



IP Multicast Routing Commands

This chapter describes the commands used to configure and monitor IP multicast routing. For IP multicast routing configuration information and examples, refer to the “Configuring IP Multicast Routing” chapter of the *Network Protocols Configuration Guide, Part 1*.

clear ip cgmp

To clear all group entries from the Catalyst switches' caches, use the **clear ip cgmp** EXEC command.

```
clear ip cgmp [type number]
```

Syntax Description

type number (Optional) Interface type and number.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

This command sends a 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.

Example

The following example clears the CGMP cache:

```
clear ip cgmp
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip cgmp

clear ip dvmrp route

To delete routes from the DVMRP routing table, use the **clear ip dvmrp route** EXEC command.

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

Syntax Description

<i>*</i>	Clears all routes from the DVMRP table.
<i>route</i>	Clears the longest matched route. Can be an IP address, a network number, or an IP DNS name.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Example

The following example deletes route 10.1.1.1 from the DVMRP routing table:

```
clear ip dvmrp route 10.1.1.1
```

clear ip igmp group

To delete entries from the IGMP cache, use the **clear ip igmp group** EXEC command.

```
clear ip igmp group [group-name | group-address | type number]
```

Syntax Description

<i>group-name</i>	(Optional) Name of the multicast group, as defined in the DNS hosts table or with the ip host command.
<i>group-address</i>	(Optional) Address of the multicast group. This is a multicast IP address in four-part, dotted notation.
<i>type number</i>	(Optional) Interface type and number.

Default

When the command is used with no arguments, all entries are deleted from the IGMP cache.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

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, it is also listed in the cache.

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

Example

The following example clears entries for the multicast group 224.0.255.1 from the IGMP cache:

```
clear ip igmp group 224.0.255.1
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip host

show ip igmp groups

show ip igmp interface

clear ip mroute

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

```
clear ip mroute {* | group [source]}
```

Syntax Description

<i>*</i>	Deletes all entries from the IP multicast routing table.
<i>group</i>	Can be either one of the following: <ul style="list-style-type: none">• Name of the multicast group, as defined in the DNS hosts table or with the ip host command.• IP address of the multicast group. This is a multicast IP address in four-part, dotted notation.
<i>source</i>	(Optional) If you specify a group name or address, you can also specify a name or address of a multicast source that is transmitting to the group. A source does not need to be a member of the group.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Examples

The following example deletes all entries from the IP multicast routing table:

```
clear ip mroute *
```

The following example deletes from the IP multicast routing table all sources on the 10.3.0.0 subnet that are transmitting to the multicast group 224.2.205.42. Note that this example deletes all sources on network 10.3, not individual sources.

```
clear ip mroute 224.2.205.42 10.3.0.0
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip host

show ip mroute

clear ip pim auto-rp

To delete entries from the Auto-RP cache, use the **clear pim auto-rp** EXEC command.

```
clear ip pim auto-rp rp-address
```

Syntax Description

rp-address Clears only the entries related to the RP at this address. If this argument is omitted, the entire Auto-RP cache is cleared.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

Example

The following example deletes all entries from the Auto-RP cache:

```
clear ip pim auto-rp
```

clear ip rtp header-compression

To clear RTP header compression structures and statistics, use the **clear ip rtp header-compression EXEC** command.

```
clear ip rtp header-compression [type number]
```

Syntax Description

type number (Optional) Interface type and number.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

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

Example

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

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

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip rtp header-compression

clear ip sdr

To delete a Session Directory Protocol (sdr) cache entry or the entire sdr cache, use the **clear ip sdr** EXEC command.

```
clear ip sdr [group-address | "session-name"]
```

Syntax Description

group-address (Optional) Deletes all sessions associated with the IP group address.

"*session-name*" (Optional) Deletes only the sdr cache entry with the specified name.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

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

Example

The following example clears the sdr cache:

```
clear ip sdr
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip sdr cache-timeout

ip sdr listen

show ip sdr

frame-relay ip rtp header-compression

To enable RTP header compression for all Frame Relay maps on a physical interface, use the **frame-relay ip rtp header-compression** interface configuration command. To disable the feature, use the **no** form of this command.

```
frame-relay ip rtp header-compression [active | passive]  
no frame-relay ip rtp header-compression [active | passive]
```

Syntax Description

active	(Optional) Compresses all outgoing RTP packets. This is the default.
passive	(Optional) Compresses the outgoing RTP/UDP/IP header only if an incoming packet had a compressed header.

Default

Disabled.

If the command is configured, **active** is the default keyword.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

When this command is used on the physical interface, all the interface maps inherit the command; that is, all maps will perform IP/UDP/RTP header compression.

Example

The following example enables RTP header compression for all Frame Relay maps on a physical interface:

```
frame-relay ip rtp header-compression
```

Related Command

You can use the master indexes or search online to find documentation of related commands.

show frame-relay ip rtp header-compression

frame-relay map ip compress

To enable both RTP and TCP header compression on a link, use the **frame-relay map ip compress** interface configuration command. To disable both RTP and TCP header compression, use the **no** form of this command.

frame-relay map ip *ip-address dci* [**broadcast**] **compress**
no frame-relay map ip *ip-address dci* [**broadcast**] **compress**

Syntax Description

<i>ip-address</i>	IP address of the destination or next hop.
<i>dci</i>	DLCI number.
broadcast	(Optional) Forwards broadcasts to the specified IP address.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

Example

The following example enables both RTP and TCP header compression on serial interface 1:

```
interface serial 1
 encapsulation frame-relay
 ip address 131.108.175.110 255.255.255.0
 frame-relay map ip 131.108.175.220 180 compress
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

show frame-relay ip rtp header-compression

frame-relay map ip rtp header-compression

To enable RTP header compression per DLCI, use the **frame-relay map ip rtp header-compression** interface configuration command. To disable the feature, use the **no** form of this command.

```
frame-relay map ip ip-address dlc rtp header-compression [active | passive]  
no frame-relay map ip ip-address dlc rtp header-compression [active | passive]
```

Syntax Description

<i>ip-address</i>	IP address of the destination or next hop.
<i>dlci</i>	DLCI number.
active	(Optional) All outgoing RTP packets are compressed. This is the default.
passive	(Optional) Compresses the outgoing RTP/UDP/IP header only if an incoming packet had a compressed header.

Default

Disabled.

If the command is configured, **active** is the default keyword.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

When this command is configured, the specified maps inherit RTP header compression. You can have multiple Frame Relay maps, with and without RTP header compression.

Example

The following example enables RTP header compression on serial interface 1:

```
interface serial 1  
  encapsulation frame-relay  
  ip address 131.108.175.110 255.255.255.0  
  frame-relay map ip 131.108.175.220 180 rtp header-compression
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

show frame-relay ip rtp header-compression

ip cgmp

To enable CGMP on an interface of a router connected to a Catalyst 5000 switch, use the **ip cgmp** interface configuration command. To disable CGMP routing, use the **no** form of this command.

```
ip cgmp [proxy]  
no ip cgmp
```

Syntax Description

proxy (Optional) Enables CGMP and the CGMP proxy function.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

When enabled on an interface, this command triggers a CGMP Join message. This command should only be used on 802 and ATM media. When a **no ip cgmp** command is issued, a triggered CGMP Leave message is sent for the router's MAC address on the interface for group 0000.0000.0000 (all groups).

When the **proxy** keyword is specified, the CGMP proxy function is 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 non-CGMP-capable router's MAC address and a group address of 0000.0000.0000.

Examples

In the following example, CGMP is enabled:

```
ip cgmp
```

In the following example, CGMP and CGMP proxy are enabled:

```
ip cgmp proxy
```

ip dvmrp accept-filter

To configure an acceptance filter for incoming DVMRP reports, use the **ip dvmrp accept-filter** interface configuration command. To disable this feature, use the **no** form of this command.

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

Syntax Description

<i>access-list-number</i>	Number of a standard IP access list. This can be a number from 0 to 99. A value of 0 means that all sources are accepted with the configured distance.
<i>distance</i>	(Optional) Administrative distance to the destination.
neighbor-list <i>access-list-number</i>	Number of a neighbor list. DVMRP reports are accepted only by those neighbors on the list.

Default

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

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. The **neighbor-list** keyword and *access-list-number* argument first appeared in Cisco IOS Release 11.2.

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

The *distance* 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. This means that they always take precedence over unicast routing table routes. If you have two paths to a source, one through unicast routing (using 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. For example, if the unicast routing protocol is Enhanced IGRP, which has a default administrative distance of 90, you could define and apply the following access list so the RPF interface used to accept multicast packets will be through the Enhanced IGRP/PIM path:

