Review Draft -- Cisco Confidential

Cisco Nexus 6000 Series NX-OS Multicast Routing Command Reference

Cisco NX-OS Release 6.x

First Published: January 2013
Last Modified: 2/20/13

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-27912-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco Nexus 6000 Series NX-OS Multicast Routing Command Reference
© 2013 Cisco Systems, Inc. All rights reserved.

Review Draft -- Cisco Confidential

CONTENTS

Preface xi

Audience xi

Document Conventions xi

Related Documentation xii

Documentation Feedback xiii

Obtaining Documentation and Submitting a Service Request xiii

xiii

Layer 3 Interfaces Commands MCR-1

H Commands MCR-3

hardware profile multicast max-limit MCR-4

I Commands MCR-5

interface ethernet (Layer 3) MCR-6

interface loopback MCR-8

interface port-channel MCR-9

N Commands MCR-11

no switchport MCR-12

IGMP Commands MCR-13

C Commands MCR-15

clear ip igmp event-history MCR-16

clear ip igmp groups MCR-17

clear ip igmp interface statistics MCR-18

clear ip igmp route MCR-19

I Commands MCR-21

ip igmp access-group MCR-22

ip igmp enforce-router-alert MCR-23

ip igmp event-history MCR-24

ip igmp flush-routes MCR-26

ip igmp group-timeout MCR-27

Review Draft -- Cisco Confidential

ip igmp immediate-leave MCR-28
ip igmp join-group MCR-29
ip igmp last-member-query-count MCR-31
ip igmp last-member-query-response-time MCR-32
ip igmp querier-timeout MCR-33
ip igmp query-interval MCR-34
ip igmp query-max-response-time MCR-35
ip igmp query-timeout MCR-36
ip igmp report-link-local-groups MCR-37
ip igmp report-policy MCR-38
ip igmp robustness-variable MCR-39
ip igmp ssm-translate MCR-40
ip igmp startup-query-count MCR-41
ip igmp startup-query-interval MCR-42
ip igmp state-limit MCR-43
ip igmp static-oif MCR-44
ip igmp version MCR-46

Show Commands MCR-47

show ip igmp event-history MCR-48
show ip igmp groups MCR-50
show ip igmp interface MCR-52
show ip igmp local-groups MCR-54
show ip igmp route MCR-55
show running-config igmp MCR-57
show startup-config igmp MCR-58

IGMP Snooping Commands MCR-59

C Commands MCR-61

clear ip igmp snooping event-history MCR-62
clear ip igmp snooping explicit-tracking vlan MCR-63
clear ip igmp snooping statistics vlan MCR-64

H Commands MCR-65

hardware multicast snooping group-limit MCR-66

Review Draft -- Cisco Confidential

I Commands MCR-69

ip igmp snooping (Global) MCR-70

ip igmp snooping (VLAN) MCR-71

ip igmp snooping event-history MCR-72

ip igmp snooping explicit-tracking MCR-74

ip igmp snooping fast-leave MCR-75

ip igmp snooping last-member-query-interval MCR-76

ip igmp snooping link-local-groups-suppression MCR-77

ip igmp snooping mrouter interface MCR-78

ip igmp snooping mrouter vpc-peer-link MCR-79

ip igmp snooping optimise-multicast-flood MCR-80

ip igmp snooping querier MCR-81

ip igmp snooping report-suppression MCR-82

ip igmp snooping static-group MCR-83

ip igmp snooping v3-report-suppression (Global) MCR-85

ip igmp snooping v3-report-suppression (VLAN) MCR-86

Show Commands MCR-87

show forwarding distribution ip igmp snooping MCR-88

show ip igmp snooping MCR-89

show ip igmp snooping event-history MCR-90

show ip igmp snooping explicit-tracking MCR-92

show ip igmp snooping groups MCR-93

show ip igmp snooping mrouter MCR-94

show ip igmp snooping querier MCR-95

show ip igmp snooping statistics MCR-96

MSDP Commands MCR-97

C Commands MCR-99

clear ip msdp event-history MCR-100

clear ip msdp peer MCR-101

clear ip msdp policy statistics sa-policy MCR-102

clear ip msdp route MCR-103

clear ip msdp sa-cache MCR-104

clear ip msdp statistics MCR-105

Review Draft -- Cisco Confidential

F Commands MCR-107

feature msdp MCR-108

I Commands MCR-109

ip msdp description MCR-110

ip msdp event-history MCR-111

ip msdp flush-routes MCR-113

ip msdp group-limit MCR-114

ip msdp keepalive MCR-115

ip msdp mesh-group MCR-116

ip msdp originator-id MCR-117

ip msdp password MCR-118

ip msdp peer MCR-119

ip msdp reconnect-interval MCR-121

ip msdp sa-interval MCR-122

ip msdp sa-limit MCR-123

ip msdp sa-policy in MCR-124

ip msdp sa-policy out MCR-125

ip msdp shutdown MCR-126

R Commands MCR-127

restart msdp MCR-128

Show Commands MCR-129

show ip msdp count MCR-130

show ip msdp event-history MCR-131

show ip msdp mesh-group MCR-132

show ip msdp peer MCR-133

show ip msdp policy statistics sa-policy MCR-134

show ip msdp route MCR-135

show ip msdp rpf MCR-136

show ip msdp sa-cache MCR-137

show ip msdp route MCR-138

show ip msdp sources MCR-139

show ip msdp summary MCR-140

show running-config msdp MCR-141

show startup-config msdp MCR-142

Review Draft -- Cisco Confidential

PIM Commands MCR-143

C Commands MCR-145

clear ip mroute MCR-146

clear ip pim event-history MCR-147

clear ip pim interface statistics MCR-148

clear ip pim policy statistics MCR-149

clear ip pim route MCR-151

clear ip pim statistics MCR-152

clear ip routing multicast event-history MCR-153

clear routing multicast MCR-154

F Commands MCR-157

feature pim MCR-158

H Commands MCR-159

hardware profile multicast max-limit MCR-160

I Commands MCR-161

ip mroute MCR-162

ip pim anycast-rp MCR-164

ip pim auto-rp MCR-165

ip pim auto-rp mapping-agent MCR-166

ip pim auto-rp mapping-agent-policy MCR-168

ip pim auto-rp rp-candidate MCR-169

ip pim auto-rp rp-candidate-policy MCR-171

ip pim bidir-rp-limit MCR-172

ip pim border MCR-174

ip pim bsr bsr-policy MCR-175

ip pim bsr-candidate MCR-176

ip pim bsr forward MCR-178

ip pim bsr listen MCR-179

ip pim bsr rp-candidate-policy MCR-180

ip pim dr-priority MCR-181

ip pim event-history MCR-182

ip pim flush-routes MCR-184

ip pim hello-authentication ah-md5 MCR-185

ip pim hello-interval MCR-187

Review Draft -- Cisco Confidential

ip pim jp-policy MCR-188
ip pim log-neighbor-changes MCR-190
ip pim neighbor-policy MCR-191
ip pim pre-build-spt MCR-192
ip pim register-policy MCR-194
ip pim register-rate-limit MCR-195
ip pim rp-address MCR-196
ip pim rp-candidate MCR-198
ip pim send-rp-announce MCR-200
ip pim send-rp-discovery MCR-202
ip pim sg-expiry-timer MCR-204
ip pim sparse-mode MCR-205
ip pim ssm policy MCR-206
ip pim ssm MCR-207
ip pim state-limit MCR-208
ip pim use-shared-tree-only MCR-210
ip routing multicast event-history MCR-211
ip routing multicast holddown MCR-213
ip routing multicast software-replicate MCR-214

Show Commands MCR-215

show ip mroute MCR-216
show ip mroute summary MCR-217
show ip pim event-history MCR-219
show ip pim group-range MCR-221
show ip pim interface MCR-222
show ip pim neighbor MCR-224
show ip pim oif-list MCR-226
show ip pim policy statistics auto-rp MCR-227
show ip pim policy statistics bsr MCR-228
show ip pim policy statistics jp-policy MCR-229
show ip pim policy statistics neighbor-policy MCR-230
show ip pim policy statistics register-policy MCR-231
show ip pim route MCR-232
show ip pim rp MCR-233
show ip pim rp-hash MCR-234

Review Draft -- Cisco Confidential

show ip pim statistics **MCR-235**
show ip pim vrf **MCR-237**
show ip static-route **MCR-239**
show routing ip multicast event-history **MCR-240**
show routing multicast **MCR-242**
show routing multicast clients **MCR-243**
show running-config pim **MCR-245**
show startup-config pim **MCR-246**

Review Draft -- Cisco Confidential

Preface

This preface describes the audience, organization, and conventions of the *Cisco Nexus 6000 Series NX-OS Multicast Routing Command Reference*. It also provides information on how to obtain related documentation.

This preface includes the following sections:

- Audience, page xi
- This publication is for experienced users who configure and maintain Cisco NX-OS devices., page xi
- Document Conventions, page xi
- Related Documentation, page xii
- Obtaining Documentation and Submitting a Service Request, page xiii

Audience

This publication is for experienced users who configure and maintain Cisco NX-OS devices.

Document Conventions

Command descriptions use these conventions:

Convention	Description
boldface font	Commands and keywords are in boldface.
italic font	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
{x | y | z}	Alternative keywords are grouped in braces and separated by vertical bars.
[x | y | z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.

Review Draft -- Cisco Confidential

Screen examples use these conventions:

`screen font`	Terminal sessions and information that the switch displays are in screen font.
`boldface screen font`	Information you must enter is in boldface screen font.
`italic screen font`	Arguments for which you supply values are in italic screen font.
< >	Nonprinting characters, such as passwords, are in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

This document uses the following conventions:

Note Means reader *take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means reader *be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

Documentation for the Cisco Nexus 6000 Series Switch is available at the following URL:

http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html

The documentation set is divided into the following categories:

Release Notes

The release notes are available at the follwing URL:

http://www.cisco.com/en/US/products/ps11541/prod_release_notes_list.html

Installation and Upgrade Guides

The installation and upgrade guides are available at the following URL:

http://www.cisco.com/en/US/products/ps11541/prod_installation_guides_list.html

Command References

The command references are available at the following URL:

http://www.cisco.com/en/US/products/ps11541/prod_command_reference_list.html

Technical References

The technical references are available at the following URL:

http://www.cisco.com/en/US/products/ps11541/prod_technical_reference_list.html

Review Draft -- Cisco Confidential

Configuration Guides

The configuration guides are available at the following URL:

http://www.cisco.com/en/US/products/ps11541/products_installation_and_configuration_guides_list.html

Error and System Messages

The system message reference guide is available at the following URL:

http://www.cisco.com/en/US/products/ps11541/products_system_message_guides_list.html

Documentation Feedback

To provide technical feedback on this document, or to report an error or omission, please send your comments to nexus6k-docfeedback@cisco.com. We appreciate your feedback.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

Layer 3 Interfaces Commands

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

H Commands

This chapter describes the Cisco NX-OS routing commands that begin with H.

Review Draft -- Cisco Confidential

hardware profile multicast max-limit

To set the maximum number of entries in the multicast routing table, use the **hardware profile multicast max-limit** command.

hardware profile multicast max-limit *max-entries*

Syntax Description

max-entries	Maximum number of entries in the multicast routing table. The range is from 0 to 8000.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

A reload is neccessary after configuring the max-limit.

This command does not require a license.

Examples

This example shows how to set the maximum number of entries in the multicast routing table to 3000:

```
switch(config)# hardware profile multicast max-limit 3000
Warning!!: The multicast and /32 unicast route limits have been changed.
           Any route exceeding the limit may get dropped.
switch(config)#
```

Related Commands

Command	Description
show hardware profile status	Displays information about the multicast routing table limits.

Review Draft -- Cisco Confidential

I Commands

This chapter describes the Cisco NX-OS routing commands that begin with I.

Review Draft -- Cisco Confidential

interface ethernet (Layer 3)

To configure a Layer 3 Ethernet IEEE 802.3 routed interface, use the **interface ethernet** command.

interface ethernet [*chassis_ID*/] *slot*/*port*[.*subintf-port-no*]

Syntax Description

chassis_ID	(Optional) Specifies the Fabric Extender chassis ID. The chassis ID is from 100 to 199. **Note** This argument is not optional when addressing the host interfaces of a Cisco Nexus 2000 Series Fabric Extender.
slot	Slot from 1 to 3. The following list defines the slots available: • Slot 1 includes all the fixed ports. A Fabric Extender only has one slot. • Slot 2 includes the ports on the upper expansion module (if populated). • Slot 3 includes the ports on the lower expansion module (if populated).
port	Port number within a particular slot. The port number is from 1 to 128.
.	(Optional) Specifies the subinterface separator.
subintf-port-no	(Optional) Port number for the subinterface. The range is from 1 to 48.

