



# Monitoring and Maintaining IP Multicast

---

This module describes many ways to monitor and maintain an IP multicast network, such as

- displaying which neighboring multicast routers are peering with the local router
- displaying multicast packet rates and loss information
- tracing the path from a source to a destination branch for a multicast distribution tree
- displaying the contents of the IP multicast routing table, information about interfaces configured for PIM, the PIM neighbors discovered by the router, and contents of the IP fast-switching cache
- clearing caches, tables, and databases
- monitoring the delivery of IP multicast packets and being alerted if the delivery fails to meet certain parameters (IP multicast heartbeat)
- using session description and announcement protocols and applications to assist the advertisement of multicast multimedia conferences and other multicast sessions and communicating the relevant session setup information to prospective participants (SAP listener support)
- storing IP multicast packet headers in a cache and displaying them to find out information such as who is sending IP multicast packets to what groups and any multicast forwarding loops in your network
- using managed objects to remotely monitor and configure PIM using Simple Network Management Protocol (SNMP)
- disabling fast switching of IP multicast in order to log debug messages

## Module History

This module was first published on May 2, 2005, and last updated on May 2, 2005.

## Finding Feature Information in This Module

Not all features may be supported in your Cisco IOS software release. Use the [“Feature Information for Monitoring and Maintaining IP Multicast” section on page 19](#) to find information about feature support and configuration.

## Contents

- [Prerequisites for Monitoring and Maintaining IP Multicast, page 2](#)



---

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

© 2007 Cisco Systems, Inc. All rights reserved.

- [How to Monitor and Maintain IP Multicast, page 2](#)
- [Configuration Examples for Monitoring and Maintaining IP Multicast, page 18](#)
- [Additional References, page 18](#)
- [Feature Information for Monitoring and Maintaining IP Multicast, page 19](#)

## Prerequisites for Monitoring and Maintaining IP Multicast

- Before performing the tasks in this module, you should be familiar with the concepts described in the “[IP Multicast Technology Overview](#)” module.
- You must also have enabled IP multicast and have Protocol Independent Multicast (PIM) configured and running on your network. Refer to the “[Configuring Basic IP Multicast](#)” module.

## How to Monitor and Maintain IP Multicast

This section contains the following procedures:

- [Displaying Multicast Peers, Packet Rates, and Loss Information, and Tracing a Path, page 2](#) (optional)
- [Displaying IP Multicast System and Network Statistics, page 4](#) (optional)
- [Clearing IP Multicast Routing Table or Caches, page 8](#) (optional)
- [Monitoring IP Multicast Delivery Using IP Multicast Heartbeat, page 9](#) (optional)
- [Advertising Multicast Multimedia Sessions Using SAP Listener, page 11](#) (optional)
- [Storing IP Multicast Headers, page 13](#) (optional)
- [Disabling Fast Switching of IP Multicast, page 15](#) (optional)
- [Enabling PIM MIB Extensions for IP Multicast, page 16](#) (optional)

## Displaying Multicast Peers, Packet Rates, and Loss Information, and Tracing a Path

Monitor IP multicast routing when you want to know which neighboring multicast routers are peering with the local router, what the multicast packet rates and loss information are, or when you want to trace the path from a source to a destination branch for a multicast distribution tree.

### SUMMARY STEPS

1. **enable**
2. **mrinfo** [*host-name* | *host-address*] [*source-address* | *interface*]
3. **mstat** {*source-name* | *source-address*} [*destination-name* | *destination-address*] [*group-name* | *group-address*]
4. **mtrace** {*source-name* | *source-address*} [*destination-name* | *destination-address*] [*group-name* | *group-address*]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>mrinfo</b> [ <i>host-name</i>   <i>host-address</i> ] [ <i>source-address</i>   <i>interface</i> ]  <b>Example:</b> Router# mrinfo	(Optional) Queries which neighboring multicast routers are “peering” with the local router.
Step 3	<b>mstat</b> { <i>source-name</i>   <i>source-address</i> } [ <i>destination-name</i>   <i>destination-address</i> ] [ <i>group-name</i>   <i>group-address</i> ]  <b>Example:</b> Router# mstat allsource	(Optional) Displays IP multicast packet rate and loss information.
Step 4	<b>mtrace</b> { <i>source-name</i>   <i>source-address</i> } [ <i>destination-name</i>   <i>destination-address</i> ] [ <i>group-name</i>   <i>group-address</i> ]  <b>Example:</b> Router# mtrace allsource	(Optional) Traces the path from a source to a destination branch for a multicast distribution tree.