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

Example

The following example applies access list 57 to the interface and sets a distance of 4:

```
access-list 57 permit 131.108.0.0 0.0.255.255
access-list 57 permit 198.92.37.0 0.0.0.255
access-list 57 deny 0.0.0.0 255.255.255.255
ip dvmrp accept-filter 57 4
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

distance

ip dvmrp metric

show ip dvmrp route

tunnel mode

ip dvmrp auto-summary

To enable DVMRP auto-summarization if it was disabled, use the **ip dvmrp auto-summary** interface configuration command. To disable the feature, 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.

Default

Enabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

DVMRP auto-summarization occurs when a unicast subnet route is collapsed into a classful network number route. This 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.

You might want to disable this feature 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 auto-summarization.

Example

The following example disables DVMRP auto-summarization:

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

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip dvmrp summary-address

ip dvmrp default-information

To advertise network 0.0.0.0 to DVMRP neighbors on an interface, use the **ip dvmrp default-information** interface configuration command. 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	Other routes more specific than 0.0.0.0 can also be advertised.
only	No DVMRP routes other than 0.0.0.0 are advertised.

Default
Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

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

You can use the **ip dvmrp 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.

Example

The following example configures the Cisco IOS software to advertise network 0.0.0.0, in addition to other networks, to DVMRP neighbors:

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

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip dvmrp metric

ip dvmrp metric

To configure the metric associated with a set of destinations for DVMRP reports, use the **ip dvmrp metric** interface configuration command. To disable this function, use the **no** form of this command.

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

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

Syntax Description

<i>metric</i>	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).
list <i>access-list-number</i>	(Optional) Number of an access list. If you specify this 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.
<i>protocol</i>	(Optional) Name of unicast routing protocol, such as bgp , eigrp , igrp , isis , ospf , rip , or static or dvmrp . If you specify these arguments, only routes learned by the specified routing protocol are advertised in DVMRP report messages.
<i>process-id</i>	(Optional) Process ID number of the unicast routing protocol.
dvmrp	(Optional) Allows routes from the DVMRP routing table to be advertised with the configured <i>metric</i> or filtered.
route-map <i>map-name</i>	Unicast routes are subject to route-map conditions before being injected into DVMRP. Route-maps cannot be used for DVMRP routes.

Default

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

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.2. The **route-map** keyword first appeared in Cisco IOS Release 11.1.

When 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 process-id* arguments to selectively list the destinations learned from a given routing protocol.

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

Example

The following example connects 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 198.92.35.0 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 198.92.35.0 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
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

debug ip dvmrp
ip dvmrp accept-filter

ip dvmrp metric-offset

To change the metrics of advertised DVMRP routes and thus favor or not favor a certain route, use the **ip dvmrp metric-offset** interface configuration command. 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) The <i>increment</i> value is added to incoming DVMRP reports and is reported in minfo replies. The default for in is 1.
out	(Optional) The <i>increment</i> value is added to outgoing DVMRP reports for routes from the DVMRP routing table. The default for out is 0.
<i>increment</i>	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.

The default for **in** is 1.

The default for **out** is 0.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

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

Example

The following example adds 10 to the incoming DVMRP reports:

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

ip dvmrp output-report-delay

To configure an interpacket delay of a DVMRP report, use the **ip dvmrp output-report-delay** interface configuration command. 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 transmitted. The default is 2 packets.

Defaults

milliseconds is 100 milliseconds
burst is 2 packets

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

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 mouted machine.

Example

The following example sets the interpacket delay to 200 milliseconds and the burst size to 3 packets. Therefore, at the periodic DVMRP report interval, if 6 packets are built, 3 packets will be sent, then a delay of 200 milliseconds occurs, then the next 3 packets are sent.

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

ip dvmrp reject-non-pruners

To configure the router so that it will not peer with a DVMRP neighbor if that neighbor does not support DVMRP pruning or grafting, use the **ip dvmrp reject-non-pruners** interface configuration command. To disable the feature, 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.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

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.

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

Example

The following example 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

To change the number of DVMRP routes allowed before a syslog warning message is issued, use the **ip dvmrp routehog-notification** global configuration command. 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.

Default

10,000 routes

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.2.

This command configures how many DVMRP routes are accepted on each interface within an approximate one-minute interval before a syslog message is issued, warning that there might be a route surge occurring. The warning is typically used to detect quickly when people have misconfigured their routers to inject a large number of routes into the 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.

Example

The following example lowers the threshold to 8000 routes:

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

Related Commands

You can use the master indexes or search online to find documentation of related commands.

show ip igmp interface

ip dvmrp route-limit

To change the limit on the number of DVMRP routes that can be advertised over an interface enabled to run DVMRP, use the **ip dvmrp route-limit** global configuration command. 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.

Default

7000 routes

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

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

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).

Example

The following example changes the limit to 5000 DVMRP routes allowed to be advertised:

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

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip dvmrp unicast-routing

ip dvmrp summary-address

To configure a DVMRP summary address to be advertised out the interface, use the **ip dvmrp summary-address** interface configuration command. To remove the summary address, use the **no** form of this command.

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

Syntax Description

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

Default

metric value is 1

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

If there is at least a single, more specific route in the unicast routing table that matches the specified *address* and *mask*, 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 address can be configured on an interface. When multiple overlapping summary addresses are configured on an interface, the one with the longest mask takes preference.

Example

The following example configures the DVMRP summary address 171.69.0.0 to be advertised out the interface:

```
ip dvmrp summary-address 171.69.0.0 255.255.0.0 metric 1
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip dvmrp auto-summary

ip dvmrp unicast-routing

To enable DVMRP unicast routing on an interface, use the **ip dvmrp unicast-routing** interface configuration command. To disable the feature, 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.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

Enabling DVMRP unicast routing means that routes in DVMRP Report messages are cached by the router in a DVMRP routing table. When PIM is running, these routes may get preference over routes in the unicast routing table. This allows PIM to run on the MBONE topology when it is different from the unicast topology.

DVMRP unicast routing can run on all interfaces, including 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/DVMRP multicast routing interaction.

Example

The following example enables DVMRP unicast routing:

```
ip dvmrp unicast-routing
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip dvmrp route-limit

ip igmp access-group

To control the multicast groups that hosts on the subnet serviced by an interface can join, use the **ip igmp access-group** interface configuration command. To disable groups on an interface, use the **no** form of this command.

ip igmp access-group *access-list-number* *version*
no ip igmp access-group *access-list-number* *version*

Syntax Description

access-list-number Number of a standard IP access list. This can be a number from 1 to 99.

version Changes IGMP version. Default is version 2.

Default

All groups are allowed on an interface.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Example

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

```
access-list 1 225.2.2.2 0.0.0.0
interface ethernet 0
 ip igmp access-group 1
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip igmp join-group

ip igmp helper-address

To cause the system to forward all IGMP Host Reports and Leave messages received on the interface to the specified IP address, use the **ip igmp helper-address** interface configuration command. 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.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2 F.

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 resent out the next-hop interface toward the IP address, with that interface's source address. This command enables a sort of "dense-mode" Join, allowing stub sites not participating in PIM to indicate membership in IP multicast groups.

Example

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

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

Router B

```
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

You can use the master indexes or search online to find documentation of related commands.

ip pim neighbor-filter

ip igmp join-group

To have the router join a multicast group, use the **ip igmp join-group** interface configuration command. To cancel membership in a multicast group, use the **no** form of this command.

```
ip igmp join-group group-address  
no ip igmp join-group group-address
```

Syntax Description

<i>group-address</i>	Address of the multicast group. This is a multicast IP address in four-part, dotted notation.
----------------------	---

Default

No multicast group memberships are predefined.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

IP packets that are addressed to the group address are passed to the IP client process in the Cisco IOS software.

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

Another reason to have a router join a multicast group is when other hosts on the network have a bug in IGRP that prevents them from correctly answering IGMP queries. Having the router join the multicast group causes upstream routers to maintain multicast routing table information for that group and keep the paths for that group active.

Example

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

```
ip igmp join-group 225.2.2.2
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip igmp access-group
ping (privileged)
ping (user)

ip igmp query-interval

To configure the frequency at which the Cisco IOS software sends IGMP host-query messages, use the **ip igmp query-interval** interface configuration command. To return to the default frequency, 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 to transmit IGMP host-query messages. The can be a number from 0 to 65535. The default is 60 seconds.

Default

60 seconds

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.2.

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

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

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

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

Note Changing this value may severely impact multicast forwarding.

Example

The following example changes the frequency at which the designated router sends IGMP host-query messages to 2 minutes:

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

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip pim query-interval
show ip igmp groups

ip igmp query-max-response-time

To configure the maximum response time advertised in IGMP queries, use the **ip igmp query-max-response-time** interface configuration command. 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.

Default

10 seconds

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

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

This command controls how long the responder has to respond to an IGMP Query message before the router deletes the group. Configuring a value less than 10 seconds enables the router to prune groups faster.

Note If the hosts do not respond fast enough, they might be pruned when you don't want them to be. Therefore, the hosts must know to respond faster than 10 seconds (or the value you configure).

Example

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

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

Related Commands

You can use the master indexes or search online to find documentation of related commands.

```
ip pim query-interval  
show ip igmp groups
```

ip igmp query-timeout

To configure the timeout time before the router takes over as the querier for the interface, after the previous querier has stopped querying, use the **ip igmp query-timeout** interface configuration command. To restore the default value, use the **no** form of this command.

```
ip igmp query-timeout seconds  
no ip igmp query-timeout
```

Syntax Description

seconds Number of seconds that the router waits after the previous querier has stopped querying and before it takes over as the querier.

Default

2 times the query interval

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1. It requires IGMP Version 2.

By default, the router waits twice the query interval specified by the **ip igmp query-interval** command, after which, if it has heard no queries, it becomes the querier. By default, the **ip igmp query-interval** defaults to 30 seconds, which means the **ip igmp query-timeout** defaults to 60 seconds.

Example

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

```
ip igmp query-timeout 30
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip igmp query-interval

ip igmp static-group

To configure the router to be a statically connected member of the specified group on the interface, use the **ip igmp static-group** interface configuration command. To remove the router as a member of the group, use the **no** form of this command.

```
ip igmp static-group group-address  
no ip igmp static-group group-address
```

Syntax Description

group-address IP multicast group address of a group that the router is a member of.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

When this command is configured, packets to the group are fast-switched out this interface, provided that packets were received on the correct RPF interface. This is unlike configuring the **ip igmp join-group** command, which also causes packets to be passed up to the process level.

If the **ip igmp join-group** command is configured 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.

Example

The following example configures 239.100.100.101 on Ethernet interface 0:

```
interface ethernet 0  
  ip igmp static-group 239.100.100.101
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip igmp join-group

ip igmp version

To configure which version of IGMP the router uses, use the **ip igmp version** interface configuration command. To restore the default value, use the **no** form of this command.

```
ip igmp version {2 | 1}  
no ip version
```

Syntax Description

2	IGMP Version 2.
1	IGMP Version 1.

Default

Version 2

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

All systems on the subnet must support the same version. The router does not automatically detect Version 1 systems and switch to Version 1, as did prior releases of the Cisco IOS software.

Configure Version 1 if your hosts do not support Version 2.

