beacon multicast routing monitor through ip dvmrp unicast-routing

beacon (multicast routing monitor)

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

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

Syntax Description

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

Command Default

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

Command Modes

MRM manager configuration (config-mrm-manager)

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

class-map type multicast-flows

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

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

Syntax Description

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

Command Default

No IGMP static group class maps are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXF5	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

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

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

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

- **group** *group-address*

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

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

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

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

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

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

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

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

Additional Guidelines for Configuring IGMP Static Group Class Maps

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

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

Examples

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

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

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

```
group 192.0.2.0 source 192.0.2.10
```

Related Commands

Command	Description
group (multicast-flows)	Defines the group entries to be associated with an IGMP static group class map.
ip igmp static-group	Configures static group membership entries on an interface.

Command	Description
show ip igmp static-group class-map	Displays the contents of IGMP static group class map configurations and the interfaces using class maps.

clear ip cgmp

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

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

Examples

The following example clears the CGMP cache:

```
Router# clear ip cgmp
```

Related Commands

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

clear ip dvmrp route

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

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

clear ip dvmrp route ***** *route*

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

clear ip igmp group

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

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

Cisco 7600 Series
clear ip igmp [**vrf** *vrf-name*] **group** [*interface interface-numbergroup-namegroup-address*] [**loopback** *interface-number* | **null** *interface-number* | **port-channel** *number* | **vlan** *vlan-id*]

Command Default

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

Command Default

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

Command Modes

Privileged EXEC

Command History

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

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

Usage Guidelines

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

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

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

Examples

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

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

Cisco 7600 Series

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

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

Related Commands

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

clear ip igmp snooping filter statistics

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

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

Syntax Description

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

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

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

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

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

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

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

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

Related Commands

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

clear ip igmp snooping statistics

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

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

Syntax Description

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

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

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

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

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

Related Commands

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

clear ip mfib counters

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

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

Syntax Description

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

Command Default

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

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

clear ip mrm status-report

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

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

Syntax Description

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

Command Default

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

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

clear ip mroute

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

clear ip mroute[**vrf** *vrf-name*][***group*[*source*]]

Syntax Description

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

Command Default

This command has no default settings

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

The *group* argument specifies one of the following:

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

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

Examples

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

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

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

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

Related Commands

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

clear ip msdp peer

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

clear ip msdp[**vrf** *vrf-name*]**peer***peer-addresspeer-name*

Syntax Description

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

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

Command	Description
ip msdp peer	Configures an MSDP peer.

clear ip msdp sa-cache

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

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

Syntax Description

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

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

Command	Description
ip host	Configures an MSDP peer.
ip msdp cache-sa-state	Enables the router to create SA state.

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

clear ip msdp statistics

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

clear ip msdp[**vrf** *vrf-name*]**statistics***peer-addresspeer-name*

Syntax Description

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

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

Related Commands

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

clear ip multicast limit

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

clear ip multicast limit [*type number*]

Syntax Description

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

Command Default

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

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

Command	Description
ip multicast limit cost	Applies costs to per interface mroute state limiters.
show ip multicast limit	Displays statistics about configured per interface mroute state limiters.

clear ip multicast redundancy statistics

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

clear ip multicast redundancy statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

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

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

Related Commands

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

clear ip pgm host

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

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

clear ip pgm host defaults | **traffic**

Syntax Description

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

Command Default

No default behavior or values

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

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

The following example clears all PGM Host traffic statistics:

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

Related Commands

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

Command	Description
show ip pgm host traffic	Displays PGM Host traffic statistics.

clear ip pgm router

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

clear ip pim auto-rp

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

clear ip pim interface count

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

clear ip pim interface count

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

clear ip pim rp-mapping

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

clear ip pim snooping statistics

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

clear ip pim snooping statistics

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Examples

This example shows how to clear the IP PIM statistics:

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

Related Commands

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

clear ip pim snooping vlan

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

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

Syntax Description

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

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

Related Commands

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

clear ip rtp header-compression

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

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

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

Related Commands

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

clear ip sap

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

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

Syntax Description

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

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

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

Examples

The following example clears the SAP cache:

```
Router# clear ip sap “Sample Session”
```

Related Commands

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

clear ip sdr

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

clear mls ip multicast bidir-rpcache

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

clear mls ip multicast bidir-rpcache

Syntax Description

This command has no keywords or arguments.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Examples

This example shows how to reset the Bidir counters:

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

Related Commands

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

clear mls ip multicast group

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

clear mls ip multicast group *ip-namegroup-address*

Syntax Description

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

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17b)SXA	Support for this command was introduced on the Supervisor Engine 720.
12.2(17b)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 2.2(17b)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to delete an IP multicast group:

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

Related Commands

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

clear mls ip multicast statistics

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

clear mls ip multicast statistics

Syntax Description

This command has no keywords or arguments.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

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

Examples

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

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

Related Commands

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

clear router-guard ip multicast statistics

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

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

Syntax Description

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

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

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

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

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

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

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

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

Related Commands

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

debug condition vrf

To limit debug output to a specific virtual routing and forwarding (VRF) instance, use the **debug condition vrf** command in privileged EXEC mode. To remove the debug condition, use the **no** form of the command.

debug condition vrf **default** | **global** | **green** | **name** *vrf-name* | **green**

no debug condition vrf **default** | **global** | **green** | **name** *vrf-name* | **green**

Syntax Description

Syntax	Description
default	Specifies the default routing table.
global	Specifies the global routing table.
green	Specifies the VRF name.
name *vrf-name*	Specifies the name of the routing table.

Command Modes

Privileged EXEC mode (#)

Command History

Release	Modification
15.1(3)S	This command was introduced.

Usage Guidelines

Use this command to limit debug output to a single VRF.

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use the **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. It is best to use the **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

Example

The following example shows how to limit debugging output to VRF red:

```
Device# debug condition vrf red
```

debug ip pim

To display PIM packets received and transmitted, as well as PIM related events, use the **debug ip pim** command in privileged EXEC mode. To disable the debug output, use the **no** form of the command.

debug ip pim [**vrf** *vrf-name*] [*ip-address* | **atm** | **auto-rp** | **bfd** | **bsr** | **crimson** | **df** *rp-address* | **drlb** | **hello** | **timers**]

no debug ip pim [**vrf** *vrf-name*] [*ip-address* | **atm** | **auto-rp** | **bfd** | **bsr** | **crimson** | **df** *rp-address* | **drlb** | **hello** | **timers**]

Syntax Description

Syntax	Description
vrf *vrf-name*	(Optional) Specifies the VPN Routing and Forwarding instance. This keyword overrides debugging of any VRFs specified in the **debug condition vrf** *vrf-name* command.
ip-address	(Optional) Specifies the IP group address.
atm	(Optional) Displays debugging information about PIM ATM signalling activity.
auto-rp	(Optional) Displays debugging information about Auto-RP information.
bfd	(Optional) Displays debugging information about BFD configuration.
bsr	(Optional) Displays debugging information about PIM Candidate-RP and BSR activity.
crimson	(Optional) Displays debugging information about Crimson database activity.
df *rp-address*	(Optional) Displays debugging information about PIM RP designated forwarder election activity.
drlb	(Optional) Displays debugging information about PIM designated router load-balancing activity.
hello	(Optional) Displays debugging information about PIM Hello packets received and sent.
timers	(Optional) Displays debugging information about PIM timer events.

Command Modes

Privileged EXEC mode (#)

Command History

Release	Modification
15.1(3)S	This command was introduced.

