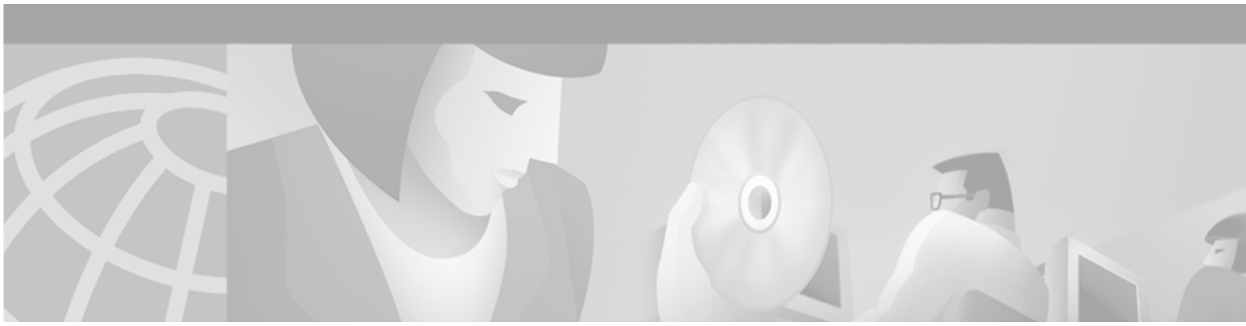

IP Multicast Routing Commands

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 *Cisco IOS IP Configuration Guide*.

clear ip cgmp

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

clear ip cgmp [*type number*]

Syntax Description

type number	(Optional) Interface type and number.

Command Modes

EXEC

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

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

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

Examples

The following example clears the CGMP cache:

```
Router# clear ip cgmp
```

Related Commands

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

clear ip dvmrp route

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

clear ip dvmrp route {* | *route*}

Syntax Description

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

Command Modes

EXEC

Command History

Release	Modification
11.0	This command was introduced.

Examples

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

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

clear ip igmp group

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

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

Syntax Description

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

Defaults

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

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

clear ip mroute

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

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

Syntax Description

*	Deletes all entries from the IP multicast routing table.
group-name	Name of the multicast group, as defined in the Domain Name System (DNS) hosts table or with the **ip host** command.
group-address	IP address of the multicast group. This is a multicast IP address in four-part, dotted notation.
source-name | *source-address*	(Optional) If you specify a group name or address, you can also specify a name or address of a multicast source that is sending to the group. A source need not be a member of the group.

Command Modes

EXEC

Command History

Release	Modification
10.0	This command was introduced.

Examples

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

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

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

```
Router# clear ip mroute 224.2.205.42 10.3.0.0
```

Related Commands

Command	Description
ip host	Defines a static host name-to-address mapping in the host cache.
show ip mroute	Displays the contents of the IP multicast routing table.

clear ip pim auto-rp

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

clear ip pim rp-mapping

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3	This command was introduced.
12.1	The **clear ip pim auto-rp** command was deprecated and replaced by the **clear ip pim rp-mapping** command.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

clear ip rtp header-compression

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

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

Syntax Description

type number	(Optional) Interface type and number.

Command Modes

EXEC

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

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

Examples

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

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

Related Commands

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

clear ip sap

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

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

Syntax Description

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

Command Modes

EXEC

Command History

Release	Modification
11.1	The **clear ip sdr** command was introduced.
12.2	The **clear ip sdr** command was replaced by the **clear ip sap** command.

Usage Guidelines

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

Examples

The following example clears the SAP cache:

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

Related Commands

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

clear ip sdr

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

frame-relay ip rtp compression-connections

To specify the maximum number of Real-Time Transport Protocol (RTP) header compression connections that can exist on a Frame Relay interface, use the **frame-relay ip rtp compression-connections** command in interface configuration mode. To restore the default, use the **no** form of this command.

frame-relay ip rtp compression-connections *number*

no frame-relay ip rtp compression-connections

Syntax Description

number	Maximum number of RTP header compression connections. The range is from 3 to 256.

Defaults

No default behavior or values.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

Before you can configure the maximum number of connections, RTP header compression must be configured on the interface using the **frame-relay ip rtp header-compression** command.

The number of RTP header compression connections must be set to the same value at each end of the connection.