Some commands require IGMP Version 2, such as the **ip igmp query-max-response-time** and **ip igmp query-timeout** commands.

Example

The following example configures the router to use IGMP Version 1:

```
ip igmp version 1
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

```
ip igmp query-max-response-time  
ip igmp query-timeout  
show ip igmp groups  
show ip igmp interface
```

ip mroute

To configure a multicast static route (mroute), use the **ip mroute** global configuration command. To remove the route, use the **no** form of this command.

```
ip mroute source mask [protocol as-number] { rpf-address | type number } [distance]  
no ip mroute source mask [protocol as-number] { rpf-address | type number } [distance]
```

Syntax Description

<i>source</i>	IP address of the multicast source.
<i>mask</i>	Mask on the IP address of the multicast source.
<i>protocol</i>	(Optional) Unicast routing protocol that you are using.
<i>as-number</i>	(Optional) Autonomous system number of the routing protocol you are using, if applicable.
<i>rpf-address</i>	Incoming interface for the mroute. If the Reverse Path Forwarding address <i>rpf-address</i> is a PIM neighbor, PIM Joins, Grafts, and Prunes are sent to it. The <i>rpf-address</i> can be a host IP address of a directly connected system or a network/subnet number. When it is a route, a recursive lookup is done from the unicast routing table to find a directly connected system. If <i>rpf-address</i> is not specified, the interface <i>type number</i> is used as the incoming interface.
<i>type number</i>	Interface type and number for the mroute.
<i>distance</i>	(Optional) Determines whether a unicast route, a 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 two RPF sources, the static mroute will take precedence. The default is 0.

Default

distance: 0

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

This command allows you to statically configure where multicast sources are located (even though the unicast routing table says something different).

When a source range is specified, the *rpf-address* applies only to those sources.

Examples

The following example configures all sources via a single interface (in this case, a tunnel):

```
ip mroute 0.0.0.0 255.255.255.255 tunnel0
```

The following example configures all specific sources within a network number are reachable through 171.68.10.13:

```
ip mroute 171.69.0.0 255.255.0.0 171.68.10.13
```

The following example causes this multicast static route to take effect if the unicast routes for any given destination go away:

```
ip mroute 0.0.0.0 255.255.255.255 serial0 200
```

ip mroute-cache

To configure IP multicast fast switching, use the **ip mroute-cache** interface configuration command. To disable IP multicast fast switching, use the **no** form of this command.

ip mroute-cache
no ip mroute-cache

Syntax Description

This command has no arguments or keywords.

Default

Enabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

If fast switching is disabled on an incoming interface for a multicast routing table entry, the packet will be 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 (like unicast routing), debug messages are not logged. If you want to log debug messages, disable fast switching.

Example

The following example disables IP multicast fast switching on the interface:

```
no ip mroute-cache
```

ip multicast boundary

To configure an administratively scoped boundary, use the **ip multicast boundary** interface configuration command. To remove the boundary, use the **no** form of this command.

```
ip multicast boundary access-list-number  
no ip multicast boundary
```

Syntax Description

access-list-number Standard IP access list number identifying an access list that controls the range of group addresses affected by the boundary.

Default

There is no boundary.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

You might set up a boundary to keep multicast packets from being forwarded.

Example

The following example sets up a boundary for all administratively scoped addresses:

```
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
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

access-list (standard)

ip multicast cache-headers

To allocate a circular buffer to store IP multicast packet headers that the router receives, use the **ip multicast cache-headers** global configuration command. To disable the feature, use the **no** form of this command.

ip multicast cache-headers
no ip multicast cache-headers

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

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

- Who is sending IP multicast packets to what groups
- Inter-packet delay
- Duplicate IP multicast packets (if any)
- Multicast forwarding loops in your network (if any)
- Scope of the group
- UDP port numbers
- Packet length

Note This feature allocates a circular buffer of approximately 32 kilobytes. Do not configure this feature if you are low on memory.

Use the **show ip mpacket** command to display the buffer.

Example

The following example allocates a buffer to store IP multicast packet headers:

```
ip multicast cache-headers
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

show ip mpacket

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** interface configuration command. To prevent this feature, use the **no** form of this command.

```
ip multicast helper-map {group-address | broadcast} {broadcast-address |  
multicast-address} extended-access-list-number  
no multicast helper-map {group-address | broadcast} {broadcast-address |  
multicast-address} extended-access-list-number
```

Syntax Description

<i>group-address</i>	Multicast group address of traffic to be converted to broadcast traffic. Use this with the <i>broadcast-address</i> .
broadcast	Specifies the traffic is being converted from broadcast to multicast. Use this with the <i>multicast-address</i> .
<i>broadcast-address</i>	Address to which broadcast traffic is sent. Use this with the <i>group-address</i> .
<i>multicast-address</i>	Specifies the IP multicast address to which the converted traffic is directed. Use this with the broadcast keyword.
<i>extended-access-list-number</i>	IP extended access list that controls which broadcast packets are translated, based on the UDP port number.

Default

No conversion between broadcast and multicast occurs.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

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. 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.

Note On the last hop router, the **ip multicast helper-map** command introduces the **ip igmp join-group** command on that interface. That command must remain for this feature to work. If you remove the **ip igmp join-group** command, the feature fails. You can move the **ip igmp join-group** command to another interface on the same router.

Example

The following example illustrates how a helper address on two routers converts from broadcast to multicast and back to broadcast.

The configuration on the first hop router converts a broadcast stream arriving at incoming interface Ethernet interface 0 destined to UDP port 4000 to a multicast stream. The access list denies other traffic from being forwarded into the multicast cloud. The traffic is sent to group address 224.5.5.5. Because fast switching does not perform such a conversion, the **ip forward-protocol** command causes the proper process level to perform the conversion.

The configuration on the last hop router converts the multicast stream at incoming interface Ethernet interface 1 back to broadcast. Again, all multicast traffic emerging from the multicast cloud is not supposed to be converted to broadcast, only the traffic destined for UDP port 4000.

First Hop Router

```
interface ethernet 0
 ip multicast helper-map broadcast 224.5.5.5 120
 ip pim dense-mode
!
access-list 120 permit any any udp 4000
access-list 120 deny any any udp
 ip forward-protocol udp 4000
```

Last Hop Router

```
interface ethernet 1
 ip multicast helper-map 224.5.5.5 178.21.34.255 135
 ip pim dense-mode
!
access-list 135 permit any any udp 4000
access-list 135 deny any any udp
 ip forward-protocol udp 4000
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip forward-protocol

ip multicast rate-limit

To control the rate a sender from the source-list can send to a multicast group in the group-list, use the **ip multicast rate-limit** interface configuration command. 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	Only packets at the rate of <i>kbps</i> or slower are accepted on the interface.
out	Only a maximum of <i>kbps</i> will be transmitted on the interface.
video	(Optional) Rate limiting is performed based on the UDP port number used by video traffic. Video traffic is identified by consulting the sdr cache.
whiteboard	(Optional) Rate limiting is performed based on the UDP port number used by whiteboard traffic. Whiteboard traffic is identified by consulting the sdr cache.
group-list access-list	(Optional) Specifies the access list number that controls which multicast groups are subject to the rate limit.
source-list access-list	(Optional) Specifies the access list number that controls which senders are subject to the rate limit.
<i>kbps</i>	Kilobits-per-second transmission rate. Any packets sent at greater than this value are silently discarded. If this command is configured, the default value is 0, meaning that no traffic is permitted. Therefore, set this to a positive value if you use this command.

Default

If this command is not configured, there is no rate limit.

If this command is configured, *kbps* defaults to 0, meaning that no traffic is permitted.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

If a router receives a packet and in the last second the user has sent over the limit, the packet is dropped; otherwise, it is forwarded.

For **video** or **whiteboard** to work, the **ip sdr listen** command must be enabled so the port number can be obtained from the sdr cache. If **ip sdr listen** is not enabled, or the group address is not in the sdr cache, no rate-limiting is done for the group.

Example

In the following example, packets to any group from sources in network 171.69.0.0 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 171.69.0.0 0.0.255.255
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip sdr listen

ip multicast-routing

To enable IP multicast routing, use the **ip multicast-routing** global configuration command. To disable IP multicast routing, use the **no** form of this command.

ip multicast-routing
no ip multicast-routing

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

When IP multicast routing is disabled, the Cisco IOS software does not forward any multicast packets.

Example

The following example enables IP multicast routing:

```
ip multicast-routing
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip pim

ip multicast ttl-threshold

To configure the time-to-live (TTL) threshold of packets being forwarded out an interface, use the **ip multicast ttl-threshold** interface configuration command. 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.

Default

0, which means that all multicast packets are forwarded out the interface.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

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, which is obsolete.

Example

In the following example, you set the TTL threshold on a border router to 200, which is a very high value. This means that 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** interface configuration command. To disable the feature, 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.

Default

IP multicast address are mapped to the MAC-layer address 0xFFFF.FFFF.FFFF.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

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, it is possible there are other protocols 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.

Example

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 1.1.1.1 255.255.255.0
 ip pim dense-mode
 ip multicast use-functional
```

ip pim

To enable PIM on an interface, use the **ip pim** interface configuration command. To disable PIM on the interface, use the **no** form of this command.

```
ip pim {dense-mode | sparse-mode | sparse-dense-mode}  
no ip pim
```

Syntax Description

dense-mode	Enables dense mode of operation.
sparse-mode	Enables sparse mode of operation.
sparse-dense-mode	The interface is treated in the mode in which the group operates.

Default

IP multicast routing is disabled on all interfaces.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0. The **sparse-dense-mode** keyword first appeared in Cisco IOS Release 11.1.

Enabling PIM on an interface also enables IGMP operation on that interface. An interface can be configured to be in dense 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. In populating the multicast routing table, dense-mode interfaces are always added to the table. 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 there are multicast group members 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.