Usage Guidelines

Caution Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use the **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. It is best to use the **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

You can debug a maximum of 8 VRFs in a PIM at a time. To debug multiple VRFs at the same time, perform the following sequence of steps:

```
debug condition vrf vrf-name1
debug condition vrf vrf-name2
.
.
.
debug condition vrf vrf-name8
debug ip pim
```

Example

The following example shows how to display the Crimson database activity:

```
Device# debug ip pim crimson
```

The following example shows how to debug the two VRFs red and green in a PIM at the same time:

```
Device# debug condition vrf red
Device# debug condition vrf green
Device# debug ip pim
```

group (multicast-flows)

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

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

Syntax Description

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

Command Default

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

Command Modes

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

Command History

Release	Modification
12.2(18)SXF5	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.
Cisco IOS XE Release 3.3SG	This command was integrated into Cisco IOS XE Release 3.3SG.

Usage Guidelines

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

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

- **group** *group-address*

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

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

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

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

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

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

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

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

Examples

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

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

Related Commands

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

ip cgmp

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

ip cgmp [**proxy** | **router-only**]
no ip cgmp

Syntax Description

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

Command Default

CGMP is disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

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

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

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

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

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

Examples

The following example enables CGMP:

```
ip cgmp
```

The following example enables CGMP and CGMP proxy:

```
ip cgmp proxy
```

ip domain multicast

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

ip domain multicast *domain-prefix*
no domain multicast *domain-prefix*

Syntax Description

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

Command Default

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

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(18) SXD3	This command was integrated into Cisco IOS Release 12.2(18)SXD3.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.

Usage Guidelines

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

Examples

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

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

Related Commands

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

ip dvmrp accept-filter

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

multicast routing), and if you want to use the PIM path, use the **ip dvmrp accept-filter** command to increase the administrative distance for DVMRP routes.

Examples

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

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

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

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

Related Commands

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

ip dvmrp auto-summary

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

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

ip dvmrp auto-summary
no ip dvmrp auto-summary

Syntax Description

This command has no arguments or keywords.

Command Default

DVMRP automatic summarization is enabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

The following example shows how to disable DVMRP automatic summarization:

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

Related Commands

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

ip dvmrp default-information

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

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

ip dvmrp default-information originate | only
no ip dvmrp default-information originate | only

Syntax Description

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

Command Default

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ip dvmrp interoperability

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

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

Syntax Description

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

Command Default

DVMRP interoperability is disabled by default.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

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

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

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

Examples

The following example shows how to enable DVMRP interoperability:

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

ip dvmrp metric

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

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

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

Syntax Description

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

Command Default

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

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

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

Related Commands

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

ip dvmrp metric-offset

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

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

ip dvmrp metric-offset[**in** | **out**]*increment*
no ip dvmrp metric-offset

Syntax Description

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

Command Default

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

Examples

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

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

ip dvmrp output-report-delay

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

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

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

Syntax Description

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

Command Default

milliseconds : 100 milliseconds *burst*: 2 packets

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

ip dvmrp reject-non-pruners

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

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

ip dvmrp reject-non-pruners
no ip dvmrp reject-non-pruners

Syntax Description

This command has no arguments or keywords.

Command Default

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

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

ip dvmrp routehog-notification

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

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

ip dvmrp routehog-notification *route-count*
no ip dvmrp routehog-notification

Syntax Description

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

Command Default

10,000 routes

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

ip dvmrp route-limit

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

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

ip dvmrp route-limit *count*
no ip dvmrp route-limit

Syntax Description

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

Command Default

count : 7000 routes

Command Modes

Global configuration

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

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

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

ip dvmrp summary-address

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

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

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

Syntax Description

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

Command Default

metric *value* : 1

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

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

Examples

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

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

Related Commands

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

ip dvmrp unicast-routing

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

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

ip dvmrp unicast-routing
no ip dvmrp unicast-routing

Syntax Description

This command has no arguments or keywords.

Command Default

DVMRP unicast routing on an interface is disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

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

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

Examples

The following example shows how to enable DVMRP unicast routing:

```
ip dvmrp unicast-routing
```

Related Commands

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