 41 through 16384 bytes. The default is 1400 bytes.
tx-adv-method (time)	Type of advanced transmit window method (data or time) for the PGM Host. The default is time.
tx-buffer-mgmt (return)	Type of transmit data buffers (keep or return) for the PGM Host. The default is return.
Receiver Session Default Values	Displays the values for receiver-specific PGM Host traffic defaults.
nak-gen-ivl (60000)	Amount of time, in milliseconds, the PGM Host waits for a PGM negative acknowledgment (NAK) data packet. The default is 60000 ms.

Table 41 show ip pgm host defaults Field Descriptions (continued)

Field	Description
nak-rb-ivl (500)	Amount of time, in milliseconds, the PGM Host waits before sending a PGM NAK data packet. The default is 500 ms.
nak-rdata-ivl (2000)	Amount of time, in milliseconds, the PGM Host waits for a re-sent PGM NAK (NAK RDATA) data packet. The default is 2000 ms.
nak-rpt-ivl (2000)	Amount of time, in milliseconds, the PGM Host waits for a PGM NAK confirmation (NAK NCF) data packet. The default is 2000 ms.
rx-buffer-mgmt (minimum)	Type of receive data buffers (full or minimum) for the PGM Host. The default is minimum.
rx-local-retrans (none)	Specifies whether a receiver has to do local retransmissions or not if it sees NAKs.
Common Default Values	Displays the values for PGM Host traffic defaults that are common between a source and a receiver.
stream-type (apdu)	Data stream type (apdu or byte) for the PGM Host. The default is apdu.
ttl (255)	Time-to-live (TTL) value on the PGM Host for sent multicast data packets. The default is 255 hops. The TTL value for a packet is decremented by 1 as the packet passes through a router.
Address used to source packets	The unicast IP address that the virtual host is using to originate PGM packets.

Related Commands

Command	Description
clear ip pgm host	Resets PGM Host connections to their default values and clears traffic statistics.
ip pgm host	Enables PGM Host.
show ip pgm host sessions	Displays open PGM Host traffic sessions.
show ip pgm host traffic	Displays PGM Host traffic statistics.

show ip pgm host sessions

Note Support for the PGM Host feature has been removed. Use of this command is not recommended.

To display open Pragmatic General Multicast (PGM) Host traffic sessions, use the **show ip pgm host sessions** command in user EXEC or privileged EXEC mode.

show ip pgm host sessions [*session-number* | *group-address*]

Syntax Description

session-number	(Optional) PGM Host traffic session number.
group-address	(Optional) PGM Host multicast group address.

Defaults

No default behavior or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If a session number or multicast group address is not specified, all open traffic sessions are displayed.

Examples

The following user EXEC example shows all open traffic sessions:

```
Router> show ip pgm host sessions

Idx  GSI           Source Port  Type     State   Dest Port  Mcast Address
1    000000000000  0            receiver listen  48059      224.3.3.3
2    9CD72EF099FA  1025         source   conn    48059      224.1.1.1
```

The following user EXEC example shows traffic information for traffic session number 2:

```
Router> show ip pgm host sessions 2

Idx  GSI           Source Port  Type     State   Dest Port  Mcast Address
2    9CD72EF099FA  1025         source   conn    48059      224.1.1.1

    stream-type (apdu), ttl (255)

    spm-ambient-ivl (6000), txw-adv-secs (6000)
```

```
    txw-adv-timeout-max (3600000), txw-rte (16384), txw-secs (30000)
    ncf-max (infinite), spm-rpt-ivl (3000), ihb-min (1000)
    ihb-max (10000), join (0), tpdu-size (16384)
    txw-adv-method (time), tx-buffer-mgmt (return)

    ODATA packets sent                      0
          bytes sent                        0
    RDATA packets sent                      0
          bytes sent                        0
    Total bytes sent                        0
    ADPUs sent                              0
    APDU  transmit memory errors            0
    SPM   packets sent                      6
    NCF   packets sent                      0
    NAK   packets received                  0
          packets received in error         0
    General bad packets                     0
    TX window lead                          0
    TX window trail                         0
```

The following user EXEC example shows traffic information for multicast group address 244.1.1.1:

```
Router> show ip pgm host sessions 244.1.1.1

Idx  GSI           Source Port  Type     State   Dest Port  Mcast Address
2    9CD72EF099FA  1025         source   conn    48059      224.1.1.1

    stream-type (apdu), ttl (255)

    spm-ambient-ivl (6000), txw-adv-secs (6000)
    txw-adv-timeout-max (3600000), txw-rte (16384), txw-secs (30000)
    ncf-max (infinite), spm-rpt-ivl (3000), ihb-min (1000)
    ihb-max (10000), join (0), tpdu-size (16384)
    txw-adv-method (time), tx-buffer-mgmt (return)

    ODATA packets sent                      0
          bytes sent                        0
    RDATA packets sent                      0
          bytes sent                        0
    Total bytes sent                        0
    ADPUs sent                              0
    APDU  transmit memory errors            0
    SPM   packets sent                      6
    NCF   packets sent                      0
    NAK   packets received                  0
          packets received in error         0
    General bad packets                     0
    TX window lead                          0
    TX window trail                         0
```

Table 42 describes the significant fields shown in the displays.

Table 42 show ip pgm host sessions Field Descriptions

Field	Description
Idx	The local index for the traffic session.
GSI	The global source identifier for the traffic session.
Source Port	The source port for the traffic session.
Type	Source or receiver session.
State	The state of the session. For example, connected or listening.

Table 42 show ip pgm host sessions Field Descriptions (continued)

Field	Description
Dest Port	The destination port for the traffic session.
Mcast Address	The IP multicast address for the traffic session.
ODATA	Normal data packet.
RDATA	Re-sent data packet.
ADPUs	Application data units.
SPM	Source path message.
NCF	Negative acknowledgment (NAK) confirmation packet.
NAK	NAK packet.

Related Commands

Command	Description
clear ip pgm host	Resets PGM Host connections to their default values and clears traffic statistics.
ip pgm host	Enables PGM Host.
show ip pgm host defaults	Displays the default values for PGM Host traffic.
show ip pgm host traffic	Displays PGM Host traffic statistics.

show ip pgm host traffic

Note Support for the PGM Host feature has been removed. Use of this command is not recommended.

To display Pragmatic General Multicast (PGM) Host traffic statistics, use the **show ip pgm host traffic** command in user EXEC or privileged EXEC mode.

show ip pgm host traffic

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to display traffic statistics at the PGM transport layer.

Examples

The following is sample output from the **show ip pgm host traffic** user EXEC command:

```
Router> show ip pgm host traffic

General Statistics :

    Sessions in                         0
             out                        0
    Bytes    in                         0
             out                        0
```

```
Source Statistics :

    ODATA packets sent                      0
          bytes sent                        0
    RDATA packets sent                      0
          bytes sent                        0
    Total bytes sent                        0
    ADPUs sent                              0
    APDU  transmit memory errors            0
    SPM   packets sent                      0
    NCF   packets sent                      0
    NAK   packets received                  0
          packets received in error         0

Receiver Statistics :

    ODATA packets received                  0
          packets received in error         0
          valid bytes received              0
    RDATA packets received                  0
          packets received in error         0
          valid bytes received              0
    Total valid bytes received              0
    Total bytes received in error           0
    ADPUs received                          0
    SPM   packets received                  0
          packets received in error         0
    NCF   packets received                  0
          packets received in error         0
    NAK   packets received                  0
          packets received in error         0
          packets sent                      0
    Undeliverable packets                   0
    General bad packets                     0
    Bad checksum packets                    0
```

Table 43 describes the significant fields shown in the display.

Table 43 show ip pgm host traffic Field Descriptions

Field	Description
General Statistics	Displays statistics that relate to both the traffic source and the receiver.
Source Statistics	Displays statistics that relate to the traffic source.
Receiver Statistics	Displays statistics that relate to the traffic receiver.

Related Commands

Command	Description
clear ip pgm host	Resets PGM Host connections to their default values and clears traffic statistics.
ip pgm host	Enables PGM Host.
show ip pgm host defaults	Displays the default values for PGM Host traffic.
show ip pgm host sessions	Displays open PGM Host traffic sessions.

show ip pgm router

To display Pragmatic General Multicast (PGM) Reliable Transport Protocol state and statistics, use the **show ip pgm router** command in user EXEC or privileged EXEC mode.

show ip pgm router [**interface** [*interface-type interface-number*] | **state** [*group-address*] | [**traffic** [*interface-type interface-number*]] [**verbose**]

Syntax Description

interface [*interface-type interface-number*]	(Optional) Displays interfaces on which PGM Router Assist is configured.
state [*group-address*]	(Optional) Displays designated local repairer (DLR) information and PGM resend state information per transport session identifier (TSI). If no group address is specified, resend state for all groups is shown.
traffic [*interface-type interface-number*]	(Optional) Displays PGM packet counters. If no interface type and number are specified, traffic on all interfaces is displayed. These statistics do not reflect the number of PGM data packets (ODATA) that are forwarded in a session, because these are forwarded transparently by IP multicast. **Note** The **traffic** keyword will display statistics for the POLRs, NAKs, RDATA that will differentiate if they are taken from the off-tree DLR (or the upstream DLR in some cases). POLLs have rows for POLLs received and POLLs discarded. In the case of POLLs for off-tree DLR discovery, the packets are discarded and are accounted for in the POLLs discarded row.
verbose	(Optional) Displays extended information about outgoing interface lists, timers, and Forward Error Connections (FECs).

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(13)T	The output display for this command was updated to include DLR information.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show ip pgm router** command with the **interface** keyword:

```
Router# show ip pgm router interface

Address         Interface
10.1.0.2        Ethernet1/0/0 (measured drop rate 0%)
```

```
10.3.0.2        Ethernet1/0/4 (measured drop rate 0%)
```

Table 44 describes the significant fields shown in the display.

Table 44 show ip pgm router Field Descriptions

Field	Description
Address	IP address of the interface running PGM Router Assist.
Interface	Interface type and number on the router that is running PGM Router Assist, plus the drop rate measured on the interface.

The following is sample output from the **show ip pgm router** command with the **traffic** keyword. An RDATA fragment is a part of an RDATA packet that has been fragmented at the IP layer while in transit. The PGM network element has seen two RDATA packets that were each fragmented into three IP fragments.

```
Router# show ip pgm router traffic

FastEthernet0/0
  NAKs received                 2
  NCFs transmitted              2
 RDATA forwarded                2
 RDATA frags forwarded          6
  SPMs received                 4
       used                     4
  SPMs forwarded               33
Serial0/0
  NAKs forwarded                2
  NAKs retransmitted            2
  NCFs received                 4
 RDATA received                 2
 RDATA frags received           6
  SPMs received                33
       used                    33
```

The following is sample output from the **show ip pgm router** command with the **state** and **verbose** keywords. The timer associated with each session is an idle timer; the TSI state is deleted when this timer expires. The measured loss rates are indicated as follows:

- link_lr: worst reported link loss rate
- path_lr: worst reported path loss rate
- receiver_lr: worst reported receiver loss rate
- cr_lead: sequence number associated with worst receiver loss rate
- cr_worst_rec: IP address that reported worst loss rate

```
Router# show ip pgm router state verbose

TSI                Group            Neighbor        TGSIZE
0A0700C85555-1000  227.7.7.7        rpf/source       N/A        00:04:25
  (link_lr 7%, path_lr 4%, receiver_lr 10%
  cr_lead 6256421, cr_worst_rec 134.45.0.126)
```

The following sample output shows state after receivers have reported loss of certain packets. Negative acknowledgments (NAKs) have been received for each of the two sessions in the previous example. After the loss, the router has state for the lost packets. The “sqn 1990” indicates that a receiver lost a packet with sequence number 1990 and is requesting that it be re-sent.

```
Router# show ip pgm router state verbose

TSI                Group            Neighbor        TGSIZE
0A0700C85555-1000  227.7.7.7        rpf/source       N/A        00:04:55
   sqn        1990            age   4 ELIM TMR
       Ethernet1/0/0
   sqn        1991            age    5 (anticipated)
0A0700C85555-2000 234.4.3.2         rpf/source       16         00:04:55
   sqn (       125,          7) age   10
       Serial5/0 prty # 7
```

For the selective TSI, the output shows resend state for sequence number 1990. This state was created by a NAK received on Ethernet interface 1/0/0. “ELIM TMR” indicates that the state is eliminating duplicates of any NAK that is pending and any new NAKs for this sequence number will not be forwarded.

State shown for sequence 1991 is anticipated state, indicating that it was created by a NAK confirmation (NCF) for a NAK sent by some other PGM router with the same PGM upstream neighbor as this router.

For the TSI with parity, the state shown was created by a parity NAK for seven packets of the Transmission Group 125. This state was received on serial interface 5/0; “# 7” indicates that seven parity packets must be forwarded out this interface.

Related Commands

Command	Description
clear ip pgm router	Clears PGM traffic statistics.
ip pgm router	Enables PGM Router Assist and thereby allows PGM to operate more efficiently on the router.

show ip pim boundary

To display information about mroutes filtered by administratively scoped IPv4 multicast boundaries configured on an interface, use the **show ip pim boundary** command in user EXEC or privileged EXEC mode.

show ip pim boundary *interface-type interface-number source-address group-address* {**in** | **out**}

Syntax Description

interface-type	Interface type. For more information, use the question mark (?) online help function.
interface-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
source-address	IP address or hostname of the source.
group-address	IP address or hostname of the group.
in	Displays whether an mroute is being filtered (blocked) by an incoming multicast boundary (a multicast boundary configured to filter source traffic coming into the interface).
out	Displays whether an mroute is being filtered (blocked) by an outgoing multicast boundary (a multicast boundary configured to prevent mroutes states from being created on an interface by filtering Protocol Independent Multicast (PIM) joins and Internet Group Management Protocol (IGMP) reports for groups or channels).

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(1)	This command was introduced in a release earlier than Cisco IOS Release 12.4(1).
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Use the the **show ip pim boundary** command to determine whether an mroute is being filtered by administratively scoped IPv4 multicast boundaries configured on an interface (using the **ip multicast boundary** command).

Examples

The following sample output from the **show ip pim boundary** command shows a blocked mroute entry. The field descriptions are self-explanatory.

```
Router# show ip pim boundary FastEthernet 0/0 10.1.1.1 239.159.1.1 in

(10.1.1.1,239.159.1.1) unblocked on FastEthernet0/0 for in option
```

The following sample output from the **show ip pim boundary** command shows an unblocked mroute entry. The field descriptions are self-explanatory.

```
Router# show ip pim boundary FastEthernet 1/1 10.1.1.2 239.159.1.2 out

(10.1.1.2,239.159.1.2) blocked on FastEthernet1/1 for out option
```

Related Commands

Command	Description
ip multicast boundary	Configures an administratively scoped IPv4 multicast boundary.

show ip pim bsr-router

To display information about a bootstrap router (BSR), use the **show ip pim bsr-router** command in user EXEC or privileged EXEC mode.

show ip pim [**vrf** *vrf-name*] **bsr-router**

Syntax Description

vrf *vrf-name*	(Optional) Displays information about a BSR associated with the multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The output includes elected BSR information and information about the locally configured candidate rendezvous point (RP) advertisement.