Sparse Mode

A sparse-mode interface is used for multicast forwarding only if a join message is received from a downstream router or if there are group members directly connected to the interface. Sparse mode assumes that there are no other multicast group members present. When sparse-mode routers want to join the shared path, they periodically send join messages toward the rendezvous point (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 to 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 a multicast routing table’s outgoing integrated list when either

- There are members or DVMRP neighbors 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 a multicast routing table’s outgoing interface when either of the following is true:

- There are members or DVMRP neighbors on the interface.
- A PIM neighbor on the interface has received an explicit Join.

Examples

The following commands enables sparse-mode PIM on tunnel interface 0 and sets 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 commands enable dense-mode PIM on Ethernet interface 1:

```
interface ethernet 1
ip pim dense-mode
```

The following example enables sparse-dense mode:

```
interface ethernet 1
ip pim sparse-dense-mode
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip multicast-routing
ip pim rp-address
show ip pim interface

ip pim accept-rp

To configure a router to accept Joins or Prunes destined for a specified RP and for a specific list of groups, use the **ip pim accept-rp** global configuration command. To remove that check, use the **no** form of this command.

```
ip pim accept-rp {address | auto-rp} [group-access-list-number]  
no ip pim accept-rp {ip-address | auto-rp} [group-access-list-number]
```

Syntax Description

<i>address</i>	RP address of the RP allowed to send Join messages to groups in the range specified by the group access list.
auto-rp	Join and Register messages are accepted only for RPs that are in the Auto-RP cache.
<i>group-access-list-number</i>	(Optional) Access list that defines which groups are subject to the check.

Default

Disabled, so all Join messages and Prune messages are processed.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.2.

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 *address* is one of the system's addresses, 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.

Example

The following example states that the router will accept Join or Prune messages destined for the RP at address 100.1.1.1 for the multicast group 224.2.2.2:

```
ip pim accept-rp 100.1.1.1 3  
access-list 3 permit 224.2.2.2
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

access-list (standard)

ip pim message-interval

To configure the frequency at which a sparse-mode PIM router sends periodic sparse-mode Join/Prune PIM messages, use the **ip pim message-interval** global configuration command. To return to the default interval, use the **no** form of this command.

ip pim message-interval *seconds*
no ip pim message-interval [*seconds*]

Syntax Description

seconds Interval, in seconds, at which periodic sparse-mode Join and Prune PIM messages are sent. It can be a number from 1 to 65535. The default is 60 seconds.

Default

60 seconds

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

The join-and-prune message interval should be the same for all routers in the network.

A router is pruned from a group if a Join message is not heard from it in three times the message interval specified by the *seconds* argument. By default, this is 3 minutes.

Note Changing this value may severely impact multicast forwarding.

Example

The following example changes the PIM message interval to 90 seconds:

```
ip pim message-interval 90
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip igmp query-interval
ip pim query-interval

ip pim minimum-vc-rate

To configure the minimum traffic rate to keep virtual circuits from being idled, use the **ip pim minimum-vc-rate** interface configuration command. To restore the default value, use the **no** form of this command.

```
ip pim minimum-vc-rate pps  
no 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.

Default

0 pps, which indicates all VCs are eligible for idling.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

This command applies to an ATM interface only and also requires IP PIM sparse mode.

An idling policy uses the **ip pim vc-count** *number* 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** are subject to the idling policy, which is described in the section “Limit the Number of Virtual Circuits” in the “Configuring IP Multicast Routing” chapter of the *Network Protocols Configuration Guide, Part 1*.

Example

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

You can use the master indexes or search online to find documentation of related commands.

ip pim vc-count

ip pim multipoint-signalling

To enable PIM to open ATM multipoint switched virtual circuits for each multicast group that a receiver joins, use the **ip pim multipoint-signalling** interface configuration command. 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.

Default

Disabled. All multicast traffic goes to the static map multipoint VC as long as the **atm multipoint-signalling** command is configured.

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

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.

Example

The following example enables PIM to open ATM multipoint switched virtual circuits for each multicast group that is joined:

```
ip pim multipoint-signalling
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

atm multipoint-signaling
ip pim minimum-vc-rate
ip pim vc-count
show ip pim vc

ip pim nbma-mode

To configure a multiaccess WAN interface to be in nonbroadcast, multiaccess mode, use the **ip pim nbma-mode** interface configuration command. To disable this feature, 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.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Use this command on Frame Relay, 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 PIM Join message is kept track of 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 **ip pim sparse-mode** is configured on the interface. This command is not recommended for LANs that have natural multicast capabilities.

Example

The following example configures an interface to be in nonbroadcast, multiaccess mode:

```
ip pim nbma-mode
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip pim sparse-mode

ip pim neighbor-filter

To prevent a router from participating in PIM (for example, to configure stub multicast routing), use the **ip pim neighbor-filter** interface configuration command. To remove the restriction, use the **no** form of this command.

```
ip pim neighbor-filter access-list-number  
no ip pim neighbor-filter access-list-number
```

Syntax Description

access-list-number Standard IP access list that denies PIM packets from a source.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

Example

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

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

Router B

```
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

You can use the master indexes or search online to find documentation of related commands.

access-list (standard)
ip igmp helper-address

ip pim query-interval

To configure the frequency of PIM router-query messages, use the **ip pim query-interval** interface configuration command. To return to the default interval, use the **no** form of this command.

```
ip pim query-interval seconds  
no ip pim query-interval [seconds]
```

Syntax Description

seconds Interval, in seconds, at which periodic PIM router-query messages are sent. It can be a number from 1 to 65535. The default is 30 seconds.

Default

30 seconds

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

Routers configured for IP multicast send PIM router-query messages to determine which router will be the designated router for each LAN segment (subnet). The designated router is responsible for sending IGMP host-query messages to all hosts on the directly connected LAN. When operating in sparse mode, the designated router is responsible for sending source registration messages to the RP. The designated router is the router with the largest IP address.

Example

The following example changes the PIM router-query message interval to 45 seconds:

```
interface tunnel 0  
 ip pim query-interval 45
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip igmp query-interval

ip pim rp-address

To configure the address of a PIM rendezvous point (RP) for a particular group, use the **ip pim rp-address** global configuration command. To remove an RP address, use the **no** form of this command.

```
ip pim rp-address ip-address [group-access-list-number] [override]  
no ip pim rp-address ip-address [group-access-list-number]
```

Syntax Description

<i>ip-address</i>	IP address of a router to be a PIM RP. This is a unicast IP address in four-part, dotted notation.
<i>group-access-list-number</i>	(Optional) Number of an access list that defines for which multicast groups the RP should be used. This is a standard IP access list. The number can be from 1 to 100.
override	(Optional) Indicates that if there is a conflict between the RP configured with this command and one learned by Auto-RP, the RP configured with this command prevails.

Default

No PIM RPs are preconfigured.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 10.2.

You must configure the IP address of RPs in leaf designated routers (DRs) only. *Leaf routers* are those routers that are directly connected either to a multicast group member or to a sender of multicast messages. Leaf DRs are the only ones that need to know about RPs. Even potential DRs (that might be elected if the primary DR fails) need to be configured to know about RPs.

First-hop routers send register packets to the RP address on behalf of source multicast hosts. Routers also use this address on behalf of multicast hosts that want to become members of a group. These routers send Join and Prune messages towards the RP. The RP must be a PIM router; however, it does not require any special configuration to recognize that it is the RP. Also, RPs are not members of the multicast group; rather, they serve as a “meeting place” for multicast sources and group members.

You can configure the Cisco IOS software to use a single RP for more than one group. The conditions specified by the access list determine which groups the RP can be used for. If no access list is configured, the RP is used for all groups.

A PIM router can use multiple RPs, but only one per group.

If there is no RP configured for a group, the router will treat the group as dense using the dense-mode PIM techniques.

If the RP for a group is learned through a dynamic mechanism, such as Auto-RP, then this command might not be required. If there is a conflict between the RP configured with this command and one learned by Auto-RP, the Auto-RP information is used, unless the **override** keyword is specified.

Examples

The following example sets the PIM RP address to 198.92.37.33 for all multicast groups:

```
ip pim rp-address 198.92.37.33
```

The following example sets the PIM RP address to 147.106.6.22 for the multicast group 225.2.2.2 only:

```
access list 1 225.2.2.2 0.0.0.0
ip pim rp-address 147.106.6.22 1
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

access-list (standard)

ip pim rp-announce-filter

To filter incoming Auto-RP announcement messages coming from the RP, use the **ip pim rp-announce-filter** global configuration command. To remove the filter, use the **no** form of this command.

```
ip pim rp-announce-filter rp-list access-list-number group-list access-list-number  
no ip rp-announce-filter rp-list access-list-number group-list access-list-number
```

Syntax Description

rp-list <i>access-list-number</i>	Standard access list of RP addresses that are allowable for the group ranges supplied in the group-list <i>access-list-number</i> .
group-list <i>access-list-number</i>	Standard access list that describes the multicast groups the RPs serve.

Default

All RP announcements are accepted.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

Configure this command on the PIM RP-mapping agent. If you are going to use more than one RP-mapping agent, make the filters among them consistent so that there are no conflicts in mapping state when the announcing agent goes down.

Example

The following example configures the router to accept RP announcements from RPs in access list 1 for group ranges described 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

You can use the master indexes or search online to find documentation of related commands.

access-list (standard)

ip pim send-rp-announce

To use Auto-RP to configure which groups the router is willing to act as RP for, use the **ip pim send-rp-announce** global configuration command. To deconfigure this router to be the RP, use the **no** form of this command.

```
ip pim send-rp-announce type number scope ttl group-list access-list-number  
no ip pim send-rp-announce
```

Syntax Description

<i>type number</i>	Interface type and number that identify the RP address.
scope <i>ttl</i>	Time-to-live value that limits the announcements.
group-list <i>access-list-number</i>	Access list that describes the group ranges for which this router is the RP.

Default

Auto-RP is disabled.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

Use this command in the router you want to be an RP. 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.

Example

The following example sends RP announcements out all PIM-enabled interfaces for a maximum of 31 hops. The IP address the router wants to be identified by as RP is the IP address associated with Ethernet interface 0. Access-list 5 describes for which groups 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

You can use the master indexes or search online to find documentation of related commands.

access-list (standard)

ip pim send-rp-discovery

To configure the router to be an RP-mapping agent, use the **ip pim send-rp-discovery** global configuration command. To restore the default value, use the **no** form of this command.