Examples

The following example shows the configuration of a maximum of 150 RTP header compression connections on serial interface 0:

```
interface serial 0
 encapsulation frame-relay
 frame-relay ip rtp header-compression
 frame-relay ip rtp compression-connections 150
```

Related Commands

Command	Description
frame-relay ip rtp header-compression	Enables RTP header compression for all Frame Relay maps on a physical interface.
frame-relay map ip compress	Enables both RTP and TCP header compression on a link.
frame-relay map ip rtp header-compression	Enables RTP header compression per DLCI.
show frame-relay ip rtp header-compression	Displays RTP header compression statistics for Frame Relay.

frame-relay ip rtp header-compression

To enable Real-Time Transport Protocol (RTP) header compression for all Frame Relay maps on a physical interface, use the **frame-relay ip rtp header-compression** command in interface configuration mode. To disable the compression, 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/User Datagram Protocol (UDP)/IP header only if an incoming packet had a compressed header.

Defaults

Disabled.

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

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

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.

Examples

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

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

Related Commands

Command	Description
frame-relay ip rtp compression-connections	Specifies maximum number of RTP header compression connections on a Frame Relay interface.
frame-relay map ip nocompress	Disables both RTP and TCP header compression on a link.
show frame-relay ip rtp header-compression	Displays RTP header compression statistics for Frame Relay.

frame-relay map ip compress

To enable both Real-Time Transport Protocol (RTP) and TCP header compression on a link, use the **frame-relay map ip compress** command in interface configuration mode.

frame-relay map ip *ip-address dlci* [**broadcast**] **compress** [**active** | **passive**]
[**connections** *number*]

Syntax Description

ip-address	IP address of the destination or next hop.
dlci	Data-link connection identifier (DLCI) number.
broadcast	(Optional) Forwards broadcasts to the specified IP address.
active	(Optional) Compresses all outgoing RTP and TCP packets. This is the default.
passive	(Optional) Compresses the outgoing RTP and TCP header only if an incoming packet had a compressed header.
connections *number*	(Optional) Specifies the maximum number of RTP and TCP header compression connections. The range is from 3 to 256.

Defaults

Disabled.

The default maximum number of header compression connections is 256.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.1(2)T	This command was modified to enable the configuration of the maximum number of header compression connections.

Examples

The following example enables both RTP and TCP header compression on serial interface 1 and sets the maximum number of RTP and TCP header connections at 16:

```
interface serial 1
 encapsulation frame-relay
 ip address 10.108.175.110 255.255.255.0
 frame-relay map ip 10.108.175.220 180 compress connections 16
```

Related Commands

Command	Description
frame-relay ip rtp compression-connections	Specifies the maximum number of RTP header compression connections on a Frame Relay interface.
frame-relay ip tcp header-compression	Enables TCP header compression for all Frame Relay maps on a physical interface.
frame-relay map ip nocompress	Disables both RTP and TCP header compression on a link.
frame-relay map ip rtp header-compression	Enables RTP header compression for all Frame Relay maps on a physical interface.
show frame-relay ip rtp header-compression	Displays RTP header compression statistics for Frame Relay.
show frame-relay ip tcp header-compression	Displays statistics and TCP/IP header compression information for the interface.

frame-relay map ip nocompress

To disable both Real-Time Transport Protocol (RTP) and TCP header compression on a link, use the **frame-relay map ip nocompress** command in interface configuration mode.

frame-relay map ip *ip-address dlci* [**broadcast**] **nocompress**

Syntax Description

ip-address	IP address of the destination or next hop.
dlci	Data-link connection identifier (DLCI) number.
broadcast	(Optional) Forwards broadcasts to the specified IP address.