Command Default

None

Command Modes

Global configuration mode
Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You must use the **no switchport** command in the interface configuration mode to configure the interface as a Layer 3 routed interface. When you configure the interface as a Layer 3 interface, all Layer 2 specific configurations on this interface are deleted.

Use the **switchport** command to convert a Layer 3 interface into a Layer 2 interface. When you configure the interface as a Layer 2 interface, all Layer 3 specific configurations on this interface are deleted.

Examples

This example shows how to enter configuration mode for a Layer 3 Ethernet interface 1/5:

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# ip address 10.1.1.1/24
switch(config-if)#
```

This example shows how to enter configuration mode for a host interface on a Fabric Extender:

```
switch(config)# interface ethernet 101/1/1
```

Review Draft -- Cisco Confidential

```
switch(config-if)# no switchport
switch(config-if)# ip address 10.1.1.1/24
switch(config-if)#
```

This example shows how to configure a Layer 3 subinterface for Ethernet interface 1/5 in the global configuration mode:

```
switch(config)# interface ethernet 1/5.2
switch(config-if)# no switchport
switch(config-subif)# ip address 10.1.1.1/24
switch(config-subif)#
```

This example shows how to configure a Layer 3 subinterface in interface configuration mode:

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# interface ethernet 1/5.1
switch(config-subif)# ip address 10.1.1.1/24
switch(config-subif)#
```

This example shows how to convert a Layer 3 interface to a Layer 2 interface:

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)# ip address 10.1.1.1/24
switch(config-if)# switchport
switch(config-if)#
```

Related Commands

Command	Description
bandwidth	Sets the bandwidth parameters for an interface.
delay	Configures the interface throughput delay value.
encapsulation	Sets the encapsulation type for an interface.
ip address	Sets a primary or secondary IP address for an interface.
inherit	Assigns a port profile to an interface.
interface vethernet	Configures a virtual Ethernet interface.
no switchport	Configures an interface as a Layer 3 interface.
service-policy	Configures a service policy for an interface.
show fex	Displays all configured Fabric Extender chassis connected to the switch.
show interface ethernet	Displays various parameters of an Ethernet IEEE 802.3 interface.

Review Draft -- Cisco Confidential

interface loopback

To create a loopback interface and enter interface configuration mode, use the **interface loopback** command. To remove a loopback interface, use the **no** form of this command.

interface loopback *number*

no interface loopback *number*

Syntax Description

number	Interface number; valid values are from 0 to 1023.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **interface loopback** command to create or modify loopback interfaces.

From the loopback interface configuration mode, the following parameters are available:

- **description**—Provides a description of the purpose of the interface.
- **ip**—Configures IP features, such as the IP address for the interface, Address Resolution Protocol (ARP) attributes, load balancing, Unicast Reverse Path Forwarding (RPF) or IP Source Guard.
- **logging**—Configure logging of events.
- **shutdown**—Shut down traffic on the interface.

This command does not require a license.

Examples

This example shows how to create a loopback interface:

```
switch(config)# interface loopback 50
switch(config-if)# ip address 10.1.1.1/24
switch(config-if)#
```

Related Commands

Command	Description
show interface loopback	Displays information about the traffic on the specified loopback interface.

Review Draft -- Cisco Confidential

interface port-channel

To create an EtherChannel interface and enter interface configuration mode, use the **interface port-channel** command. To remove an EtherChannel interface, use the **no** form of this command.

interface port-channel *channel-number*[*.subintf-channel-no*]

no interface port-channel *channel-number*[*.subintf-channel-no*]

Syntax Description

channel-number	Channel number that is assigned to this EtherChannel logical interface. The range is from 1 to 4096.
.	(Optional) Specifies the subinterface separator. **Note** Applies to Layer 3 interfaces.
subintf-channel-no	(Optional) Port number of the EtherChannel subinterface. The range is from 1 to 4093. **Note** Applies to Layer 3 interfaces.

Command Default

None

Command Modes

Global configuration mode
Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

A port can belong to only one channel group.

When you use the **interface port-channel** command for Layer 2 interfaces, follow these guidelines:

- If you are using CDP, you must configure it only on the physical interface and not on the EtherChannel interface.
- If you do not assign a static MAC address on the EtherChannel interface, a MAC address is automatically assigned. If you assign a static MAC address and then later remove it, the MAC address is automatically assigned.
- The MAC address of the EtherChannel is the address of the first operational port added to the channel group. If this first-added port is removed from the channel, the MAC address comes from the next operational port added, if there is one.

You must use the **no switchport** command in the interface configuration mode to configure the EtherChannel interface as a Layer 3 interface. When you configure the interface as a Layer 3 interface, all Layer 2 specific configurations on this interface are deleted.

Use the **switchport** command to convert a Layer 3 EtherChannel interface into a Layer 2 interface. When you configure the interface as a Layer 2 interface, all Layer 3 specific configurations on this interface are deleted.

Review Draft -- Cisco Confidential

You can configure one or more subinterfaces on a port channel made from routed interfaces.

Examples

This example shows how to create an EtherChannel group interface with channel-group number 50:

```
switch(config)# interface port-channel 50
switch(config-if)#
```

This example shows how to create a Layer 3 EtherChannel group interface with channel-group number 10:

```
switch(config)# interface port-channel 10
switch(config-if)# no switchport
switch(config-if)# ip address 192.0.2.1/24
switch(config-if)#
```

This example shows how to configure a Layer 3 EtherChannel subinterface with channel-group number 1 in interface configuration mode:

```
switch(config)# interface port-channel 10
switch(config-if)# no switchport
switch(config-if)# interface port-channel 10.1
switch(config-subif)# ip address 192.0.2.2/24
switch(config-subif)#
```

This example shows how to configure a Layer 3 EtherChannel subinterface with channel-group number 20.1 in global configuration mode:

```
switch(config)# interface port-channel 20.1
switch(config-subif)# ip address 192.0.2.3/24
switch(config-subif)#
```

Related Commands

Command	Description
encapsulation	(Layer 3 interfaces) Sets the encapsulation type for an interface.
ip address	(Layer 3 interfaces) Sets a primary or secondary IP address for an interface.
no switchport	(Layer 3 interfaces) Configures an interface as a Layer 3 interface.
show interface	Displays configuration information about interfaces.
show lacp	Displays LACP information.
show port-channel summary	Displays information on the EtherChannels.
vtp (interface)	Enables VLAN Trunking Protocol (VTP) on an interface.

Review Draft -- Cisco Confidential

N Commands

This chapter describes the Cisco NX-OS routing commands that begin with N.

Review Draft -- Cisco Confidential

no switchport

To configure the interface as a Layer 3 Ethernet interface, use the **no switchport** command.

no switchport

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You can configure any Ethernet port as a routed interface. When you configure an interface as a Layer 3 interface, any configuration specific to Layer 2 on this interface is deleted.

If you want to configure a Layer 3 interface for Layer 2, enter the **switchport** command. Then, if you change a Layer 2 interface to a routed interface, enter the **no switchport** command.

Examples

This example shows how to enable an interface as a Layer 3 routed interface:

```
switch(config)# interface ethernet 1/5
switch(config-if)# no switchport
switch(config-if)#
```

This example shows how to configure a Layer 3 interface as a Layer 2 interface:

```
switch(config)# interface ethernet 1/5
switch(config-if)# switchport
switch(config-if)#
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration file.
ip address	Sets a primary or secondary IP address for an interface.
show interfaces	Displays interface information.

Review Draft -- Cisco Confidential

IGMP Commands

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

C Commands

This chapter describes the Cisco NX-OS IGMP commands that begin with C.

Review Draft -- Cisco Confidential

clear ip igmp event-history

To clear information in the IGMP event history buffers, use the **clear ip igmp event-history** command.

clear ip igmp event-history {**cli** | **debugs** | **errors** | **events** | **ha** | **igmp-internal** | **mtrace** | **policy** | **vrf**}

Syntax Description

cli	Clears the CLI event history buffer.
debugs	Clears the debug event history buffer.
events	Clears the event history buffer.
ha	Clears the high availability (HA) event history buffer.
igmp-internal	Clears the IGMP internal event history buffer.
mtrace	Clears the mtrace event history buffer.
policy	Clears the polilcy event history buffer.
vrf	Clears the virtual routing and forwarding (VRF) event history buffer.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear information in the IGMP HA event history buffer:

```
switch(config)# clear ip igmp event-history ha
switch(config)#
```

Related Commands

Command	Description
ip igmp event-history	Configures the size of the IGMP event history buffers.

Review Draft -- Cisco Confidential

clear ip igmp groups

To clear IGMP-related information in the IPv4 multicast routing table, use the **clear ip igmp groups** command.

clear ip igmp groups {* | *group* [*source*] | *group-prefix*} [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

*	Specifies all routes.
group	Group address in the format *A.B.C.D*.
source	(Optional) Source (S, G) route.
group-prefix	Group prefix in the format *A.B.C.D/length*.
vrf	(Optional) Clears the virtual routing and forwarding (VRF) instance information.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies that all VRF entries be cleared from the IPv4 multicast routing table.
default	Specifies that the default VRF entry be cleared from the IPv4 multicast routing table.
management	Specifies that the management VRF entry be cleared from the IPv4 multicast routing table.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **clear ip igmp route** command is an alternative form of this command.

This command does not require a license.

Examples

This example shows how to clear all the IGMP-related routes in the IPv4 multicast routing table:

```
switch(config)# clear ip igmp groups *
switch(config)#
```

Related Commands

Command	Description
clear ip igmp route	Clears IGMP-related information in the IPv4 multicast routing table.
show ip mroute	Displays information about the IPv4 multicast routing table.

Review Draft -- Cisco Confidential

clear ip igmp interface statistics

To clear the IGMP statistics for an interface, use the **clear ip igmp interface statistics** command.

clear ip igmp interface statistics [**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number*[**.***sub_if_number*]]

Syntax Description

ethernet *slot/port*	(Optional) Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	(Optional) Specifies the loopback interface. The loopback interface number is from 0 to 1023.
port-channel *number*	(Optional) Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
sub_if-number	(Optional) Subinterface number. The range is from 1 to 4093.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear IGMP statistics for an interface:

```
switch# clear ip igmp interface statistics ethernet 2/1
switch#
```

Related Commands

Command	Description
show ip igmp interface	Displays information about IGMP interfaces.

Review Draft -- Cisco Confidential

clear ip igmp route

To clear IGMP-related information in the IPv4 multicast routing table, use the **clear ip igmp route** command.

clear ip igmp route {* | *group* [*source*] | *group-prefix*} [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

*	Specifies all routes.
group	Group address in the format *A.B.C.D*.
source	(Optional) Source (S, G) route.
group-prefix	Group prefix in the format *A.B.C.D/length*.
vrf	(Optional) Clears the virtual routing and forwarding (VRF) instance information.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies that all VRF entries be cleared from the IPv4 multicast routing table.
default	Specifies that the default VRF entry be cleared from the IPv4 multicast routing table.
management	Specifies that the management VRF entry be cleared from the IPv4 multicast routing table.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **clear ipigmp groups** command is an alternative form of this command.

This command does not require a license.

Examples

This example shows how to clear all the IGMP-related routes in the IPv4 multicast routing table:

```
switch(config)# clear ip igmp route *
switch(config)#
```

Related Commands

Command	Description
clear ip igmp groups	Clears IGMP-related information in the IPv4 multicast routing table.
show ip mroute	Displays information about the IPv4 multicast routing table.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

I Commands

This chapter describes the Cisco NX-OS IGMP commands that begin with I.

Review Draft -- Cisco Confidential

ip igmp access-group

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

ip igmp access-group *policy-name*

no ip igmp access-group [*policy-name*]

Syntax Description

policy-name	Route-map policy name. The route map name can be a maximum of 100 alphanumeric characters.

Command Default

Disabled

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **ip igmp access-group** command is an alias of the **ip igmp report-policy** command.

This command does not require a license.