```
ip pim send-rp-discovery scope ttl  
no ip pim send-rp-discovery
```

Syntax Description

scope ttl Time-to-live value in the IP header that keeps the discovery messages within this number of hops.

Default

The router is not an RP mapping agent.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

Configure this command on the router designated as an RP-mapping agent. Specify a TTL large enough to cover your PIM domain.

When Auto-RP is used, the following steps occur:

- 1 The RP-mapping agent listens on well-known group address CISCO-RP-ANNOUNCE (224.0.1.39), which candidate RPs send to.
- 2 The RP-mapping agent sends RP-to-group mappings in an Auto-RP RP discovery message to the well-known group CISCO-RP-DISCOVERY (224.0.1.40). The TTL value limits how many hops the message can take.
- 3 PIM designated routers listen to this group and use the RPs they learn about from the discovery message.

Example

The following example limits Auto-RP RP Discovery messages to 20 hops:

```
ip pim send-rp-discovery scope 20
```

ip pim spt-threshold

To configure when a PIM leaf router should join the shortest path source-tree for the specified group, use the **ip pim spt-threshold** global configuration command. To restore the default value, use the **no** form of this command.

```
ip pim spt-threshold {kbps | infinity} [group-list access-list-number]  
no ip pim spt-threshold
```

Syntax Description

<i>kbps</i>	Traffic rate in kilobits per second.
infinity	Causes all sources for the specified group to use the shared-tree.
group-list <i>access-list-number</i>	(Optional) Indicates what groups the threshold applies to. Must be a standard IP access list number. If the value is 0 or is omitted, the threshold applies to all groups.

Default

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 Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

If a source sends at a rate greater than or equal to 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 what groups the threshold applies to.

If the traffic rate from the source drops below the threshold *kbps* value, the leaf router will, after some amount of time, switch back to the shared tree and send a Prune message toward the source.

Example

The following example sets a threshold of 4 kbps, above which traffic to a group from a source will cause the router to switch to the shortest path tree to that source:

```
ip pim spt-threshold 4
```

ip pim vc-count

To change the maximum number of virtual circuits that PIM can open, use the **ip pim vc-count** interface configuration command. 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 virtual circuits that PIM can open. The default is 200 virtual circuits. The range is from 1 to 65535.

Default

200 virtual circuits per ATM interface or subinterface

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

Example

The following example allows PIM to open a maximum of 250 virtual circuits:

```
ip pim vc-count 250
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip pim minimum-vc-rate
ip pim multipoint-signalling
ip pim sparse-mode
show ip pim vc

ip rtp compression-connections

To specify the total number of RTP header compression connections that can exist on an interface, use the **ip rtp compression-connections** interface configuration command. To restore the default value, use the **no** form of this command.

ip rtp compression-connections *number*
no ip rtp compression-connections

Syntax Description

number Number of connections the cache supports, in the range from 3 to 256. The default is 16 connections.

Default

16 connections

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

Example

The following example changes the number of RTP header compression connections supported to 24:

```
interface serial 0
  encapsulation ppp
  ip rtp header-compression
  ip rtp compression-connections 24
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip rtp header-compression

ip rtp header-compression

To enable RTP header compression, use the **ip rtp header-compression** interface configuration command. To disable RTP header compression, use the **no** form of this command.

```
ip rtp header-compression [passive]  
no ip rtp header-compression [passive]
```

Syntax Description

passive (Optional) Compresses outgoing RTP packets only if incoming RTP packets on the same interface are compressed.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

If you use this command without the **passive** keyword, the software compresses all RTP traffic.

You can compress IP/UDP/RTP headers to reduce the size of your packets. This is especially useful for RTP, since RTP payload can be as small as 20 bytes, and the uncompressed header is 40 bytes.

RTP header compression is supported on serial lines using Frame Relay, HDLC, or PPP encapsulation. You must enable compression on both ends of a serial connection.

This feature can compress unicast or multicast RTP packets, and hence MBONE traffic can also be compressed over slow links. The compression scheme is beneficial only when you have small payload sizes, as in audio traffic.

Example

The following example enables RTP header compression on serial interface 0 and limits the number of RTP header compression connections to 10:

```
interface serial 0  
  encapsulation ppp  
  ip rtp header-compression  
  ip rtp compression-connections 10
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

```
clear ip rtp header-compression  
ip rtp compression-connections  
show ip rtp header-compression
```

ip sdr cache-timeout

To limit how long an sdr cache entry stays active in the cache, use the **ip sdr cache-timeout** global configuration command. To restore the default value, use the **no** form of this command.

```
ip sdr cache-timeout minutes  
no ip sdr cache-timeout
```

Syntax Description

minutes Time, in minutes, that an sdr cache entry is active in the cache.

Default

Disabled, which means entries are never deleted from the cache.

Command Mode

Global configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.2.

You might want to limit how long sdr cache entries remain active because, otherwise, the source might stop advertising sdr's. You don't want to keep old advertisements needlessly.

Example

The following example causes sdr cache entries to remain in the cache for only 30 minutes:

```
ip sdr cache-timeout 30
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

```
clear ip sdr  
show ip sdr
```

ip sdr listen

To enable the Cisco IOS software to listen to session directory advertisements, use the **ip sdr listen** interface configuration command. To disable the feature, use the **no** form of this command.

ip sdr listen
no ip sdr listen

Syntax Description

This command has no arguments or keywords.

Default

Disabled

Command Mode

Interface configuration

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1. This command replaces the **ip sd listen** command, which is obsolete.

Session Directory Protocol (sdr) is a multicast application for setting up desktop conferencing sessions. It allocates group addresses and allows the user to specify the scope of the group and whether audio, video, or whiteboard applications will be invoked when users open the session.

Use this command to store session advertisements sent to the group. The **ip sdr listen** command merely enables the software to listen to session directory advertisements. The router joins the default session directory group (group 224.2.127.254) on the interface. Use this command to get contact information.

Example

The following example enables a router to listen to session directory advertisements:

```
ip sdr listen
```

Related Commands

You can use the master indexes or search online to find documentation of related commands.

clear ip sdr
show ip sdr

mrinfo

To query what neighboring multicast routers are peering with the local router, use the **mrinfo** EXEC command.

```
mrinfo [hostname-or-address] [source-address-or-interface]
```

Syntax Description

<i>hostname-or-address</i>	(Optional) Queries the DNS name or IP address of the multicast router. If omitted, the router queries itself.
<i>source-address-or-interface</i>	(Optional) Source address used on mrinfo requests. If omitted, the source address is based on the outbound interface for the destination.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

The mrinfo command is the MBONE's original tool to determine what neighboring multicast routers are peering with a multicast router. Cisco routers have supported responding to mrinfo requests since Cisco IOS Release 10.2.

Now you can query a multicast router using this command. The output format is identical to DVMRP's mrouted version. (The mrouted software is the UNIX software that implements DVMRP.)

Sample Display

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

```
Router # mrinfo

192.31.7.37 (barnnet-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]
  131.119.26.10 -> 131.119.26.9 (su-pr2.bbplanet.net) [1/32/pim]
```

The flags indicate the following:

P = prune-capable
M = mtrace-capable
S = SNMP-capable
A = Auto-RP-capable

mstat

To display IP multicast packet rate and loss information, use the **mstat** user EXEC command.

mstat *source* [*destination*] [*group*]

Syntax Description

- source* DNS name or the IP address of the multicast-capable source.
- destination* (Optional) DNS name or address of the destination. If omitted, the command uses the system at which the command is typed.
- group* (Optional) DNS name or multicast address of the group to be displayed. Default address is 224.2.0.1 (the group used for MBONE Audio).

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

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.

Sample Display

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

```
Router# mstat lwei-home-ss2 171.69.58.88 224.0.255.255

Type escape sequence to abort.
Mtrace from 171.69.143.27 to 171.69.58.88 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
171.69.143.27    171.69.62.144    All Multicast Traffic      From 171.69.143.27
      |           ___/ rtt 48   ms    Lost/Sent = Pct Rate      To 224.0.255.255
      v           /   hop 48   ms    -----
171.69.143.25    lwei-cisco-isdn.cisco.com
      |           ^     ttl 1
      v           |     hop 31   ms    0/12 = 0%      1 pps    0/1 = --%  0 pps
171.69.121.84
171.69.121.45    eng-frmt12-pri.cisco.com
      |           ^     ttl 2
      v           |     hop -17  ms    -735/12 = --%  1 pps    0/1 = --%  0 pps
171.69.121.4
171.69.5.27      eng-cc-4.cisco.com
      |           ^     ttl 3
      v           |     hop -21  ms    -678/23 = --%  2 pps    0/1 = --%  0 pps
171.69.5.21
171.69.62.130    eng-ios-2.cisco.com
      |           ^     ttl 4
      v           |     hop 5    ms    605/639 = 95%  63 pps    1/1 = --%  0 pps
```

```

171.69.62.144
171.69.58.65   eng-ios-f-5.cisco.com
  |           \__  ttl  5
  v           \  hop  0  ms      4      0 pps      0      0 pps
171.69.58.88   171.69.62.144
Receiver       Query Source

```

Table 70 describes the fields shown in the display.

Table 70 Mstat Field Descriptions

Field	Description
Source	Traffic source of packet.
Response Dest	Place where the router sends the results of 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 ... 0/2	0 packets dropped out of 2 packets received. If, for example, -2/2 was indicated, then there are 2 extra packets; this could indicate a loop condition.

Related Commands

You can use the master indexes or search online to find documentation of related commands.

mtrace

mtrace

To trace the path from a source to a destination branch for a multicast distribution tree, use the **mtrace** user EXEC command.