Examples

The following is sample output from the **show ip pim bsr-router** command:

```
Router# show ip pim bsr-router

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds

Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

Table 45 describes the significant fields shown in the display.

Table 45 show ip pim bsr-router Field Descriptions

Field	Description
BSR address	IP address of the BSR.
Uptime	Length of time that this router has been up (in hours, minutes, and seconds).
BSR Priority	Priority as configured with the **ip pim bsr-candidate** command.
Hash mask length	Length of a mask (32 bits maximum) that is to be ANDed with the group address before the hash function is called. This value is configured with the **ip pim bsr-candidate** command.
Next bootstrap message in	Time (in hours, minutes, and seconds) in which the next bootstrap message is due from this BSR.
Next Cand_RP_advertisement in	Time (in hours, minutes, and seconds) in which the next candidate RP advertisement will be sent.
RP	List of RP IP addresses.
Group acl	Standard IP access list number that defines the group prefixes that are advertised in association with the RP address. This value is configured with the **ip pim rp-candidate** command.

Related Commands

Command	Description
ip pim bsr-candidate	Configures the router to announce its candidacy as a BSR.
ip pim rp-candidate	Configures the router to advertise itself as a PIM Version 2 candidate RP to the BSR.
show ip pim rp	Displays active RPs that are cached with associated multicast routing entries.
show ip pim rp-hash	Displays which RP is being selected for a specified group.

show ip pim interface

To display information about interfaces configured for Protocol Independent Multicast (PIM), use the **show ip pim interface** command in user EXEC or privileged EXEC mode.

show ip pim [**vrf** *vrf-name*] **interface** [*type number*] [**df** | **count**] [*rp-address*] [**detail**] [**stats**]

Syntax Description

vrf *vrf-name*	(Optional) Displays information about PIM interfaces associated with the Multicast Virtual Private Network (MVPN) virtual routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
type number	(Optional) Interface type and number.
df	(Optional) When bidirectional PIM (bidir-PIM) is used, displays the IP address of the elected designated forwarder (DF) for each rendezvous point (RP) of an interface.
count	(Optional) Specifies the number of packets received and sent out the interface.
rp-address	(Optional) RP IP address.
detail	(Optional) Displays PIM details of each interface.
stats	(Optional) Displays multicast PIM interface octet counts.

Command Default

If no interface is specified, all interfaces are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
11.2(11)GS	This command was integrated into Cisco IOS Release 11.2(11)GS.
12.0(5)T	This command was modified. The flag “H” was added in the output display to indicate that an outgoing interface is hardware-switched in the case of IP multicast Multilayer Switching (MMLS).
12.0(18)ST	This command was integrated into Cisco IOS Release 12.0(18)ST.
12.1(2)T	This command was modified. The **df** keyword and *rp-address* argument were added.
12.1(5)T	This command was modified. The **detail** keyword was added.
12.0(22)S	This command was modified. The command output changed to show when the query interval is set to milliseconds.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(31)S	This command was modified. The **stats** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.3(17)	This command was modified. The **stats** keyword was added.

Release	Modification
12.4(7)	This command was modified. The **stats** keyword was added.
12.4(6)T	This command was modified. The **stats** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was modified. The "FS" column was removed from the output of the **show ip pim interface count** command due to the introduction of the IPv4 MFIB architecture.
15.0(1)M	This command was modified. The "FS" column was removed from the output of the **show ip pim interface count** command due to the introduction of the IPv4 MFIB architecture.
12.2(33)SRE	This command was modified. The "FS" column was removed from the output of the **show ip pim interface count** command due to the introduction of the IPv4 MFIB architecture.

Usage Guidelines

Use the **show ip pim interface count** command to display switching counts for Multicast Distributed Switching (MDS) and other switching statistics.

Note In Cisco IOS releases that support the IPv4 Multicast Forwarding Information Base (MFIB), use the **show ip mfib interface** command to display MFIB-related information about interfaces and their forwarding status.

Examples

The following is sample output from the **show ip pim interface** command:

```
Router# show ip pim interface

Address          Interface                Ver/   Nbr    Query  DR     DR
                                          Mode   Count  Intvl  Prior
10.1.0.1         GigabitEthernet0/0       v2/SD  0      30     1      10.1.0.1
10.6.0.1         GigabitEthernet0/1       v2/SD  1      30     1      10.6.0.2
10.2.0.1         ATM1/0.1                 v2/SD  1      30     1      0.0.0.0
```

The following is sample output from the **show ip pim interface** command when an interface is specified:

```
Router# show ip pim interface Ethernet1/0

Address          Interface                Ver/   Nbr    Query  DR     DR
                                          Mode   Count  Intvl  Prior
172.16.1.4       Ethernet1/0              v2/S   1      100 ms 1      172.16.1.4
```

The following is sample output from the **show ip pim interface** command when the **count** keyword is specified:

```
Router# show ip pim interface count

Address          Interface          FS  Mpackets In/Out
172.16.121.35    Ethernet0          *   548305239/13744856
172.16.121.35    Serial0.33         *   8256/67052912
192.168.12.73    Serial0.1719       *   219444/862191
```

The following is sample output from the **show ip pim interface** command when the **count** keyword is specified and IP MMLS is enabled. The example lists the PIM interfaces that are fast switched and process switched, and the packet counts for these interfaces. The H flag is added to interfaces where IP MMLS is enabled.

```
Router# show ip pim interface count

States: FS - Fast Switched, H - Hardware Switched
Address          Interface          FS  Mpackets In/Out
192.168.10.2       Vlan10             * H 40886/0
192.168.11.2       Vlan11             * H 0/40554
192.168.12.2       Vlan12             * H 0/40554
192.168.23.2       Vlan23             *   0/0
192.168.24.2       Vlan24             *   0/0
```

The following are two sample outputs from the **show ip pim interface** command when the **df** keyword is specified:

```
Router# show ip pim interface df

Interface          RP               DF Winner        Metric          Uptime
Ethernet3/3        10.10.0.2        10.4.0.2         0               00:03:49
                   10.10.0.3        10.4.0.3         0               00:01:49
                   10.10.0.5        10.4.0.4         409600          00:01:49
Ethernet3/4        10.10.0.2        10.5.0.2         0               00:03:49
                   10.10.0.3        10.5.0.2         409600          00:02:32
                   10.10.0.5        10.5.0.2         435200          00:02:16
Loopback0          10.10.0.2        10.10.0.2        0               00:03:49
                   10.10.0.3        10.10.0.2        409600          00:02:32
                   10.10.0.5        10.10.0.2        435200          00:02:16

Router# show ip pim interface Ethernet3/3 df 10.10.0.3

Designated Forwarder election for Ethernet3/3, 10.4.0.2, RP 10.10.0.3
  State                           Non-DF
  Offer count is                  0
  Current DF ip address           10.4.0.3
  DF winner up time               00:02:33
  Last winner metric preference   0
  Last winner metric              0
```

Table 46 describes the significant fields shown in the displays.

Table 46 show ip pim interface Field Descriptions

Field	Description
Address	Interface IP address of the next hop router.
Interface	Interface type and number that is configured to run PIM.
Ver/Mode	PIM version and multicast mode in which the Cisco IOS software is operating.
Nbr Count	Number of PIM neighbors that have been discovered through this interface. If the Neighbor Count is 1 for a DVMRP tunnel, the neighbor is active (receiving probes and reports).
Query Interval	Frequency, in seconds, of PIM hello messages, as set by the **ip pim query-interval** interface configuration command. The default is 30 seconds.
DR	IP address of the designated router (DR) on a network. **Note** Point-to-point interfaces do not have designated routers, so the IP address would be shown as 0.0.0.0.

Table 46 show ip pim interface Field Descriptions (continued)

Field	Description
FS	An asterisk (*) in this column indicates that fast switching is enabled.
Mpackets In/Out	Number of packets into and out of the interface since the router has been up.
RP	IP address of the RP.
DF Winner	IP address of the elected DF.
Metric	Unicast routing metric to the RP announced by the DF.
Uptime	Length of time the RP has been up, in days and hours. If less than 1 day, time is shown in hours:minutes:seconds.
State	Indicates whether the specified interface is an elected DF.
Offer count is	Number of PIM DF election offer messages that the router has sent out the interface during the current election interval.
Current DF ip address	IP address of the current DF.
DF winner up time	Length of time the current DF has been up, in days and hours. If less than 1 day, time is shown in hours:minutes:seconds.
Last winner metric preference	The preference value used for selecting the unicast routing metric to the RP announced by the DF.
Last winner metric	Unicast routing metric to the RP announced by the DF.

The following is sample output from the **show ip pim interface** command with the **detail** keyword for Fast Ethernet interface 0/1:

```
Router# show ip pim interface fastethernet 0/1 detail

FastEthernet0/1 is up, line protocol is up
  Internet address is 172.16.8.1/24
  Multicast switching:process
  Multicast packets in/out:0/0
  Multicast boundary:not set
  Multicast TTL threshold:0
  PIM:enabled
    PIM version:2, mode:dense
    PIM DR:172.16.8.1 (this system)
    PIM neighbor count:0
    PIM Hello/Query interval:30 seconds
    PIM State-Refresh processing:enabled
    PIM State-Refresh origination:enabled, interval:60 seconds
    PIM NBMA mode:disabled
    PIM ATM multipoint signalling:disabled
    PIM domain border:disabled
  Multicast Tagswitching:disabled
```

Table 47 describes the significant fields shown in the display.

Table 47 show ip pim interface detail Field Descriptions

Field	Description
Internet address	IP address of the specified interface.
Multicast switching:	The type of multicast switching enabled on the interface: process, fast, or distributed.

Table 47 show ip pim interface detail Field Descriptions (continued)

Field	Description
Multicast boundary:	Indicates whether an administratively scoped boundary is configured.
Multicast TTL threshold:	The time-to-live (TTL) threshold of multicast packets being forwarded out the interface.
PIM:	Indicates whether PIM is enabled or disabled.
PIM version:	Indicates whether PIM version 1 or version 2 is configured.
mode:	Indicates whether PIM sparse mode, dense mode, or sparse-dense mode is configured.
PIM DR:	The IP address of the DR.
PIM State-Refresh processing:	Indicates whether the processing of PIM state refresh control messages is enabled.
PIM State-Refresh origination:	Indicates whether the origination of the PIM state refresh control messages is enabled.
interval:	Indicates the configured interval for the origination of the PIM state refresh control messages. The available interval range is from 4 to 100 seconds.
PIM NBMA mode:	Indicates whether the interface is enabled for nonbroadcast multiaccess (NBMA) mode.
PIM ATM multipoint signalling:	Indicates whether the interface is enabled for ATM multipoint signaling.
PIM domain border:	Indicates whether the interface is enabled as a PIM domain border.
Multicast Tagswitching:	Indicates whether multicast tag switching is enabled.

The following is sample output from the **show ip pim interface** command when the **stats** keyword is specified:

```
Router# show ip pim interface stats

Interface        Mpackets In    Mpackets Out         Octets In        Octets Out

Loopback0                  0               0                 0                 0
Loopback1                  0               0                 0                 0
Ethernet0/0                0               0                 0                 0
Ethernet0/3                0               0                 0                 0
Ethernet1/1                0               0                 0                 0
```

For all of the count descriptions, a packet is counted as a multicast packet if either of the following two conditions is met:

- The IP address contained in the IP header of the packet specifies a multicast (class D) IP address.
- The IP address contained in the IP header of the packet specifies an IP address located on this router and the packet contains an encapsulated packet for which the IP header of the encapsulated packet specifies a multicast (class D) IP address.

Table 48 describes the significant fields shown in the display.

Table 48 show ip pim interface stats Field Descriptions

Field	Description
Mpackets In	The number of multicast packets received on each interface listed in the output.
Mpackets Out	The number of multicast packets sent on each interface listed in the output.
Octets In	Cumulative byte count for data bytes (including IP header bytes) contained within multicast packets received on each interface listed in the output.
Octets Out	Cumulative byte count for data bytes (including IP header bytes) contained within multicast packets sent on each interface listed in the output.

Related Commands

Command	Description
ip pim	Enables PIM on an interface.
ip pim query-interval	Configures the frequency of PIM router query messages.
ip pim state-refresh disable	Disables the processing and forwarding of PIM dense mode state refresh control messages on a PIM router.
ip pim state-refresh origination-interval	Configures the origination of and the interval for PIM dense mode state refresh control messages on a PIM router.
show ip mfib interface	Displays MFIB-related information about interfaces and their forwarding status.
show ip pim neighbor	Displays information about PIM neighbors.

show ip pim mdt bgp

To show details about the Border Gateway Protocol (BGP) advertisement of the route distinguisher (RD) for the multicast distribution tree (MDT) default group, use the **show ip pim mdt bgp** command in user EXEC or privileged EXEC mode.

show ip pim [**vrf** *vrf-name*] **mdt bgp**

Syntax Description

vrf *vrf-name*	(Optional) Displays information about the BGP advertisement of the RD for the MDT default group associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to show detailed BGP advertisement of the RD for the MDT default group.

Examples

The following is sample output from the **show ip pim mdt bgp** command:

```
Router# show ip pim mdt bgp

MDT-default group 232.2.1.4
 rid:10.1.1.1 next_hop:10.1.1.1
```

Table 49 describes the significant fields shown in the display.

Table 49 show ip pim mdt bgp Field Descriptions

Field	Description
MDT-default group	The MDT default groups that have been advertised to this router.
rid:10.1.1.1	The BGP router ID of the advertising router.
next_hop:10.1.1.1	The BGP next hop address that was contained in the advertisement.

show ip pim mdt history

To display information about the history of data multicast distribution tree (MDT) groups that have been reused, use the **show ip pim mdt history** command in privileged EXEC mode.

show ip pim vrf *vrf-name* **mdt history interval** *minutes*

Syntax Description

vrf *vrf-name*	Displays the history of data MDT groups that have been reused for the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
interval *minutes*	Specifies the interval (in minutes) for which to display information about the history of data MDT groups that have been reused. The range is from 1 to 71512 minutes (7 weeks).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The output of the **show ip pim mdt history** command displays the history of reused MDT data groups for the interval specified with the **interval** keyword and *minutes* argument. The interval is from the past to the present, that is, from the time specified for the *minutes* argument to the time at which the command is issued.

Examples

The following is sample output from the **show ip pim mdt history** command:

```
Router# show ip pim vrf vrf1 mdt history interval 20

   MDT-data send history for VRF - vrf1 for the past 20 minutes

MDT-data group        Number of reuse
     10.9.9.8           3
     10.9.9.9           2
```

Table 50 describes the significant fields shown in the display.

Table 50 show ip pim mdt history Field Descriptions

Field	Description
MDT-data group	The MDT data group for which information is being shown.
Number of reuse	The number of data MDTs that have been reused in this group.

show ip pim mdt receive

To display the data multicast distribution tree (MDT) group mappings received from other provider edge (PE) routers, use the **show ip pim mdt receive** command in privileged EXEC mode.

show ip pim vrf *vrf-name* **mdt receive** [**detail**]

Syntax Description

vrf *vrf-name*	Displays the data MDT group mappings for the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
detail	(Optional) Provides a detailed description of the data MDT advertisements received.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When a router wants to switch over from the default MDT to a data MDT, it advertises the VRF source, the group pair, and the global multicast address over which the traffic will be sent. If the remote router wants to receive this data, then it will join this global address multicast group.

Examples

The following is sample output from the **show ip pim mdt receive** command using the **detail** keyword for further information:

```
Router# show ip pim vrf vpn8 mdt receive detail

Joined MDT-data groups for VRF:vpn8
group:172.16.8.0 source:10.0.0.100 ref_count:13
(10.101.8.10, 225.1.8.1), 1d13h/00:03:28/00:02:26, OIF count:1, flags:TY
(10.102.8.10, 225.1.8.1), 1d13h/00:03:28/00:02:27, OIF count:1, flags:TY
```

Table 51 describes the significant fields shown in the display.

Table 51 show ip pim mdt receive Field Descriptions

Field	Description
group:172.16.8.0	Group that caused the data MDT to be built.
source:10.0.0.100	VRF source that caused the data MDT to be built.
ref_count:13	Number of (S, G) pairs that are reusing this data MDT.
OIF count:1	Number of interfaces out of which this multicast data is being forwarded.
flags:	Information about the entry. • A—candidate Multicast Source Discovery Protocol (MSDP) advertisement • B—bidirectional group • D—dense • C—connected • F—register flag • I—received source-specific host report • J—join shortest path source tree (SPT) • L—local • M—MSDP created entry • P—pruned • R—RP bit set • S—sparse • s—Source Specific Multicast (SSM) group • T—SPT bit set • X—proxy join timer running • U—URL Rendezvous Directory (URD) • Y—joined MDT data group • y—sending to MDT data group • Z—multicast tunnel

show ip pim mdt send

To display the data multicast distribution tree (MDT) groups in use, use the **show ip pim mdt send** command in privileged EXEC mode.

show ip pim vrf *vrf-name* **mdt send**

Syntax Description

vrf *vrf-name*	Displays the data MDT groups in use by the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Releaes 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command to show the data MDT groups in use by a specified MVRF.

Examples

The following is sample output from the **show ip pim mdt send** command:

```
Router# show ip pim vrf vpn8 mdt send

MDT-data send list for VRF:vpn8
  (source, group)                    MDT-data group      ref_count
  (10.100.8.10, 225.1.8.1)           232.2.8.0           1
  (10.100.8.10, 225.1.8.2)           232.2.8.1           1
  (10.100.8.10, 225.1.8.3)           232.2.8.2           1
  (10.100.8.10, 225.1.8.4)           232.2.8.3           1
  (10.100.8.10, 225.1.8.5)           232.2.8.4           1
  (10.100.8.10, 225.1.8.6)           232.2.8.5           1
  (10.100.8.10, 225.1.8.7)           232.2.8.6           1
  (10.100.8.10, 225.1.8.8)           232.2.8.7           1
  (10.100.8.10, 225.1.8.9)           232.2.8.8           1
  (10.100.8.10, 225.1.8.10)          232.2.8.9           1
```

Table 52 describes the significant fields shown in the display.

Table 52 show ip pim mdt send Field Descriptions

Field	Description
source, group	Source and group addresses that this router has switched over to data MDTs.
MDT-data group	Multicast address over which these data MDTs are being sent.
ref_count	Number of (S, G) pairs that are reusing this data MDT.

show ip pim neighbor

To display information about Protocol Independent Multicast (PIM) neighbors discovered by PIMv1 router query messages or PIMv2 hello messages, use the **show ip pim neighbor** command in user EXEC or privileged EXEC mode.

show ip pim [**vrf** *vrf-name*] **neighbor** [*interface-type interface-number*]

Syntax Description

vrf *vrf-name*	(Optional) Displays information about PIM neighbors associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
interface-type	(Optional) Interface type.
interface-number	(Optional) Interface number.

Command Default

Information about all PIM neighbors is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(22)S	This command was modified. The command output was updated to display the PIM protocol version.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.0(30)S	This command was modified. The “P” flag was added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was modified. The “P” flag was added.
12.2(31)SB2	This command was modified. The “P” flag was added.
12.2(33)SXH	This command was modified. The “P” flag was added.
12.4(20)T	This command was modified. The “P” flag was added.
12.2(33)SXI	This command was modified. The “G” flag was added.
12.2(33)SRE	This command was modified. The “G” flag was added.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S.

Usage Guidelines

Use this command to display PIM neighbors discovered by PIMv1 router query messages or PIMv2 hello messages.

Use the optional *interface-type* and *interface-number* arguments to restrict the output to display only information about the PIM neighbor reachable on the specified interface.

Examples

The following is sample output from the **show ip pim neighbor** command:

```
Router# show ip pim neighbor

PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      S - State Refresh Capable
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
10.0.0.1          GigabitEthernet10/2      00:01:29/00:01:15 v2    1 / S
10.0.0.3          GigabitEthernet10/3      00:01:15/00:01:28 v2    1 / DR S P
```

Table 53 describes the significant fields shown in the display.

Table 53 show ip pim neighbor Field Descriptions

Field	Description
Neighbor Address	IP address of the PIM neighbor.
Interface	Interface type and number on which the neighbor is reachable.
Uptime	The total uptime of the neighbor (in hours:minutes:seconds).
Expires	The time before a neighbor is timed out and until the next PIM hello is received (in hours:minutes:seconds).
Ver	The version of PIM running on the neighbor's interface.
DR Prio	The priority of the PIM interface for designated router (DR) election. The possible values that can be displayed under this column are as follows: a value from 0 to 4294967294 or the "N" flag. The default DR priority is set to 1. **Note** The DR priority can be modified using the **ip pim dr-priority** command in interface configuration mode. When a DR is a candidate for election, the following conditions apply: • The router with the highest priority value configured on an interface will be elected as the DR. If this priority value is the same on multiple routers, then the router with the highest IP address configured on an interface will be elected as the DR. • If a router does not advertise a priority value in its hello messages, the router is regarded as having the highest priority and will be elected as the DR. If there are multiple routers with this priority status, then the router with the highest IP address configured on an interface will be elected as the DR.

Table 53 show ip pim neighbor Field Descriptions (continued)

Field	Description
	Note For interoperability, if a PIM neighbor is running a release prior to Cisco IOS Release 12.1(2)T, which does not support the DR priority feature, the "DR Prio" column displays the "N" flag. If the neighbor is the only router displaying the "N" flag for a PIM interface, it becomes the DR regardless of which router actually has the highest IP address. If there are several PIM neighbors with the "N" flag listed under this column, the tiebreaker is the highest IP address among them.
Mode	Information about the DR and other PIM capabilities: • B—Indicates that the PIM neighbor is bidirectional PIM (bidir-PIM) capable. In a bidir-PIM network, this capability is necessary for the routers to successfully perform the designated forwarder election process. If a router detects through PIM hello messages that one of its PIM neighbors is not bidir-PIM capable, the designated forwarder election process is aborted and forwarding of bidir-PIM traffic to and from that interface would stop. • DR—Indicates that the PIM neighbor is acting as the DR. • G—Indicates that the PIM neighbor supports Generation ID (GenID) capabilities, which enable fast PIM multicast route (mroute) reconvergence times after a switchover. • P—Indicates that the neighbor has announced through PIM hello messages its capability to handle Reverse Path Forwarding (RPF) vectors in PIM join messages. All Cisco IOS versions that support the PIM RPF Vector feature announce this PIM hello option. An RPF vector is included in PIM messages only when all PIM neighbors on a RPF interface support it. • S—Indicates that the PIM neighbor supports PIM-DM state refresh capabilities (applies only to PIM neighbors running in dense mode). This flag was introduced in support of the PIM Dense Mode State Refresh feature. PIM-DM state refresh capabilities protect pruned state in PIM dense mode from timing out by periodically forwarding a control message down the source-based distribution tree. The control message refreshes the prune state on the outgoing interfaces of each router in the distribution tree. By default, all PIM routers that are operating in dense mode (and are running a Cisco IOS software release that supports the PIM Dense Mode State Refresh feature) automatically process and forward state refresh control messages.

Related Commands

Command	Description
ip pim state-refresh disable	Disables the processing and forwarding of PIM dense mode state refresh control messages on a PIM router.
ip pim state-refresh origination-interval	Configures the origination of and the interval for the PIM dense mode state refresh control messages on a PIM router.
show ip pim interface	Displays information about interfaces configured for PIM.

show ip pim rp

To display active rendezvous points (RPs) that are cached with associated multicast routing entries, use the **show ip pim rp** command in user EXEC or privileged EXEC mode.

show ip pim [**vrf** *vrf-name*] **rp** [**mapping** | **metric**] [*rp-address*]

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
mapping	(Optional) Displays all group-to-RP mappings of which the router is aware (either configured or learned from Auto-RP).
metric	(Optional) Displays the unicast routing metric to the RPs configured statically or learned via Auto-RP or the bootstrap router (BSR).
rp-address	(Optional) RP IP address.

Defaults

If no RP is specified, all active RPs are displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.2	This command was introduced.
12.1(2)T	The **metric** keyword and *rp-address* argument were added.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The Protocol Independent Multicast (PIM) version known for an RP influences the type of PIM register messages (Version 1 or Version 2) that the router sends when acting as the designated router (DR) for an active source. If an RP is statically configured, the PIM version of the RP is not set and the router, if required to send register packets, tries to send PIM Version 2 register packets. If sending PIM Version 2 packets fails, the router sends PIM Version 1 register packets.

The version of the RP displayed in the **show ip pim rp** command output can change according to the operations of the router. When the group is created, the version shown is for the RP in the RP mapping cache. Later, the version displayed by this command may change. If this router is acting as a DR for an

active source, the router sends PIM register messages. The PIM register messages are answered by the RP with PIM register stop messages. The router learns from these PIM register stop messages the actual PIM version of the RP. Once the actual PIM version of the RP is learned, this command displays only this version. If the router is not acting as a DR for active sources on this group, then the version shown for the RP of the group does not change. In this case, the PIM version of the RP is irrelevant to the router because the version of the RP influences only the PIM register messages that this router must send.

When you enter the **show ip pim rp mapping** command, the version of the RP displayed in the output is determined only by the method through which an RP is learned. If the RP is learned from Auto-RP then the RP displayed is either "v1" or "v2, v1." If the RP is learned from a static RP definition, the RP version is undetermined and no RP version is displayed in the output. If the RP is learned from the BSR, the RP version displayed is "v2."

Examples

The following is sample output from the **show ip pim rp** command:

```
Router# show ip pim rp

Group:227.7.7.7, RP:10.10.0.2, v2, v1, next RP-reachable in 00:00:48
```

The following is sample output from the **show ip pim rp** command when the **mapping** keyword is specified:

```
Router# show ip pim rp mapping

PIM Group-to-RP Mappings
This system is an RP (Auto-RP)
This system is an RP-mapping agent

Group(s) 227.0.0.0/8
  RP 10.10.0.2 (?), v2v1, bidir
    Info source:10.10.0.2 (?), via Auto-RP
         Uptime:00:01:42, expires:00:00:32
Group(s) 228.0.0.0/8
  RP 10.10.0.3 (?), v2v1, bidir
    Info source:10.10.0.3 (?), via Auto-RP
         Uptime:00:01:26, expires:00:00:34
Group(s) 229.0.0.0/8
  RP 10.10.0.5 (mcast1.cisco.com), v2v1, bidir
    Info source:10.10.0.5 (mcast1.cisco.com), via Auto-RP
         Uptime:00:00:52, expires:00:00:37
Group(s) (-)230.0.0.0/8
  RP 10.10.0.5 (mcast1.cisco.com), v2v1, bidir
    Info source:10.10.0.5 (mcast1.cisco.com), via Auto-RP
         Uptime:00:00:52, expires:00:00:37
```

The following is sample output from the **show ip pim rp** command when the **metric** keyword is specified:

```
Router# show ip pim rp metric

RP Address      Metric Pref    Metric       Flags   RPF Type   Interface
10.10.0.2       0              0              L     unicast    Loopback0
10.10.0.3       90             409600         L     unicast    Ethernet3/3
10.10.0.5       90             435200         L     unicast    Ethernet3/3
```

Table 54 describes the significant fields shown in the displays.

Table 54 show ip pim rp Field Descriptions

Field	Description
Group	Address of the multicast group about which to display RP information.
RP	Address of the RP for that group.
v2	Indicates that the RP is running PIM version 2.
v1	Indicates that the RP is running PIM version 1.
bidir	Indicates that the RP is operating in bidirectional mode.
Info source	RP mapping agent that advertised the mapping.
(?)	Indicates that no Domain Name System (DNS) name has been specified.
via Auto-RP	Indicates that RP was learned via Auto-RP.
Uptime	Length of time the RP has been up (in days and hours). If less than 1 day, time is shown in hours, minutes, and seconds.
expires	Time in (hours, minutes, and seconds) in which the entry will expire.
Metric Pref	The preference value used for selecting the unicast routing metric to the RP announced by the designated forwarder (DF).
Metric	Unicast routing metric to the RP announced by the DF.
Flags	Indicates the flags set for the specified RP. The following are descriptions of possible flags: • C—RP is configured. • L—RP learned via Auto-RP or the BSR.
RPF Type	Routing table from which this route was obtained, either unicast, Distance Vector Multicast Routing Protocol (DVMRP), or static mroute.
Interface	Interface type and number that is configured to run PIM.

show ip pim rp mapping

To display the mappings for the PIM group to the active rendezvous points, use the **show ip pim rp mapping** command in user EXEC or privileged EXEC mode.

show ip pim [**vrf** *vrf-name*] **rp mapping** [*rp-address*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
rp-address	(Optional) Rendezvous-point IP address.

Defaults

If you do not specify an *rp-address*, the mappings for all the active rendezvous points are displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXE	This command was changed to add the **vrf** *vrf-name* keyword and argument.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to display the mappings for the PIM group to the active rendezvous points:

```
Router# show ip pim rp mapping
PIM Group-to-RP Mappings
This system is an RP-mapping agent
Group(s) 172.16.0.0/16
RP 10.6.6.6 (?), v2v1
Info source: 10.6.6.6 (?), elected via Auto-RP ---> learned via Auto-RP
and the elected RP.
Uptime: 22:36:49, expires: 00:02:04
Group(s) 192.168.0.0/24
RP 10.9.9.9 (?), v2v1, bidir
Info source: 10.9.9.9 (?), elected via Auto-RP
Uptime: 22:36:20, expires: 00:02:37
Group(s) 172.16.0.0/24
RP 10.2.2.2 (?), v2v1, bidir
Info source: 10.2.2.2 (?), elected via Auto-RP
Uptime: 22:36:24, expires: 00:02:29
Group(s) 172.16.0.0/24
RP 10.9.9.9 (?), v2v1, bidir
Info source: 10.9.9.9 (?), elected via Auto-RP
Uptime: 22:36:21, expires: 00:02:35
```

Table 55 describes the fields that are shown in the example.

Table 55 show ip pim rp mapping Field Descriptions

Field	Description
Info source	ACL number.
Static	Group-to-mapping information from the static rendezvous-point configuration.
Bidir Mode	Status of whether the rendezvous point is operating in bidirectional mode.
RP	Address of the rendezvous point for that group.
(?)	Status that shows no Domain Name System (DNS) name has been specified.

show ip pim rp-hash

To display which rendezvous point (RP) is being selected for a specified group, use the **show ip pim rp-hash** command in user EXEC or privileged EXEC mode.

show ip pim [**vrf** *vrf-name*] **rp-hash** {*group-address* | *group-name*}

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
group-address | *group-name*	RP information for the specified group address or name as defined in the Domain Name System (DNS) hosts table.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command displays which RP was selected for the group specified. It also shows whether this RP was selected by Auto-RP or the PIM Version 2 bootstrap mechanism.

Examples

The following is sample output from the **show ip pim rp-hash** command with the group address 239.1.1.1 specified:

```
Router# show ip pim rp-hash 239.1.1.1

RP 172.16.24.12 (mt1-47a.cisco.com), v2
    Info source: 172.16.24.12 (mt1-47a.cisco.com), via bootstrap
         Uptime: 05:15:33, expires: 00:02:01
```

Table 56 describes the significant fields shown in the display.

Table 56 show ip pim rp-hash Field Descriptions

Field	Description
RP 172.16.24.12 (mt1-47a.cisco.com), v2	Address of the RP for the group specified (239.1.1.1). Within parentheses is the DNS name of the RP. If the address of the RP is not registered in the DNS, a question mark (?) is displayed. PIM Version 2 configured.
Info source: 172.16.24.12 (mt1-47a.cisco.com), via bootstrap	Indicates from which system the router learned this RP information, along with the DNS name of the source. RP was selected by the bootstrap mechanism. In this case, the BSR is also the RP.
Uptime	Length of time (in hours, minutes, and seconds) that the router has known about this RP.
expires	Time (in hours, minutes, and seconds) after which the information about this RP expires. If the router does not receive any refresh messages in this time, it will discard information about this RP.

show ip pim rp-hash (BSR)

To display which rendezvous point is being selected for a specified group, use the **show ip pim rp-hash** command in user EXEC or privileged EXEC mode.

show ip pim [**vrf** *vrf-name*] **rp-hash** {*group-address* | *group-name*}

Syntax Description

vrf *vrf-name*	(Optional) Specifies the name that is assigned to the multicast VPN routing and forwarding (VRF) instance.
group-address | *group-name*	Rendezvous-point information for the specified group address or name as defined in the DNS hosts table.

Defaults

This command has no default settings.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command displays which rendezvous point was selected for the group specified. It also shows whether this rendezvous point was selected by Auto-RP or the PIM Version 2 bootstrap mechanism.

Examples

This example shows how to display which rendezvous point is being selected for a specified group:

```
Router# show ip pim rp-hash 239.1.1.1

RP 172.16.24.12 (mt1-47a.cisco.com), v2
    Info source: 172.16.24.12 (mt1-47a.cisco.com), via bootstrap
         Uptime: 05:15:33, expires: 00:02:01
```

Table 56 describes the fields shown in the display.

Table 57 show ip pim rp-hash Field Descriptions

Field	Description
RP 172.16.24.12 (mt1-47a.cisco.com), v2	Address of the rendezvous point for the group specified (239.1.1.1). The DNS name of the rendezvous point within the parentheses. If the address of the rendezvous point is not registered in the DNS, a question mark (?) is displayed. PIM Version 2 is configured.
Info source: 172.16.24.12 (mt1-47a.cisco.com), via bootstrap	Which system the router learned this rendezvous-point information and the DNS name of the source. The rendezvous point was selected by the bootstrap mechanism. In this case, the BSR is also the rendezvous point.
Uptime	Length of time (in hours, minutes, and seconds) that the router has known about this rendezvous point.
expires	Time (in hours, minutes, and seconds) after which the information about this rendezvous point expires. If the router does not receive any refresh messages in this time, it discards information about this rendezvous point.

show ip pim snooping

To display the information about IP PIM snooping, use the **show ip pim snooping** command in user EXEC or privileged EXEC mode.

Global Status

show ip pim snooping

VLAN Status

show ip pim snooping vlan *vlan-id* [**neighbor | mac-group | statistics | mroute** [*source-ip | group-ip*]]

Syntax Description

vlan *vlan-id*	Displays information for a specific VLAN; valid values are from 1 to 4094.
neighbor	(Optional) Displays information about the neighbor database.
mac-group	(Optional) Displays information about the GDA database in Layer 2.
statistics	(Optional) Displays information about the VLAN statistics.
mroute	(Optional) Displays information about the mroute database.
source-ip	(Optional) Source IP address.
group-ip	(Optional) Group IP address.

Defaults

This command has no default settings.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to display the information about the global status:

```
Router# show ip pim snooping

Global runtime mode: Enabled
Global admin mode  : Enabled
Number of user enabled VLANs: 1
User enabled VLANs: 10
```

This example shows how to display the information about a specific VLAN:

```
Router# show ip pim snooping vlan 10

3 neighbors (0 DR priority incapable, 0 Bi-dir incapable)
6 mroutes, 3 mac entries
DR is 10.10.10.4
RP DF Set
```

This example shows how to display the information about the neighbor database for a specific VLAN:

```
Router# show ip pim snooping vlan 10 neighbor

IP Address       Mac address     Port Uptime/Expires    Flags
10.10.10.2       000a.f330.344a  3/13 00:09:57/00:01:22
10.10.10.1       000a.f330.334a  3/12 00:09:44/00:01:21
10.10.10.4       000a.f330.3c00 15/01 00:09:57/00:01:22 DR
Number of Neighbors = 3
```

This example shows how to display the information about the GDA database for a specific VLAN in Layer 2:

```
Router# show ip pim snooping vlan 10 mac-group

Mac address    Group address    Uptime/Expires       Outgoing Ports
VLAN 10: 4 mac entries
0100.5e03.0101 225.3.1.1        4d01h/00:03:04       1/2 1/3 1/48 15/1
0100.5e02.0101 225.2.1.1        4d01h/00:03:13       1/2 1/3 1/48 15/1
0100.5e05.0101 225.5.1.1        4d01h/00:03:01       1/2 1/3 1/48 15/1
0100.5e04.0101 225.4.1.1        4d01h/00:03:19       1/2 1/3 1/48 15/1
PE.100#
PE.100#
PE.100#
PE.100#
```

This example shows how to display the detailed statistics for a specific VLAN:

```
Router# show ip pim snooping vlan 10 statistics

PIMv2 statistics for vlan 10:
Hello                                          : 811
Join/Prunes                                    : 1332
RP DF Election                                 : 0
Asserts                                        : 133
Other types                                    : 0

Hello option holdtime [1]                      : 811
Hello option Generation ID[20]                 : 544
Hello option DR priority[19]                   : 544
Hello option Bi-dir capable[22]                : 0
Hello option Fast Hold[65005]                  : 0
Hello option Lan Prune Delay[2]                : 0
Hello option Tag switching [17]                : 0
Hello option PIM-DM State Refresh[21]          : 544
Hello option Deprecated Cisco DR priority[18]  : 0
Error - Hello length too short                 : 0
Error - Hello hold option missing              : 0
Error - Hello option length                    : 0
Error - Hello option unknown                   : 0

Error - Join/Prune Address Family              : 0
Error - Join/Prune Parser malloc failure       : 0
Error - Join/Prune Unknown up/down neighbor    : 0
Error - Join/Prune Malformed packet discards   : 0
```

```
Error - RPDF election Address Family            : 0
Error - RPDF Unknown up/down neighbor           : 0

Error - Generic packet input error              : 0
```

This example shows how to display the information about the mroute database for all mrouters in a specific VLAN:

```
Router# show ip pim snooping vlan 10 mroute

Number of Mroutes = 6
Flags: J/P - (*,G) Join/Prune, j/p - (S,G) Join/Prune
       SGR-P - (S,G,R) Prune

VLAN 10: 4 mroutes
(*, 225.3.1.1), 4d01h/00:03:06
  10.10.10.120->10.10.10.105, 4d01h/00:03:06 , J
  Downstream ports: 1/2
  Upstream ports: 1/48
  Outgoing ports: 1/2 1/48

(*, 225.2.1.1), 4d01h/00:03:11
  10.10.10.130->10.10.10.120, 4d01h/00:03:11 , J
  Downstream ports: 1/3
  Upstream ports: 1/2
  Outgoing ports: 1/2 1/3

(*, 225.5.1.1), 4d01h/00:02:57 10.10.10.120->
  10.10.10.10, 4d01h/00:02:49 , J
  10.10.10.130->10.10.10.10, 4d01h/00:02:57 , J
  10.10.10.105->10.10.10.10, 4d01h/00:02:41 , J
  Downstream ports: 1/2 1/3 1/48
  Upstream ports: 15/1
  Outgoing ports: 1/2 1/3 1/48 15/1

(*, 225.4.1.1), 4d01h/00:03:16
  10.10.10.105->10.10.10.130, 4d01h/00:03:16 , J
  Downstream ports: 1/48
  Upstream ports: 1/3
  Outgoing ports: 1/3 1/48
```

This example shows how to display the information about the PIM mroute for a specific source address:

```
Router# show ip pim snooping vlan 10 mroute 172.16.100.100

(*, 172.16.100.100), 00:16:36/00:02:36
  10.10.10.1->10.10.10.2, 00:16:36/00:02:36, J
  Downstream ports: 3/12
  Upstream   ports: 3/13
  Outgoing   ports: 3/12 3/13
```

This example shows how to display the information about the PIM mroute for a specific source and group address:

```
Router# show ip pim snooping vlan 10 mroute 192.168.0.0 172.16.10.10

(192.168.0.0, 172.16.10.10), 00:03:04/00:00:25
  10.10.10.1->10.10.10.2, 00:03:04/00:00:25, j
  Downstream ports: 3/12
  Upstream   ports: 3/13
  Outgoing   ports: 3/12 3/13
```

Related Commands

Command	Description
ip pim snooping (global configuration)	Enables PIM snooping globally.
ip pim snooping (interface configuration)	Enables PIM snooping on an interface.

show ip pim tunnel

To display information about Protocol Independent Multicast (PIM) tunnel interfaces, use the **show ip pim tunnel** command in user EXEC or privileged EXEC mode.

show ip pim [**all-vrfs** | **vrf** *vrf-name*] **tunnel** [*interface-number*] [**verbose**]

Syntax Description

all-vrfs	(Optional) Displays information about PIM tunnel interfaces associated with Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instances (including the global table).
vrf *vrf-name*	(Optional) Displays information about PIM tunnel interfaces associated with the MVRF instances associated with MVRF specified for the *vrf-name* argument.
interface-number	(Optional) PIM tunnel interface number.
verbose	(Optional) Displays detailed information about PIM tunnel interfaces.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.1	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.

Usage Guidelines

Use the **show ip pim tunnel** command to display information about PIM tunnel interfaces.

PIM tunnel interfaces are used by the IPv4 Multicast Forwarding Information Base (MFIB) for the PIM sparse mode (PIM-SM) registration process. Two types of PIM tunnel interfaces are used by the the IPv4 MFIB:

- A PIM encapsulation tunnel (PIM Encap Tunnel)
- A PIM decapsulation tunnel (PIM Decap Tunnel).

The PIM Encap Tunnel is dynamically created whenever a group-to-Rendezvous Point (RP) mapping is learned (via Auto-RP, bootstrap router (BSR), or static RP configuration). The PIM Encap Tunnel is used to encapsulate multicast packets sent by first-hop Designated Routers (DRs) that have directly connected sources.

Similar to the PIM Encap Tunnel, the PIM Decap Tunnel interface is dynamically created—with the exception that it is created only on the RP whenever a group-to-RP mapping is learned. The PIM Decap Tunnel interface is used by the RP to decapsulate PIM register messages.

Note PIM tunnels will not appear in the running configuration.

The following syslog message will appear when a PIM tunnel interface is created:

```
* %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel<interface_number>, changed state
to up
```

Examples

The following is sample output from the **show ip pim tunnel** command taken from a RP. The output is used to verify the PIM Encap and Decap Tunnel on the RP.

```
Router# show ip pim tunnel

Tunnel0
  Type  : PIM Encap
  RP    : 192.168.6.6*
  Source: 192.168.6.6
Tunnel1
  Type  : PIM Decap
  RP    : 192.168.6.6*
  Source: -
```

Note The asterisk (*) indicates that the router is the RP. The RP will always have a PIM Encap and Decap Tunnel interface.

The following is sample output from the **show ip pim tunnel** command taken from a non-RP. The output is used to confirm that a PIM Encap Tunnel has been created on a non-RP router.

```
Router# show ip pim tunnel

Tunnel0
  Type  : PIM Encap
  RP    : 192.168.6.6
  Source: 192.168.67.7
```

show ip pim vc

To display ATM virtual circuit (VC) status information for multipoint VCs opened by Protocol Independent Multicast (PIM), use the **show ip pim vc** command in user EXEC or privileged EXEC mode.

show ip pim vc [*group-address* | *group-name*] [*interface-type interface-number*]

Syntax Description

group-address | *group-name*	(Optional) IP multicast group or name. Displays only the single group.
interface-type interface-number	(Optional) Interface type and number. Displays only the single ATM interface.

Defaults

VC status information is displayed for all ATM interfaces.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show ip pim vc** command:

```
Router# show ip pim vc

IP Multicast ATM VC Status
ATM0/0 VC count is 5, max is 200
Group            VCD   Interface    Leaf Count  Rate
224.2.2.2        26    ATM0/0       1           0 pps
224.1.1.1        28    ATM0/0       1           0 pps
224.4.4.4        32    ATM0/0       2           0 pps
224.5.5.5        35    ATM0/0       1           0 pps
```

Table 58 describes the significant fields shown in the display.

Table 58 show ip pim vc Field Descriptions

Field	Description
ATM0/0	ATM slot and port number on the interface.
VC count	Number of VCs opened by PIM.

Table 58 show ip pim vc Field Descriptions (continued)

Field	Description
max	Maximum number of VCs that PIM is allowed to open, as configured by the **ip pim vc-count** command.
Group	IP address of the multicast group to which the router is multicasting.
VCD	Virtual circuit descriptor.
Interface	Outgoing interface.
Leaf Count	Number of routers that have joined the group and are members of that multipoint VC.
Rate	Rate (in packets per second) as configured by the **ip pim minimum-vc-rate** command.

Related Commands

Command	Description
ip pim multipoint-signalling	Enables PIM to open ATM multipoint switched VCs for each multicast group that a receiver joins.

show ip rpf

To display the information that IP multicast routing uses to perform the Reverse Path Forwarding (RPF) check for a multicast source, use the **show ip rpf** command in user EXEC or privileged EXEC mode.

show ip rpf [**vrf** *vrf-name*] {*route-distinguisher* | *source-address* [*group-address*] [**rd** *route-distinguisher*]} [**metric**]

Cisco ASR 1000 Series

show ip rpf [**vrf** *vrf-name*] *source-address* [*group-address*] [**rd** *route-distinguisher*] [**metric**]

Syntax Description

vrf *vrf-name*	(Optional) Displays the information that IP multicast routing uses to perform the RPF check for a multicast source associated with the Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.
route-distinguisher	Route distinguisher (RD) of a VPNv4 prefix. Entering the *route-distinguisher* argument displays RPF information related to the specified VPN route. You can enter an RD in either of these formats: • 16-bit autonomous system (AS) number: your 32-bit number, for example, 101:3 • 32-bit IP address: your 16-bit number, for example, 192.168.122.15:1
source-address	IP address or name of a multicast source for which to display RPF information.
group-address	(Optional) IP address or name of a multicast group for which to display RPF information.
rd *route-distinguisher*	(Optional) Displays the Border Gateway Protocol (BGP) RPF next hop for the VPN route associated with the RD specified for the *route-distinguisher* argument. You can enter an RD in either of these formats: • 16-bit autonomous system (AS) number: your 32-bit number, for example, 101:3 • 32-bit IP address: your 16-bit number, for example, 192.168.122.15:1
metric	(Optional) Displays the unicast routing metric.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.1(2)T	This command was modified. The **metric** keyword was added.
12.0(23)S	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Release	Modification
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.0(29)S	This command was modified. The *group-address* argument, **rd** keyword, and *route-distinguisher* argument were added for the Multicast VPN Inter-AS Support feature.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The *group-address* argument, **rd** keyword, and *route-distinguisher* argument were added for the Multicast VPN Inter-AS Support feature.
12.2(31)SB2	This command was modified. The output was modified to indicate that the Multicast VPN Extranet VRF Select feature is being used to perform the RPF lookup based on the group address and the VRF where the RPF lookup is being performed.
12.2(33)SXH	This command was modified. The *group-address* argument, **rd** keyword, and *route-distinguisher* argument were added for the Multicast VPN Inter-AS Support feature.
12.4(20)T	This command was modified. The *group-address* argument, **rd** keyword, and *route-distinguisher* argument were added for the Multicast VPN Inter-AS Support feature.
15.0(1)M	This command was modified. The output was modified to indicate that the Multicast VPN Extranet VRF Select feature is being used to perform the RPF lookup based on the group address and the VRF where the RPF lookup is being performed.
Cisco IOS XE Release 3.2S	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

Use the **show ip rpf** command to display the information that IP multicast routing uses to perform the Reverse Path Forwarding (RPF) check for a multicast source. When performing the RPF calculation, the router can use multiple routing tables (the unicast routing table, Multiprotocol Border Gateway Protocol (MBGP) table, Distance Vector Multicast Routing Protocol [DVMRP] routing table, or static multicast routes) to determine the interface on which traffic from a source should arrive (the RPF interface). Because the RPF check can be performed from multiple routing tables, the **show ip rpf** command can be used to identify the source of the retrieved information.

In a Multi-Topology Routing (MTR) routing environment, a router can perform RPF lookups from multiple unicast Routing Information Bases (RIBs)—instead of only looking at the original unique unicast RIB. By default, the Cisco IOS software supports the pre-MTR IP multicast behavior; that is, the RPF check is performed on routes in the unicast RIB (base unicast topology).

Note MTR introduces a multicast topology (base multicast topology) that is completely independent from the unicast topology. MTR integration with multicast allows the path of multicast traffic to be controlled in the network.

Examples

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

```
Router# show ip rpf 172.16.10.13

RPF information for host1 (172.16.10.13)
  RPF interface: BRI0
  RPF neighbor: sj1.cisco.com (172.16.121.10)
  RPF route/mask: 172.16.0.0/255.255.0.0
  RPF type: unicast
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
```

The following is sample output from the **show ip rpf** command with the optional **vrf** keyword, *vrf-name* argument, and *group-address* argument:

```
Router# show ip rpf vrf green 10.1.1.100 232.6.6.6

RPF information for ? (10.1.1.100)
  RPF interface: Ethernet3/0
  RPF neighbor: ? (10.1.1.5)
  RPF route/mask: 10.1.1.0/24
  RPF type: unicast (rip)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
  Using Group Based VRF Select, RPF VRF: blue
```

The following is sample output from the **show ip rpf** command with the **metric** keyword:

```
Router# show ip rpf 172.16.10.13 metric

RPF information for host1.cisco.com (172.16.10.13)
  RPF interface: BRI0
  RPF neighbor: neighbor.cisco.com (172.16.121.10)
  RPF route/mask: 172.16.0.0/255.255.0.0
  RPF type: unicast
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
  Metric preference: 110
  Metric: 11
```

The following is sample output from the **show ip rpf** command in an MTR routing environment. In Cisco IOS releases that support MTR, the "RPF topology" field was introduced to indicate which RIB topology is being used for the RPF lookup. For the "RPF topology" field in this example, the first topology listed (ipv4 multicast base) indicates where the nexthop of the RPF lookup is being conducted and the second topology listed (ipv4 unicast data) indicates where the route originated from.

```
Router# show ip rpf 10.30.30.32

RPF information for ? (10.30.30.32)
  RPF interface: Ethernet1/0
  RPF neighbor: ? (10.1.1.32)
  RPF route/mask: 10.30.30.32/32
  RPF type: unicast (ospf 100)
  Doing distance-preferred lookups across tables
  RPF topology: ipv4 multicast base, originated from ipv4 unicast data
```

Table 59 describes the fields shown in the displays.T

Table 59 show ip rpf Field Descriptions

Field	Description
RPF information for	Hostname and source address for which RPF information is displayed.
RPF interface	For the given source, the interface from which the router expects to receive packets.
RPF neighbor	For the given source, the neighbor from which the router expects to receive packets.
RPF route/mask	Route number and mask that matched against this source.
RPF type	Routing table from which this route was obtained, either unicast, MBGP, DVMRP, or static mroutes.
RPF recursion count	The number of times the route is recursively resolved.
Doing distance-preferred	Whether RPF was determined based on distance or length of mask.
Using Group Based VRF Select, RPF VRF:	The RPF lookup was based on the group address and the VRF where the RPF lookup is being performed.
Metric preference	The preference value used for selecting the unicast routing metric to the RP announced by the designated forwarder (DF).
Metric	Unicast routing metric to the RP announced by the DF.
RPF topology	RIB topology being used for the RPF lookup, and, if originated from a different RIB topology, which RIB topology the route originated from.

The following is sample output from the **show ip rpf** command in a Multicast only Fast Re-Route (MoFRR) enabled environment. The command output shows that MoFRR is enabled for the 209.165.200.226 multicast source IP address. The relevant command output is shown in bold.