Examples

This example shows how to enable a route-map policy:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip igmp access-group my_access_group_policy
switch(config-if)#
```

This example shows how to disable a route-map policy:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip igmp access-group
switch(config-if)#
```

Related Commands

Command	Description
show ip igmp interface	Displays IGMP information about the interface.

Review Draft -- Cisco Confidential

ip igmp enforce-router-alert

To enable the enforce router alert option check for IGMPv2 and IGMPv3 packets, use the **ip igmp enforce-router-alert** command. To disable the option check, use the **no** form of this command.

ip igmp enforce-router-alert

no ip igmp enforce-router-alert

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable the enforce router alert option check:

```
switch(config)# ip igmp enforce-router-alert
```

This example shows how to disable the enforce router alert option check:

```
switch(config)# no ip igmp enforce-router-alert
```

Related Commands

Command	Description
show running-config igmp	Displays information about the IGMP running-system configuration.

Review Draft -- Cisco Confidential

ip igmp event-history

To configure the size of the IGMP event history buffers, use the **ip igmp event-history** command. To revert to the default buffer size, use the **no** form of this command.

ip igmp event-history {**cli** | **group-debugs** | **group-events** | **ha** | **igmp-internal** | **interface-debugs** | **interface-events** | **msgs** | **mtrace** | **policy** | **statistics** | **vrf**} **size** *buffer-size*

no ip igmp event-history {**clis** | **group-debugs** | **group-events** | **ha** | **igmp-internal** | **interface-debugs** | **interface-events** | **msgs** | **mtrace** | **policy** | **statistics** | **vrf**} **size** *buffer-size*

Syntax Description

clis	Configures the IGMP CLI event history buffer size.
group-debugs	Configures the IGMP group debug event history buffer size.
group-events	Configures the IGMP group-event event history buffer size.
ha	Configures the IGMP HA event history buffer size.
igmp-internal	Configures the IGMP IGMP-internal event history buffer size.
interface-debugs	Configures the IGMP interface debug event history buffer size.
interface-events	Configures the IGMP interface-event event history buffer size.
msgs	Configures the message event history buffer size.
mtrace	Configures the IGMP mtrace event history buffer size.
policy	Configures the IGMP policy event history buffer size.
statistics	Configures the statistics event history buffer size.
vrf	Configures the IGMP VRF event history buffer size.
size	Specifies the size of the buffer to allocate.
buffer-size	Buffer size that is one of the following values: **disabled**, **large**, **medium**, or **small**. The default buffer size is **small**.

Command Default

All history buffers are allocated as small.

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the IGMP HA event history buffer size:

Review Draft -- Cisco Confidential

```
switch(config)# ip igmp event-history ha size large
switch(config)#
```

Related Commands

Command	Description
clear ip igmp event-history	Clears the contents of IGMP event history buffers.
show ip igmp event-history	Displays information in the IGMP event history buffers.
show running-config igmp	Displays information about the IGMP running-system configuration.

Review Draft -- Cisco Confidential

ip igmp flush-routes

To remove routes when the IGMP process is restarted, use the **ip igmp flush-routes** command. To leave routes in place, use the **no** form of this command.

ip igmp flush-routes

no ip igmp flush-routes

Syntax Description

This command has no arguments or keywords.

Command Default

The routes are not flushed.

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

To display whether flush routes are configured, use this command line:

```
switch(config)# show running-config | include flush-routes
```

This command does not require a license.

Examples

This example shows how to remove routes when the IGMP process is restarted:

```
switch(config)# ip igmp flush-routes
```

This example shows how to leave routes in place when the IGMP process is restarted:

```
switch(config)# no ip igmp flush-routes
```

Related Commands

Command	Description
show running-config	Displays information about the running-system configuration.

Review Draft -- Cisco Confidential

ip igmp group-timeout

To configure a group membership timeout for IGMPv2, use the **ip igmp group-timeout** command. To return to the default timeout, use the **no** form of this command.

ip igmp group-timeout *timeout*

no ip igmp group-timeout [*timeout*]

Syntax Description

timeout	Timeout in seconds. The range is from 3 to 65,535. The default is 260.

Command Default

The group membership timeout is 260 seconds.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a group membership timeout:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip igmp group-timeout 200
switch(config-if)#
```

This example shows how to reset a group membership timeout to the default:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip igmp group-timeout
switch(config-if)#
```

Related Commands

Command	Description
show ip igmp interface	Displays IGMP information about the interface.

Review Draft -- Cisco Confidential

ip igmp immediate-leave

To enable the device to remove the group entry from the multicast routing table immediately upon receiving a leave message for the group, use the **ip igmp immediate-leave** command. To disable the immediate leave option, use the **no** form of this command.

ip igmp immediate-leave

no ip igmp immediate-leave

Syntax Description

This command has no arguments or keywords.

Command Default

The immediate leave feature is disabled.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip igmp immediate-leave** command only when there is one receiver behind the interface for a given group.

This command does not require a license.

Examples

This example shows how to enable the immediate leave feature:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip igmp immediate-leave
```

This example shows how to disable the immediate leave feature:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip igmp immediate-leave
```

Related Commands

Command	Description
show ip igmp interface	Displays IGMP information about the interface.

Review Draft -- Cisco Confidential

ip igmp join-group

To statically bind a multicast group to an interface, use the **ip igmp join-group** command. To remove a group binding, use the **no** form of this command.

ip igmp join-group {*group* [**source** *source*] | **route-map** *policy-name*}

no ip igmp join-group {*group* [**source** *source*] | **route-map** *policy-name*}

Syntax Description

group	Multicast group IP address.
source *source*	(Optional) Configures a source IP address for the IGMPv3 (S,G) channel.
route-map *policy-name*	Specifies the route-map policy name that defines the group prefixes where this feature is applied. The route map name can be a maximum of 63 alphanumeric characters.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

If you specify only the group address, the (*, G) state is created. If you specify the source address, the (S, G) state is created.

If you use the route map, the only **match** command that is read from the route map is the **match ip multicast** command. You can specify the group prefix and source prefix.

Note A source tree is built for the (S, G) state only if you enable IGMPv3.

Caution When you enter this command, the traffic generated is handled by the device CPU, not the hardware.

This command does not require a license.

Examples

This example shows how to statically bind a group to an interface:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip igmp join-group 230.0.0.0
switch(config-if)#
```

This example shows how to remove a group binding from an interface:

Review Draft -- Cisco Confidential

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip igmp join-group 230.0.0.0
switch(config-if)#
```

Related Commands

Command	Description
show ip igmp interface	Displays IGMP information about the interface.

Review Draft -- Cisco Confidential

ip igmp last-member-query-count

To configure the number of times that the software sends an IGMP query in response to a host leave message, use the **ip igmp last-member-query-count** command. To reset the query interval to the default, use the **no** form of this command.

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

no ip igmp last-member-query-count [*count*]

Syntax Description

count	Query count. The range is from 1 to 5. The default is 2.

Command Default

The query count is 2.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a query count:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip igmp last-member-query-count 3
switch(config-if)#
```

This example shows how to reset a query count to the default:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip igmp last-member-query-count
switch(config-if)#
```

Related Commands

Command	Description
show ip igmp interface	Displays IGMP information about the interface.

Review Draft -- Cisco Confidential

ip igmp last-member-query-response-time

To configure a query interval in which the software sends membership reports and then deletes the group state, use the **ip igmp last-member-query-response-time** command. To reset the query interval to the default, use the **no** form of this command.

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

no ip igmp last-member-query-response-time [*interval*]

Syntax Description

interval	Query interval in seconds. The range is from 1 to 25. The default is 1.

Command Default

The query interval is 1 second.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a query interval:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip igmp last-member-query-response-time 3
switch(config-if)#
```

This example shows how to reset a query interval to the default:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip igmp last-member-query-response-time
switch(config-if)#
```

Related Commands

Command	Description
show ip igmp interface	Displays IGMP information about the interface.

Review Draft -- Cisco Confidential

ip igmp querier-timeout

To configure a querier timeout that the software uses when deciding to take over as the querier, use the **ip igmp querier-timeout** command. To reset to the querier timeout to the default, use the **no** form of this command.

ip igmp querier-timeout *timeout*

no ip igmp querier-timeout [*timeout*]

Syntax Description

timeout	Timeout in seconds. The range is from 1 to 65,535. The default is 255.

Command Default

The querier timeout is 255 seconds.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **ip igmp query-timeout** command is an alternative form of this command.

This command does not require a license.

Examples

This example shows how to configure a querier timeout:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip igmp querier-timeout 200
switch(config-if)#
```

This example shows how to reset a querier timeout to the default:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip igmp querier-timeout
switch(config-if)#
```

Related Commands

Command	Description
ip igmp query-timeout	Configures a querier timeout.
show ip igmp interface	Displays IGMP information about the interface.

Review Draft -- Cisco Confidential

ip igmp query-interval

To configure a query interval used when the IGMP process starts up, use the **ip igmp query-interval** command. To reset the query interval to the default, use the **no** form of this command.

ip igmp query-interval *interval*

no ip igmp query-interval [*interval*]

Syntax Description

interval	Interval in seconds. The range is from 1 to 18,000. The default is 125.

Command Default

The query interval is 125 seconds.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a query interval:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip igmp query-interval 100
switch(config-if)#
```

This example shows how to reset a query interval to the default:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip igmp query-interval
switch(config-if)#
```

Related Commands

Command	Description
show ip igmp interface	Displays IGMP information about the interface.

Review Draft -- Cisco Confidential

ip igmp query-max-response-time

To configure a query maximum response time that is advertised in IGMP queries, use the **ip igmp query-max-response-time** command. To reset the response time to the default, use the **no** form of this command.

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

no ip igmp query-max-response-time [*time*]

Syntax Description

time	Query maximum response time in seconds. The range is from 1 to 25. The default is 10.

Command Default

The query maximum response time is 10 seconds.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a query maximum response time:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip igmp query-max-response-time 15
switch(config-if)#
```

This example shows how to reset a query maximum response time to the default:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip igmp query-max-response-time
switch(config-if)#
```

Related Commands

Command	Description
show ip igmp interface	Displays IGMP information about the interface.

Review Draft -- Cisco Confidential

ip igmp query-timeout

To configure a query timeout that the software uses when deciding to take over as the querier, use the **ip igmp query-timeout** command. To reset to the querier timeout to the default, use the **no** form of this command.

ip igmp query-timeout *timeout*

no ip igmp query-timeout [*timeout*]

Syntax Description

timeout	Timeout in seconds. The range is from 1 to 65,535. The default is 255.

Command Default

The query timeout is 255 seconds.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **ip igmp querier-timeout** command is an alternative form of this command.

This command does not require a license.

Examples

This example shows how to configure a querier timeout:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip igmp query-timeout 200
switch(config-if)#
```

This example shows how to reset a querier timeout to the default:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip igmp query-timeout
switch(config-if)#
```

Related Commands

Command	Description
ip igmp querier-timeout	Configures a querier timeout.
show ip igmp interface	Displays IGMP information about the interface.

Review Draft -- Cisco Confidential

ip igmp report-link-local-groups

To enable IGMP to send reports for link-local groups, use the **ip igmp report-link-local-groups** command. To disable sending reports to link-local groups, use the **no** form of this command.

ip igmp report-link-local-groups

no ip igmp report-link-local-groups

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable sending reports to link-local groups:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip igmp report-link-local-groups
switch(config-if)#
```

This example shows how to disable sending reports to link-local groups:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip igmp report-link-local-groups
switch(config-if)#
```

Related Commands

Command	Description
show ip igmp interface	Displays IGMP information about the interface.

Review Draft -- Cisco Confidential

ip igmp report-policy

To enable an access policy that is based on a route-map policy for IGMP reports, use the **ip igmp report-policy** command. To disable the route-map policy, use the **no** form of this command.

ip igmp report-policy *policy-name*

no ip igmp report-policy [*policy-name*]

Syntax Description

policy-name	Route-map policy name. The route name is a maximum of 100 alphanumeric characters.

Command Default

Disabled

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Use the **ip igmp report-policy** command to filter incoming messages. You can configure the route map to prevent state from being created in the multicast routing table.

The **ip igmp report-policy** command is an alias of the **ip igmp access-group** command.

If you use the route map, the only **match** command that is read from the route map is the **match ip multicast** command. You can specify the group prefix, group range, and source prefix to filter messages.