```
mtrace source [destination] [group]
```

Syntax Description

<i>source</i>	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.
<i>destination</i>	(Optional) DNS name or address of the unicast destination. If omitted, the mtrace starts from the system at which the command is typed.
<i>group</i>	(Optional) DNS name or multicast address of the group to be traced. Default address is 224.2.0.1 (the group used for MBONE Audio). When address 0.0.0.0 is used, the software invokes a weak mtrace . A weak mtrace is one that follows the RPF path to the source, regardless of whether any router along the path has multicast routing table state.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

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 destination to 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.

Sample Display

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

```
Router# mtrace 171.69.215.41 171.69.215.67 239.254.254.254

Type escape sequence to abort.
Mtrace from 171.69.215.41 to 171.69.215.67 via group 239.254.254.254
From source (?) to destination (?)
Querying full reverse path...
 0 171.69.215.67
-1 171.69.215.67 PIM thresh^ 0 0 ms
-2 171.69.215.74 PIM thresh^ 0 2 ms
-3 171.69.215.57 PIM thresh^ 0 894 ms
-4 171.69.215.41 PIM thresh^ 0 893 ms
-5 171.69.215.12 PIM thresh^ 0 894 ms
-6 171.69.215.98 PIM thresh^ 0 893 ms
```

Table 71 describes the fields shown in the display.

Table 71 Mtrace Field Descriptions

Field	Description
Mtrace from 171.69.215.41 to 171.69.215.67 via group 239.254.254.254	Name and address of source, destination, and group for which routes are being traced.
-3 171.69.215.57	Hops away from destination (-3) and address of intermediate router.
PIM thresh^ 0	Multicast protocol in use on this hop, and ttl threshold.
893 ms	Time taken for trace to be forwarded between hops.

Related Commands

You can use the master indexes or search online to find documentation of related commands.

mstat

ping

To send an ICMP Echo Request to a multicast group, use the **ping** EXEC command.

ping [*group-name-or-address*]

Syntax Description

group-name-or-address (Optional) Sends an ICMP Echo Request to the specified multicast group.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.2.

If you use this command with no argument, the system prompts you. We highly recommend you specify a TTL when you are prompted.

show frame-relay ip rtp header-compression

To show Frame Relay's RTP header compression statistics, use the **show frame-relay ip rtp header-compression** EXEC command.

```
show frame-relay ip rtp header-compression [interface type number]
```

Syntax Description

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

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

Sample Display

The following is sample output from the **show frame-relay ip rtp header-compression** command:

```
Router# show frame-relay ip rtp header-compression

DLCI 17 Link/Destination info: ip 165.3.3.2
Interface Serial0:
  Rcvd:    0 total, 0 compressed, 0 errors
          0 dropped, 0 buffer copies, 0 buffer failures
  Sent:    6000 total, 5998 compressed,
          227922 bytes saved, 251918 bytes sent
          1.90 efficiency improvement factor
  Connect: 16 rx slots, 16 tx slots, 2 long searches, 2 misses
          99% hit ratio, five minute miss rate 0 misses/sec, 0 max
```

Table 72 describes the significant fields in the display.

Table 72 Show Frame Relay IP RTP Header-Compression Field Descriptions

Field	Description
Interface Serial0	Type and number of interface.
Rcvd: total	Number of packets received on the interface.
compressed	Number of packets with compressed header.
errors	Number of errors.
dropped	Number of dropped packets.
buffer copies	Number of buffers that had to be copied.
buffer failures	Number of failures in allocating buffers.
Sent: total	Total number of packets sent.
compressed	Number of packets sent with compressed header.
bytes saved	Total savings in bytes due to compression.
bytes sent	Total bytes sent after compression.

Table 72 Show Frame Relay IP RTP Header-Compression Field Descriptions (Continued)

Field	Description
efficiency improvement factor	Compression efficiency.
Connect: rx slots	Total number of receive slots.
tx slots	Total number of transmit slots.
long searches	Searches that needed more than one lookup.
misses	Number of new states that were created.
hit ratio	Number of times existing states were revised.
five minute miss rate	Average miss rate.
max	Maximum miss rate.

Related Commands

You can use the master indexes or search online to find documentation of related commands.

frame-relay ip rtp header-compression

frame-relay map ip compress

frame-relay map ip rtp header-compression

show ip rtp header-compression

show ip dvmrp route

To display the contents of the DVMRP routing table, use the **show ip dvmrp route** EXEC command.

```
show ip dvmrp route [name | ip-address]
```

Syntax Description

name | *ip-address* (Optional) Name or IP address of an entry in the DVMRP routing table.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.3.

Sample Display

The following is sample output of the **show ip dvmrp route** command:

```
Router# show ip dvmrp route

DVMRP Routing Table - 1 entry
171.68.0.0/16 [100/11] uptime 07:55:50, expires 00:02:52
  via 137.39.3.93, Tunnel3
```

Table 73 describes the fields shown in the display

Table 73 Show IP DVMRP Route Field Descriptions

Field	Description
1 entry	Number of entries in the DMVRP routing table.
171.68.0.0/16	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 137.39.3.93	Next-hop router to the source network.
Tunnel3	Interface to the source network.

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip dvmrp accept-filter

show ip igmp groups

To display the multicast groups that are directly connected to the router and that were learned via IGMP, use the **show ip igmp groups** EXEC command.

```
show ip igmp groups [group-name | group-address | type number]
```

Syntax Description

<i>group-name</i>	(Optional) Name of the multicast group, as defined in the DNS hosts table.
<i>group-address</i>	(Optional) Address of the multicast group. This is a multicast IP address in four-part, dotted notation.
<i>type</i>	(Optional) Interface type.
<i>number</i>	(Optional) Interface number.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

If you omit all optional arguments, the **show ip igmp groups** command displays by group address and interface type and number all directly connected multicast groups.

Sample Display

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
224.0.255.1        Ethernet0      18:51:41    0:02:15     198.92.37.192
224.2.226.60       Ethernet0      1:51:31     0:02:17     198.92.37.192
224.2.127.255      Ethernet0      18:51:45    0:02:17     198.92.37.192
226.2.2.2          Ethernet1      18:51:47    never        0.0.0.0
224.2.0.1          Ethernet0      18:51:43    0:02:14     198.92.37.192
225.2.2.2          Ethernet0      18:51:43    0:02:21     198.92.37.33
225.2.2.2          Ethernet1      18:51:47    never        0.0.0.0
225.2.2.4          Ethernet0      18:18:02    0:02:20     198.92.37.192
225.2.2.4          Ethernet1      18:23:32    0:02:55     198.92.36.128
```

Table 74 describes the fields shown in the display.

Table 74 Show IP IGMP Groups Field Descriptions

Field	Description
Group address	Address of the multicast group.
Interface	Interface through which the group is reachable.
Uptime	How long in hours, minutes, and seconds this multicast group has been known.
Expires	How long in hours, minutes, and seconds until the entry is removed from the IGMP groups table.
Last Reporter	Last host to report being a member of the multicast group.

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip igmp query-interval

show ip igmp interface

To display multicast-related information about an interface, use the **show ip igmp interface EXEC** command.

```
show ip igmp interface [type number]
```

Syntax Description

<i>type</i>	(Optional) Interface type.
<i>number</i>	(Optional) Interface number.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

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 DVMRP routers on the interface.

Sample Display

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 198.92.37.6, 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 198.92.37.33
  No multicast groups joined
Ethernet1 is up, line protocol is up
  Internet address is 198.92.36.129, 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 198.92.36.131
  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 75 describes the fields shown in the display.

Table 75 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 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-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).
Multicast groups joined: 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

You can use the master indexes or search online to find documentation of related commands.

ip address

ip igmp access-group

ip igmp query-interval

ip multicast ttl-threshold

ip pim

show ip mcache

To display the contents of the IP fast-switching cache, use the **show ip mcache** EXEC command.

```
show ip mcache [group [source]]
```

Syntax Description

group (Optional) Displays the fast-switching cache for the single group. The *group* argument can be either a Class D IP address or a DNS name.

source (Optional) If *source* is also specified, displays a single multicast cache entry. The *source* argument can be either a unicast IP address or a DNS name.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

Sample Display

The following is sample output from the **show ip mcache** command. This entry shows a specific source (wrn-source 204.62.246.73) sending to the World Radio Network group (224.2.143.24).

```
Router> show ip mcache wrn wrn-source

IP Multicast Fast-Switching Cache
(204.62.246.73/32, 224.2.143.24), Fddi0, Last used: 00:00:00
Ethernet0      MAC Header: 01005E028F1800000C1883D30800
Ethernet1      MAC Header: 01005E028F1800000C1883D60800
Ethernet2      MAC Header: 01005E028F1800000C1883D40800
Ethernet3      MAC Header: 01005E028F1800000C1883D70800
```

Table 76 describes the significant fields in the display.

Table 76 Show IP Mcache Field Descriptions

Field	Description
204.62.246.73	Source address.
224.2.143.24	Destination address.
Fddi0	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.
Ethernet0 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 mpacket

To display the contents of the circular cache-header buffer, use the **show ip mpacket EXEC** command.

```
show ip mpacket [source-address-or-name] [group-address-or-name] [detail]
```

Syntax Description

source-address-or-name (Optional) Displays cache headers matching the specified source address or name.

group-address-or-name (Optional) Displays cache headers matching the specified group address or group name.

detail (Optional) In addition to the summary information, displays the rest of the IP header fields on an additional line, plus the first 8 bytes after the IP header (usually the UDP port numbers).

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

This command is only applicable 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, TTL, source and destination IP addresses, and a local timestamp when the packet was received.

The two arguments and one keyword can be used in the same command in any combination.

Sample Display

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

```
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 (ABC-xy.company.com) 198.15.228.10 224.5.6.7
7302/113 206417.908 (school.edu) 147.12.2.17 224.5.6.7
6CB2/114 206417.412 (MSSRS.company.com) 154.2.19.40 224.5.6.7
D782/117 206417.868 (ABC-xy.company.com) 198.15.228.10 224.5.6.7
E2E9/123 206418.488 (Newman.com) 211.1.8.10 224.5.6.7
1CA7/127 206418.544 (teller.company.com) 192.4.6.10 224.5.6.7
```

Table 77 describes the fields in the display.

