PIM RPF Vector

First Published: November 8, 2004
Last Updated: November 6, 2006

The PIM RPF Vector feature was introduced to allow Protocol Independent Multicast (PIM) to work properly in an environment where core routers do not maintain external routing information. When this feature is configured, the address of the exit router is used as the Reverse Path Forwarding (RPF) vector and is inserted in the PIM join message. The core routers can then perform a RPF check on an IP address of the exit router instead of on the source router. This feature enables routers in an Multiprotocol Label Switching (MPLS) provider core to build multicast distribution trees without the need for the Border Gateway Protocol (BGP).

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for PIM RPF Vector" section on page 11.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

Contents

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Restrictions for PIM RPF Vector

- All upstream routers on the interface must support the PIM RPF vector.
- The PIM RPF Vector can not be used in conjuction with Bootstrap Router (BSR).

Information About PIM RPF Vector

To configure the PIM VPF Vector feature, you should understand the following concepts:

- PIM Join Format, page 3
- PIM Join Format, page 3

Overview of PIM RPF Vector

In an MPLS-enabled network, any unicast packet that needs to travel outside the network can be tunneled using MPLS from one provider edge (PE) router to another. Consider, for example, the case where the network is an AS and the PE routers are deployed as exterior BGP (eBGP) speakers. In this network environment, the provider (P) routers constitute what is referred to as *BGP-free core* because the PE routers must distribute BGP routes to each other, but not to the P routers. To handle a unicast packet which must travel outside the network, a PE router needs to know which of the other edge routers is the best exit point from the network for that packet's destination IP address. The P routers, however, do not need to have any knowledge of routes which lead outside the network; as they handle only tunneled packets, they only need to know how to reach the other PE routers and P routers in the provider core. However, when multicast packets are considered, the strategy of keeping the core routers free of external routes is more problematic. When using PIM sparse mode (PIM-SM), Source Specific Multicast (SSM), or bidirectional PIM (bidir-PIM) to build a multicast distribution tree for a particular multicast group, the P routers need to fully participate in the PIM protocol to ensure efficient multicast in the provider core. The P routers, thus, must be able to correctly process PIM Join messages for the group, which in turn means that the P routers must be able to send the Join messages towards the root of the distribution tree. If the root of the tree lies outside the network's borders (for example, in a different AS) and the P routers do not maintain external routing information, then the PIM Join messages cannot be processed, and the multicast distribution tree cannot be created.

The PIM RPF Vector feature was introduced to allow PIM to work properly in an environment where the core routers do not maintain external routing information. When the PIM RPF Vector feature is configured and a PE router sends a PIM join message into the core, it must include in that message a vector, which specifies the IP address of the next edge router along the path to the root of the multicast distribution tree. The core routers can then process the Join message by sending it towards the next hop. In effect, the vector serves as an attribute, within a particular network, for the root of the tree.

Note The PIM RPF Vector feature can also be used in the construction of a multicast distribution tree towards a Rendezvous Point (RP).

Note The PIM RPF vector feature cannot be used in conjunction with BSR (in scenarios where BSR messages cannot be forwarded

PIM Join Format

A new PIM join format with a new PIM encoding type has been introduced because there is no space in the default PIM join type to include an extra IP address as vector. A new PIM hello option is introduced to determine if the upstream router is capable of parsing the new encoding. Other routers on the LAN may need to override a prune or cancel sending a join, creating the need to be able to parse the PIM join.

How to Configure PIM RPF Vector

This section contains the following procedures:

Enabling the Multicast PIM RPF Vector

Perform this task to enable the multicast PIM RPF vector.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast rpf proxy vector**
4. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast rpf proxy vector** **Example:** `Router(config)# ip multicast rpf proxy vector`	Enables the RPF vector on the exit router in the global table.
Step 4	**end** **Example:** `Router(config)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Verifying the Multicast PIM RPF Vector

Perform this optional task to verify the configuration of the multicast PIM RPF vector.

SUMMARY STEPS

1. **show ip mroute proxy**
2. **show ip pim neighbor**

DETAILED STEPS

Step 1 **show ip mr proxy**

Use this command to display information about RPF vector proxies received on a multicast router. This information can be used to determine if an RPF vector proxy is received on a core router.

The following is sample output from the **show ip mroute proxy** command:

```
Router# show ip mroute proxy

Proxy Table
Proxy        Assigner      Origin   Uptime/Expire
10.0.0.1     10.0.2.2      PIM      00:02:16/00:02:14
```

Step 2 **show ip pim neighbor**

Use this command display information about PIM neighbors.