This command requires the Enterprise Services license.

Examples

This example shows how to enable an access policy for IGMP reports:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip igmp report-policy my_report_policy
switch(config-if)#
```

This example shows how to disable an access policy for IGMP reports:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip igmp report-policy
switch(config-if)#
```

Related Commands

Command	Description
show ip igmp interface	Displays IGMP information about the interface.

Review Draft -- Cisco Confidential

ip igmp robustness-variable

To configure a robustness count that you can tune to reflect expected packet loss on a congested network, use the **ip igmp robustness-variable** command. To reset the count to the default, use the **no** form of this command.

ip igmp robustness-variable *count*

no ip igmp robustness-variable [*count*]

Syntax Description

count	Robustness count. The range is from 1 to 7. The default is 2.

Command Default

The robustness count is 2.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a robustness count:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip igmp robustness-variable 3
switch(config-if)#
```

This example shows how to reset a robustness count to the default:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip igmp robustness-variable
switch(config-if)#
```

Related Commands

Command	Description
show ip igmp interface	Displays IGMP information about the interface.

Review Draft -- Cisco Confidential

ip igmp ssm-translate

To translate IGMPv1 or IGMPv2 membership reports to create the (S, G) state so that the router treats them as IGMPv3 membership reports, use the **ip igmp ssm-translate** command. To remove the translation, use the **no** form of this command.

ip igmp ssm-translate *group source*

no ip igmp ssm-translate *group source*

Syntax Description

group	IPv4 multicast group range. By default, the group prefix range is 232.0.0.0/8. To modify the IPv4 Protocol Independent Multicast (PIM) SSM range, see the **ip pim ssm range** command.
source	IP multicast address source.

Command Default

None

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

To display SSM translation commands, use this command line:

```
switch(config)# show running-config | include ssm-translation
```

This command does not require a license.

Examples

This example shows how to configure a translation:

```
switch# configure terminal
switch(config)# ip igmp ssm-translate 232.0.0.0/8 10.1.1.1
switch(config)#
```

This example shows how to remove a translation:

```
switch# configure terminal
switch(config)# no ip igmp ssm-translate 232.0.0.0/8 10.1.1.1
switch(config)#
```

Related Commands

Command	Description
show running-config	Displays information about the running-system configuration.

Review Draft -- Cisco Confidential

ip igmp startup-query-count

To configure the query count used when the IGMP process starts up, use the **ip igmp startup-query-count** command. To reset the query count to the default, use the **no** form of this command.

ip igmp startup-query-count *count*

no ip igmp startup-query-count [*count*]

Syntax Description

count	Query count. The range is from 1 to 10. The default is 2.

Command Default

The query count is 2.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a query count:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip igmp startup-query-count 3
switch(config-if)#
```

This example shows how to reset a query count to the default:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip igmp startup-query-count
switch(config-if)#
```

Related Commands

Command	Description
show ip igmp interface	Displays IGMP information about the interface.

Review Draft -- Cisco Confidential

ip igmp startup-query-interval

To configure the query interval used when the IGMP process starts up, use the **ip igmp startup-query-interval** command. To reset the query interval to the default, use the **no** form of this command.

ip igmp startup-query-interval *interval*

no ip igmp startup-query-interval [*interval*]

Syntax Description

interval	Query interval in seconds. The range is from 1 to 18,000. The default is 31.

Command Default

The query interval is 31 seconds.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a startup query interval:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip igmp startup-query-interval 25
switch(config-if)#
```

This example shows how to reset a startup query interval to the default:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip igmp startup-query-interval
switch(config-if)#
```

Related Commands

Command	Description
show ip igmp interface	Displays IGMP information about the interface.

Review Draft -- Cisco Confidential

ip igmp state-limit

To configure the maximum states allowed, use the **ip igmp state-limit** command. To remove the state limit, use the **no** form of this command.

ip igmp state-limit *max-states* [**reserved** *reserve-policy max-reserved*]

no ip igmp state-limit [*max-states* [**reserved** *reserve-policy max-reserved*]]

Syntax Description

max-states	Maximum states allowed. The range is from 1 to 4,294,967,295.
reserved *reserve-policy max-reserved*	(Optional) Specifies to use the route-map policy name for the reserve policy. The route map name can be a maximum of 100 alphanumeric characters.
max-reserved	(Optional) Maximum number of (*, G) and (S, G) entries allowed on the interface.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a state limit:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip igmp state-limit 5000
switch(config-if)#
```

This example shows how to remove a state limit:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip igmp state-limit
switch(config-if)#
```

Related Commands

Command	Description
show ip igmp interface	Displays IGMP information about the interface.

Review Draft -- Cisco Confidential

ip igmp static-oif

To statically bind a multicast group to the outgoing interface (OIF), which is handled by the device hardware, use the **ip igmp static-oif** command. To remove a static group, use the **no** form of this command.

ip igmp static-oif {*group* [**source** *source*] | **route-map** *policy-name*}

no ip igmp static-oif {*group* [**source** *source*] | **route-map** *policy-name*}

Syntax Description

group	Multicast group IPv4 address. If you specify only the group address, the (*, G) state is created.
source *source*	(Optional) Configures the source IP address for IGMPv3 and creates the (S, G) state. **Note** A source tree is built for the (S, G) state only if you enable IGMPv3.
route-map *policy-name*	Specifies the route-map policy name that defines the group prefixes where this feature is applied. The route map name can be a maximum of 63 alphanumeric characters.

Command Default

None

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Before you use this command, make sure that you enable Protocol Independent Multicast (PIM) on the interface by using the **ip pim sparse-mode** command.

This command does not require a license.

Examples

This example shows how to statically bind a group to the OIF:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no switchport
switch(config-if)# ip igmp static-oif 230.0.0.0
switch(config-if)#
```

This example shows how to remove a static binding from the OIF:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no switchport
switch(config-if)# no ip igmp static oif 230.0.0.0
switch(config-if)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
ip pim sparse-mode	Enables IPv4 PIM sparse mode on an interface.
no switchport	Configures the interface as a routed interface.
show ip igmp local-groups	Displays information about the IGMP local group membership.

Review Draft -- Cisco Confidential

ip igmp version

To configure the IGMP version to use on an interface, use the **ip igmp version** command. To reset the IGMP version to the default, use the **no** form of this command.

ip igmp version *version*

no ip igmp version [*version*]

Syntax Description

version	Version number. The number is 2 or 3. The default is 2.

Command Default

The version number is 2.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the IGMP version to use on an interface:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip igmp version 3
switch(config-if)#
```

This example shows how to reset the IGMP version to the default:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip igmp version
switch(config-if)#
```

Related Commands

Command	Description
show ip igmp interface	Displays IGMP information about the interface.

Review Draft -- Cisco Confidential

Show Commands

This chapter describes the Cisco NX-OS IGMP **show** commands.

Review Draft -- Cisco Confidential

show ip igmp event-history

To display information in the IGMP event history buffers, use the **show ip igmp event-history** command.

show ip igmp event-history {**clis** | **debugs** | **errors** | **events** | **ha** | **igmp-internal** | **msgs** | **mtrace** | **policy** | **statistics** | **vrf**}

Syntax Description

clis	Displays events of type CLI.
debugs	Displays events of type debug.
errors	Displays events of type error.
events	Displays events of type event.
ha	Displays events of type HA.
igmp-internal	Displays events of type IGMP internal.
msgs	Displays events of type msg.
mtrace	Displays events of type mtrace.
policy	Displays events of type policy.
statistics	Displays events of type statistics.
vrf	Displays events of type VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information in the IGMP HA event history buffer:

```
switch(config)# show ip igmp event-history ha

 ha events for IGMP process
2008 Apr 12 04:01:32.339950 igmp [4588]: : Router-port PSS entry for vlan 20 upd
ated [count 0]
2008 Apr 12 04:00:05.118545 igmp [4588]: : Handling existing vlans notification
2008 Apr 12 04:00:04.824730 igmp [4588]: : PSS entry for global updatedswitch(config)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
clear ip igmp event-history	Clears the contents of the IGMP event history buffers.
ip igmp event-history	Configures the size of IGMP event history buffers.

Review Draft -- Cisco Confidential

show ip igmp groups

To display information about IGMP-attached group membership, use the **show ip igmp groups** command.

show ip igmp groups [{*source* [*group*]} | {*group* [*source*]}] [**ethernet** *slot*/*port* | **port-channel** *channel-number*[**.***sub_if_number*] | **vlan** *vlan-id*] [**vrf** {*vrf-name* | **all**}]

Syntax Description

source	Source IP address.
group	(Optional) Multicast IP address of the single group to display.
ethernet *slot*/*port*	(Optional) Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
port-channel *number*	(Optional) Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
sub_if_number	(Optional) Subinterface number. The range is from 1 to 4093.
vlan *vlan-id*	(Optional) Specifies the VLAN. The range is from 1 to 4094.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **show ip igmp route** command is an alternative form of this command.

This command does not require a license.

Examples

This example shows how to display information about the IGMP-attached group membership:

```
switch(config)# show ip igmp groups
IGMP Connected Group Membership for VRF "default" - 0 total entries
Type: S - Static, D - Dynamic, L - Local, T - SSM Translated
Group Address      Type Interface           Uptime    Expires   Last Reporter
switch(config)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
show ip igmp route	Displays information about the IGMP-attached group membership.

Review Draft -- Cisco Confidential

show ip igmp interface

To display information about IGMP on interfaces, use the **show ip igmp interface** command.

show ip igmp interface {**ethernet** *slot*/*port* | **port-channel** *channel-number*[**.***sub_if_number*] | **vlan** *vlan-id*}

show ip igmp interface [**brief**] [**vrf** {*vrf-name* | **all**}]

Syntax Description

ethernet *slot*/*port*	Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
port-channel *number*	Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
sub_if_number	Subinterface number. The range is from 1 to 4093.
vlan *vlan-id*	Specifies the VLAN. The range is from 1 to 4094.
brief	(Optional) Displays one line status per interface.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information about IGMP on an interface (if IGMP is not in vPC mode, the vPC information is not displayed):

```
switch(config)# show ip igmp interface vlan 5
IGMP Interfaces for VRF "default"
Vlan20, Interface status: protocol-down/link-down/admin-down
  IP address: 20.1.1.3, IP subnet: 20.1.1.0/24
  Active querier: 0.0.0.0
  Membership count: 0
  Old Membership count 0
  Route-queue depth: 0
  IGMP version: 2, host version: 0
  IGMP query interval: 125 secs, configured value: 125 secs
  IGMP max response time: 10 secs, configured value: 10 secs
```

Review Draft -- Cisco Confidential

```
  IGMP startup query interval: 31 secs, configured value: 31 secs
  IGMP startup query count: 2
  IGMP last member mrt: 1 secs
  IGMP last member query count: 2
  IGMP group timeout: 260 secs, configured value: 260 secs
  IGMP querier timeout: 255 secs, configured value: 255 secs
  IGMP unsolicited report interval: 10 secs
  IGMP robustness variable: 2, configured value: 2
  IGMP reporting for link-local groups: disabled
  IGMP interface enable refcount: 1
  IGMP interface immediate leave: disabled
  IGMP Report Policy: None
  IGMP State Limit: None
  IGMP interface statistics:
    General (sent/received):
      v1-reports: 0/0
      v2-queries: 0/0, v2-reports: 0/0, v2-leaves: 0/0
      v3-queries: 0/0, v3-reports: 0/0
    Errors:
      General Queries received with invalid destination address; v2: 0, v3: 0
      Checksum errors: 0, Packet length errors: 0
      Packets with Local IP as source: 0, Source subnet check failures: 0
      Query from non-querier:0
      Report version mismatch: 0, Query version mismatch: 0
      Unknown IGMP message type: 0
      Invalid v1 reports: 0, Invalid v2 reports: 0, Invalid v3 reports: 0
    Packets dropped due to router-alert check: 0
  Interface PIM DR: No
  Interface vPC CFS statistics:
    DR queries sent: 0
    DR queries rcvd: 0
    DR queries fail: 0
    DR updates sent: 0
    DR updates rcvd: 0
    DR updates fail: 0
switch(config)#
```

This example shows how to display information about IGMP on an interface in a brief format:

```
switch(config)# show ip igmp interface brief
IGMP Interfaces for VRF "default", count: 1
Interface            IP Address      IGMP Querier    Membership  Version
                                                     Count
Vlan20               20.1.1.3        0.0.0.0         0           v2
switch(config)#
```

Review Draft -- Cisco Confidential

show ip igmp local-groups

To display information about IGMP local groups, use the **show ip igmp local-groups** command.

show ip igmp local-groups [**ethernet** *slot/port* | **port-channel** *channel-number*[**.***sub_if_number*] | **vlan** *vlan-id*] [**vrf** {*vrf-name* | **all**}]

Syntax Description

ethernet *slot/port*	Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
port-channel *number*	Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
sub_if_number	Subinterface number. The range is from 1 to 4093.
vlan *vlan-id*	Specifies the VLAN. The range is from 1 to 4094.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information about IGMP local groups:

```
switch(config)# show ip igmp local-groups
```

Review Draft -- Cisco Confidential

show ip igmp route

To display information about the IGMP-attached group membership, use the **show ip igmp route** command.

show ip igmp route [{*source* [*group*]} | {*group* [*source*]}] [**ethernet** *slot*/*port* | **port-channel** *channel-number*[**.***sub_if_number*] | **vlan** *vlan-id*] [**vrf** {*vrf-name* | **all**}]

Syntax Description

source	Source IP address.
group	(Optional) Multicast IP address of single group to display.
ethernet *slot*/*port*	Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
port-channel *number*	Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
sub_if_number	Subinterface number. The range is from 1 to 4093.
vlan *vlan-id*	Specifies the VLAN. The range is from 1 to 4094.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **show ip igmp groups** command is an alternative form of this command.

This command does not require a license.

Examples

This example shows how to display information about the IGMP-attached group membership:

```
switch# show ip igmp route
IGMP Connected Group Membership for VRF "default" - 1 total entries
Type: S - Static, D - Dynamic, L - Local, T - SSM Translated
Group Address      Type Interface           Uptime    Expires   Last Reporter
230.0.0.0          S    Ethernet1/5         00:31:47  never     0.0.0.0
switch#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
show ip igmp groups	Displays information about the IGMP-attached group membership.

Review Draft -- Cisco Confidential

show running-config igmp

To display information about the running-system configuration for IGMP, use the **show running-config igmp** command.

show running-config igmp [**all**]

Syntax Description		
	all	(Optional) Displays configured and default information.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	6.0(2)N1(1)	This command was introduced.

Usage Guidelines This command requires the LAN Base Services license.

Examples This example shows how to display information about the IGMP running-system configuration:

Need new output

```
switch(config)# show running-config igmp

!Command: show running-config igmp
!Time: Fri May  2 08:05:08 2008

version 5.0(3)N1(1)

interface Ethernet1/5
  ip igmp static-oif 230.0.0.0

switch(config)#
```

Review Draft -- Cisco Confidential

show startup-config igmp

To display information about the startup-system configuration for IGMP, use the **show startup-config igmp** command.

show startup-config igmp [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about the IGMP startup-system configuration:

```
switch(config)# show startup-config igmp
```

Review Draft -- Cisco Confidential

IGMP Snooping Commands

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

C Commands

This chapter describes the Cisco NX-OS IGMP snooping commands that begin with C.

Review Draft -- Cisco Confidential

clear ip igmp snooping event-history

To clear information from IGMP snooping event history buffers, use the **clear ip igmp snooping event-history** command.

clear ip igmp snooping event-history {**rib** | **vpc** | **igmp-snoop-internal** | **mfdm** | **mfdm-sum** | **vlan** | **vlan-events**}

Syntax Description

rib	Clears the unicast Routing Information Base (RIB) event history buffer.
vpc	Clears the virtual port channel (vPC) event history buffer.
igmp-snoop-internal	Clears the IGMP snooping internal event history buffer.
mfdm	Clears the multicast FIB distribution (MFDM) event history buffer.
mfdm-sum	Clears the MFDM sum event history buffer.
vlan	Clears the VLAN event history buffer.
vlan-events	Clears the VLAN-events event history buffer.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear information in the IGMP snooping VLAN event history buffer:

```
switch(config)# clear ip igmp event-history vlan
switch(config)#
```

Related Commands

Command	Description
ip igmp snooping event-history	Configures the size of the IGMP snooping event history buffers.

Review Draft -- Cisco Confidential

clear ip igmp snooping explicit-tracking vlan

To clear the IGMP snooping explicit host tracking information for VLANs, use the **clear ip igmp snooping explicit-tracking vlan** command.

clear ip igmp snooping explicit-tracking vlan *vlan-id*

Syntax Description

vlan-id	VLAN number. The range is from 1 to 3968 and 4049 to 4093.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear the explicit tracking information for VLAN 1:

```
switch# clear ip igmp snooping explicit-tracking vlan 1
switch#
```

Related Commands

Command	Description
show ip igmp snooping explicit-tracking vlan	Displays explicit host tracking information for IGMPv3.

Review Draft -- Cisco Confidential

clear ip igmp snooping statistics vlan

To clear the IGMP snooping statistics for VLANs, use the **clear ip igmp snooping statistics vlan** command.

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

Syntax Description

vlan-id	(Optional) VLAN number. The range is from 1 to 3968 and 4049 to 4093.
all	(Optional) Applies to all VLANs.

Command Default

All VLANs

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear IGMP snooping statistics for VLAN 1:

```
switch# clear ip igmp snooping statistics vlan 1
switch#
```

Related Commands

Command	Description
show ip igmp snooping statistics vlan	Displays IGMP snooping statistics by VLAN.

Review Draft -- Cisco Confidential

H Commands

This chapter describes the Cisco NX-OS IGMP snooping commands that begin with H.

Review Draft -- Cisco Confidential

hardware multicast snooping group-limit

To configure the number of groups learned through IGMP Snooping, use the **hardware multicast snooping group-limit** command.

hardware multicast snooping group-limit *limit*

Syntax Description

limit	Number of groups learned through IGMP Snooping. The range is from 100 to 8000.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Before setting a new group-limit, you must either clear the MAC address table or clear the groups already learned.

The unique OIFL (output interface list) combinations can only be 2000.

Use the vPC type-2 inconsistency to show the configuraitons on vPC peers.

A reload is not neccessary after configuring the group-limit.

This command does not require a license.

Examples

This example shows how to set the maximum number of groups to 500:

```
switch(config)# hardware multicast snooping group-limit 500
switch(config)#
```

Related Commands

Command	Description
show ip igmp snooping groups	Displays information about the group membership for IGMP snooping.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear the explicit tracking information for VLAN 1:

Review Draft -- Cisco Confidential

```
switch# clear ip igmp snooping explicit-tracking vlan 1
switch#
```

Related Commands

Command	Description
show ip igmp snooping explicit-tracking vlan	Displays explicit host tracking information for IGMPv3.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

I Commands

This chapter describes the Cisco NX-OS IGMP snooping commands that begin with I.

Review Draft -- Cisco Confidential

ip igmp snooping (Global)

To enable IGMP snooping, use the **ip igmp snooping** command. To disable IGMP snooping, use the **no** form of this command.

ip igmp snooping

no ip igmp snooping

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

If the global configuration of IGMP snooping is disabled, then all VLANs are treated as disabled, whether they are enabled or not.

This command does not require a license.

Examples

This example shows how to enable IGMP snooping:

```
switch(config)# ip igmp snooping
switch(config)#
```

This example shows how to disable IGMP snooping:

```
switch(config)# no ip igmp snooping
switch(config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

Review Draft -- Cisco Confidential

ip igmp snooping (VLAN)

To enable IGMP snooping on specified VLAN interfaces, use the **ip igmp snooping** command. To disable IGMP snooping on the interface, use the **no** form of this command.

ip igmp snooping

no ip igmp snooping

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

VLAN configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

If the global configuration of IGMP snooping is disabled, then all VLANs are treated as disabled, whether they are enabled or not.

This command does not require a license.

Examples

This example shows how to enable IGMP snooping on a VLAN interface:

```
switch(config)# vlan 1
switch(config-vlan)# ip igmp snooping
switch(config-vlan)#
```

This example shows how to disable IGMP snooping on a VLAN interface:

```
switch(config)# vlan 1
switch(config-vlan)# no ip igmp snooping
switch(config-vlan)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

Review Draft -- Cisco Confidential

ip igmp snooping event-history

To configure the size of the IGMP snooping event history buffers, use the **ip igmp snooping event-history** command. To revert to the default buffer size, use the **no** form of this command.

ip igmp snooping event-history {**igmp-snoop-internal** | **mfdm** | **mfdm-sum** | **rib** | **vlan** | **vlan-events** | **vpc**} **size** *buffer-size*

no ip igmp snooping event-history {**igmp-snoop-internal** | **mfdm** | **mfdm-sum** | **rib** | **vlan** | **vlan-events** | **vpc**} **size** *buffer-size*

Syntax Description

igmp-snoop-internal	Clears the IGMP snooping internal event history buffer.
mfdm	Clears the multicast FIB distribution (MFDM) event history buffer.
mfdm-sum	Clears the MFDM sum event history buffer.
rib	Clears the Routing Information Base (RIB) event history buffer.
vlan	Clears the VLAN event history buffer.
vlan-events	Clears the VLAN-event event history buffer.
vpc	Clears the virtual port channel (vPC) event history buffer.
size	Specifies the size of the buffer to allocate.
buffer-size	Buffer size that is one of the following values: **disabled**, **large**, **medium**, or **small**. The default buffer size is **small**.

Command Default

All history buffers are allocated as small.

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the IGMP snooping VLAN event history buffer size:

```
switch(config)# ip igmp snooping event-history vlan size large
switch(config)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
clear ip igmp snooping event-history	Clears the contents of the IGMP snooping event history buffers.
show ip igmp snooping event-history	Displays information in the IGMP snooping event history buffers.
show running-config igmp	Displays information about the IGMP running-system configuration.

Review Draft -- Cisco Confidential

ip igmp snooping explicit-tracking

To enable tracking of IGMPv3 membership reports from individual hosts for each port on a per-VLAN basis, use the **ip igmp snooping explicit-tracking** command. To disable tracking, use the **no** form of this command.

ip igmp snooping explicit-tracking

no ip igmp snooping explicit-tracking

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

VLAN configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to enable tracking of IGMPv3 membership reports on a VLAN interface:

```
switch(config)# vlan 1
switch(config-vlan)# ip igmp snooping explicit-tracking
switch(config-vlan)#
```

This example shows how to disable IGMP snooping on a VLAN interface:

```
switch(config)# vlan 1
switch(config-vlan)# no ip igmp snooping explicit-tracking
switch(config-vlan)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

Review Draft -- Cisco Confidential

ip igmp snooping fast-leave

To enable support of IGMPv2 hosts that cannot be explicitly tracked because of the host report suppression mechanism of the IGMPv2 protocol, use the **ip igmp snooping fast-leave** command. To disable support of IGMPv2 hosts, use the **no** form of this command.

ip igmp snooping fast-leave

no ip igmp snooping fast-leave

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

VLAN configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

When you enable fast leave, the IGMP software assumes that no more than one host is present on each VLAN port.

This command does not require a license.

Examples

This example shows how to enable support of IGMPv2 hosts:

```
switch(config)# vlan 1
switch(config-vlan)# ip igmp snooping fast-leave
switch(config-vlan)#
```

This example shows how to disable support of IGMPv2 hosts:

```
switch(config)# vlan 1
switch(config-vlan)# no ip igmp snooping fast-leave
switch(config-vlan)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

Review Draft -- Cisco Confidential

ip igmp snooping last-member-query-interval

To configure a query interval in which the software removes a group, use the **ip igmp snooping last-member-query-interval** command. To reset the query interval to the default, use the **no** form of this command.

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

no ip igmp snooping last-member-query-interval [*interval*]

Syntax Description

interval	Query interval in seconds. The range is from 1 to 25. The default is 1.

Command Default

The query interval is 1.

Command Modes

VLAN configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a query interval in which the software removes a group:

```
switch(config)# vlan 1
switch(config-vlan)# ip igmp snooping last-member-query-interval 3
switch(config-vlan)#
```

This example shows how to reset a query interval to the default:

```
switch(config)# vlan 1
switch(config-vlan)# no ip igmp snooping last-member-query-interval
switch(config-vlan)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

Review Draft -- Cisco Confidential

ip igmp snooping link-local-groups-suppression

To enable suppression of IGMP reports from link-local groups, use the **ip igmp snooping link-local-groups-suppression** command. To disable suppression of these reports, use the **no** form of this command.

ip igmp snooping link-local-groups-suppression

no ip igmp snooping link-local-groups-suppression

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration mode
VLAN configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

If this setting is disabled on the entire device, then it is disabled on all VLANs on device, irrespective of the specific VLAN setting.