```
Router# show ip rpf 209.165.200.226

RPF information for ? (209.165.200.226) MoFRR Enabled
  RPF interface: Ethernet1/4
  RPF neighbor: ? (209.165.201.2)
  RPF route/mask: 255.255.255.225
  RPF type: unicast (ospf 200)
  Doing distance-preferred lookups across tables
  RPF topology: ipv4 multicast base, originated from ipv4 unicast base
  Secondary RPF interface: Ethernet1/3
  Secondary RPF neighbor: ? (209.165.202.128)
```

Table 60 describes the fields shown in the displays.

Table 60 show ip rpf Command Output in an MoFRR-Enabled Environment: Field Descriptions

Field	Description
RPF information for	Hostname and source address for which RPF information is displayed, including MoFRR status.
RPF interface	For the given source, the interface from which the router expects to receive packets.
RPF neighbor	For the given source, the neighbor from which the router expects to receive packets.
RPF route/mask	Route number and mask that matched against this source.
RPF type	Routing table from which this route was obtained, either unicast, MBGP, DVMRP, or static mroutes.
Doing distance preferred	Whether RPF was determined based on distance or length of mask.
RPF topology	RIB topology being used for the RPF lookup, and, if originated from a different RIB topology, which RIB topology the route originated from.
Secondary RPF interface	For the given source, the secondary interface from which the router expects to receive packets.
Secondary RPF neighbor	For the given source, the secondary neighbor from which the router expects to receive packets.

show ip rpf events

To display the last 15 triggered multicast Reverse Path Forwarding (RPF) check events, use the **show ip rpf events** command in user EXEC or privileged EXEC mode.

show ip rpf [**vrf** *vrf-name*] **events**

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to determine the most recent triggered multicast RPF check events.

Examples

The following is sample output from the **show ip rpf events** command:

```
Router# show ip rpf events

Last 15 triggered multicast RPF check events

RPF backoff delay:500 msec
RPF maximum delay:5 sec

DATE/TIME            BACKOFF    PROTOCOL   EVENT         RPF CHANGES
Mar 7 03:24:10.505   500 msec   Static     Route UP        0
Mar 7 03:23:11.804   1000 sec   BGP        Route UP        3
Mar 7 03:23:10.796   500 msec   ISIS       Route UP        0
Mar 7 03:20:10.420   500 msec   ISIS       Route Down      3
Mar 7 03:19:51.072   500 msec   Static     Route Down      0
Mar 7 02:46:32.464   500 msec   Connected  Route UP        3
Mar 7 02:46:24.052   500 msec   Static     Route Down      0
Mar 7 02:46:10.200   1000 sec   Connected  Route UP        3
Mar 7 02:46:09.060   500 msec   OSPF       Route UP        3
Mar 7 02:46:07.416   500 msec   OSPF       Route Down      0
```

```
Mar 7 02:45:50.423    500 msec   EIGRP      Route UP        3
Mar 7 02:45:09.679    500 msec   EIGRP      Route Down      0
Mar 7 02:45:06.322    500 msec   EIGRP      Route Down      2
Mar 7 02:33:09.424    500 msec   Connected  Route UP        0
Mar 7 02:32:28.307    500 msec   BGP        Route UP        3
```

The following is sample output from the **show ip rpf events** command when the **ip multicast rpf backoff** command is used with the **disable** keyword, disabling the triggered RPF check function:

```
Router# show ip rpf events

Last 15 triggered multicast RPF check events

Note:Triggered RPF disabled!

RPF backoff delay:50 msec
RPF maximum delay:2 sec

DATE/TIME             BACKOFF    PROTOCOL   EVENT         RPF CHANGES
Sep 4 06:25:31.707    500 msec   Connected  Route UP        0
Sep 4 06:25:30.099    500 msec   Connected  Route UP        0
```

Table 61 describes the significant fields shown in the display.

Table 61 show ip rpf events Field Descriptions

Field	Description
RPF backoff delay	The configured amount of time (in milliseconds) allowed for the initial backoff delay.
RPF maximum delay	The maximum configured amount of time (in seconds) allowed for a backoff delay.
DATE/TIME	The date and time (in hours:minutes:seconds) an RPF event occurred.
BACKOFF	The actual backoff delay (in milliseconds) after which the RPF check was done.
PROTOCOL	The protocol that triggered the RPF check.
EVENT	This RPF check was caused by a route that went up or down, or was modified.
RPF CHANGES	The number of multicast routes that were affected by the RPF change.

show ip rpf select

To display group-to-VPN routing and forwarding (VRF) mappings, use the **show ip rpf select** command in user EXEC or privileged EXEC mode.

show ip rpf [**vrf** *vrf-name*] **select**

Syntax Description

vrf *vrf-name*	(Optional) Displays the multicast group-to-VRF mappings for the Multicast VPN (MVPN) routing and forwarding (MVRF) instance specified for the *vrf-name* argument.

Command Default

If the optional **vrf** keyword and *vrf-name* argument are omitted, the **show ip rpf select** command displays all group-to-VRF mappings.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **show ip rpf select** command after configuring group-based VRF selection policies to display the configured group-to-VRF mappings. The output displays information about group-based VRF selection policies, including the group address, the VRF mapped to the group where the Reverse Path Forwarding (RPF) lookup is performed, and the name of the access control list (ACL) applied to the policy.

Use the **ip multicast rpf select** command to configure group-based VRF selection policies. By defining group-based VRF selection policies, you can configure RPF lookups originating in a receiver MVRF or in the global routing table to be resolved in a source MVRF or in the global routing table based on group address.

Examples

The following is sample output from the **show ip rpf select** command:

```
Router# show ip rpf select

Multicast Group-to-Vrf Mappings

Group(s): 227.7.1.1/32, RPF vrf: blue, Acl: 20
Group(s): 227.7.7.7/32, RPF vrf: blue, Acl: 20
Group(s): 239.1.1.1/32, RPF vrf: blue, Acl: 20
```

Table 62 describes the significant fields shown in the display.

Table 62 show ip rpf select Field Descriptions

Field	Description
Group(s)	Multicast group address that is being mapped.
RPF vrf	VRF where the RPF lookup for the multicast group is performed.
Acl	ACL that the multicast group matched.

Related Commands

Command	Description
ip multicast rpf select	Configures RPF lookups based on group address.

show ip sap

To display the Session Announcement Protocol (SAP) cache, use the **show ip sap** command in user EXEC or privileged EXEC mode.

show ip sap [*group-address* | **"***session-name***"** | **detail**]

Syntax Description

group-address	(Optional) The sessions defining the specified multicast group address.
"*session-name***"**	(Optional) Displays the single session in detail format. The session name is enclosed in quotation marks (**" "**) that the user must enter.
detail	(Optional) Displays all sessions in detail format.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.1	The **show ip sdr** command was introduced.
12.2	The **show ip sdr** command was replaced by the **show ip sap** command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If the router is configured to be a member of multicast group 224.2.127.254 (the default session directory group), it will cache SAP announcements.

If no arguments or keywords are used with this command, the system displays a sorted list of session names.

Examples

The following is sample output from the **show ip sap** command for a session using multicast group 224.2.197.250:

```
Router# show ip sap 224.2.197.250

SAP Cache - 198 entries
Session Name: Session1
   Description: This broadcast is brought to you courtesy of Name1.
   Group: 0.0.0.0, ttl: 0, Contiguous allocation: 1
   Lifetime: from 10:00:00 PDT Jul 4 1999 until 10:00:00 PDT Aug 1 1999
   Uptime: 4d05h, Last Heard: 00:01:40
   Announcement source: 128.102.84.134
   Created by: sample 3136541828 3139561476 IN IP4 128.102.84.134
   Phone number: Sample Digital Video Lab (555) 555-5555
   Email: email1 <name@email.com>
   URL: http://url.com/
   Media: audio 20890 RTP/AVP 0
     Media group: 224.2.197.250, ttl: 127
```

```
    Attribute: ptime:40
  Media: video 62806 RTP/AVP 31
    Media group: 224.2.190.243, ttl: 127
```

Table 63 describes the significant fields shown in the display.

Table 63 show ip sap Field Descriptions

Field	Description
SAP Cache - 198 entries	Number of entries (sessions) in the cache.
Session Name:	Name of session.
Description:	Description of the session. Individual media may have their own Description field.
Group:	IP multicast group addresses used for this session. The 0.0.0.0 IP address is displayed if individual media define separate multicast groups.
ttl:	The time-to-live (TTL) value associated with the multicast groups.
Contiguous Allocation:	Number of continuously ascending IP multicast group addresses allocated to this session.
Lifetime:	Period of time during which this session is presumed to carry traffic in the network.
Uptime:	How long (in hours, minutes, and seconds) this announcement has been stored.
Last Heard:	How long ago (in hours, minutes, and seconds) this announcement was last heard. This time is always less than the timeout value configured using the **sap cache-timeout** command.
Announcement source:	IP address of the host from which this session announcement was received.
Created by:	Information for identifying and tracking the session announcement.
Phone number:	Telephone number of the person or entity responsible for the session.
Email:	E-mail address of the person or entity responsible for the session.
URL:	URL for the location where further information about this session can be found.
Media:	Indicates the media type (audio, video, or data), transport port that the medium stream is sent to, transport protocol used for these media (common values are User Datagram Protocol [UDP] and Real-Time Transport Protocol [RTP]/attribute-value pair [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.
Media group:	Indicates the IP multicast group address over which the media instance is sent.
Attribute:	Indicates attributes specific to each media instance.

Related Commands

Command	Description
clear ip sap	Deletes a SAP cache entry or the entire SAP cache.
ip sap cache-timeout	Limits how long a SAP cache entry stays active in the cache.
ip sap listen	Enables the Cisco IOS software to listen to session directory announcements.

show ip sdr

The **show ip sdr** command is replaced by the **show ip sap** command. See the description of the **show ip sap** command for more information.

show mls ip multicast

To display the MLS IP information, use the **show mls ip multicast** command in user EXEC or privileged EXEC mode.

show mls ip multicast [**capability** [**module** *num*] | **connected** | **group** *hostname* | *ip-address* [*ip-mask*] | **interface** *type number* | **module** *number* | **mdt** | **source** *hostname* | *ip-address* | **statistics** | **summary**]

Syntax Description

capability	Displays information about the multicast-replication capabilities.
module *num*	(Optional) Specifies the module number.
connected	(Optional) Displays the installed interface or mask entries.
group	(Optional) Displays the entries for a specific multicast-group address.
hostname	Group IP hostname.
ip-address	Group IP address.
ip-mask	(Optional) IP mask for group IP address.
interface	(Optional) Specifies an interface.
type	Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**.
number	Module and port number; see the "Usage Guidelines" section for valid values.
module *number*	(Optional) Displays the entries that are downloaded on the specified module; see the "Usage Guidelines" section for valid values.
mdt	(Optional) Displays hardware-accelerated MDT information.
source *hostname*	(Optional) Displays the entries for a specific source address.
source *ip-address*	(Optional) Displays the entries for a specific source IP address.
statistics	(Optional) Displays the statistics from multicast entries.
summary	(Optional) Displays a summary of statistics from multicast entries.

Defaults

This command has no default settings.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command is supported on releases prior to Release 12.2(17a)SX only.
12.2(17b)SXA	On Cisco 7600 series routers that are configured with a Supervisor Engine 720, this command is replaced by the **show mls netflow ip** command.

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release. This command was changed to include the **capability** [**module** *num*] keywords.
12.2(18)SXF	The output of the **show mls ip multicast capability** command was changed to include egress information.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The output of the **show mls ip multicast capability** command on Cisco 6500 and Cisco 7600 series routers that are configured with a Supervisor Engine 32 does not include egress information.

The **pos**, **atm**, and **ge-wan** keywords are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

The following syntax is supported on Cisco 6500 and Cisco 7600 series routers that are configured with a Supervisor Engine 2:

show mls ip multicast [**complete | partial** [**group** *hostname | ip-address* [*ip-mask* **| interface** *interface interface-number*] **| source** *hostname | ip-address*]]

show mls ip multicast [**connected | summary**]

show mls ip multicast statistics [**group** *hostname | ip-address* [**source** *hostname | ip-address*]]

The *number* argument designates the module and port number. Valid values for *number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48. These valid values also apply when entering the **module** *number* keyword and argument.

When you view the output, note that a colon (:) is used to separate the fields.

Examples

This example shows how to display general MLS IP-multicast information:

```
Router# show mls ip multicast

Multicast hardware switched flows:
(*, 224.1.1.1) Incoming interface: Vlan0, Packets switched: 0
Hardware switched outgoing interfaces: Vlan202
RPF-MFD installed
Total hardware switched flows : 1
```

This example shows how to display a summary of MLS information:

```
Router# show mls ip multicast summary

1 MMLS entries using 168 bytes of memory
Number of partial hardware-switched flows: 0
Number of complete hardware-switched flows: 1
Directly connected subnet entry install is enabled
Aggregation of routed oif is enabled
Hardware shortcuts for mvpn mroutes supported
Egress Mode of replication is enabled
Maximum route support is enabled
Router#
```

This example shows how to display MLS information on a specific interface:

```
Router# show mls ip multicast interface fastethernet 5/9

DstIP           SrcIP           Dst i/f:DstMAC       Pkts         Bytes
---------------------------------------------------------------------------
SrcDstPorts   SrcDstEncap Age   LastSeen
---------------------------------------
172.20.52.37    0.0.0.0         100: 00d0.5870.a4ff 1            129
Fa5/9,----- ARPA,ARPA   107   06:10:02
172.20.52.36    0.0.0.0         100 : 0050.7312.0cff 50           6403
Fa5/9,----- ARPA,ARPA   107   06:10:04
 Number of Entries Found = 2
```

This example shows how to display information about the multicast-replication capabilities:

```
Router# show mls ip multicast capability

Current mode of replication is Ingress
auto replication mode detection is ON

 Slot           Multicast replication capability
    2                      Egress
    5                      Egress
    6                      Egress
    8                      Ingress
    9                      Ingress
```

Related Commands

Command	Description
mls ip multicast (interface configuration)	Enables MLS IP shortcuts on the interface.
show mls ip multicast consistency-check	Displays consistency-checker information.

show mls ip multicast bidir

To display the Bidir hardware-switched entries, use the **show mls ip multicast bidir** command in user EXEC or privileged EXEC mode..

show mls ip multicast bidir [**group** *hostname* | *ip-address* [*ip-mask*] | **interface** *type number* | **source** *hostname* | *ip-address*]

Syntax Description

group	(Optional) Displays the entries for a specific multicast-group address.
hostname	Group IP hostname.
ip-address	Group IP address.
ip-mask	(Optional) IP mask for group IP address.
interface	(Optional) Specifies an interface.
type	Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, and **tengigabitethernet**.
number	Module and port number.
source *hostname*	(Optional) Displays the entries for a specific source address.
source *ip-address*	(Optional) Displays the entries for a specific source IP address.

Defaults

This command has no default settings.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command is supported on releases prior to Release 12.2(17a)SX only.
12.2(17b)SXA	This command is replaced by the **show mls netflow ip** command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to display the Bidir hardware-switched entries:

```
Router# show mls ip multicast bidir

Multicast hardware switched flows:
(*, 226.1.4.0) Incoming interface: Vlan51, Packets switched: 0
Hardware switched outgoing interfaces: Vlan51 Vlan30
RPF-MFD installed
(*, 227.1.4.0) Incoming interface: Gi2/1, Packets switched: 0
Hardware switched outgoing interfaces: Gi2/1 Vlan30
RPF-MFD installed
```

Related Commands

Command	Description
mls ip multicast bidir gm-scan-interval	Sets the RPF scan interval for the Bidir rendezvous point.

show mls ip multicast rp-mapping

To display the mappings for the PIM-Bidir group to active rendezvous points, use the **show mls ip multicast rp-mapping** command in user EXEC or privileged EXEC mode.

show mls ip multicast rp-mapping [*rp-address*] [**df-cache** | **gm-cache**]

Syntax Description

rp-address	(Optional) Rendezvous-point address.
df-cache	(Optional) Displays information on the DF list in the rendezvous-point mapping cache in the hardware.
gm-cache	(Optional) Displays information on the group/mask ranges in the rendezvous-point mapping cache in the hardware.

Defaults

This command has no default settings.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command is supported on releases prior to Release 12.2(17a)SX only.
12.2(17b)SXA	This command is replaced by the **show mls netflow ip** command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to display the mappings for the PIM group-to-active rendezvous points:

```
Router# show mls ip multicast rp-mapping

RP Address State DF-count GM-count
10.2.2.2 H 1 1
10.9.9.9 H 1 2
```

This example shows how to display information that is based on the DF list in the mapping cache of the route processor:

```
Router# show mls ip multicast rp-mapping df-cache

RP Address   State   DF    State
10.9.9.9      H       Vl30  H
```

This example shows how to display information that is based on the mapping cache of the route processor:

```
Router# show mls ip multicast rp-mapping gm-cache

State: H - Hardware Switched, I - Install Pending, D - Delete Pending,
Z - Zombie
RP Address State Group Mask State Packet/Byte-count
10.0.0.60 H 172.16.0.0 255.255.0.0 H 100/6400
```

show mls ip multicast sso

To display information about multicast high-availability SSO, use the **show mls ip multicast sso** command in user EXEC or privileged EXEC mode .

show mls ip multicast sso [**statistics**]

Syntax Description

statistics	(Optional) Displays multicast high-availability SSO statistical information.

Defaults

This command has no default settings.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to display multicast high-availability SSO information:

```
Router# show mls ip multicast sso

Multicast SSO is enabled
Multicast HA Parameters
-------------------------------------------------+------+
protocol convergence timeout                     120 secs
flow leak percent                                10
flow leak interval                               20 secs
heartquake#
```

This example shows how to display statistical information about multicast high-availability SSO:

```
Router# show mls ip multicast sso statistics

Multicast HA Statistics: ACTIVE
-------------------------------------------------+------+
CHKPT msgs sent                                  5
CHKPT msgs send failed                           0
CHKPT msgs send aborted                          0
CHKPT met add msg sent                           5
CHKPT met del msg sent                           1
CHKPT icroif msg sent                            1
MET HA met add enqueued                          5
MET HA met del enqueued                          1
ICROIF HA add enqueued                           1
```

```
ICROIF HA del enqueued                              0
CHKPT buffer failure                                0

MET HA Reconstruction Statistics
-------------------------------------------------+------+
Number of met blks reconstructed                    0
Number of normal sets reconstructed                 0
Number of fixed sets reconstructed                  0
Number of sets deleted                              0
Number of blks not found                            0
normal sets reconstruction failed                   0
fixed set reconstruction failed                     0

Multicast HA Statistics: STANDBY
-------------------------------------------------+------+
CHKPT msgs rcvd                                     5
CHKPT met add msg rcvd                              5
CHKPT met del msg rcvd                              1
CHKPT icroif msg rcvd                               1
CHKPT msg unknown                                   0
CHKPT buffer failure                                0
```

Related Commands

Command	Description
mls ip multicast sso	Configures the SSO parameters.

show mpls mldp bindings

To display the bindings (the upstream and downstream label assignments) for Multicast Label Distribution Protocol (MLDP) traffic, use the **show mpls mldp bindings** command in user EXEC or privileged EXEC mode.

show mpls mldp bindings [**id** *id*] [**opaque_type** *type*] [**summary**]

Syntax Description

id *id*	(Optional) The Label Switched Multicast (LSM) ID whose MLDP entry is to be displayed.
opaque_type *type*	(Optional) The opaque type to be used for filtering. The following types are supported: • **ipv4** *source-group*—this represents the "IPv4 Protocol Independent Source-Specific Transit" multicast application type. The IPv4 source address and group address are also specified. • **ipv6** *source-group*—this represents the "IPv6 Protocol Independent Source-Specific Transit" multicast application type.The IPv6 source address and group address are also specified. • **mdt** *vpn-id mdt-number*—this represents the "Multicast Virtual Private Network (MVPN)" multicast application type. The VPN identifier and the Multicast Distribution Tree (MDT) number are also specified. • **vpnv4** *source-group route-distinguisher*—this represents the "Direct MDT (VPNv4) " multicast application type.The IPv4 source address, group address, and the VPN route distinguisher are also specified. • *type-number*—the type-number. Valid values are from 0-65535.
summary	(Optional) The MLDP database summary.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

This command displays the bindings (the upstream and downstream label assignments) for MLDP traffic. The bindings map Multicast Data Trees (MDTs) to Multicast Label Switch Paths (LSPs). LSPs are used to transmit multicast traffic within an MPLS core network.

Examples

The following is sample output from the **show mpls mldp bindings** command.

```
Router# show mpls mldp bindings

System ID: D3000001
Type: MP2MP, Root Node: 172.30.20.1, Opaque Len: 14
Opaque value: [mdt 1:1 0]
lsr: 172.30.20.1:0, remote binding[U]: 30, local binding[D]: 30 active
```

Table 64 describes the significant fields shown in the display.

Table 64 show mpls mldp bindings Field Descriptions

Field	Description
System ID	The LSM ID whose MLDP entry is displayed.
Type	The type of LSP used (can be point-to-multipoint (P2MP) or multipoint-to-multipoint (MP2MP)).
Root Node	The root of the MDT.
Opaque value	A value which is used to uniquely identify the MP LSP.
lsr	The Label Switched Router ID.
remote binding	The label used remotely to map MDTs to Multicast LSPs.
local binding	The label used locally to map MDTs to Multicast LSPs.

Related Commands

Command	Description
show mpls mldp database	Displays MLDP information.

show mpls mldp count

To display Multicast Label Distribution Protocol (MLDP) count information, use the **show mpls mldp count** command in user EXEC or privileged EXEC mode.

show mpls mldp count

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Examples

The following is sample output from the **show mpls mldp label count** command:

```
Router# show mpls mldp label count

MLDP Database Summary:
  Number of MP2MP Entries : 1
  Number of P2MP Entries  : 0
  Total Number of Entries : 1
```

Usage Guidelines

This command displays the MLDP count information, which is the total number of MLDP entries in the MLDP database. An entry can be a point-to-multipoint (P2MP) Label Switched Path (LSP) or an multipoint-to-multipoint (MP2MP) LSP. These statistics provide a summary on the usage of MLDP. LSPs are used to transmit multicast traffic within an MPLS core network.

Related Commands

Command	Description
show mpls mldp database	Displays MLDP information.

show mpls mldp database

To display Multicast Label Distribution Protocol (MLDP) information, use the **show mpls mldp database** command in user EXEC or privileged EXEC mode.

show mpls mldp database [**id** *id*] [**opaque_type** *type*] [**summary**]

Syntax Description

id *id*	(Optional) The Label Switched Multicast (LSM) ID whose MLDP entry is to be displayed.
opaque_type *type*	(Optional) The opaque type to be used for filtering. The following types are supported: • **ipv4** *source-group*—this represents the "IPv4 Protocol Independent Source-Specific Transit" multicast application type. The IPv4 source address and group address are also specified. • **ipv6** *source-group*—this represents the "IPv6 Protocol Independent Source-Specific Transit" multicast application type.The IPv6 source address and group address are also specified. • **mdt** *vpn-id mdt-number*—this represents the "Multicast Virtual Private Network (MVPN)" multicast application type. The VPN identifier and the Multicast Distribution Tree (MDT) number are also specified. • **vpnv4** *source-group route-distinguisher*—this represents the "Direct MDT (VPNv4) " multicast application type.The IPv4 source address, group address, and the VPN route distinguisher are also specified. • *type-number*—the type-number. Valid values are from 0-65535.
summary	(Optional) The MLDP database summary.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

This command displays the contents for MLDP entries in the MLDP database. Each MLDP entry provides the configuration details associated with each point-to-multipoint (P2MP) and multipoint-to-multipoint (MP2MP) Label Switched Path (LSP) used to transmit multicast traffic within an MPLS core network.

Examples

The following is sample output from the **show mpls mldp database** command.

```
Router# show mpls mldp database opaque_type mdt 100:2

* Indicates MLDP recursive forwarding is enabled

LSM ID : D3000001 (RNR LSM ID: 8A000002)   Type: MP2MP   Uptime : 00:04:54
  FEC Root           : 172.30.20.1
  Opaque decoded     : [mdt 100:2 0]
  Opaque length      : 11 bytes
  Opaque value       : 07 000B 00000100000000100000000
  RNR active LSP     : (this entry)
  Upstream client(s) :
    172.30.20.1:0    [Active]
      Expires        : Never         Path Set ID  : 99000001
      Out Label (U)  : 32            Interface    : Ethernet1/0*
      Local Label (D): 30            Next Hop     : 10.0.1.7
  Replication client(s):
    MDT  (VRF blue)
      Uptime         : 00:04:54      Path Set ID  : 5000002
      Interface      : Lspvif0
```

Table 65 describes the significant fields shown in the display.

Table 65 show mpls mldp database Field Descriptions

Field	Description
LSM ID	The LSM ID whose MLDP entry is displayed.
Type	The type of LSP used. This can P2MP or MP2MP.
FEC Root	The root of the MDT.
Opaque value	A value which is used to uniquely identify the MP LSP.
RNR active LSP	The primary root for upstream forwarding.
Upstream client(s)	The upstream clients are the upstream nodes of the MP2MP LSP.
Replication client(s)	The Replication Clients are the downstream nodes of the MP2MP LSP. They receive multipoint replicated traffic.

Related Commands

Command	Description
show mpls mldp bindings	Displays the bindings (the upstream and downstream label assignments) for MLDP traffic.

show mpls mldp label release

To display Multicast Label Distribution Protocol (MLDP) labels that have been withdrawn and awaiting release, use the **show mpls mldp label release** command in user EXEC or privileged EXEC mode.

show mpls mldp label release

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

This command displays the MLDP labels that have been withdrawn and awaiting release. These are the labels that are no longer being used by point-to-multipoint (P2MP) Label Switched Paths (LSPs) or multipoint-to-multipoint (MP2MP) LSPs. LSPs are used to transmit multicast traffic within an MPLS core network.

Examples

The following is sample output from the **show mpls mldp label release** command:

```
Router# show mpls mldp label release

Label releaseQ, scan scheduled in: 00:00:12
Label 30   expire: 00:00:12
```

Related Commands

Command	Description
mpls mldp	Enables the MLDP feature.

show mpls mldp neighbors

To display Multicast Label Distribution Protocol (MLDP) neighbor information, use the **show mpls mldp neighbors** command in user EXEC or privileged EXEC mode.

show mpls mldp neighbors [*hostname* | *source-address*]

Syntax Description

hostname	(Optional) The neighbor hostname.
source-address	(Optional) The source address whose MLDP entry is to be displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

This command displays the MLDP peers (neighbors) known to the router. It also displays the associated Label Switched Path (LSP). LSPs are used to transmit multicast traffic within an MPLS core network.

Examples

The following is sample output from the **show mpls mldp neighbors** command:

```
Router# show mpls mldp neighbors

MLDP peer ID    : 172.30.20.2:0, uptime 00:05:10 Up,
  Target Adj     : No
  Session hndl   : 1
  Upstream count : 0
  Branch count   : 0
  Path count     : 1
  Path(s)        : 10.0.1.4          LDP Ethernet1/0
  Nhop count     : 0

MLDP peer ID    : 172.30.20.2:0, uptime 00:05:09 Up,
  Target Adj     : No
  Session hndl   : 2
  Upstream count : 1
  Branch count   : 0
  Path count     : 1
  Path(s)        : 10.0.1.7          LDP Ethernet1/0
  Nhop count     : 1
  Nhop list      : 10.0.1.7
```

Table 65 describes the significant fields shown in the display.

Table 66 show mpls mldp neighbors Field Descriptions

Field	Description
MLDP peer ID	The MLDP identifier of the neighbor (peer).
Upstream count	The number of nodes upstream of the LSP.
Path count	The number of LSPs.
Path(s)	A value which is used to uniquely identify the MP LSP.
Nhop count	The number of configured next hops.
Nhop list	The addresses of the next hops.

Related Commands

Command	Description
show mpls mldp database	Displays MLDP information.

show mpls mldp root

To display Multicast Label Distribution Protocol (MLDP) root information, use the **show mpls mldp root** command in user EXEC or privileged EXEC mode.

show mpls mldp root [*hostname* | *source-address*]

Syntax Description

hostname	(Optional) The root hostname.
source-address	(Optional) The source address whose MLDP entry is to be displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Usage Guidelines

This command displays Multicast Label Distribution Protocol (MLDP) root information. The root is the common entry between multiple Label Switch Paths (LSPs). LSPs are used to transmit multicast traffic within an MPLS core network.

Examples

The following is sample output from the **show mpls mldp label root** command:

```
Router# show mpls mldp label root 10.0.0.1

Root node    : 172.30.20.1
  Metric      : 20
  Distance    : 115
  Interface   : Ethernet1/0 (via unicast RT)
  FEC count   : 1
  Path count  : 1
  Path(s)     : 10.0.1.7         LDP nbr: 100.100.100.100:0 Ethernet1/0
```

Table 65 describes the significant fields shown in the display.

Table 67 show mpls mldp root Field Descriptions

Field	Description
Root node	The root node ID.
Path count	The number of LSPs.
Path(s)	A value which is used to uniquely identify the MP LSP.

Related Commands

Command	Description
show mpls mldp database	Displays MLDP information.

show platform software multicast ip bidir

Todisplay bidirectional (Bidir) information, use the **show platform software multicast ip bidir** command in privileged EXEC mode.

show platform software multicast ip bidir [**group** *group-name* | **interface** [**gigabitethernet** *1-6* | **port-channel** *1-256* | **tengigabitethernet** *1-6* | **vlan** *1-4094]*| **source** *A.B.C.D.*]

Syntax Description

group	Displays entries for a specific multicast group address.
group-name	Hostname or group IP address.
interface	Displays entries for a specific interface.
gigabitethernet *1-6*	Specifies the GigabitEthernet interface number. The range is 1 through 6.
port-channel *1-256*	Specifies the port-channel interface number. The range is 1 through 256.
tengigabitethernet *1-6*	Specifies the TenGigabitEthernet interface number. The range is 1 through 6.
vlan *1-4094*	Specifies the VLAN interface number. The range is 1 through 4094.
source	Displays entries for a specific source.
A.B.C.D.	Specifies source IP address.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRE	This command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to display bidirectional (Bidir) information:

```
Router# show platform software multicast ip bidir
Multicast hardware switched flows:

Total hardware switched flows: 0
```

This example shows how to display bidirectional (Bidir) information for a specific multicast group address:

```
Router# show platform software multicast ip bidir group 232.0.1.4
Multicast hardware switched flows:

Total hardware switched flows: 0

Router#
```

This example shows how to display bidirectional (Bidir) information for a specific interface:

```
Router# show platform software multicast ip bidir interface tengigabitethernet 4/2
Multicast hardware switched flows:

Total hardware switched flows: 0
```

```
Router#
```

This example shows how to display bidirectional (Bidir) information for a specific source:

```
Router# show platform software multicast ip bidir source 40.0.0.2
Multicast hardware switched flows:

Total hardware switched flows: 0

Router#
```

Related Commands

Command	Description
show platform software multicast ip bidir	Displays bidirectional (Bidir) information.
show platform software multicast ip capability	Displays multicast replication capability.
show platform software multicast ip complete	Displays complete hardware switched entries.
show platform software multicast ip connected	Displays installed interface and mask entries.
show platform software multicast ip group	Displays entries for a specific multicast group address.
show platform software multicast ip interface	Displays entries for a specific interface.
show platform software multicast ip partial	Displays partially hardware switched entries for a specific interface.
show platform software multicast ip source	Displays partially hardware switched entries for a specific source.
show platform software multicast ip statistics	Displays partially hardware switched entries for a specific source.
show platform software multicast ip summary	Displays a summary of installed-hardware shortcuts.
show platform software multicast ip vrf	Displays entries for a specific VRF.

show platform software multicast ip capability

To display multicast replication capability, use the **show platform software multicast ip capability** command in privileged EXEC mode.

show platform software multicast ip capability [**module** *module-id*]

Syntax Description		
	module *module-id*	(Optional) Displays module specific multicast repliecation capability. The *module-id* range is 1 through 6.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRE	This command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to display multicast replication capability:

```
Router# show platform software multicast ip capability
Current System HW Replication Mode : Egress
Auto-detection of Replication Mode : ON

Slot Replication-Capability Replication-Mode
   2 Egress                 Egress
   3 Egress                 Egress
   4 Egress                 Egress
   6 Egress                 Egress
Router#
```

Related Commands

Command	Description
show platform software multicast ip bidir	Displays bidirectional (Bidir) information.
show platform software multicast ip capability	Displays multicast replication capability.
show platform software multicast ip complete	Displays complete hardware switched entries.
show platform software multicast ip connected	Displays installed interface and mask entries.
show platform software multicast ip group	Displays entries for a specific multicast group address.

Command	Description
show platform software multicast ip interface	Displays entries for a specific interface.
show platform software multicast ip partial	Displays partially hardware switched entries for a specific interface.
show platform software multicast ip source	Displays partially hardware switched entries for a specific source.
show platform software multicast ip statistics	Displays partially hardware switched entries for a specific source.
show platform software multicast ip summary	Displays a summary of installed-hardware shortcuts.
show platform software multicast ip vrf	Displays entries for a specific VRF.

show platform software multicast ip complete

To display complete hardware switched entries, use the **show platform software multicast ip complete** command in privileged EXEC mode.

show platform software multicast ip complete [**group** *A.B.C.D.* | **interface** [**gigabitethernet** *1-6* | **port-channel** *1-256* | **tengigabitethernet** *1-6* | **vlan** *1-4094]* | **source** *A.B.C.D.*]

Syntax Description

group	Displays entries for a specific multicast group address.
A.B.C.D	Specifies the group IP address.
interface	Displays entries for a specific interface.
gigabitethernet *1-6*	Specifies the GigabitEthernet interface number. The range is 1 through 6.
port-channel *1-256*	Specifies the port-channel interface number. The range is 1 through 256.
tengigabitethernet *1-6*	Specifies the TenGigabitEthernet interface number. The range is 1 through 6.
vlan *1-4094*	Specifies the VLAN interface number. The range is 1 through 4094.
source	Displays entries for a specific source.
A.B.C.D.	Specifies source IP address.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRE	This command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to display complete hardware switched entries:

```
Router# show platform software multicast ip complete
Multicast hardware switched flows:

(40.0.0.2, 232.0.1.4) Incoming interface: GigabitEthernet3/2/1, Packets Switched: 6610137
Hardware switched outgoing interfaces:
     Tunnel10

Total hardware switched flows: 1

Router
```

This example shows how to display entries for a specific multicast group address:

```
Router# show platform software multicast ip complete group 232.0.1.4
Multicast hardware switched flows:

(40.0.0.2, 232.0.1.4) Incoming interface: GigabitEthernet3/2/1, Packets Switched: 6799184
Hardware switched outgoing interfaces:
     Tunnel10

Total hardware switched flows: 1

Router#
```

This example shows how to display complete hardware switched entries for a specific inteface:

```
Router# show platform software multicast ip complete interface gigabitethernet 3/2/1
Multicast hardware switched flows:

(40.0.0.2, 232.0.1.4) Incoming interface: GigabitEthernet3/2/1, Packets Switched: 7008473
Hardware switched outgoing interfaces:
     Tunnel10

Total hardware switched flows: 1

Router#
```

This example shows how to display complete hardware switched entries for a specific group:

```
Router# show platform software multicast ip complete group 232.0.1.4
Multicast hardware switched flows:

(40.0.0.2, 232.0.1.4) Incoming interface: GigabitEthernet3/2/1, Packets Switched: 7163170
Hardware switched outgoing interfaces:
     Tunnel10

Total hardware switched flows: 1

PE1-7600#
```

Related Commands

Command	Description
show platform software multicast ip bidir	Displays bidirectional (Bidir) information.
show platform software multicast ip capability	Displays multicast replication capability.
show platform software multicast ip complete	Displays complete hardware switched entries.
show platform software multicast ip connected	Displays installed interface and mask entries.
show platform software multicast ip group	Displays entries for a specific multicast group address.
show platform software multicast ip interface	Displays entries for a specific interface.
show platform software multicast ip partial	Displays partially hardware switched entries for a specific interface.
show platform software multicast ip source	Displays partially hardware switched entries for a specific source.

Command	Description
show platform software multicast ip statistics	Displays partially hardware switched entries for a specific source.
show platform software multicast ip summary	Displays a summary of installed-hardware shortcuts.
show platform software multicast ip vrf	Displays entries for a specific VRF.

show platform software multicast ip connected

To display installed interface and mask entries, use the **show platform software multicast ip connected** command in privileged EXEC mode.

show platform software multicast ip connected

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRE	This command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to display installed interface and mask entries:

```
Router# show platform software multicast ip connected
Multicast CEF Entries for VPN#0
Flags: R - Control, S - Subnet, B - Bidir, C - Complete, P - Partial, E - Encapsulation, D
- Decapsulation, M - MAC rewrite, T - Forwarding
       c - Central Rewrite, p - Primary Input, r - Recirculation, h - Entry sitting on
Encap/Decap VRF layer
Source/mask         Destination/mask    RPF/DF  Flags  #packets      #bytes
rwindex  Output Vlans/Info
+-------------------+-------------------+-------+------+-------------+------------------+-
-------+------------------------------+
Found 0 entries. 0 are mfd entries
PE1-7600
```

Related Commands

Command	Description
show platform software multicast ip bidir	Displays bidirectional (Bidir) information.
show platform software multicast ip capability	Displays multicast replication capability.
show platform software multicast ip complete	Displays complete hardware switched entries.
show platform software multicast ip connected	Displays installed interface and mask entries.
show platform software multicast ip group	Displays entries for a specific multicast group address.

Command	Description
show platform software multicast ip interface	Displays entries for a specific interface.
show platform software multicast ip partial	Displays partially hardware switched entries for a specific interface.
show platform software multicast ip source	Displays partially hardware switched entries for a specific source.
show platform software multicast ip statistics	Displays partially hardware switched entries for a specific source.
show platform software multicast ip summary	Displays a summary of installed-hardware shortcuts.
show platform software multicast ip vrf	Displays entries for a specific VRF.

show platform software multicast ip interface

To display entries for a specific interface, use the **show platform software multicast ip interface** command in privileged EXEC mode.

show platform software multicast ip interface [**gigabitethernet** *1-6* | **port-channel** *1-256* | **tengigabitethernet** *1-6* | **vlan** *1-4094]* | **source** *A.B.C.D.*]

Syntax Description

gigabitethernet *1-6*	Specifies the GigabitEthernet interface number. The range is 1 through 6.
port-channel *1-256*	Specifies the port-channel interface number. The range is 1 through 256.
tengigabitethernet *1-6*	Specifies the TenGigabitEthernet interface number. The range is 1 through 6.
vlan *1-4094*	Specifies the VLAN interface number. The range is 1 through 4094.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRE	This command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to display entries for a gigabitethernet interface:

```
Router# show platform software multicast ip interface gigabitethernet 3/2/1
Multicast hardware switched flows:

(40.0.0.2, 232.0.1.4) Incoming interface: GigabitEthernet3/2/1, Packets Switched: 8206582
Hardware switched outgoing interfaces:
     Tunnel10

Total hardware switched flows: 1

PE1-7600#
```

Related Commands

Command	Description
show platform software multicast ip bidir	Displays bidirectional (Bidir) information.
show platform software multicast ip capability	Displays multicast replication capability.
show platform software multicast ip complete	Displays complete hardware switched entries.
show platform software multicast ip connected	Displays installed interface and mask entries.

Command	Description
show platform software multicast ip group	Displays entries for a specific multicast group address.
show platform software multicast ip interface	Displays entries for a specific interface.
show platform software multicast ip partial	Displays partially hardware switched entries for a specific interface.
show platform software multicast ip source	Displays partially hardware switched entries for a specific source.
show platform software multicast ip statistics	Displays partially hardware switched entries for a specific source.
show platform software multicast ip summary	Displays a summary of installed-hardware shortcuts.
show platform software multicast ip vrf	Displays entries for a specific VRF.

show platform software multicast ip partial

To display partially hardware switched entries, use the **show platform software multicast ip partial** command in privileged EXEC mode.

show platform software multicast ip partial [**group** *group-name* | **interface** [**gigabitethernet** *1-6* | **port-channel** *1-256* | **tengigabitethernet** *1-6* | **vlan** *1-4094]*| **source** *A.B.C.D.*]

Syntax Description

group	Displays entries for a specific multicast group address.
group-name	Hostname or group IP address.
interface	Displays entries for a specific interface.
gigabitethernet *1-6*	Specifies the GigabitEthernet interface number. The range is 1 through 6.
port-channel *1-256*	Specifies the port-channel interface number. The range is 1 through 256.
tengigabitethernet *1-6*	Specifies the TenGigabitEthernet interface number. The range is 1 through 6.
vlan *1-4094*	Specifies the VLAN interface number. The range is 1 through 4094.
source	Displays entries for a specific source.
A.B.C.D.	Specifies source IP address.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRE	This command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to display partially hardware switched entries for a specific group:

```
Router# show platform software multicast ip partial group 232.0.1.4
Multicast hardware switched flows:

Total hardware switched flows: 0

PE1-7600#
```

This example shows how to display partially hardware switched entries for a specific interface:

```
Router# show platform multicast ip partial interface gigabitethernet 3/2/1
Multicast hardware switched flows:

Total hardware switched flows: 0

PE1-7600
```

Related Commands

Command	Description
show platform software multicast ip bidir	Displays bidirectional (Bidir) information.
show platform software multicast ip capability	Displays multicast replication capability.
show platform software multicast ip complete	Displays complete hardware switched entries.
show platform software multicast ip connected	Displays installed interface and mask entries.
show platform software multicast ip group	Displays entries for a specific multicast group address.
show platform software multicast ip interface	Displays entries for a specific interface.
show platform software multicast ip partial	Displays partially hardware switched entries for a specific interface.
show platform software multicast ip source	Displays partially hardware switched entries for a specific source.
show platform software multicast ip statistics	Displays partially hardware switched entries for a specific source.
show platform software multicast ip summary	Displays a summary of installed-hardware shortcuts.
show platform software multicast ip vrf	Displays entries for a specific VRF.

show platform software multicast ip source

To display partially hardware switched entries for a specific source, use the **show platform software multicast ip source** command in privileged EXEC mode.

show platform software multicast ip source *source-ip*

Syntax Description		
	source *source-ip*	Displays hardware-entry information based on the specified source IP address.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRE	This command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to display partially hardware switched entries for a specific source:

```
PE1-7600# show platform software multicast ip source 40.0.0.2
Multicast hardware switched flows:

(40.0.0.2, 232.0.1.4) Incoming interface: GigabitEthernet3/2/1, Packets Switched: 8778143
Hardware switched outgoing interfaces:
     Tunnel10

Total hardware switched flows: 1

PE1-7600#
```

Related Commands

Command	Description
show platform software multicast ip bidir	Displays bidirectional (Bidir) information.
show platform software multicast ip capability	Displays multicast replication capability.
show platform software multicast ip complete	Displays complete hardware switched entries.
show platform software multicast ip connected	Displays installed interface and mask entries.
show platform software multicast ip group	Displays entries for a specific multicast group address.

Command	Description
show platform software multicast ip interface	Displays entries for a specific interface.
show platform software multicast ip partial	Displays partially hardware switched entries for a specific interface.
show platform software multicast ip source	Displays partially hardware switched entries for a specific source.
show platform software multicast ip statistics	Displays partially hardware switched entries for a specific source.
show platform software multicast ip summary	Displays a summary of installed-hardware shortcuts.
show platform software multicast ip vrf	Displays entries for a specific VRF.

show platform software multicast ip statistics

To display partially hardware switched entries for a specific source, use the **show platform software multicast ip statistics** command in privileged EXEC mode.

show platform software multicast ip statistics [**group** *group-id*]

Syntax Description

group *group-id*	(Optional) Displays hardware-entry information that is based on the specified group IP address.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRE	This command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to display partially hardware switched entries for a specific source:

```
Router# show platform software multicast ip statistics group 232.0.1.4
Warning: No stats to be printed
```

Related Commands

Command	Description
show platform software multicast ip bidir	Displays bidirectional (Bidir) information.
show platform software multicast ip capability	Displays multicast replication capability.
show platform software multicast ip complete	Displays complete hardware switched entries.
show platform software multicast ip connected	Displays installed interface and mask entries.
show platform software multicast ip group	Displays entries for a specific multicast group address.
show platform software multicast ip interface	Displays entries for a specific interface.
show platform software multicast ip partial	Displays partially hardware switched entries for a specific interface.

Command	Description
show platform software multicast ip source	Displays partially hardware switched entries for a specific source.
show platform software multicast ip statistics	Displays partially hardware switched entries for a specific source.
show platform software multicast ip summary	Displays a summary of installed-hardware shortcuts.
show platform software multicast ip vrf	Displays entries for a specific VRF.

show platform software multicast ip summary

To display a summary of installed-hardware shortcuts, use the **show platform software multicast ip summary** command in privileged EXEC mode.

show platform software multicast ip summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRE	This command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to display a summary of installed-hardware shortcuts:

```
Router# show platform software multicast ip summary

IPv6 Multicast Netflow SC summary on Slot[7]:
Shortcut Type               Shortcut count
--------------------------+--------------
(S, G)                      0

IPv6 Multicast FIB SC summary on Slot[7]:
Shortcut Type               Shortcut count
--------------------------+--------------
(*, G/128)                  0
(*, G/m)                    0
```

Related Commands

Command	Description
show platform software multicast ip bidir	Displays bidirectional (Bidir) information.
show platform software multicast ip capability	Displays multicast replication capability.
show platform software multicast ip complete	Displays complete hardware switched entries.
show platform software multicast ip connected	Displays installed interface and mask entries.
show platform software multicast ip group	Displays entries for a specific multicast group address.

Command	Description
show platform software multicast ip interface	Displays entries for a specific interface.
show platform software multicast ip partial	Displays partially hardware switched entries for a specific interface.
show platform software multicast ip source	Displays partially hardware switched entries for a specific source.
show platform software multicast ip statistics	Displays partially hardware switched entries for a specific source.
show platform software multicast ip summary	Displays a summary of installed-hardware shortcuts.
show platform software multicast ip vrf	Displays entries for a specific VRF.

show platform software multicast ip vrf

To display entries for a specific VRF, use the **show platform software multicast ip vrf** command in privileged EXEC mode.

show platform software multicast ip vrf vrf*p-id*

Syntax Description		
vrf *vrf-id*	Displays hardware-entry information that is based on the specified VRF ID; valid values are from 0 to 4095.	

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRE	This command was introduced on the Cisco 7600 series routers.

Examples

This example shows how to display entries for a specific VRF:

```
Router# show platform software multicast ip vrf vrfp-id
SIP-600-3#sh platform software multicast ip cmfib vrf red 232.5.5.5 verbose
Multicast CEF Entries for VPN#3
(10.0.0.1, 232.5.5.5)
IOSVPN:258  (1) PI:1 (1) CR:0 (1) Recirc:0 (1)
Vlan:1037 AdjPtr:131076 FibRpfNf:1 FibRpfDf:1 FibAddr:0x30056
rwvlans:1037 rwindex:0x7FFA adjmac:0008.e287.65c0 rdt:1 E:0 CAP1:0
fmt:Mcast l3rwvld:1 DM:0 mtu:1518 rwtype:L2&L3 met2:0xD met3:0x7
packets:0000001266681 bytes:000000000506672400
Starting Offset: 0x000D
V E L0 C:1019 I:0x0200F ----------->index of egress multicast vlan of vrf
Starting Offset: 0x0007
V E C:1041

MLSVPN:264  (1) PI:1 (1) CR:1 (1) Recirc:1 (1)
Vlan:1037 AdjPtr:131078 FibRpfNf:1 FibRpfDf:1 FibAddr:0x3005A
rwvlans:1037 rwindex:0x7FFF adjmac:0000.0000.0000 rdt:1 E:0 CAP1:0
fmt:Mcast l3rwvld:0 DM:0 mtu:1522 rwtype:- met2:0x0 met3:0x0
packets:0000000000000 bytes:000000000000000000
IOSVPN:258  (1) PI:0 (1) CR:1 (1) Recirc:0 (1)
Vlan:1019 AdjPtr:131077 FibRpfNf:0 FibRpfDf:1 FibAddr:0x30058
rwvlans:1019 rwindex:0x7FFA adjmac:0008.e287.65c0 rdt:1 E:0 CAP1:0
fmt:Mcast l3rwvld:1 DM:0 mtu:1518 rwtype:L3 met2:0x0 met3:0x7
packets:0000000000000 bytes:000000000000000000
Starting Offset: 0x0007
V E C:1041