The following is sample output from the **show ip pim neighbor** command:

```
Router# show ip pim neighbor

PIM Neighbor Table
```

```
Neighbor         Interface              Uptime/Expires    Ver     DR
Address                                                           Priority/Mode
126.1.33.11      GigabitEthernet2/1     1d11h/00:00:02    v2      N / DR
126.1.34.12      GigabitEthernet2/1     1d11h/00:00:02    v2      N / DR
126.104.20.56    Serial4/1/0/1:0.104    1d11h/00:00:02    v2      1 / S
126.105.20.58    Serial4/1/0/2:0.105    1d00h/00:01:31    v2      1 / S
10.0.1.4         Ethernet0/0            4d21h/00:01:39    v2      1 / P
```

Additional References

The following sections provide references related to the PIM RPF Vector feature.

Related Documents

Related Topic	Document Title
Multicast commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples	*Cisco IOS IP Multicast Command Reference*, Release 12.2SB
Configuration tasks for MVPN	*Cisco IOS IP Multicast Configuration Guide*, Release 12.4

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
draft-ietf-pim-rpf-vector-02	*PIM RPF Vector TLV*

Technical Assistance

Description	Link
The Cisco Technical Support & Documentation website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, tools, and technical documentation. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Command Reference

This section documents new and modified commands only.

- **ip multicast rpf proxy vector**
- **show ip mroute**
- **show ip pim neighbor**

ip multicast rpf proxy vector

To enable a router to perform a Reverse Path Forwarding (RPF) check on an IP address of the exit router in the global table or a specified VPN, use the **ip multicast rpf proxy vector** command in global configuration mode. To disable the RPF check, use the **no** form of this command.

ip multicast [**vrf** *vrf-name*] **rpf proxy** [**rd**] **vector**

no ip multicast [**vrf** *vrf-name*] **rpf proxy** [**rd**] **vector**

Syntax Description

vrf	(Optional) VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
rd	(Optional) Enables the route distinguisher (RD) vector.

Defaults

RPF proxy vectors are disabled.

Command Modes

Global configuration

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.

Usage Guidelines

This command can be used with or without VPNs. Edge routers configured with this command will include the BGP next-hop of a prefix into the PIM join message. This included IP address is used in the core routers to select the RPF path to the next-hop router, which is the exit point in the network for this prefix.

Use the **rd** keyword to enable a route distinguisher (RD) vector.

All upstream routers on the interface must support the RPF proxy vector.

Use the **show ip pim neighbor** command to see if a router supports this mode. The proxy encoding will be represented by the letter P.

Examples

The following example shows how to enable an RPF proxy vector:

```
ip multicast rpf proxy vector
```

Related Commands

Command	Description
show ip mr proxy	Displays information about RPF proxy vectors.
show ip pim neighbor	Displays information about PIM neighbors.

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** [*kpbs*] [**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** [*kpbs*] [**interface** *type number*]]

Syntax Description

vrf *vrf-name*	(Optional) Filters the output to display only the contents of the mroute table that pertain to the multicast VPN routing and forwarding (VRF) 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 (kpbs). Active sources are those sending at the *kbps* value or higher. The range is from 1 to 4294967295. The *kbps* argument defaults to 4 kbps.
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.
dense	(Optional) Filters the output to display only information about dense mode routes in the mroute table.
group-address	(Optional) IP address or Domain Name System (DNS) name of a multicast group.
interface *type number*	(Optional) Filters the output to display only mroute table information related to the interface specified for the *type number* arguments.
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.
source-address	(Optional) IP address or DNS name of a multicast source.
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.
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.

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	The H flag for multicast multilayer switching (MMLS) was added in the output display.
12.1(3)T	The U, s, and I flags keyword for Source Specific Multicast (SSM) were introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.0(30)S	The **proxy** keyword for the PIM RPF Vector and Inter-AS Multicast VPN features was 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. The **vrf** keyword and *vrf-name* argument were added
12.3	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	The **terse** keyword was added.
12.4(7)	The **terse** keyword was added.
12.2(18)SXF2	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.
12.2(31)SB2	The E flag for MVPN extranet support was introduced. The **proxy** keyword was added to support the PIM RPF Vector and Inter-AS Multicast VPN features. The **terse** keyword was added.