Defaults

No default behaviors or values.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Examples

The following example disables RTP and TCP header compression on DLCI 180:

```
interface serial 1
 encapsulation frame-relay
 frame-relay map ip 10.108.175.220 180 nocompress
```

Related Commands

Command	Description
frame-relay ip rtp header-compression	Enables RTP header compression for all Frame Relay maps on a physical interface.
frame-relay ip tcp header-compression	Enables TCP header compression for all Frame Relay maps on a physical interface.
frame-relay map ip compress	Enables RTP and TCP header compression on a link.
show frame-relay ip rtp header-compression	Displays RTP header compression statistics for Frame Relay.
show frame-relay ip tcp header-compression	Displays statistics and TCP/IP header compression information for the interface.

frame-relay map ip rtp header-compression

To enable Real-Time Transport Protocol (RTP) header compression per data-link connection identifier (DLCI), use the **frame-relay map ip rtp header-compression** command in interface configuration mode.

frame-relay map ip *ip-address dlci* [**broadcast**] **rtp header-compression** [**active** | **passive**] [**connections** *number*]

Syntax Description

ip-address	IP address of the destination or next hop.
dlci	DLCI number.
broadcast	(Optional) Forwards broadcasts to the specified IP address.
active	(Optional) Compresses 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.
connections *number*	(Optional) Specifies the maximum number of RTP header compression connections. The range is from 3 to 256.

Defaults

Disabled.

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

The default maximum number of header compression connections is 256.

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.
12.1(2)T	This command was modified to enable the configuration of the maximum number of header compression connections.

Usage Guidelines

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. If you do not specify the number of RTP header compression connections, the map will inherit the current value from the interface.

Examples

The following example enables RTP header compression on serial interface 1 and sets the maximum number of RTP header compression connections at 64:

```
interface serial 1
 encapsulation frame-relay
 ip address 10.108.175.110 255.255.255.0
 frame-relay map ip 10.108.175.220 180 rtp header-compression connections 64
```

Related Commands

Command	Description
frame-relay ip rtp compression-connections	Specifies the maximum number of RTP header compression connections on a Frame Relay interface.
frame-relay ip rtp header-compression	Enables RTP header compression for all Frame Relay maps on a physical interface.
frame-relay map ip compress	Enables both RTP and TCP header compression on a link.
show frame-relay ip rtp header-compression	Displays RTP header compression statistics for Frame Relay.

ip cgmp

To enable Cisco Group Management Protocol (CGMP) on an interface of a router connected to a Cisco Catalyst 5000 family switch, use the **ip cgmp** command in interface configuration mode. To disable CGMP routing, use the **no** form of this command.

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

no ip cgmp

Syntax Description

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

Defaults

CGMP is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2	The **router-only** keyword was added.

Usage Guidelines

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

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

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

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

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

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

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

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

Examples

The following example enables CGMP:

```
ip cgmp
```

The following example enables CGMP and CGMP proxy:

```
ip cgmp proxy
```

ip dvmrp accept-filter

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

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

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

Syntax Description

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

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2	The **neighbor-list** keyword and *access-list-number* argument were added.

Usage Guidelines

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

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

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

Examples

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

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

The following example 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

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

ip dvmrp auto-summary

To enable Distance Vector Multicast Routing Protocol (DVMRP) automatic summarization if it was disabled, use the **ip dvmrp auto-summary** command in interface configuration mode. To disable 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.

Defaults

Enabled

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

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

Disable this 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 automatic-summarization.

Examples

The following example disables DVMRP automatic summarization:

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

Related Commands

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

ip dvmrp default-information

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

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

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

Syntax Description

originate	Other routes more specific than 0.0.0.0 may be advertised.
only	No DVMRP routes other than 0.0.0.0 are advertised.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

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

You can use the **ip 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.

Examples

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

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

ip dvmrp metric

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

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

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

Syntax Description

metric	Metric associated with a set of destinations for DVMRP reports. It can be a value from 0 to 32. A value of 0 means that the route is not advertised. A value of 32 is equivalent to infinity (unreachable).
list *access-list*	(Optional) Number name 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.
route-map *map-name*	(Optional) Name of the route map. Only the destinations that match the route map are reported with the configured metric. Unicast routes are subject to route map conditions before being injected into DVMRP. Route maps cannot be used for DVMRP routes.
mbgp	(Optional) Configures redistribution of only IP version 4 (IPv4) multicast routes into DVMRP.
protocol	(Optional) Name of unicast routing protocol, such as **bgp**, **eigrp**, **igrp**, **isis**, **ospf**, **rip**, **static**, or **dvmrp**. If you specify these arguments, only routes learned by the specified routing protocol are advertised in DVMRP report messages.
process-id	(Optional) Process ID number of the unicast routing protocol.