## Examples

The following is sample output from the **mrinfo** command:

```
Router# mrinfo
192.31.7.37 (labs-allcompany) [version cisco 12.3] [flags: PMSA]:
192.31.7.37 -> 192.31.7.34 (lab-southwest) [1/0/pim]
192.31.7.37 -> 192.31.7.47 (lab-northwest) [1/0/pim]
192.31.7.37 -> 192.31.7.44 (lab-southeast) [1/0/pim]
131.119.26.10 -> 131.119.26.9 (lab-northeast) [1/32/pim]
```

The following is sample output from the **mstat** command in user EXEC mode:

```
Router> mstat labs-in-china 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 (labs-in-china) to destination (labs-in-africa)
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      labs-in-england
| ^ ttl 1
v | hop 31 ms 0/12 = 0% 1 pps 0/1 = --% 0 pps
172.16.0.2
```

```

172.16.0.3   infolabs.com
| ^ ttl 2
v | hop -17 ms -735/12 = --% 1 pps 0/1 = --% 0 pps
172.16.0.4
172.16.0.5   infolabs2.com
| ^ ttl 3
v | hop -21 ms -678/23 = --% 2 pps 0/1 = --% 0 pps
172.16.0.6
172.16.0.7   infolabs3.com
| ^ ttl 4
v | hop 5 ms 605/639 = 95% 63 pps 1/1 = --% 0 pps
172.16.0.8
172.16.0.9   infolabs.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

```

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

```

## Displaying IP Multicast System and Network Statistics

Display IP multicast system statistics to show the contents of the IP multicast routing table, information about interfaces configured for PIM, the PIM neighbors discovered by the router, contents of the IP fast-switching cache, and the contents of the circular cache header buffer.

### SUMMARY STEPS

1. **enable**
2. **ping** [*group-name* | *group-address*]
3. **show ip mroute** [*group-address* | *group-name*] [*source-address* | *source-name*] [*type number*] [**summary**] [**count**] [**active kbps**]
4. **show ip pim interface** [*type number*] [**df** | **count**] [*rp-address*] [**detail**]
5. **show ip pim neighbor** [*type number*]
6. **show ip mcache** [*group-address* | *group-name*] [*source-address* | *source-name*]
7. **show ip mpacket** [*group-address* | *group-name*] [*source-address* | *source-name*] [**detail**]
8. **show ip pim rp** [**mapping** | **metric**] [*rp-address*]
9. **show ip rpf** {*source-address* | *source-name*} [**metric**]

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> Router&gt; enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<p><b>ping</b> [<i>group-name</i>   <i>group-address</i>]</p> <p><b>Example:</b> Router# ping cbone-audio</p>	(Optional) Sends an ICMP echo request message to a multicast group address or group name.
Step 3	<p><b>show ip mroute</b> [<i>group-address</i>   <i>group-name</i>] [<i>source-address</i>   <i>source-name</i>] [<i>type number</i>] [<b>summary</b>] [<b>count</b>] [<b>active kbps</b>]</p> <p><b>Example:</b> Router# show ip mroute cbone-audio</p>	(Optional) Displays the contents of the IP multicast routing table.
Step 4	<p><b>show ip pim interface</b> [<i>type number</i>] [<b>df</b>   <b>count</b>] [<i>rp-address</i>] [<b>detail</b>]</p> <p><b>Example:</b> Router# show ip pim interface ethernet1/0 detail</p>	(Optional) Displays information about interfaces configured for PIM.
Step 5	<p><b>show ip pim neighbor</b> [<i>type number</i>]</p> <p><b>Example:</b> Router# show ip pim neighbor</p>	(Optional) Lists the PIM neighbors discovered by the router.
Step 6	<p><b>show ip mcache</b> [<i>group-address</i>   <i>group-name</i>] [<i>source-address</i>   <i>source-name</i>]</p> <p><b>Example:</b> Router# show ip mcache</p>	(Optional) Displays the contents of the IP fast-switching cache.
Step 7	<p><b>show ip mpacket</b> [<i>group-address</i>   <i>group-name</i>] [<i>source-address</i>   <i>source-name</i>] [<b>detail</b>]</p> <p><b>Example:</b> Router# show ip mpacket smallgroup</p>	(Optional) Displays the contents of the circular cache header buffer.
Step 8	<p><b>show ip pim rp</b> [<b>mapping</b>   <b>metric</b>] [<i>rp-address</i>]</p> <p><b>Example:</b> Router# show ip pim rp metric</p>	(Optional) Displays the RP routers associated with a sparse mode multicast group.
Step 9	<p><b>show ip rpf</b> {<i>source-address</i>   <i>source-name</i>} [<b>metric</b>]</p> <p><b>Example:</b> Router# show ip rpf 172.16.10.13</p>	(Optional) Displays how the router is doing RPF (that is, from the unicast routing table, DVMRP routing table, or static mroutes). Also displays the unicast routing metric.

## Examples

### show ip mroute

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
```