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 Reverse Path Forwarding [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

(192.168.37.100/32, 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
  (172.16.160.67/32, 224.2.127.254), 00:02:46/00:00:12, flags: CLJT
  (172.16.244.217/32, 224.2.127.254), 00:02:15/00:00:40, flags: CLJT
  (172.16.8.33/32, 224.2.127.254), 00:00:25/00:02:32, flags: CLJT
  (172.16.2.62/32, 224.2.127.254), 00:00:51/00:02:03, flags: CLJT
  (172.16.8.3/32, 224.2.127.254), 00:00:26/00:02:33, flags: CLJT
  (172.16.60.189/32, 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 1 describes the significant fields shown in the display.

Table 1 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. • 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 is typically 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.

Table 1 show ip mroute Field Descriptions (continued)

Field	Description
	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.
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.

Table 1 show ip mroute Field Descriptions (continued)

Field	Description
Flags: (continued)	• 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. • 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 (192.168.37.100/32, 224.0.255.1)	Entry in the IP multicast routing table. The entry consists of the IP address of the source router 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.

Table 1 show ip mroute Field Descriptions (continued)

Field	Description
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.
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 nonSSM 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.

Table 2 describes the significant fields shown in the display.

Table 2 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 2 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 Group: displays 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 Source: 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 count: 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 do 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 pim neighbor

To list the Protocol Independent Multicast (PIM) neighbors discovered by the Cisco IOS software, 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	(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(22)S	The command output was updated to display the PIM protocol version.
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.
12.0(30)S	The “P” mode was added to show if an RPF vector proxy is received on a core router.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA. The “P” mode was added to show if an RPF vector proxy is received on a core router.
12.2(31)SB2	The “P” mode was added to show if an RPF vector proxy is received on a core router.

Usage Guidelines

Use this command to determine which routers on the LAN are configured for PIM.

Examples

The following is sample output from the **show ip pim neighbor** command:

```
Router# show ip pim neighbor

PIM Neighbor Table
Neighbor        Interface              Uptime/Expires   Ver     DR
Address                                                         Priority/Mode
126.1.33.11     GigabitEthernet2/1     1d11h/00:00:02   v2      N / DR
126.1.34.12     GigabitEthernet2/1     1d11h/00:00:02   v2      N / DR
126.104.20.56   Serial4/1/0/1:0.104    1d11h/00:00:02   v2      1 / S
126.105.20.58   Serial4/1/0/2:0.105    1d00h/00:01:31   v2      1 / S
```

```
10.0.1.4        Ethernet0/0             4d21h/00:01:39   v2      1 / P
```

Table 3 describes the significant fields shown in the display.

Table 3 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/Expires	Uptime shows how long (in hours:minutes:seconds) the entry has been in the PIM neighbor table. Expires shows how long (in hours:minutes:seconds or in milliseconds) until the entry will be removed from the IP multicast routing table.
Ver	PIM protocol version.
DR Prio/Mode	Priority and mode of the designated router (DR). Possible modes are S (sparse mode) or B (bidirectional mode) N (neighbor does not include the DR-Priority Option in its Hello messages), and P (RPF vector proxy is received). [1]

1. The "P" flag, introduced by the PIM RPF Vector Feature in Cisco IOS Release 12.0(30)S, indicates that the neighbor has announced (via a PIM Hello option) its capability to handle RPF and RD RPF Vector proxies in PIM join messages. All Cisco IOS versions implementing the PIM RPF Vector feature always announce this PIM Hello option. All PIM neighbors on a LAN must support the RPF/RD-RPF Vector proxy or else this router will not include the RPF/RD-RPF Vector proxy into its joins. To ensure correct operations of the PIM RPF Vector feature, you must ensure that neighbors run software that also supports this feature.

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.

Feature Information for PIM RPF Vector

Table 4 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 4 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 4 Feature Information for Multicast VPN MIB

Feature Name	Releases	Feature Information
PIM RPF Vector	12.0(30)S 12.2(33)SRA 12.2(31)SB2	The PIM RPF Vector feature was introduced to allow Protocol Independent Multicast (PIM) to work properly in an environment where the core routers do not maintain external routing information. When this feature is configured, the address of the exit router is used as the Reverse Path Forwarding (RPF) vector and is inserted in the PIM join message. The core routers can then perform a RPF check on an IP address of the exit router instead of on the source router. This feature enables routers in an MPLS provider core to build multicast distribution trees without the need for Border Gateway Protocol (BGP). The following commands were introduced or modified by this feature: **ip multicast rpf proxy vector**, **show ip mroute**, and **show ip pim neighbor**.