This command does not require a license.

Examples

This example shows how to enable suppression of IGMP reports from link-local groups:

```
switch(config)# vlan 1
switch(config-vlan)# ip igmp snooping link-local-groups-suppression
switch(config-vlan)#
```

This example shows how to disable suppression of IGMP reports from link-local groups:

```
switch(config)# vlan 1
switch(config-vlan)# no ip igmp snooping link-local-groups-suppression
switch(config-vlan)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

Review Draft -- Cisco Confidential

ip igmp snooping mrouter interface

To configure a static connection to a multicast router, use the **ip igmp snooping mrouter interface** command. To remove the static connection, use the **no** form of this command.

ip igmp snooping mrouter interface {**ethernet** *slot*/*port* | **port-channel** *number*[**.***sub_if_number*]}

no ip igmp snooping mrouter interface {**ethernet** *slot*/*port* | **port-channel** *number*[**.***sub_if_number*]}

Syntax Description

ethernet *slot*/*port*	(Optional) Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
port-channel *number*	(Optional) Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
sub_if_number	(Optional) Subinterface number. The range is from 1 to 4093.

Command Default

None

Command Modes

VLAN configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The interface to the router must be in the selected VLAN.

This command does not require a license.

Examples

This example shows how to configure a static connection to a multicast router:

```
switch(config)# vlan 1
switch(config-vlan)# ip igmp snooping mrouter interface ethernet 2/1
switch(config-vlan)#
```

This example shows how to remove a static connection to a multicast router:

```
switch(config)# vlan 1
switch(config-vlan)# no ip igmp snooping mrouter interface ethernet 2/1
switch(config-vlan)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

Review Draft -- Cisco Confidential

ip igmp snooping mrouter vpc-peer-link

To configure a static connection to a virtual port channel (vPC) peer link, use the **ip igmp snooping mrouter vpc-peer-link** command. To remove the static connection, use the **no** form of this command.

ip igmp snooping mrouter vpc-peer-link

no ip igmp snooping mrouter vpc-peer-link

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

By default, a vPC Peer-link is considered an IGMP snooping mrouter port. The multicast traffic is sent over to a peer-link for the source VLAN and for each receiving VLAN. If you use the **no ip igmp snooping mrouter vpc-peer-link** command, the multicast traffic is not sent over to a peer-link for the source VLAN and receiver VLAN unless there are orphan ports in the VLAN.

This command does not require a license.

Examples

This example shows how to configure a static connection to a vPC peer link:

```
switch(config)# ip igmp snooping mrouter vpc-peer-link
switch(config)#
```

This example shows how to remove a static connection to a vPC peer link:

```
switch(config)# no ip igmp snooping mrouter vpc-peer-link
Warning: IGMP Snooping mrouter vpc-peer-link should be globally disabled on peer
 VPC switch as well.
switch(config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

Review Draft -- Cisco Confidential

ip igmp snooping optimise-multicast-flood

To configure Optimized Multicast Flood (OMF) on all VLANs, use the **ip igmp snooping optimise-multicast-flood** command. To remove the OMF from all VLANs, use the **no** form of this command.

ip igmp snooping optimise-multicast-flood

no ip igmp snooping optimise-multicast-flood

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure OMF on all VLANs:

```
switch(config)# ip igmp snooping optimise-multicast-flood
switch(config)#
```

This example shows how to remove OMF from all VLANs:

```
switch(config)# no ip igmp snooping optimise-multicast-flood
switch(config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

Review Draft -- Cisco Confidential

ip igmp snooping querier

To configure a snooping querier on an interface when you do not enable Protocol Independent Multicast (PIM) because multicast traffic does not need to be routed, use the **ip igmp snooping querier** command. To remove the snooping querier, use the **no** form of this command.

ip igmp snooping querier *querier*

no ip igmp snooping querier [*querier*]

Syntax Description

querier	Querier IP address.

Command Default

None

Command Modes

VLAN configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The querier IP address cannot be a multicast address.

This command does not require a license.

Examples

This example shows how to configure a snooping querier:

```
switch(config)# vlan 1
switch(config-vlan)# ip igmp snooping querier 172.20.52.106
switch(config-vlan)#
```

This example shows how to disable IGMP snooping on a VLAN interface:

```
switch(config)# vlan 1
switch(config-vlan)# no ip igmp snooping querier
switch(config-vlan)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

Review Draft -- Cisco Confidential

ip igmp snooping report-suppression

To enable limiting the membership report traffic sent to multicast-capable routers, use the **ip igmp snooping report-suppression** command. To disable the limitation, use the **no** form of this command.

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration mode
VLAN configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

When you disable report suppression, all IGMP reports are sent as is to multicast-capable routers.

This command does not require a license.

Examples

This example shows how to enable limiting the membership report traffic:

```
switch(config)# vlan 1
switch(config-vlan)# ip igmp snooping report-suppression
switch(config-vlan)#
```

This example shows how to disable limiting the membership report traffic:

```
switch(config)# vlan 1
switch(config-vlan)# no ip igmp snooping report-suppression
switch(config-vlan)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

Review Draft -- Cisco Confidential

ip igmp snooping static-group

To configure a Layer 2 port of a VLAN as a static member of a multicast group, use the **ip igmp snooping static-group** command. To remove the static member, use the **no** form of this command.

ip igmp snooping static-group *group* [**source** *source*] **interface** {**ethernet** *slot*/*port* | **port-channel** *number*[**.***sub_if_number*]}

no ip igmp snooping static-group *group* [**source** *source*] **interface** {**ethernet** *slot*/*port* | **port-channel** *number*[**.***sub_if_number*]}

Syntax Description

group	Group IP address.
source *source*	(Optional) Configures a static (S, G) channel for the source IP address.
interface	Specifies an interface for the static group.
ethernet *slot*/*port*	Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
port-channel *number*	Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
sub_if_number	(Optional) Subinterface number. The range is from 1 to 4093.

Command Default

None

Command Modes

VLAN configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a static member of a multicast group:

```
switch(config)# vlan 1
switch(config-vlan)# ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1
switch(config-vlan)#
```

This example shows how to remove a static member of a multicast group:

```
switch(config)# vlan 1
switch(config-vlan)# no ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1
switch(config-vlan)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

Review Draft -- Cisco Confidential

ip igmp snooping v3-report-suppression (Global)

To configure IGMPv3 report suppression and proxy reporting for VLANs on the entire device, use the **ip igmp snooping v3-report-suppression** command. To remove IGMPv3 report suppression, use the **no** form of this command.

ip igmp snooping v3-report-suppression

no ip igmp snooping v3-report-suppression

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure IGMPv3 report suppression and proxy reporting for VLANs:

```
switch(config)# ip igmp snooping v3-report-suppression
```

This example shows how to remove IGMPv3 report suppression:

```
switch(config)# no ip igmp snooping v3-report-suppression
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

Review Draft -- Cisco Confidential

ip igmp snooping v3-report-suppression (VLAN)

To configure IGMPv3 report suppression and proxy reporting for VLANs, use the **ip igmp snooping v3-report-suppression** command. To remove IGMPv3 report suppression, use the **no** form of this command.

ip igmp snooping v3-report-suppression

no ip igmp snooping v3-report-suppression

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

VLAN configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

If this setting is disabled for the device, which is the default value, then it is disabled for all VLANs, irrespective of how you set this value for an individual VLAN. However, once you set the global setting to enabled, the settings for all the VLANs are enabled by default.

This command does not require a license.

Examples

This example shows how to configure IGMPv3 report suppression and proxy reporting for specified VLANs:

```
switch(config)# vlan 10-20
switch(config-vlan)# ip igmp snooping v3-report-suppression
```

This example shows how to remove IGMPv3 report suppression on specified VLANs:

```
switch(config)# vlan 10-20
switch(config-vlan)# no ip igmp snooping v3-report-suppression
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

Review Draft -- Cisco Confidential

Show Commands

This chapter describes the Cisco NX-OS IGMP snooping **show** commands.

Review Draft -- Cisco Confidential

show forwarding distribution ip igmp snooping

To display information about Layer 2 IGMP snooping multicast Forwarding Information Base (FIB) distribution, use the **show forwarding distribution ip igmp snooping** command.

show forwarding distribution ip igmp snooping [**vlan** *vlan-id* [**group** *group-addr* [**source** *source-addr*]]]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN. The range is from 1 to 3967 and 4048 to 4093.
group *group-addr*	(Optional) Specifies a group address.
source *source-addr*	(Optional) Specifies a source address.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information about Layer 2 IGMP snooping multicast FIB distribution:

```
switch(config)# show forwarding distribution ip igmp snooping
```

Related Commands

Command	Description
test forwarding distribution perf	Tests the forwarding distribution performance of the Forwarding Information Base (FIB).

Review Draft -- Cisco Confidential

show ip igmp snooping

To display information about IGMP snooping, use the **show ip igmp snooping** command.

show ip igmp snooping [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN. The range is from 1 to 3967 and 4048 to 4093. The default is all VLANs.

Command Default

Displays all VLANs.

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information about IGMP snooping for a VLAN:

```
switch(config)# show ip igmp snooping vlan 20
IGMP Snooping information for vlan 20
  IGMP snooping enabled
  Optimised Multicast Flood (OMF) disabled
  IGMP querier none
  Switch-querier disabled
  IGMPv3 Explicit tracking enabled
  IGMPv2 Fast leave disabled
  IGMPv1/v2 Report suppression enabled
  IGMPv3 Report suppression disabled
  Link Local Groups suppression enabled
  Router port detection using PIM Hellos, IGMP Queries
  Number of router-ports: 1
  Number of groups: 0
  Active ports:
    Eth1/21     Po100
switch(config)#
```

Review Draft -- Cisco Confidential

show ip igmp snooping event-history

To display information in the IGMP snooping event history buffers, use the **show ip igmp snooping event-history** command.

show ip igmp snooping event-history {**vpc** | **igmp-snoop-internal** | **mfdm** | **mfdm-sum** | **vlan** | **vlan-events**}

Syntax Description

vpc	Displays the event history buffer of type virtual port channel (vPC).
igmp-snoop-internal	Displays the event history buffer of type IGMP snooping internal.
mfdm	Displays the event history buffer of type multicast FIB distribution (MFDM).
mfdm-sum	Displays the event history buffer of type MFDM sum.
vlan	Displays the event history buffer of type VLAN.
vlan-events	Displays the event history buffer of type VLAN events.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information in the IGMP snooping VLAN event history buffer:

```
switch(config)# show ip igmp snooping event-history vlan

 vlan Events for IGMP snoopprocess
2008 Apr 12 06:30:47.790031 igmp [4588]: : IGMPv3 proxy report: no routers found
2008 Apr 12 06:30:47.790012 igmp [4588]: : IGMPv3 proxy report: no records to se
nd
2008 Apr 12 06:30:47.789882 igmp [4588]: : IGMPv3 proxy report: no routers found
2008 Apr 12 06:30:47.789740 igmp [4588]: : IGMPv3 proxy report: no routers found
2008 Apr 12 06:30:47.789721 igmp [4588]: : IGMPv3 proxy report: no records to se
nd
2008 Apr 12 06:30:47.789584 igmp [4588]: : IGMPv3 proxy report: no routers found
2008 Apr 12 06:13:17.022028 igmp [4588]: : Received a STP Topology change notifi
cation, 1 vlans
2008 Apr 12 06:13:17.022023 igmp [4588]: : Received a STP Topology change notifi
cation
2008 Apr 12 06:13:15.022294 igmp [4588]: : Received a STP Topology change notifi
cation, 1 vlans
2008 Apr 12 06:13:15.022289 igmp [4588]: : Received a STP Topology change notifi
```

Review Draft -- Cisco Confidential