Table 77 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	Timestamp sequence number of the packet.
(name)	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 that the packet is sent to. In this example, the group address of "smallgroup."

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip multicast cache-headers

show ip mroute

To display the contents of the IP multicast routing table, use the **show ip mroute** EXEC command.

```
show ip mroute [group-name | group-address] [source] [summary] [count] [active kbps]
```

Syntax Description

<i>group-name</i> <i>group-address</i>	(Optional) IP address, name, or interface of the multicast group as defined in the DNS hosts table.
<i>source</i>	(Optional) IP address or name of a multicast source.
summary	(Optional) Displays a one-line, abbreviated summary of each entry in the IP multicast routing table.
count	(Optional) Displays statistics about the group and source, including number of packets, packets per second, average packet size, and bits per second.
active kbps	(Optional) Displays the rate that active sources are sending to multicast groups. Active sources are those sending at a rate of <i>kbps</i> or higher. The <i>kbps</i> argument defaults to 4 kbps.

Default

The **show ip mroute** command displays all groups and sources.

The **show ip mroute active** command displays all sources sending at a rate greater than or equal to 4 kbps.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

If you omit all optional arguments and keywords, the **show ip mroute** command displays all entries in the IP multicast routing table.

The Cisco IOS software populates the multicast routing table by creating source, group (S,G) entries from star, group (*,G) entries. The star 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, via Reverse Path Forwarding [RPF]).

Sample Displays

The following is sample output from the **show ip mroute** command for a router operating in dense mode. This command 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, C - Connected, L - Local, P - Pruned
      R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.0.255.1), uptime 0:57:31, expires 0:02:59, RP is 0.0.0.0, flags: DC
  Incoming interface: Null, RPF neighbor 0.0.0.0, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Dense, 0:57:31/0:02:52
    Tunnel0, Forward/Dense, 0:56:55/0:01:28

(198.92.37.100/32, 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 for a router operating in sparse mode:

```
Router# show ip mroute

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
      R - RP-bit set, F - Register flag, T - SPT-bit set
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.0.255.3), uptime 5:29:15, RP is 198.92.37.2, flags: SC
  Incoming interface: Tunnel0, RPF neighbor 10.3.35.1, Dvmrp
  Outgoing interface list:
    Ethernet0, Forward/Sparse, 5:29:15/0:02:57

(198.92.46.0/24, 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 that shows the VCD value, because an ATM interface with PIM multipoint signaling is enabled:

```
Router# show ip mroute 224.1.1.1

IP Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned
      R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 224.1.1.1), 00:03:57/00:02:54, RP 130.4.101.1, flags: SJ
  Incoming interface: Null, RPF nbr 0.0.0.0
  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, C - Connected, L - Local, P - Pruned
      R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, Next-Hop, State/Mode

(*, 224.255.255.255), 2d16h/00:02:30, RP 171.69.10.13, flags: SJPC

(*, 224.2.127.253), 00:58:18/00:02:00, RP 171.69.10.13, flags: SJC

(*, 224.1.127.255), 00:58:21/00:02:03, RP 171.69.10.13, flags: SJC

(*, 224.2.127.254), 2d16h/00:00:00, RP 171.69.10.13, flags: SJCL
(128.9.160.67/32, 224.2.127.254), 00:02:46/00:00:12, flags: CLJT
(129.48.244.217/32, 224.2.127.254), 00:02:15/00:00:40, flags: CLJT
(130.207.8.33/32, 224.2.127.254), 00:00:25/00:02:32, flags: CLJT
(131.243.2.62/32, 224.2.127.254), 00:00:51/00:02:03, flags: CLJT
(140.173.8.3/32, 224.2.127.254), 00:00:26/00:02:33, flags: CLJT
(171.69.60.189/32, 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

Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
  Source: 146.137.28.69 (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: 130.129.52.160 (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: 130.129.52.160 (webcast3-e1.acm97.interop.net)
  Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

The following is sample output from the **show ip mroute** command with the **count** keyword:

```
Router# show ip mroute count

IP Multicast Statistics - Group count: 8, Average sources per group: 9.87
Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kilobits per second

Group: 224.255.255.255, Source count: 0, Group pkt count: 0
  RP-tree: 0/0/0/0

Group: 224.2.127.253, Source count: 0, Group pkt count: 0
  RP-tree: 0/0/0/0

Group: 224.1.127.255, Source count: 0, Group pkt count: 0
  RP-tree: 0/0/0/0

Group: 224.2.127.254, Source count: 9, Group pkt count: 14
  RP-tree: 0/0/0/0
  Source: 128.2.6.9/32, 2/0/796/0
  Source: 128.32.131.87/32, 1/0/616/0
  Source: 128.125.51.58/32, 1/0/412/0
  Source: 130.207.8.33/32, 1/0/936/0
  Source: 131.243.2.62/32, 1/0/750/0
```

```

Source: 140.173.8.3/32, 1/0/660/0
Source: 146.137.28.69/32, 1/0/584/0
Source: 171.69.60.189/32, 4/0/447/0
Source: 204.162.119.8/32, 2/0/834/0

Group: 224.0.1.40, Source count: 1, Group pkt count: 3606
RP-tree: 0/0/0/0
Source: 171.69.214.50/32, 3606/0/48/0, RPF Failed: 1203

Group: 224.2.201.241, Source count: 36, Group pkt count: 54152
RP-tree: 7/0/108/0
Source: 13.242.36.83/32, 99/0/123/0
Source: 36.29.1.3/32, 71/0/110/0
Source: 128.9.160.96/32, 505/1/106/0
Source: 128.32.163.170/32, 661/1/88/0
Source: 128.115.31.26/32, 192/0/118/0
Source: 128.146.111.45/32, 500/0/87/0
Source: 128.183.33.134/32, 248/0/119/0
Source: 128.195.7.62/32, 527/0/118/0
Source: 128.223.32.25/32, 554/0/105/0
Source: 128.223.32.151/32, 551/1/125/0
Source: 128.223.156.117/32, 535/1/114/0
Source: 128.223.225.21/32, 582/0/114/0
Source: 129.89.142.50/32, 78/0/127/0
Source: 129.99.50.14/32, 526/0/118/0
Source: 130.129.0.13/32, 522/0/95/0
Source: 130.129.52.160/32, 40839/16/920/161
Source: 130.129.52.161/32, 476/0/97/0
Source: 130.221.224.10/32, 456/0/113/0
Source: 132.146.32.108/32, 9/1/112/0

```

Table 78 explains the fields shown in the displays.

Table 78 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.
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.
P - Pruned	Route has been pruned. The Cisco IOS software keeps this information in case a downstream member wants to join the source.
R - Rp-bit set	Indicates that the (S,G) entry is pointing towards 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.
Timers:	Uptime/Expires.
Interface state:	Interface, Next-Hop or VCD, State/Mode.

Table 78 Show IP Mroute Field Descriptions (Continued)

Field	Description
(* , 224.0.255.1) (198.92.37.100/32, 224.0.255.1)	Entry in the IP multicast routing table. The entry consists of the IP address of the source router followed by 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.
uptime	How long in hours, minutes, and seconds the entry has been in the IP multicast routing table.
expires	How long in hours, minutes, and seconds until the entry will be removed from the IP multicast routing table on the outgoing interface.
RP	Address of the rendezvous point (RP) router. For routers and access servers operating in sparse mode, this address is always 0.0.0.0.
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	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.
Dvmrp or Mroute	Indicates if the RPF information is obtained from the DVMRP routing table or the static mroutes configuration.
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 PIM neighbor is also displayed.
Ethernet0	Name and number of the outgoing interface.
Next hop or VCD	Next hop specifies downstream neighbor’s IP address. Virtual circuit descriptor number. VCD0 means the group is using the static-map virtual circuit.
Forward/Dense	Indicates that packets will be forwarded on the interface if there are no restrictions due to access lists or TTL threshold. Following the slash (/), mode in which the interface is operating (dense or sparse).
Forward/Sparse	Sparse-mode interface is in forward mode.
time/time (uptime/expiration time)	Per interface, how long in hours, minutes, and seconds the entry has been in the IP multicast routing table. Following the slash (/), how long in hours, minutes, and seconds until the entry will be removed from the IP multicast routing table.

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip multicast-routing
ip pim

show ip pim interface

To display information about interfaces configured for PIM, use the **show ip pim interface EXEC** command.

show ip pim interface [*type number*] [**count**]

Syntax Description

<i>type</i>	(Optional) Interface type.
<i>number</i>	(Optional) Interface number.
count	(Optional) Number of packets received and sent out the interface.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

This command works only on interfaces that are configured for PIM.

Sample Displays

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

```
Router# show ip pim interface

Address          Interface      Mode   Neighbor  Query   DR
                Count         Interval
198.92.37.6      Ethernet0     Dense  2          30      198.92.37.33
198.92.36.129    Ethernet1     Dense  2          30      198.92.36.131
10.1.37.2        Tunnel0       Dense  1          30      0.0.0.0
```

The following is sample output from the **show ip pim interface** command with a **count**:

```
Router# show ip pim interface count

Address          Interface      FS   Mpackets In/Out
171.69.121.35    Ethernet0     *    548305239/13744856
171.69.121.35    Serial0.33    *    8256/67052912
198.92.12.73     Serial0.1719  *    219444/862191
```

Table 79 describes the fields shown in the display.

Table 79 Show IP PIM Interface Field Descriptions

Field	Description
Address	IP address of the next-hop router.
Interface	Interface type and number that is configured to run PIM.
Mode	Multicast mode in which the Cisco IOS software is operating. This can be dense mode or sparse mode. DVMRP indicates a DVMRP tunnel is configured.