### show ip pim interface

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
                  Interface          Mode   Count Intvl  Prior
172.16.1.4       Ethernet1/0       v2/S   1     100 ms 1      172.16.1.4
```

### show ip mcache

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)
```

### show ip mpacket

The following is sample output from the **show ip mpacket** command with the *group-name* argument:

```
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.company.com) 192.168.228.10 224.5.6.7
7302/113 206417.908 (school.edu) 172.16.2.17 224.5.6.7
6CB2/114 206417.412 (company2.company.com) 172.16.19.40 224.5.6.7
D782/117 206417.868 (company1.company.com) 192.168.228.10 224.5.6.7
```

```
E2E9/123 206418.488 (company3.com) 239.1.8.10 224.5.6.7
1CA7/127 206418.544 (company4.com) 192.168.6.10 224.5.6.7
```

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
```

### show ip pim rp

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

### show ip rpf

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 when the **metric** keyword is specified:

```
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

```

## Clearing IP Multicast Routing Table or Caches

Clear IP multicast caches and tables to delete entries from the IP multicast routing table, the Auto-RP cache, the IGMP cache, and the caches of Catalyst switches. When these entries are cleared, the information is refreshed by being relearned, thus eliminating any incorrect entries.

### SUMMARY STEPS

1. **enable**
2. **clear ip mroute** { \* | *group-name* [*source-name* | *source-address*] | *group-address* [*source-name* | *source-address*]}
3. **clear ip pim auto-rp** *rp-address*
4. **clear ip mcache**
5. **clear ip igmp group** [*group-name* | *group-address* | *interface-type interface-number*]
6. **clear ip cgmp** [*interface-type interface-number*]

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>clear ip mroute</b> { *   <i>group-name</i> [ <i>source-name</i>   <i>source-address</i> ]   <i>group-address</i> [ <i>source-name</i>   <i>source-address</i> ]}  <b>Example:</b> Router# clear ip mroute 224.2.205.42 228.3.0.0	(Optional) Deletes entries from the IP multicast routing table.
Step 3	<b>clear ip pim auto-rp</b> <i>rp-address</i>  <b>Example:</b> Router# clear ip pim auto-rp 224.5.6.7	(Optional) Clears the Auto-RP cache.
Step 4	<b>clear ip mcache</b>  <b>Example:</b> Router # clear ip mcache	(Optional) Clears the multicast cache.

	Command or Action	Purpose
Step 5	<pre>clear ip igmp group [group-name   group-address   interface-type interface-number]</pre> <p><b>Example:</b> Router# clear ip igmp group 224.0.255.1</p>	(Optional) Deletes entries from the IGMP cache.
Step 6	<pre>clear ip cgmp [interface-type interface-number]</pre> <p><b>Example:</b> Router# clear ip cgmp</p>	(Optional) Clears all group entries from the caches of Catalyst switches.

## Monitoring IP Multicast Delivery Using IP Multicast Heartbeat

The IP multicast heartbeat feature provides a way to monitor the status of IP multicast delivery and be informed when the delivery fails (via Simple Network Management Protocol [SNMP] traps).

### IP Multicast Heartbeat

The IP Multicast Heartbeat feature enables you to monitor the delivery of IP multicast packets and to be alerted if the delivery fails to meet certain parameters.

Although you could alternatively use MRM to monitor IP multicast, you can perform the following tasks with IP multicast heartbeat that you cannot perform with MRM:

- Generate an SNMP trap
- Monitor a production multicast stream

When IP multicast heartbeat is enabled, the router monitors IP multicast packets destined for a particular multicast group at a particular interval. If the number of packets observed is less than a configured minimum amount, the router sends an SNMP trap to a specified network management station to indicate a loss of heartbeat exception.