Defaults

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

Command Modes

Interface configuration

Command History

Release	Modification
10.2	This command was introduced.
11.1	The **route-map** keyword was added.
12.1	The **mbgp** keyword was added.

Usage Guidelines

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

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

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

Examples

The following example 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
```

The following example redistributes IPv4 multicast routes into DVMRP neighbors with a metric of 1:

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

Related Commands

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

ip dvmrp metric-offset

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

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

no ip dvmrp metric-offset

Syntax Description

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

Defaults

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

The default for **in** is 1.

The default for **out** is 0.

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

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

Examples

The following example adds 10 to the incoming DVMRP reports:

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

ip dvmrp output-report-delay

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

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

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

Syntax Description

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

Defaults

milliseconds: 100 milliseconds

burst: 2 packets

Command Modes

Interface configuration

Command History

Release	Modification
11.3	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

ip dvmrp reject-non-pruners

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

ip dvmrp reject-non-pruners

no ip dvmrp reject-non-pruners

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

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

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

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

Examples

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

ip dvmrp routehog-notification *route-count*

no ip dvmrp routehog-notification

Syntax Description

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

Defaults

10,000 routes

Command Modes

Global configuration

Command History

Release	Modification
10.2	This command was introduced.

Usage Guidelines

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

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

Examples

The following example lowers the threshold to 8000 routes:

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

Related Commands

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

ip dvmrp route-limit

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

ip dvmrp route-limit *count*

no ip dvmrp route-limit

Syntax Description

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

Defaults

7000 routes

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

Related Commands

Command	Description
ip dvmrp unicast-routing	Enables DVMRP unicast routing on an interface.

ip dvmrp summary-address

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

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

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

Syntax Description

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

Defaults

metric *value*: 1

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.

Usage Guidelines

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

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

Multiple summary 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.

Examples

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

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

ip dvmrp unicast-routing

To enable Distance Vector Multicast Routing Protocol (DVMRP) unicast routing on an interface, use the **ip dvmrp unicast-routing** command in interface configuration mode. To disable 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.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.3	This command was introduced.

Usage Guidelines

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

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

Examples

The following example enables DVMRP unicast routing:

```
ip dvmrp unicast-routing
```

Related Commands

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

ip igmp access-group

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

ip igmp access-group *access-list version*

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

Syntax Description

access-list	Number or name of a standard IP access list. The access list can be a number from 1 to 99.
version	Changes Internet Group Management Protocol (IGMP) version. Default is version 2.

Defaults

All groups are allowed on an interface.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Examples

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

Command	Description
ip igmp join-group	Causes the router to join a multicast group.

ip igmp helper-address

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

ip igmp helper-address *ip-address*

no ip igmp helper-address

Syntax Description

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

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
11.2 F	This command was introduced.

Usage Guidelines

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

Examples

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

Router A Configuration

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

Router B Configuration

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

Related Commands

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

ip igmp immediate-leave

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

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

no ip igmp immediate-leave

Syntax Description

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

Defaults

Disabled

Command Modes

Global configuration
Interface configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

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

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

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

Global Configuration Mode

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

Interface Configuration Mode

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

Examples

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

```
ip multicast-routing
igmp immediate-leave group-list all-groups

interface ethernet 0
  ip address 10.0.10.1 255.255.255.0
  ip pim sparse-dense mode

 ip access-list standard all-groups
permit 224.0.0.0 15.255.255.255
```

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

```
ip multicast-routing

interface ethernet 0
  ip address 10.0.10.1 255.255.255.0
  ip pim sparse-dense-mode
  igmp immediate-leave group-list tv-groups