Annotation-data: [0x4E2B1B80]
A-vlan: 1037 NS-vlan: 0 RP-rpf-vlan: 0
Anntn flags: [0x100010]  H MT
MTU: 1500 Retry-count: 65534
Sec-entries count: 2
Met-handle: 0x46C8E080 New-Met-handle: 0x0
Met2-handle: 0x56141BAC
```

```
HAL L3-data : [0x56141E28]
Flags: 0x4 FIB-index: 0x86C ADJ-index: 0x20004 NF-addr: 0x0
ML3 entry type: 0x0 [(S,G) shortcut]
Flags: 0xA1000000 Vpn: 258 Rpf: 1037 Rw_index: 0x7FFA
Adj_mtu: 1514 Met2: 0xD Met3: 0x7
V6-data: NULL

---Secondary entry [1]---

HAL L3-data : [0x56141EE4]
Flags: 0x4 FIB-index: 0x86E ADJ-index: 0x20006 NF-addr: 0x0
ML3 entry type: 0x0 [(S,G) shortcut]
Flags: 0xB9400000 Vpn: 264 Rpf: 1037 Rw_index: 0x7FFF
Adj_mtu: 1514 Met2: 0x0 Met3: 0x0
V6-data: NULL

---Secondary entry [2]---

HAL L3-data : [0x46C8E37C]
Flags: 0x4 FIB-index: 0x86D ADJ-index: 0x20005 NF-addr: 0x0
ML3 entry type: 0x0 [(S,G) shortcut]
Flags: 0x90000000 Vpn: 258 Rpf: 1019 Rw_index: 0x7FFA
Adj_mtu: 1514 Met2: 0x0 Met3: 0x7
V6-data: NULL

---TE entries---
```

Related Commands

Command	Description
show platform software multicast ip bidir	Displays bidirectional (Bidir) information.
show platform software multicast ip capability	Displays multicast replication capability.
show platform software multicast ip complete	Displays complete hardware switched entries.
show platform software multicast ip connected	Displays installed interface and mask entries.
show platform software multicast ip group	Displays entries for a specific multicast group address.
show platform software multicast ip interface	Displays entries for a specific interface.
show platform software multicast ip partial	Displays partially hardware switched entries for a specific interface.
show platform software multicast ip source	Displays partially hardware switched entries for a specific source.

Command	Description
show platform software multicast ip statistics	Displays partially hardware switched entries for a specific source.
show platform software multicast ip summary	Displays a summary of installed-hardware shortcuts.
ipv6 mfib hardware-switching	Configures hardware switching for IPv6 multicast packets on a global basis.

show router-guard

To display router guard status and configuration information, use the **show router-guard** command in privileged EXEC mode.

show router-guard [**interface** [*type mod*/*port*]]

Syntax Description

interface	(Optional) Specifies a list of all interfaces.
type	(Optional) Specifies the interface type; possible valid values are **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **port-channel** *num*, and **vlan** *vlan-id*.
mod/*port*	Module and port number.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

If the port is in the shutdown state, the system cannot determine if the port is in trunk mode or access mode, and you will not be able to display the status by entering the **show router-guard** command. In this case, you can enter the **show running-config interface** command to display the configuration.

Examples

Note This section does not contain output description tables as the output fields are self-explanatory.

The following example shows how to display global router guard configuration information:

```
Router# show router-guard

Router Guard for IP Multicast:
  Globally enabled for all switch ports
```

The following example shows how to display a list of all interfaces for which router guard is enabled:

```
Router# show router-guard interface

Router Guard for IP Multicast:
Globally enabled for all switchports
Interfaces:
Gi1/3/46: Disabled on this port for VLANS: ALL
```

The following example shows how to display router guard configuration and statistics for a specified interface:

```
Router# show router-guard interface gigabitethernet 1/3/48

Router Guard for IP Multicast:
Globally enabled for all switch ports
Enabled on this interface
Packets denied:
  IGMP Queries:                x
  PIMv2 Messages:              x
  PIMv1 Messages:              x
  DVMRP Messages:              x
  RGMP Messages:               x
  CGMP Messages:               x
```

Related Commands

Command	Description
clear router-guard ip multicast statistics	Clears the router guard statistical information.
router-guard ip multicast	Enables or disables the router guard for switch ports that are connected to multicast routers.
router-guard ip multicast switchports	Enables or disables the router guard on all switch ports.
show running-config interface	

snmp-server enable traps mvpn

To enable Multicast Virtual Private Network (MVPN) routing and forwarding (MVRF) trap notifications, use the **snmp-server enable traps mvpn** command in global configuration mode. To disable MVRF trap notifications, use the **no** form of this command.

snmp-server enable traps mvpn

no snmp-server enable traps mvpn

Syntax Description

This command has no arguments or keywords.

Command Default

MVRF traps are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(29)S	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

SNMP notifications can be sent as traps or informs. This command enables trap notification requests only.

This command controls (enables or disables) MVRF (ciscoMvpnMvrfChange) trap notifications. A ciscoMvpnMvrfChange trap notification signifies a change about a MVRF in the device. The change event can be the creation of an MVRF, the deletion of an MVRF, or an update on the default or data multicast distribution tree (MDT) configuration of an MVRF. The change event is indicated by the ciscoMvpnGenOperStatusChange object embedded in the trap notification.

MVRF trap notifications are defined by the ciscoMvpnMvrfChange object in the MVPN MIB. When this object is queried from a network management system (NMS) workstation, one of the following values is appended to the object to indicate the configuration state of MVRF trap notifications:

- true(1)—MVRF trap notifications are enabled.
- false(2)—MVRF trap notifications are disabled.

The following MVPN MIB tables can be queried to gather details about MVRF change events:

- ciscoMvpnGenericTable
- ciscoMvpnMdtDefaultTable
- ciscoMvpnMdtDataTable

Note For a complete description of the ciscoMvpnMvrfChange trap notification and MVPN MIB tables, see the CISCO_MVPN_MIB.my file, available on Cisco.com at http://www.cisco.com/go/mibs.

The **snmp-server enable traps mvpn** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

The following example shows how to enable MVRF traps to the host at IP address 10.3.32.154 using the community string defined as public:

```
snmp-server enable traps mvpn
snmp-server host 10.3.32.154 version 2c public
```

Related Commands

Command	Description
snmp-server community	Enables SNMP and sets the community string and access privileges.
snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp-server enable traps pim

To enable Protocol Independent Multicast (PIM) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps pim** command in global configuration mode. To disable PIM-specific SNMP notifications, use the **no** form of this command.

snmp-server enable traps pim [**neighbor-change** | **rp-mapping-change** | **invalid-pim-message**]

no snmp-server enable traps pim

Syntax Description

neighbor-change	(Optional) Enables notifications indicating when a router's PIM interface is disabled or enabled, or when a router's PIM neighbor adjacency expires.
rp-mapping-change	(Optional) Enables notifications indicating a change in the rendezvous point (RP) mapping information due to either Auto-RP or bootstrap router (BSR) messages.
invalid-pim-message	(Optional) Enables invalid PIM message traps. For example, an invalid PIM message could result when a router receives a join or prune message for which the RP specified in the packet is not the RP for the multicast group.

Command Default

SNMP notifications are disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests for the specified notification types. PIM notifications are defined in the CISCO-PIM-MIB.my and PIM-MIB.my files, available from Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Examples

The following example shows how to configure a router to generate notifications indicating that a PIM interface on the router has been enabled:

```
! Configure PIM traps to be sent as SNMPv2c traps to host with IP address 10.0.0.1.
Router(config)# snmp-server host 10.0.0.1 traps version 2c public pim

! Configure router to send the neighbor-change class of notifications to host.
```

```
Router(config)# snmp-server enable traps pim neighbor-change

! Enable PIM sparse-dense mode on Ethernet interface 0/0.
Router(config)# interface ethernet0/0
Router(config-if)# ip pim sparse-dense-mode
```

Related Commands

Command	Description
snmp-server enable traps	Enables all available SNMP notifications on your system.
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface from which an SNMP trap should originate.

tunnel udlr address-resolution

To enable the forwarding of the Address Resolution Protocol (ARP) and Next Hop Resolution Protocol (NHRP) over a unidirectional link (UDL), use the **tunnel udlr address-resolution** command in interface configuration mode. To disable forwarding, use the **no** form of this command.

tunnel udlr address-resolution

no tunnel udlr address-resolution

Syntax Description

This command has no arguments or keywords.

Defaults

The command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is configured on the send-only tunnel interface of a downstream router.

Examples

The following example shows how to configure the **tunnel udlr address-resolution** command on an interface to enable ARP and NHRP over a send-only tunnel. An ARP address resolution request received from the upstream router on the UDL (Ethernet interface 0) will be replied to over the send-only tunnel of the receiver. Likewise, an ARP request may be sent by the downstream router over the send-only tunnel, and the response will be received over the UDL.

```
interface tunnel 0
tunnel udlr send-only ethernet 0
tunnel udlr address-resolution
```

Related Commands

Command	Description
tunnel udlr send-only	Configures a unidirectional, GRE tunnel to act as a back channel that can send messages, when another interface is configured for UDLR to receive messages.

tunnel udlr receive-only

To configure a unidirectional, generic routing encapsulation (GRE) tunnel to act as a back channel that can receive messages, when another interface is configured for unidirectional link routing (UDLR) to send messages, use the **tunnel udlr receive-only** command in interface configuration mode. To remove the tunnel, use the **no** form of this command.

tunnel udlr receive-only *interface-type interface-number*

no tunnel udlr receive-only *interface-type interface-number*

Syntax Description

interface-type interface-number	Interface type and number. The *interface-type* and *interface-number* arguments must match the unidirectional send-only interface type and number specified by the **interface** command. Thus, when packets are received over the tunnel, the upper layer protocols will treat the packets as if they are received over the unidirectional send-only interface.

Defaults

No UDLR tunnel is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to configure a router that has a unidirectional interface with send-only capabilities. One example of when you might configure this command is if you have traffic traveling via a satellite.

The *interface-type* and *interface-number* arguments must match the send-only interface type and number specified by the **interface** command.

You must configure the **tunnel udlr send-only** command at the opposite end of the tunnel.

If you have a large number of receivers, you should configure UDLR by an alternative means: Internet Group Management Protocol (IGMP) UDLR. See the description of the **ip igmp unidirectional-link** command.

Examples

In the following example, Router A (the upstream router) is configured with Open Shortest Path First (OSPF) and Protocol Independent Multicast (PIM). Serial interface 0 has send-only capability. Therefore, the UDLR tunnel is configured as receive-only, and points to serial interface 0.

Router A Configuration

```
ip multicast-routing
!
! Serial0 has send-only capability
!
interface serial 0
 encapsulation hdlc
 ip address 10.1.0.1 255.255.0.0
 ip pim sparse-dense-mode
!
! Configure tunnel as receive-only UDLR tunnel.
!
interface tunnel 0
 tunnel source ethernet 0
 tunnel destination <downstream-router>
 tunnel udlr receive-only serial 0
!
! Configure OSPF.
!
router ospf <pid>
 network 10.0.0.0 0.255.255.255 area 0
```

Router B (the downstream router) is configured with OSPF and PIM. Serial interface 1 has receive-only capability. Therefore, the UDLR tunnel is configured as send-only, and points to serial interface 1.

Router B Configuration

```
ip multicast-routing
!
! Serial1 has receive-only capability
!
interface serial 1
 encapsulation hdlc
 ip address 10.1.0.2 255.255.0.0
 ip pim sparse-dense-mode

!
! Configure tunnel as send-only UDLR tunnel.
!
interface tunnel 0
 tunnel source ethernet 0
 tunnel destination <upstream-router>
 tunnel udlr send-only serial 1
!
! Configure OSPF.
!
router ospf <pid>
 network 10.0.0.0 0.255.255.255 area 0
```

Related Commands

Command	Description
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
interface tunnel	Configures a tunnel interface.

Command	Description
ip igmp unidirectional-link	Configures an interface to be unidirectional and enables it for IGMP UDLR.
tunnel udlr send-only	Configures a unidirectional, GRE tunnel to act as a back channel that can send messages, when another interface is configured for UDLR to receive messages.

tunnel udlr send-only

To configure a unidirectional, generic routing encapsulation (GRE) tunnel to act as a back channel that can send messages, when another interface is configured for unidirectional link routing (UDLR) to receive messages, use the **tunnel udlr send-only** command in interface configuration mode. To remove the tunnel, use the **no** form of this command.

tunnel udlr send-only *interface-type interface-number*

no tunnel udlr send-only *interface-type interface-number*

Syntax Description

interface-type interface-number	Interface type and number. The *interface-type* and *interface-number* arguments must match the unidirectional receive-only interface type and number specified by the **interface** command. Thus, when packets are sent by upper layer protocols over the interface, they will be redirected and sent over this GRE tunnel.

Defaults

No UDLR tunnel is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to configure a router that has a unidirectional interface with receive-only capabilities. The UDLR tunnel will act as a back channel. One example of when you might configure this command is if you have traffic traveling via a satellite.

The *interface-type* and *interface-number* arguments must match the receive-only interface type and number specified by the **interface** command.

You must configure the **tunnel udlr receive-only** command at the opposite end of the tunnel.

Examples

In the following example, Router A (the upstream router) is configured with Open Shortest Path First (OSPF) and Protocol Independent Multicast (PIM). Serial interface 0 has send-only capability. Therefore, the UDLR tunnel is configured as receive-only, and points to serial interface 0.

Router A Configuration

```
ip multicast-routing
!
! Serial0 has send-only capability
```

```
!
interface serial 0
 encapsulation hdlc
 ip address 10.1.0.1 255.255.0.0
 ip pim sparse-dense-mode
!
! Configure tunnel as receive-only UDLR tunnel.
!
interface tunnel 0
 tunnel source ethernet 0
 tunnel destination <downstream-router>
 tunnel udlr receive-only serial 0
```

Router B (the downstream router) is configured with OSPF and PIM. Serial interface 1 has receive-only capability. Therefore, the UDLR tunnel is configured as send-only, and points to serial interface 1.

Router B Configuration

```
ip multicast-routing
!
! Serial1 has receive-only capability
!
interface serial 1
 encapsulation hdlc
 ip address 10.1.0.2 255.255.0.0
 ip pim sparse-dense-mode

!
! Configure tunnel as send-only UDLR tunnel.
!
interface tunnel 0
 tunnel source ethernet 0
 tunnel destination <upstream-router>
 tunnel udlr send-only serial 1
```

Related Commands

Command	Description
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
interface tunnel	Configures a tunnel interface.
ip igmp unidirectional-link	Configures an interface to be unidirectional and enables it for IGMP UDLR.
tunnel udlr address-resolution	Enables the forwarding of ARP and NHRP over a UDL.
tunnel udlr receive-only	Configures a unidirectional, GRE tunnel to act as a back channel that can receive messages, when another interface is configured for UDLR to send messages.

udp-port

To change the User Datagram Protocol (UDP) port numbers to which a Test Sender sends test packets or a Test Receiver sends status reports during Multicast Routing Monitor (MRM) tests, use the **udp-port** command in MRM manager configuration mode. To restore the default settings, use the **no** form of this command.

udp-port [**test-packet** *port-number*] [**status-report** *port-number*]

no udp-port

Syntax Description

test-packet *port-number*	(Optional) Specifies the UDP port number to which test packets are sent by a Test Sender. The port number must be even if the packets are Real-Time Transport Protocol (RTP)-encapsulated. The range is from 16384 to 65535. By default, the Test Sender uses UDP port number 16834 to send test packets.
status-report *port-number*	(Optional) Specifies the UDP port number to which status reports are sent by a Test Receiver. The port number must be odd if the packets are RTP Control Protocol (RTCP)-encapsulated. The range is from 16834 to 65535. By default, the Test Receiver uses UDP port number 65535 to send status reports.

Command Default

Test Senders use UDP port number 16834 to send test packets, and Test Receivers use UDP port number 65535 to send status reports.

Command Modes

MRM manager configuration (config-mrm-manager)

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to change the UDP port to which test packets are sent by a Test Sender to UDP port number 20302:

```
ip mrm manager test
 udp-port test-packet 20302
```

Related Commands

Command	Description
ip mrm	Configures an interface to operate as a Test Sender or Test Receiver, or both, for MRM.