Table 79 Show IP PIM Interface Field Descriptions (Continued)

Field	Description
Neighbor 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 router-query messages, as set by the ip pim query-interval interface configuration command. The default is 30 seconds.
DR	IP address of the designated router on the LAN. Note that serial lines do not have designated routers, so the IP address is shown as 0.0.0.0.
FS	An asterisk (*) in this column indicates fast switching is enabled.
Mpackets In/Out	Number of packets into and out of the interface since the box has been up.

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip pim
show ip pim neighbor

show ip pim neighbor

To list the PIM neighbors discovered by the Cisco IOS software, use the **show ip pim neighbor EXEC** command.

show ip pim neighbor [*type number*]

Syntax Description

type (Optional) Interface type.

number (Optional) Interface number.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.0.

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

Sample Display

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

```
Router# show ip pim neighbor

PIM Neighbor Table
Neighbor Address  Interface      Uptime    Expires    Mode
198.92.37.2      Ethernet0     17:38:16  0:01:25   Dense
198.92.37.33     Ethernet0     17:33:20  0:01:05   Dense (DR)
198.92.36.131    Ethernet1     17:33:20  0:01:08   Dense (DR)
198.92.36.130    Ethernet1     18:56:06  0:01:04   Dense
10.1.22.9        Tunnel0       19:14:59  0:01:09   Dense
```

Table 80 describes the fields shown in the display.

Table 80 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	How long in hours, minutes, and seconds the entry has been in the PIM neighbor table.
Expires	How long in hours, minutes, and seconds until the entry will be removed from the IP multicast routing table.
Mode	Mode in which the interface is operating.
(DR)	Indicates that this neighbor is a designated router on the LAN.

Related Commands

You can use the master indexes or search online to find documentation of related commands.

show ip pim interface

show ip pim rp

To display active rendezvous points (RPs) that are cached with associated multicast routing entries, use the **show ip pim rp EXEC** command.

```
show ip pim rp [group-name | group-address] [mapping]
```

Syntax Description

<i>group-name</i>	(Optional) Name of the group about which to display RPs.
<i>group-address</i>	(Optional) Address of the group about which to display RPs.
mapping	(Optional) Displays all group-to-RP mappings that the router is aware of (either configured or learned from Auto-RP).

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 10.2.

Sample Displays

The following is sample output of the **show ip pim rp** command:

```
Router # show ip pim rp

Group: 224.2.240.30, RP: 171.69.10.13, v1, uptime 1d03h, expires 00:04:17
Group: 224.1.127.255, RP: 171.69.10.13, v1, uptime 16:39:28, expires 00:04:05
Group: 224.2.127.254, RP: 171.69.10.13, v1, uptime 4d01h, expires 00:03:42
Group: 224.2.128.253, RP: 171.69.10.13, v1, uptime 12:06:25, expires 00:04:17
Group: 224.2.182.251, RP: 171.69.10.13, v1, uptime 3d10h, expires 00:03:16
```

The following is sample output of the **show ip pim rp** command when **mapping** is specified:

```
Router # show ip pim rp mapping

PIM Group-to-RP Mappings
This system is an RP
This system is an RP-mapping agent

Group(s) 224.0.1.39/32, uptime: 1w4d, expires: never
  RP 171.69.10.13 (sj-eng-mbone.cisco.com)
  Info source: local
Group(s) 224.0.1.40/32, uptime: 1w4d, expires: never
  RP 171.69.10.13 (sj-eng-mbone.cisco.com)
  Info source: local
Group(s) 239.255.0.0/16, uptime: 1d03h, expires: 00:02:28
  RP 171.69.143.25 (lwei-cisco-isdn.cisco.com), PIMv2 v1
  Info source: 171.69.143.25 (lwei-cisco-isdn.cisco.com)
Group(s): 224.0.0.0/4, Static
  RP: 171.69.10.13 (sj-eng-mbone.cisco.com)
```

Table 81 describes the fields in the displays.

Table 81 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.
v1	Indicates the RP is running PIM Version 1.
uptime	Length of time the RP has been up in days and hours. If less than 1 day, time is expressed in hours:minutes:seconds.
expires	Time in hours:minutes:seconds in which the entry will expire.
Info source	RP mapping agent that advertised the mapping.

show ip pim vc

To display ATM virtual circuit status information for multipoint VCs opened by PIM, use the **show ip pim vc EXEC** command.

```
show ip pim vc [group-or-name] [type number]
```

Syntax Description

group-or-name (Optional) IP multicast group or name. Displays only the single group.

type number (Optional) Interface type and number. Displays only the single ATM interface.

Default

Displays VC status information for all ATM interfaces.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

Sample Display

The following is sample output for 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 82 describes the significant fields in the display.

Table 82 Show IP PIM VC Field Descriptions

Field	Description
ATM0/0	ATM slot and port number on the interface.
VC count	Number of virtual circuits opened by PIM.
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.

Table 82 Show IP PIM VC Field Descriptions (Continued)

Field	Description
Leaf Count	Number of routers that have joined the group and are a member of that multipoint virtual circuit.
Rate	Rate in packets per second as configured by the ip pim minimum-vc-rate command.

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip pim multipoint-signalling

show ip rpf

To display how IP multicast routing does Reverse-Path Forwarding (RPF), use the **show ip rpf EXEC** command.

show ip rpf *source-address-or-name*

Syntax Description

source-address-or-name Source name or address of the host for which the RPF information is displayed.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.0.

The router can Reverse-Path Forward from multiple routing tables (that is, the unicast routing table, DVMRP routing table, or static mroutes). This command tells you where the information is retrieved from.

Sample Display

The following is sample output of the **show ip rpf** command:

```
Router # show ip rpf 171.69.10.13

RPF information for sj-eng-mbone.cisco.com (171.69.10.13)
RPF interface: BRI0
RPF neighbor: eng-isdn-pri3.cisco.com (171.69.121.10)
RPF route/mask: 171.69.0.0/255.255.0.0
RPF type: unicast
```

Table 83 describes the significant fields in the display.

Table 83 Show IP RPF Field Descriptions

Field	Description
RPF information for <i>name (address)</i>	Host name and address that this information concerns.
RPF interface	For the given source, interface from which router expects to get packets.
RPF neighbor	For given source, neighbor from which router expects to get 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, DVMRP, or static mroute.

show ip rtp header-compression

To show RTP header compression statistics, use the **show ip rtp header-compression EXEC** command.

show ip rtp header-compression [*type number*] [**detail**]

Syntax Description

type number (Optional) Interface type and number.

detail (Optional) Displays details of each connection.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.3.

Sample Display

The following is sample output from the **show ip rtp header-compression** command:

```
Router# show ip rtp header-compression

RTP/UDP/IP header compression statistics:
Interface Serial1:
  Rcvd: 0 total, 0 compressed, 0 errors
      0 dropped, 0 buffer copies, 0 buffer failures
  Sent: 430 total 429 compressed,
      15122 bytes saved, 139318 bytes sent
      1.10 efficiency improvement factor
  Connect: 16 rx slots, 16 tx slots, 1 long searches, 1 misses
      99% hit ratio, five minute miss rate 0 misses/sec, 0 max.
```

Table 84 describes the significant fields in the display.

Table 84 Show IP RTP Header-Compression Field Descriptions

Field	Description
Interface Serial1	Type and number of interface.
Rcvd: total	Number of packets received on the interface.
compressed	Number of packets with compressed header.
errors	Number of errors.
dropped	Number of dropped packets.
buffer copies,	Number of buffers that had to be copied.
buffer failures	Number of failures in allocating buffers.
Sent: total	Total number of packets sent.
compressed	Number of packets sent with compressed header.

Table 84 Show IP RTP Header-Compression Field Descriptions (Continued)

Field	Description
bytes saved	Total savings in bytes due to compression.
bytes sent	Total bytes sent after compression.
efficiency improvement factor	Compression efficiency.
Connect: rx slots	Total number of receive slots.
tx slots	Total number of transmit slots.
long searches	Searches that needed more than one lookup.
misses	Number of new states that were created.
hit ratio	Number of times existing states were revised.
five minute miss rate	Average miss rate.
max.	Maximum miss rate.

Related Commands

You can use the master indexes or search online to find documentation of related commands.

ip rtp header-compression

show ip sdr

To display the session directory cache, use the **show ip sdr** EXEC command.

```
show ip sdr [group | "session-name" | detail]
```

Syntax Description

<i>group</i>	(Optional) Displays the sessions defining the multicast group in detail format.
" <i>session-name</i> "	(Optional) Displays the single session in detail format. The session name is enclosed in quotation marks ("").
detail	(Optional) Displays all sessions in detail format.

Command Mode

EXEC

Usage Guidelines

This command first appeared in Cisco IOS Release 11.1.

If the router is configured to be a member of 224.2.127.254 (the default sd group), it will cache sdr announcements.

If no arguments or keywords are used with this command, the system displays a sorted list of session names.

Sample Display

The following is sample output of the **show ip sdr** command:

```
Router # show ip sdr

SDR Cache - 198 entries
!Cannes Film Festival
Alan Kay: Georgia Tech Distinguished Lecture
ANL TelePresence Microscopy Collabratory
ASC MSRC Ribbon Cutting Ceremony
audio test
Basler Fasnacht 1997 !
BayLISA meeting
Bellcore testing
Bellcore testing2
Bielsko-Biala
calren2 - private
Cannes Testing
Cbay session
CERN ATLAS
CERN LEPC meeting
CERN LHCC
CILEA pre-test for Archaeonet
cisco Beta
cisco PIM users
CMU
CMU-UKA
CRAY T3E (Course)
```

Table 85 describes the fields in the display.

Table 85 Show IP SDR Field Descriptions

Field	Description
SDR Cache - <i>x</i> entries	Number of entries (sessions) in the cache.
!Cannes Film Festival	Name of session.

Related Commands

You can use the master indexes or search online to find documentation of related commands.

- clear ip sdr**
- ip sdr cache-timeout**
- ip sdr listen**