 ip access-list standard tv-groups
permit 239.192.20.0 0.0.0.255
```

Related Commands

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

ip igmp join-group

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

ip igmp join-group *group-address*

no ip igmp join-group *group-address*

Syntax Description

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

Defaults

No multicast group memberships are predefined.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Usage Guidelines

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, which 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 Interior Gateway Routing Protocol (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.

Examples

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

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

Related Commands

Command	Description
ip igmp access-group	Controls the multicast groups that hosts on the subnet serviced by an interface can join.
ping (privileged)	Diagnoses basic network connectivity (in privileged EXEC mode) on Apollo, AppleTalk, CLNS, DECnet, IP, Novell IPX, VINES, or XNS networks.
ping (user)	Diagnoses basic network connectivity (in user EXEC mode) on Apollo, AppleTalk, CLNS, DECnet, IP, Novell IPX, VINES, or XNS networks.

ip igmp last-member-query-count

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

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

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

Syntax Description

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

Defaults

LMQC is 2

Command Modes

Interface configuration

Command History

Release	Modification
12.1	This command was introduced.

Usage Guidelines

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

Caution

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

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

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

Examples

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

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

Related Commands

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

ip igmp last-member-query-interval

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

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

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

Syntax Description

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

Defaults

interval: 1000 milliseconds (1 second)

Command Modes

Interface configuration

Command History

Release	Modification
12.1	This command was introduced.
12.2(4)T	The highest *interval* integer value accepted was changed from 65,535 to 25,500.

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

ip igmp querier-timeout

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

ip igmp querier-timeout *seconds*

no ip igmp querier-timeout

Syntax Description

seconds	Number of seconds that the router waits after the previous querier has stopped querying and before it takes over as the querier. The range is from 30 to 300 seconds.

Command Default

The default timeout period is two times the query interval. The default query interval is 120 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command requires IGMP Version 2 (or higher).

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 60 seconds, which means the **ip igmp querier-timeout** defaults to 120 seconds.

Examples

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

```
ip igmp querier-timeout 30
```

Related Commands

Command	Description
ip igmp query-interval	Configures the frequency at which Cisco IOS software sends IGMP host query messages.

ip igmp query-interval

To configure the frequency at which Cisco IOS software sends Internet Group Management Protocol (IGMP) host query messages, use the **ip igmp query-interval** command in interface configuration mode. 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 send IGMP host query messages. It can be a number from 0 to 65535. The default is 60 seconds.

Defaults

60 seconds

Command Modes

Interface configuration

Command History

Release	Modification
10.2	This command was introduced.

Usage Guidelines

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

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

- For IGMP Version 1, 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.

Caution Changing this value may severely impact multicast forwarding.

Examples

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

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

ip igmp query-max-response-time

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

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

no ip igmp query-max-response-time

Syntax Description

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

Defaults

10 seconds

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ip igmp static-group

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

ip igmp static-group {* | *group-address* [**source** {*source-address* | **ssm-map**}]}

no ip igmp static-group {* | *group-address* [**source** {*source-address* | **ssm-map**}]}

Syntax Description

*	Places the interface into all newly created multicast route (mroute) entries.
group-address	IP multicast group address of a group to which the router belongs.
source	(Optional) Statically forwards a (S, G) channel out of the interface.
source-address	(Optional) IP address of a system where multicast data packets originate.
ssm-map	(Optional) Configures Source Specific Multicast (SSM) mapping to be used to determine the source associated with this group. The resulting (S, G) channels are statically forwarded.

Defaults

A router is not a statically connected member of an IP multicast group.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.3(2)T	The **source** and the **ssm-map** keywords were added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

When you configure the **ip igmp static-group** command, packets to the group are fast-switched out the interface, provided that packets were received on the correct reverse path forwarding (RPF) interface.

Configuring the **ip igmp static-group** command is unlike configuring the **ip igmp join-group** command, which allows the router to join the multicast group. This configuration of the **ip igmp static-group** command would cause the upstream routers to maintain the multicast routing table information for that group, which would ensure that all the paths to that multicast group are active.

If you configure the **ip igmp join-group** command for the same group address as the **ip igmp static-group** command, the **ip igmp join-group** command takes precedence, and the group behaves like a locally joined group.

The use of SSM mapping determines the source or sources associated with a specific source (S) and group (G) combination and puts the particular interface in the outging interface list (OIL) for that (S, G) entry. Traffic coming from source S destined toward group G will be forwarded out that interface regardless of a receiver joining the group on that interface.

Examples

The following example configures group address 192.168.2.2 on Ethernet interface 0:

```
interface ethernet 0
 ip igmp static-group 192.168.2.2
```

The following example shows how to configure group address 192.168.2.3 to use SSM mapping for statically forwarded groups on Ethernet interface 0:

```
interface ethernet 0
 ip igmp static-group 192.168.2.3 source ssm-map
```

Related Commands

Command	Description
ip igmp join-group	Causes the router to join a multicast group.
ip igmp ssm-map enable	Enables SSM mapping for groups in a configured SSM range.
ip igmp ssm-map query dns	Configures DNS-based SSM mapping.
ip igmp ssm-map static	Enables static SSM mapping.
ip pim ssm	Defines the SSM range of IP multicast addresses.

ip igmp v3lite

To enable acceptance and processing of Internet Group Management Protocol Version 3 lite (IGMP v3lite) membership reports on an interface, use the **ip igmp v3lite** command in interface configuration mode. To disable IGMP v3lite, use the **no** form of this command.

ip igmp v3lite

no ip igmp v3lite

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.

Usage Guidelines

To use this command, you must define a Source Specific Multicast (SSM) range of IP addresses using the **ip pim ssm** global configuration command. When IGMP v3lite is enabled, it is supported in the SSM range of addresses only.

Examples

The following example shows how to configure IGMP v3lite on Ethernet interface 3/1:

```
interface ethernet 3/1
ip igmp v3lite
```

Related Commands

Command	Description
ip pim ssm	Defines the SSM range of IP multicast addresses.

ip igmp version

To configure which version of Internet Group Management Protocol (IGMP) the router uses, use the **ip igmp version** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ip igmp version {**1** | **2** | **3**}

no ip igmp version

Syntax Description

1	IGMP Version 1.
2	IGMP Version 2.
3	IGMP Version 3.

Defaults

Version 2

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.1(5)T	The **3** keyword was added.

Usage Guidelines

All routers on the subnet must support the same version. The router does not automatically detect Version 1 routers and switch to Version 1 as did earlier releases of the Cisco IOS software. Hosts can have any IGMP version (1, 2, or 3) and the router will correctly detect their presence and query them appropriately.

Some commands require IGMP Version 2 or 3, such as the **ip igmp query-max-response-time** and **ip igmp query-timeout** commands.

Examples

The following example configures the router to use IGMP Version 3:

```
ip igmp version 3
```

Related Commands

Command	Description
ip igmp query-max-response-time	Configures the maximum response time advertised in IGMP queries.
ip igmp static-group	Configures the timeout time before the router takes over as the querier for the interface, after the previous querier has stopped querying.
show ip igmp groups	Displays the multicast groups that are directly connected to the router and that were learned through IGMP.
show ip igmp interface	Displays multicast-related information about an interface.

ip mroute

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

ip mroute *source-address mask* [*protocol as-number*] {*rpf-address* | *type number*} [*distance*]

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

Syntax Description

source-address	IP address of the multicast source.
mask	Mask on the IP address of the multicast source.
protocol	(Optional) Unicast routing protocol that you are using.
as-number	(Optional) Autonomous system number of the routing protocol you are using, if applicable.
rpf-address	Incoming interface for the mroute. If the Reverse Path Forwarding (RPF) address *rpf-address* is a Protocol Independent Multicast (PIM) neighbor, PIM join, graft, and prune messages are sent to it. The *rpf-address* argument 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 the *rpf-address* argument is not specified, the interface *type number* value is used as the incoming interface.
type number	Interface type and number for the mroute.
distance	(Optional) Determines whether a unicast route, a Distance Vector Multicast Routing Protocol (DVMRP) route, or a static mroute should be used for the RPF lookup. The lower distances have better preference. If the static mroute has the same distance as the other two RPF sources, the static mroute will take precedence. The default is 0.

Defaults

distance: 0

Command Modes

Global configuration

Command History

Release	Modification
11.0	This command was introduced.

Usage Guidelines

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

When a source range is specified, the *rpf-address* argument 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 0.0.0.0 tunnel0
```

The following example configures all specific sources within a network number to be reachable through 172.30.10.13:

```
ip mroute 172.16.0.0 255.255.0.0 172.30.10.13
```