The **ip multicast heartbeat** command does not create a heartbeat if there is no existing multicast forwarding state for *group* in the router. This 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 host ipmulticast** command to enable the sending of IP multicast traps to specific receiver hosts. Use the **debug ip mhbeat** command to debug the Multicast Heartbeat feature.

### SNMP Notifications

A key feature of SNMP is the ability to generate notifications from an SNMP agent. These notifications do not require that requests be sent from the SNMP manager. Unsolicited (asynchronous) notifications can be generated as traps or inform requests. Traps are messages alerting the SNMP manager to a condition on the network. Inform requests (informs) are traps that include a request for confirmation of receipt from the SNMP manager. Notifications can indicate improper user authentication, restarts, the closing of a connection, loss of connection to a neighbor router, or other significant events.

Traps are less reliable than informs because the receiver does not send any acknowledgment when it receives a trap. The sender cannot determine if the trap was received. An SNMP manager that receives an inform request acknowledges the message with an SNMP response protocol data unit (PDU). If the

manager does not receive an inform request, it does not send a response. If the sender never receives a response, the inform request can be sent again. Thus, informs are more likely to reach their intended destination.

However, traps are often preferred because informs consume more resources in the router and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Also, traps are sent only once, while an inform may be retried several times. The retries increase traffic and contribute to a higher overhead on the network. Thus, traps and inform requests provide a trade-off between reliability and resources. If it is important that the SNMP manager receives every notification, use inform requests. However, if you are concerned about traffic on your network or memory in the router and you need not receive every notification, use traps.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing**
4. **snmp-server host** {hostname | ip-address} [traps | informs] [version {1 | 2c | 3 [auth | noauth | priv]]] community-string [udp-port port] [notification-type]
5. **snmp-server enable traps ipmulticast**
6. **ip multicast heartbeat** group-address minimum-number window-size interval

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip multicast-routing</b>  <b>Example:</b> Router(config)# ip multicast-routing	Enables IP multicast routing.
Step 4	<b>snmp-server host</b> {hostname   ip-address} [traps   informs] [version {1   2c   3 [auth   noauth   priv]]] community-string [udp-port port] [notification-type]  <b>Example:</b> Router(config)# snmp-server host 224.1.0.1 traps public	Specifies the recipient of an SNMP notification operation.

	Command or Action	Purpose
Step 5	<pre>snmp-server enable traps ipmulticast</pre> <p><b>Example:</b> Router(config)# snmp-server enable traps ipmulticast</p>	Enables the router to send IP multicast traps.
Step 6	<pre>ip multicast heartbeat group-address minimum-number window-size interval</pre> <p><b>Example:</b> Router(config)# ip multicast heartbeat ethernet0 224.1.1.1 1 1 10</p>	<p>Enables the monitoring of the IP multicast packet delivery.</p> <ul style="list-style-type: none"> <li>The <i>interval</i> should be set to a multiple of 10 seconds on platforms that use Multicast Distributed Fast Switching (MDFS) because on those platforms, the packet counters are only updated once every 10 seconds. Other platforms may have other increments.</li> </ul>

## Examples

The following example shows how to monitor IP multicast packets forwarded through this router to group address 224.1.1.1. If no packet for this group is received in a 10-second interval, an SNMP trap will be sent to the SNMP management station with the IP address of 224.1.0.1.