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 0.0.0.0 serial0 200
```

ip mroute-cache

To configure IP multicast fast switching or multicast distributed switching (MDS), use the **ip mroute-cache** command in interface configuration mode. To disable either of these features, use the **no** form of this command.

ip mroute-cache [**distributed**]

no ip mroute-cache [**distributed**]

Syntax Description

distributed	(Optional) Enables MDS on the interface. In the case of RSP, this keyword is optional; if it is omitted, fast switching occurs. On the GSR, this keyword is required because the GSR does only distributed switching.

Defaults

On the RSP, IP multicast fast switching is enabled; MDS is disabled.

On the GSR, MDS is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.
11.2(11)GS	The **distributed** keyword was added.

Usage Guidelines

On the RSP

If multicast 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 multicast fast switching is disabled on an outgoing interface for a multicast routing table entry, the packet is process-level switched for that interface, but may be fast switched for other interfaces in the outgoing interface list.

When multicast fast switching is enabled (like unicast routing), debug messages are not logged. If you want to log debug messages, disable fast switching.

If MDS is not enabled on an incoming interface that is capable of MDS, incoming multicast packets will not be distributed switched; they will be fast switched at the Route Processor (RP) as before. Also, if the incoming interface is not capable of MDS, packets will get fast switched or process-switched at the RP as before.

If MDS is enabled on the incoming interface, but at least one of the outgoing interfaces cannot fast switch, packets will be process-switched. We recommend that you disable fast switching on any interface when MDS is enabled.

On the GSR

On the GSR, all interfaces should be configured for MDS because that is the only switching mode.

Examples

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

```
ip mroute-cache
```

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

```
no ip mroute-cache
```

The following example enables MDS on the interface:

```
ip mroute-cache distributed
```

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

```
no ip mroute-cache distributed
```

ip msdp cache-rejected-sa

To track rejected Source-Active (SA) request messages from a Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp cache-rejected-sa** command in global configuration mode. To stop tracking SA request messages, use the **no** form of this command.

ip msdp cache-rejected-sa *number-of-entries*

no ip msdp cache-rejected-sa *number-of-entries*

Syntax Description

number-of-entries	Number of entries that need to be cached. The range is from 1 to 32766.

Defaults

Rejected SA request messages are not tracked.

Command Modes

Global configuration

Command History

Release	Modification
12.0(22)S	This command was introduced.
12.1E	This command was integrated into Cisco IOS Release 12.1E.
12.2	This command was integrated into Cisco IOS Release 12.2.

Usage Guidelines

The **ip msdp cache-rejected-sa** command displays the history of SA messages that have been recently received from an MSDP peer but were rejected by the local router. If the cache overflows, entries are overwritten, starting from the first entry.

Examples

The following example enables the MSDP peer to track rejected MSDP SA request messages:

```
Router(config)# ip msdp cache-rejected-sa 200
```

Related Commands

Command	Description
show snmp engineID	Displays the identification of the local SNMP engine and all remote engines that have been configured on the router.
snmp-server host	Specifies the recipient (SNMP manager) of an SNMP trap notification.

ip multicast boundary

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

ip multicast boundary *access-list* [**filter-autorp**]

no ip multicast boundary [**filter-autorp**]

Syntax Description

access-list	Number or name identifying an access list that controls the range of group addresses affected by the boundary.
filter-autorp	(Optional) Filters Auto-RP messages denied by the boundary access control list (ACL).

Defaults

There is no boundary.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.0(22)S	The **filter-autorp** keyword was added.
12.1(12c)E	The **filter-autorp** keyword was integrated into Cisco IOS Release 12.1(12c)E.
12.2(11)	The **filter-autorp** keyword was integrated into Cisco IOS Release 12.2(11).
12.2(13)T	The **filter-autorp** keyword was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Use this command to configure an administratively scoped boundary on an interface to filter multicast group addresses in the range defined by the *access-list* argument. A standard access list defines the range of addresses affected. When this command is configured, no multicast data packets are allowed to flow across the boundary from either direction. Restricting multicast data packet flow enables reuse of the same multicast group address in different administrative domains.

If you configure the **filter-autorp** keyword, the administratively scoped boundary also examines Auto-RP discovery and announcement messages and removes any Auto-RP group range announcements from the Auto-RP packets that are denied by the boundary ACL. An Auto-RP group range announcement is permitted and passed by the boundary only if all addresses in the Auto-RP group range are permitted by the boundary ACL. If any address is not permitted, the entire group range is filtered and removed from the Auto-RP message before the Auto-RP message is forwarded.

Examples

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

Command	Description
access-list (IP standard)	Defines a standard IP access list.