```
!
ip multicast-routing
!
snmp-server host 224.1.0.1 traps public
snmp-server enable traps ipmulticast
ip multicast heartbeat ethernet0 224.1.1.1 1 1 10
```

## Advertising Multicast Multimedia Sessions Using SAP Listener

Enable SAP listener support when you want to use session description and announcement protocols and applications to assist the advertisement of multicast multimedia conferences and other multicast sessions and to communicate the relevant session setup information to prospective participants.

### Session Announcement Protocol (SAP)

Session Announcement Protocol (SAP) listener support is needed to use session description and announcement protocols and applications to assist the advertisement of multicast multimedia conferences and other multicast sessions and to communicate the relevant session setup information to prospective participants.

Sessions are described by the Session Description Protocol (SDP), which is defined in RFC 2327. SDP provides a formatted, textual description of session properties (for example, contact information, session lifetime, and the media) being used in the session (for example, audio, video, and whiteboard) with their specific attributes such as time-to-live (TTL) scope, group address, and User Datagram Protocol (UDP) port number.

Many multimedia applications rely on SDP for session descriptions. However, they may use different methods to disseminate these session descriptions. For example, IP/TV relies on the web to disseminate session descriptions to participants. In this example, participants must know of a web server that provides the session information.

MBONE applications (for example, vic, vat, and wb) and other applications rely on multicast session information sent throughout the network. In these cases, SAP is used to transport the SDP session announcements. SAP Version 2 uses the well-known session directory multicast group 224.2.127.254 to disseminate SDP session descriptions for global scope sessions and group 239.255.255.255 for administrative scope sessions.

**Note**

The Session Directory (SDR) application is commonly used to send and receive SDP/SAP session announcements.

**SUMMARY STEPS**

1. **enable**
2. **configure terminal**
3. **ip sap cache-timeout** *minutes*
4. **interface** *type number*
5. **ip sap listen**
6. **end**
7. **clear ip sap** [*group-address* | "*session-name*"]
8. **show ip sap** [*group-address* | "*session-name*" | **detail**]

**DETAILED STEPS**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>ip sap cache-timeout</b> <i>minutes</i>  <b>Example:</b> Router(config)# ip sap cache-timeout 600	(Optional) Limits how long a SAP cache entry stays active in the cache. <ul style="list-style-type: none"> <li>• By default, SAP cache entries are deleted 24 hours after they are received from the network.</li> </ul>
<b>Step 4</b>	<b>interface</b> <i>type number</i>  <b>Example:</b> Router(config)# interface ethernet 1	Selects an interface that is connected to hosts on which IGMPv3 can be enabled.
<b>Step 5</b>	<b>ip sap listen</b>  <b>Example:</b> Router(config-if)# ip sap listen	Enables the Cisco IOS software to listen to session directory announcements.

	Command or Action	Purpose
Step 6	<pre>end</pre> <p><b>Example:</b> Router(config-if)# end</p>	Ends the session and returns to EXEC mode.
Step 7	<pre>clear ip sap [group-address   "session-name"]</pre> <p><b>Example:</b> Router# clear ip sap "Sample Session"</p>	Deletes a SAP cache entry or the entire SAP cache.
Step 8	<pre>show ip sap [group-address   "session-name"   detail]</pre> <p><b>Example:</b> Router# show ip sap 224.2.197.250 detail</p>	(Optional) Displays the SAP cache.

## Examples

The following example enables a router to listen to session directory announcements and changes the SAP cache timeout to 30 minutes.

```
ip multicast routing
ip sap cache-timeout 30
interface loopback 0
 ip address 10.0.0.51 255.255.255.0
 ip pim sparse-dense mode
 ip sap listen
```

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
```

## Storing IP Multicast Headers

You can store IP multicast packet headers in a cache and then display them to determine any of the following information:

- Who is sending IP multicast packets to what groups

- Interpacket delay
- Duplicate IP multicast packets (if any)
- Multicast forwarding loops in your network (if any)
- Scope of the group
- UDP port numbers
- Packet length

Perform this task if you need any of the information listed above.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast cache-headers [rtp]**
4. **exit**
5. **show ip mpacket [group-address | group-name] [source-address | source-name] [detail]**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
Step 3	<b>ip multicast cache-headers [rtp]</b>  <b>Example:</b> Router(config)# ip multicast cache-headers	Allocates a circular buffer to store IP multicast packet headers that the router receives.
Step 4	<b>exit</b>  <b>Example:</b> Router(config)# exit	Returns to privilege EXEC mode.
Step 5	<b>show ip mpacket [group-address   group-name] [source-address   source-name] [detail]</b>  <b>Example:</b> Router# show ip mpacket smallgroup	(Optional) Displays the contents of the circular cache-header buffer.

## 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.company.com) 192.168.228.10 224.5.6.7
7302/113 206417.908 (school.edu) 172.16.2.17 224.5.6.7
6CB2/114 206417.412 (company2.company.com) 172.16.19.40 224.5.6.7
D782/117 206417.868 (company1.company.com) 192.168.228.10 224.5.6.7
E2E9/123 206418.488 (company3.com) 239.1.8.10 224.5.6.7
1CA7/127 206418.544 (company4.company.com) 192.168.6.10 224.5.6.7
```

## Disabling Fast Switching of IP Multicast

Disable fast switching if you want to log debug messages, because when fast switching is enabled, debug messages are not logged.

You might also want to disable fast switching, which places the router in process switching, if packets are not reaching their destinations. If fast switching is disabled and packets are reaching their destinations, then switching may be the cause.

## Fast Switching of IP Multicast

Fast switching of IP multicast packets is enabled by default on all interfaces (including generic routing encapsulation [GRE] and DVMRP tunnels), with one exception: It is disabled and not supported over X.25 encapsulated interfaces. The following are properties of fast switching:

- If fast switching is disabled on an *incoming* interface for a multicast routing table entry, the packet is sent at process level for all interfaces in the outgoing interface list.
- If 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 fast switching is enabled, debug messages are not logged.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ip pim mroute-cache**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> <code>Router&gt; enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>Enter your password if prompted.</li> </ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> <code>Router# configure terminal</code>	Enters global configuration mode.
Step 3	<code>interface type number</code>  <b>Example:</b> <code>Router(config)# interface ethernet 1</code>	Specifies an interface.
Step 4	<code>no ip mroute-cache</code>  <b>Example:</b> <code>Router(config-if)# no ip mroute-cache</code>	Disables fast switching of IP multicast.

## Enabling PIM MIB Extensions for IP Multicast

PIM MIB extensions for IP multicast introduce support in Cisco IOS software for the CISCO-PIM-MIB, which is an extension of RFC 2934 and an enhancement to the former Cisco implementation of the PIM MIB.

### PIM MIB Extensions

Protocol Independent Multicast (PIM) is an IP multicast routing protocol used for routing multicast data packets to multicast groups. RFC 2934 defines the PIM for IPv4 MIB, which describes managed objects that enable users to remotely monitor and configure PIM using Simple Network Management Protocol (SNMP).

PIM MIB extensions introduce the following new classes of PIM notifications:

- neighbor-change—This notification results from the following conditions:
  - When a router's PIM interface is disabled or enabled (using the `ip pim` command in interface configuration mode)
  - When a router's PIM neighbor adjacency expires or is established (defined in RFC 2934)
- rp-mapping-change—This notification results from a change in the rendezvous point (RP) mapping information due to either Auto-RP or bootstrap router (BSR) messages.
- invalid-pim-message—This notification results from the following conditions:
  - When an invalid (\*, G) Join or Prune message is received by the device (for example, 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)

- When an invalid PIM register message is received by the device (for example, when a router receives a register message from a multicast group for which it is not the RP)

## Benefits of PIM MIB Extensions

PIM MIB extensions have the following benefits:

- Allow users to identify changes in the multicast topology of their network by detecting changes in the RP mapping.
- Provide traps to monitor the PIM protocol on PIM-enabled interfaces.
- Help users identify routing issues when multicast neighbor adjacencies expire or are established on a multicast interface.
- Enable users to monitor RP configuration errors (for example, errors due to flapping in dynamic RP allocation protocols like Auto-RP).

## Restrictions for PIM MIB Extensions

The following MIB tables are not supported in Cisco IOS software:

- pimIpMRouteTable
- pimIpMRouteNextHopTable
- The pimInterfaceVersion object was removed from RFC 2934 and, therefore, is no longer supported in Cisco IOS software.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps pim [neighbor-change | rp-mapping-change | invalid-pim-message]**
4. **snmp-server host host-address [traps | informs] community-string pim**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode.  • Enter your password if prompted.
Step 2	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.

	Command or Action	Purpose
Step 3	<pre>snmp-server enable traps pim [neighbor-change   rp-mapping-change   invalid-pim-message]</pre> <p><b>Example:</b> Router(config)# snmp-server enable traps pim neighbor-change</p>	<p>(Optional) Enables a router to send PIM notifications. The keywords are as follows:</p> <ul style="list-style-type: none"> <li>• <b>neighbor-change</b>—Enables notifications indicating when a router’s PIM interface is disabled or enabled, or when a router’s PIM neighbor adjacency expires or is established.</li> <li>• <b>rp-mapping-change</b>—Enables notifications indicating a change in RP mapping information due to either Auto-RP or BSR messages.</li> <li>• <b>invalid-pim-message</b>—Enables notifications for monitoring invalid PIM protocol operations (for example, 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 or when a router receives a register message from a multicast group for which it is not the RP).</li> </ul>
Step 4	<pre>snmp-server host host-address [traps   informs] community-string pim</pre> <p><b>Example:</b> Router(config)# snmp-server host 10.10.10.10 traps public pim</p>	Specifies the recipient of a PIM SNMP notification operation.

## Configuration Examples for Monitoring and Maintaining IP Multicast

This section provides the following configuration example:

- [Generating Notifications That PIM Is Enabled: Example, page 18](#)

### Generating Notifications That PIM Is Enabled: Example

The following example shows how to configure a router to generate notifications indicating that a PIM interface of the router has been enabled. The first line configures PIM traps to be sent as SNMP v2c traps to the host with IP address 10.0.0.1. The second line configures the router to send the neighbor-change class of notification to the host.

```
snmp-server host 10.0.0.1 traps version 2c public pim
snmp-server enable traps pim neighbor-change
interface ethernet0/0
 ip pim sparse-dense-mode
```

## Additional References

The following sections provide references related to monitoring and maintaining IP multicast.

## Related Documents

Related Topic	Document Title
IP multicast SNMP notifications	“Configuring SNMP Support” module
IP multicast commands: complete command syntax, command mode, defaults, usage guidelines, and examples	<i>Cisco IOS IP Multicast Command Reference</i>

## MIBs

MIBs	MIBs Link
<ul style="list-style-type: none"> <li>CISCO-IPMROUTE-MIB</li> <li>MSDP-MIB</li> <li>IGMP-STD-MIB</li> </ul>	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p>

## RFCs

RFCs	Title
RFC 2934	<i>Protocol Independent Multicast for IPv4 MIB</i>

## Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	<a href="http://www.cisco.com/public/support/tac/home.shtml">http://www.cisco.com/public/support/tac/home.shtml</a>

## Feature Information for Monitoring and Maintaining IP Multicast

Table 1 lists the features in this module and provides links to specific configuration information. Only features that were introduced or modified in Cisco IOS Releases 12.2(1) or 12.0(3)S or later appear in the table.

Not all commands may be available in your Cisco IOS software release. For details on when support for specific commands was introduced, see the command reference documents.

If you are looking for information on a feature in this technology that is not documented here, see the “Configuring IP Multicast Roadmap”.

Cisco IOS software images are specific to a Cisco IOS software release, a feature set, and a platform. Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator (<http://www.cisco.com/go/fn>). You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click Cancel at the login dialog box and follow the instructions that appear.



**Note** Table 1 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 1** Feature Information for Monitoring and Maintaining IP Multicast

Feature Names	Releases	Feature Configuration Information
PIM MIB Extensions	12.2(4)T	<p>Protocol Independent Multicast (PIM) is an IP multicast routing protocol used for routing multicast data packets to multicast groups. RFC 2934 defines the PIM for IPv4 MIB, which describes managed objects that enable users to remotely monitor and configure PIM using Simple Network Management Protocol (SNMP).</p> <p>The following sections provide information about this feature:</p> <p><a href="#">“Enabling PIM MIB Extensions for IP Multicast” section on page 16</a></p>
PIM MIB Extensions	Cisco IOS XE Release 2.1	This feature was introduced on Cisco ASR 1000 Series Routers.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0711R)

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.

© 2005–2008 Cisco Systems, Inc. All rights reserved.