```
cation
2008 Apr 12 06:13:14.662417 igmp [4588]: : Received a STP Topology change notifi
cation, 1 vlans
2008 Apr 12 06:13:14.662412 igmp [4588]: : Received a STP Topology change notifi
cation
2008 Apr 12 06:13:12.642393 igmp [4588]: : Received a STP Topology change notifi
cation, 1 vlans
2008 Apr 12 06:13:12.642388 igmp [4588]: : Received a STP Topology change notifi
cation
2008 Apr 12 06:13:11.946051 igmp [4588]: : Received a STP Topology change notifi
cation, 1 vlans
2008 Apr 12 06:13:11.946046 igmp [4588]: : Received a STP Topology change notifi
cation
<--Output truncated-->
switch(config)#
```

Related Commands

Command	Description
ip igmp snooping event-history	Configures the size of the IGMP snooping event history buffers.
clear ip igmp snooping event-history	Clears information in the IGMP snooping event history buffers.

Review Draft -- Cisco Confidential

show ip igmp snooping explicit-tracking

To display information about explicit tracking for IGMP snooping, use the **show ip igmp snooping explicit-tracking** command.

show ip igmp snooping explicit-tracking [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN. The range is from 1 to 3967 and 4048 to 4093.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

When you use this command without the optional **vlan** argument, the system displays information for all VLANs.

This command does not require a license.

Examples

This example shows how to display information about explicit tracking for IGMP snooping for VLAN 33:

```
switch# show ip igmp snooping explicit-tracking vlan 33
```

Related Commands

Command	Description
clear ip igmp snooping explicit-tracking vlan	Clears the IGMP snooping explicit host tracking information for VLANs.
ip igmp snooping explicit-tracking	Enables tracking of IGMPv3 membership reports from individual hosts for each port on a VLAN.

Review Draft -- Cisco Confidential

show ip igmp snooping groups

To display information about the group membership for IGMP snooping, use the **show ip igmp snooping groups** command.

show ip igmp snooping groups [{*source* [*group*]} | {*group* [*source*]}] [**vlan** *vlan-id*] [**detail**]

Syntax Description

source	(Optional) Source address for route.
group	(Optional) Group address for route.
vlan *vlan-id*	(Optional) Specifies a VLAN. The range is from 1 to 3967 and 4048 to 4093.
detail	(Optional) Displays detailed information for the group.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information about the group membership for IGMP snooping:

```
switch(config)# show ip igmp snooping groups
TType: S - Static, D - Dynamic, R - Router port

Vlan  Group Address      Ver  Type  Port list
20    */*                -    R     Vlan20
switch(config)#
```

Review Draft -- Cisco Confidential

show ip igmp snooping mrouter

To display the multicast routers detected by IGMP snooping, use the **show ip igmp snooping mrouter** command.

show ip igmp snooping mrouter [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN. The range is from 1 to 3967 and 4048 to 4093.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display the multicast routers detected by IGMP snooping:

```
switch(config)# show ip igmp snooping mrouter
Type: S - Static, D - Dynamic, V - vPC Peer Link
Type: S - Static, D - Dynamic, V - vPC Peer Link, I - Internal
Vlan  Router-port   Type      Uptime      Expires
20    Vlan20        I         04:16:16    never (down)

switch(config)#
```

Review Draft -- Cisco Confidential

show ip igmp snooping querier

To display information about IGMP snooping queriers, use the **show ip igmp snooping querier** command.

show ip igmp snooping querier [**vlan** *vlan-id*]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN. The range is from 1 to 3967 and 4048 to 4093.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to display information about IGMP snooping queriers:

```
switch(config)# show ip igmp snooping querier
```

Review Draft -- Cisco Confidential

show ip igmp snooping statistics

To display information about IGMP snooping statistics, use the **show ip igmp snooping statistics** command.

show ip igmp snooping statistics [**vlan** *vlan-id* | **global**]

Syntax Description

vlan *vlan-id*	(Optional) Specifies a VLAN. The range is from 1 to 3967 and 4048 to 4093.
global	(Optional) Specifies the global statistics.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

When you use this command without any options, the system prints statistics for all VLANs.

This command does not require a license.

Examples

This example shows how to display information about IGMP snooping statistics for VLAN 1:

```
switch(config)# show ip igmp snooping statistics vlan 1
```

Review Draft -- Cisco Confidential

MSDP Commands

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

C Commands

This chapter describes the Cisco NX-OS MSDP commands that begin with C.

Review Draft -- Cisco Confidential

clear ip msdp event-history

To clear information in the Multicast Source Discovery Protocol (MSDP) event history buffers, use the **clear ip msdp event-history** command.

clear ip msdp event-history

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to clear information in the MSDP event history buffers:

```
switch(config)# clear ip msdp event-history
switch(config)#
```

Related Commands

Command	Description
ip msdp event-history	Configures the size of the MSDP event history buffers.
show ip msdp event-history	Displays information in the MSDP event history buffers.

Review Draft -- Cisco Confidential

clear ip msdp peer

To clear a TCP connection to Multicast Source Discovery Protocol (MSDP) peers, use the **clear ip msdp peer** command.

clear ip msdp peer *peer-address* [**vrf** *vrf-name* | **default** | **management**]

Syntax Description

peer-address	IP address of the MSDP peer.
vrf	(Optional) Clears the virtual routing and forwarding (VRF) instance information.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
default	Specifies that the default VRF entry be cleared from the multicast routing table.
management	Specifies that the management VRF entry be cleared from the multicast routing table.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to clear a TCP connection to an MSDP peer:

```
switch# clear ip msdp peer 192.168.1.10
switch#
```

Related Commands

Command	Description
show ip msdp peer	Displays information about MSDP peers.

Review Draft -- Cisco Confidential

clear ip msdp policy statistics sa-policy

To clear the Source-Active (SA) policy for Multicast Source Discovery Protocol (MSDP) peers, use the **clear ip msdp policy statistics sa-policy** command.

clear ip msdp policy statistics sa-policy *peer-address* {**in** | **out**} [**vrf** *vrf-name* | **default** | **management**]

Syntax Description

peer-address	IP address of the MSDP peer for the SA policy.
in	Specifies the input policy.
out	Specifies the output policy.
vrf	(Optional) Clears the virtual routing and forwarding (VRF) instance information.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
default	(Optional) Specifies that the default VRF entry be cleared from the multicast routing table.
management	(Optional) Specifies that the management VRF entry be cleared from the multicast routing table.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to clear an SA policy for an MSDP peer:

```
switch# clear ip msdp policy statistics sa-policy
switch#
```

Related Commands

Command	Description
show ip msdp peer	Displays information about MSDP peers.

Review Draft -- Cisco Confidential

clear ip msdp route

To clear routes that match group entries in the Multicast Source Discovery Protocol (MSDP) Source-Active (SA) cache, use the **clear ip msdp route** command.

clear ip msdp route {* | *group* | *group-prefix*} [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

*	Specifies all sources for the group from the SA cache.
group	Group address in the format *A.B.C.D*.
group-prefix	Group prefix in the format *A.B.C.D/length*.
vrf	(Optional) Clears the virtual routing and forwarding (VRF) instance information.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies that all VRF entries be cleared from the SA-cache.
default	Specifies that the default VRF entry be cleared from the SA-cache.
management	Specifies that the management VRF entry be cleared from the SA-cache.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You can also use the **clear ip msdp sa-cache** command for the same function.

This command requires the LAN Base Services license.

Examples

This example shows how to clear the MSDP SA cache:

```
switch# clear ip msdp route *
switch#
```

Related Commands

Command	Description
clear ip msdp sa-cache	Clears the MSDP SA cache.

Review Draft -- Cisco Confidential

clear ip msdp sa-cache

To clear routes that match group entries in the Multicast Source Discovery Protocol (MSDP) Source-Active (SA) cache, use the **clear ip msdp sa-cache** command.

clear ip msdp sa-cache {* | *group* | *group-prefix*} [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

*	Specifies all sources for the group from the SA cache.
group	Group address in the format *A.B.C.D*.
group-prefix	Group prefix in the format *A.B.C.D/length*.
vrf	(Optional) Clears the virtual routing and forwarding (VRF) instance information.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies that all VRF entries be cleared from the SA-cache.
default	Specifies that the default VRF entry be cleared from the SA-cache.
management	Specifies that the management VRF entry be cleared from the SA-cache.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You can also use the **clear ip msdp route** command for the same function.

This command requires the LAN Base Services license.

Examples

This example shows how to clear the MSDP SA cache:

```
switch# clear ip msdp sa-cache
switch#
```

Related Commands

Command	Description
clear ip msdp route	Clears the MSDP SA cache.
show ip msdp sa-cache	Displays route information in the MSDP Source-Active cache.

Review Draft -- Cisco Confidential

clear ip msdp statistics

To clear statistics for Multicast Source Discovery Protocol (MSDP) peers, use the **clear ip msdp statistics** command.

clear ip msdp statistics [*peer-address*] [**vrf** *vrf-name* | **default** | **management**]

Syntax Description

peer-address	(Optional) IP address of the MSDP peer.
vrf	(Optional) Clears the virtual routing and forwarding (VRF) instance information.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
default	(Optional) Specifies that the default VRF entry be cleared from the multicast routing table.
management	(Optional) Specifies that the management VRF entry be cleared from the multicast routing table.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to clear MSDP statistics for all MSDP peers:

```
switch# clear ip msdp statistics
switch#
```

Related Commands

Command	Description
show ip msdp peer	Displays information about MSDP peers.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

F Commands

This chapter describes the Cisco NX-OS MSDP commands that begin with F.

Review Draft -- Cisco Confidential

feature msdp

To enable Multicast Source Discovery Protocol (MSDP), use the **feature msdp** command. To disable PIM, use the **no** form of this command.

feature msdp

no feature msdp

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modified
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You must enable the MSDP feature before you can configure MSDP.

This command requires the LAN Base Services license.

Examples

This example shows how to enable a MSDP configuration:

```
switch(config)# feature msdp
switch(config#
```

Related Commands

Command	Description
show running-configuration msdp	Displays the MSDP running configuration information.
show feature	Displays the status of features on a switch.
ip msdp peer	Configures a MSDP peer.

Review Draft -- Cisco Confidential

I Commands

This chapter describes the Cisco NX-OS MSDP commands that begin with I.

Review Draft -- Cisco Confidential

ip msdp description

To configure a description for the Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp description** command. To remove the description for the peer, use the **no** form of this command.

ip msdp description *peer-address text*

no ip msdp description *peer-address* [*text*]

Syntax Description

peer-address	IP address of MSDP peer.
text	Text description.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to configure an MSDP peer description:

```
switch(config)# ip msdp description 192.168.1.10 engineering peer
```

This example shows how to remove an MSDP peer description:

```
switch(config)# no ip msdp description 192.168.1.10
```

Related Commands

Command	Description
show ip msdp peer	Displays information about MSDP peers.

Review Draft -- Cisco Confidential

ip msdp event-history

To configure the size of the Multicast Source Discovery Protocol (MSDP) event history buffers, use the **ip msdp event-history** command. To revert to the default buffer size, use the **no** form of this command.

ip msdp event-history {**cli** | **events** | **msdp-internal** | **routes** | **tcp**} **size** *buffer-size*

no ip msdp event-history {**cli** | **events** | **msdp-internal** | **routes** | **tcp**} **size** *buffer-size*

Syntax Description

cli	Configures the CLI event history buffer.
events	Configures the peer-events event history buffer.
msdp-internal	Configures the MSDP internal event history buffer.
routes	Configures the routes event history buffer.
tcp	Configures the TCP event history buffer.
size	Specifies the size of the buffer to allocate.
buffer-size	Buffer size that is one of the following values: **disabled**, **large**, **medium**, or **small**. The default buffer size is **small**.

Command Default

All history buffers are allocated as small.

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to configure the size of the MSDP event history buffer:

```
switch(config)# ip msdp event-history events size medium
switch(config)#
```

Related Commands

Command	Description
clear ip routing multicast event-history	Clears information in the IPv4 MRIB event history buffers.

Review Draft -- Cisco Confidential

Command	Description
show routing ip multicast event-history	Displays information in the IPv4 MRIB event history buffers.
show running-config msdp	Displays information about the running-system MSDP configuration.

Review Draft -- Cisco Confidential

ip msdp flush-routes

To flush routes when the Multicast Source Discovery Protocol (MSDP) process is restarted, use the **ip msdp flush-routes** command. To leave routes in place, use the **no** form of this command.

ip msdp flush-routes

no ip msdp flush-routes

Syntax Description

This command has no arguments or keywords.

Command Default

The routes are not flushed.

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

To display whether flush routes are configured, use this command line:

```
switch(config)# show running-config | include flush-routes
```

This command requires the LAN Base Services license.

Examples

This example shows how to configure flushing routes when the MSDP process is restarted:

```
switch(config)# ip msdp flush-routes
```

This example shows how to configure leaving routes when the MSDP process is restarted:

```
switch(config)# no ip msdp flush-routes
```

Related Commands

Command	Description
show running-config	Displays information about the running-system configuration.

Review Draft -- Cisco Confidential

ip msdp group-limit

To configure the Multicast Source Discovery Protocol (MSDP) maximum number of (S, G) entries that the software creates for the specified prefix, use the **ip msdp group-limit** command. To remove the group limit, use the **no** form of this command.

ip msdp group-limit *limit* **source** *prefix*

no ip msdp group-limit *limit* **source** *prefix*

Syntax Description

limit	Limit on number of groups. The range is from 0 to 4294967295. The default is no limit.
source *prefix*	Specifies the prefix to match sources against.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to configure the maximum number of (S, G) entries to create for a source:

```
switch(config)# ip msdp group-limit 4000 source 192.168.1.0/24
```

This example shows how to remove the limit entries to create:

```
switch(config)# no ip msdp group-limit 4000 source 192.168.1.0/24
```

Related Commands

Command	Description
show ip msdp sources	Displays information about the MSDP learned sources and group limit.

Review Draft -- Cisco Confidential

ip msdp keepalive

To configure a Multicast Source Discovery Protocol (MSDP) peer keepalive interval and timeout, use the **ip msdp keepalive** command. To reset the timeout and interval to the default, use the **no** form of this command.

ip msdp keepalive *peer-address interval timeout*

no ip msdp keepalive *peer-address* [*interval timeout*]

Syntax Description

peer-address	IP address of an MSDP peer.
interval	Keepalive interval in seconds. The range is from 1 to 60. The default is 60.
timeout	Keepalive timeout in seconds. The range is from 1 to 90. The default is 90.

Command Default

The keepalive interval is 60 seconds.
The keepalive timeout is 90 seconds.

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to configure an MSDP peer keepalive interval and timeout:

```
switch(config)# ip msdp keepalive 192.168.1.10 60 80
```

This example shows how to reset a keepalive interval and timeout to the default:

```
switch(config)# no ip msdp keepalive 192.168.1.10
```

Related Commands

Command	Description
show ip msdp peer	Displays information about MSDP peers.

Review Draft -- Cisco Confidential

ip msdp mesh-group

To configure a Multicast Source Discovery Protocol (MSDP) mesh group with a peer, use the **ip msdp mesh-group** command. To remove the peer from one or all mesh groups, use the **no** form of this command.

ip msdp mesh-group *peer-address name*

no ip msdp mesh-group *peer-address* [*name*]

Syntax Description

peer-address	IP address of an MSDP peer in a mesh group.
name	Name of a mesh group.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to configure a mesh group with a peer:

```
switch(config)# ip msdp mesh-group 192.168.1.10 my_admin_mesh
```

This example shows how to remove a peer from a mesh group:

```
switch(config)# no ip msdp mesh-group 192.168.1.10 my_admin_mesh
```

Related Commands

Command	Description
show ip msdp mesh-group	Displays information about MSDP mesh groups.

Review Draft -- Cisco Confidential

ip msdp originator-id

To configure the IP address used in the RP field of a Source-Active message entry, use the **ip msdp originator-id** command. To reset the value to the default, use the **no** form of this command.

ip msdp originator-id {**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number* | **vlan** *vlan-id*}

no ip msdp originator-id [{**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number* | **vlan** *vlan-id*}]

Syntax Description

ethernet *slot/port*	Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	Specifies the loopback interface. The loopback interface number is from 0 to 1023.
port-channel *number*	Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
vlan *vlan-id*	Specifies the VLAN interface. The range is from 1 to 4094.

Command Default

The MSDP process uses the RP address of the local system.

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to configure the IP address used in the RP field of SA messages:

```
switch(config)# ip msdp originator-id loopback0
```

This example shows how to reset the RP address to the default:

```
switch(config)# no ip msdp originator-id loopback0
```

Related Commands

Command	Description
show ip msdp summary	Displays a summary of MDSP information.

Review Draft -- Cisco Confidential

ip msdp password

To enable a Multicast Source Discovery Protocol (MSDP) MD5 password for the peer, use the **ip msdp password** command. To disable an MD5 password for a peer, use the **no** form of this command.

ip msdp password *peer-address password*

no ip msdp password *peer-address* [*password*]

Syntax Description

peer-address	IP address of an MSDP peer.
password	MD5 password.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to enable an MD5 password for a peer:

```
switch(config)# ip msdp password 192.168.1.10 my_password
```

This example shows how to disable an MD5 password for a peer:

```
switch(config)# no ip msdp password 192.168.1.10
```

Related Commands

Command	Description
show ip msdp peer	Displays MDSP peer information.

Review Draft -- Cisco Confidential

ip msdp peer

To configure a Multicast Source Discovery Protocol (MSDP) peer with the specified peer IP address, use the **ip msdp peer** command. To remove an MDSP peer, use the **no** form of this command.

ip msdp peer *peer-address* **connect-source** {**ethernet** *slot*/*port* | **loopback** *if_number* | **port-channel** *number* | **vlan** *vlan-id*} [**remote-as** *asn*]

no ip msdp peer *peer-address* [**connect-source** {**ethernet** *slot*/*port* | **loopback** *if_number* | **port-channel** *number* | **vlan** *vlan-id*}] [**remote-as** *asn*]

Syntax Description

peer-address	IP address of the MSDP peer.
connect-source	Configures a local IP address for a TCP connection.
ethernet *slot*/*port*	Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	Specifies the loopback interface. The loopback interface number is from 0 to 1023.
port-channel *number*	Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
vlan *vlan-id*	Specifies the VLAN interface. The range is from 1 to 4094.
remote-as *asn*	(Optional) Configures a remote autonomous system (AS) number.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The software uses the source IP address of the interface for the TCP connection with the peer. If the AS number is the same as the local AS, then the peer is within the Protocol Independent Multicast (PIM) domain; otherwise, this peer is external to the PIM domain.

This command requires the LAN Base Services license.

Examples

This example shows how to configure an MSDP peer:

```
switch(config)# ip msdp peer 192.168.1.10 connect-source ethernet 1/0 remote-as 8
```

This example shows how to remove an MSDP peer:

```
switch(config)# no ip msdp peer 192.168.1.10
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
show ip msdp summary	Displays a summary of MSDP information.

Review Draft -- Cisco Confidential

ip msdp reconnect-interval

To configure a reconnect interval for the TCP connection, use the **ip msdp reconnect-interval** command. To reset a reconnect interval to the default, use the **no** form of this command.

ip msdp reconnect-interval *interval*

no ip msdp reconnect-interval [*interval*]

Syntax Description

interval	Reconnect interval in seconds. The range is from 1 to 60. The default is 10.

Command Default

The reconnect interval is 10 seconds.

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to configure a reconnect interval for the TCP connection:

```
switch(config)# ip msdp reconnect-interval 20
```

This example shows how to reset a reconnect interval to the default:

```
switch(config)# no ip msdp reconnect-interval
```

Related Commands

Command	Description
show ip msdp peer	Displays information about MSDP peers.

Review Draft -- Cisco Confidential

ip msdp sa-interval

To configure the interval at which the software transmits Source-Active (SA) messages, use the **ip msdp sa-interval** command. To reset the interval to the default, use the **no** form of this command.

ip msdp sa-interval *interval*

no ip msdp sa-interval [*interval*]

Syntax Description

interval	SA transmission interval in seconds. The range is from from 60 to 65,535. The default is 60.

Command Default

The SA message interval is 60 seconds.

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

To display the SA interval configuration command, use this command line:

```
switch(config)# show running-config | include sa-interval
```

This command requires the LAN Base Services license.

Examples

This example shows how to configure an SA transmission interval:

```
switch(config)# ip msdp sa-interval 100
```

This example shows how to reset the interval to the default:

```
switch(config)# no ip msdp sa-interval
```

Related Commands

Command	Description
show running-config	Displays information about the running-system configuration.

Review Draft -- Cisco Confidential

ip msdp sa-limit

To configure a limit on the number of (S, G) entries accepted from the peer, use the **ip msdp sa-limit** command. To remove the limit, use the **no** form of this command.

ip msdp sa-limit *peer-address limit*

no ip msdp sa-limit *peer-address* [*limit*]

Syntax Description

peer-address	IP address of an MSDP peer.
limit	Number of (S, G) entries. The range is from 0 to 4294967295. The default is none.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to configure a Source-Active (SA) limit for a peer:

```
switch(config)# ip msdp sa-limit 192.168.1.10 5000
```

This example shows how to reset the limit to the default:

```
switch(config)# no ip msdp sa-limit 192.168.1.10
```

Related Commands

Command	Description
show ip msdp peer	Displays information about MSDP peers.

Review Draft -- Cisco Confidential

ip msdp sa-policy in

To enable filtering of incoming Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages, use the **ip msdp sa-policy in** command. To disable filtering, use the **no** form of this command.

ip msdp sa-policy *peer-address policy-name* **in**

no ip msdp sa-policy *peer-address policy-name* **in**

Syntax Description

peer-address	IP address of an MSDP peer.
policy-name	Route-map policy name.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to enable filtering of incoming SA messages:

```
switch(config)# ip msdp sa-policy 192.168.1.10 my_incoming_sa_policy in
```

This example shows how to disable filtering:

```
switch(config)# no ip msdp sa-policy 192.168.1.10 my_incoming_sa_policy in
```

Related Commands

Command	Description
show ip msdp peer	Displays information about MSDP peers.

Review Draft -- Cisco Confidential

ip msdp sa-policy out

To enable filtering of outgoing Source-Active (SA) messages, use the **ip msdp sa-policy out** command. To disable filtering, use the **no** form of this command.

ip msdp sa-policy *peer-address policy-name* **out**

no ip msdp sa-policy *peer-address policy-name* **out**

Syntax Description

peer-address	IP address of an MSDP peer.
policy-name	Route-map policy name.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to enable filtering of SA messages:

```
switch(config)# ip msdp sa-policy 192.168.1.10 my_incoming_sa_policy out
```

This example shows how to disable filtering:

```
switch(config)# no ip msdp sa-policy 192.168.1.10 my_incoming_sa_policy out
```

Related Commands

Command	Description
show ip msdp peer	Displays information about MSDP peers.

Review Draft -- Cisco Confidential

ip msdp shutdown

To shut down a Multicast Source Discovery Protocol (MSDP) peer, use the **ip msdp shutdown** command. To enable the peer, use the **no** form of this command.

ip msdp shutdown *peer-address*

no ip msdp shutdown *peer-address*

Syntax Description

peer-address	IP address of an MSDP peer.

Command Default

Enabled

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to disable an MSDP peer:

```
switch(config)# ip msdp shutdown 192.168.1.10
```

This example shows how to enable an MSDP peer:

```
switch(config)# no ip msdp shutdown 192.168.1.10
```

Related Commands

Command	Description
show ip msdp peer	Displays information about MSDP peers.

Review Draft -- Cisco Confidential

R Commands

This chapter describes the Cisco NX-OS MSDP commands that begin with R.

Review Draft -- Cisco Confidential

restart msdp

To restart the Multicast Source Discovery Protocol (MSDP) process, use the **restart msdp** command.

restart msdp

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to restart the MSDP process:

```
switch(config)# restart msdp
```

Related Commands

Command	Description
ip msdp flush-routes	Enables flushing routes when the MSDP process is restarted.

Review Draft -- Cisco Confidential

Show Commands

This chapter describes the Cisco NX-OS MSDP **show** commands.

Review Draft -- Cisco Confidential

show ip msdp count

To display information about Multicast Source Discovery Protocol (MSDP) counts, use the **show ip msdp count** command.

show ip msdp count [*asn*] [**vrf** {*vrf-name* | **all**}]

Syntax Description

asn	(Optional) Autonomous system (AS) number.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display MSDP counts:

```
switch(config)# show ip msdp count
```

Review Draft -- Cisco Confidential

show ip msdp event-history

To display information in the Multicast Source Discovery Protocol (MSDP) event history buffers, use the **show ip msdp event-history** command.

show ip msdp event-history {**errors** | **msgs** | **statistics**}

Syntax Description

errors	Displays events of type error.
msgs	Displays events of type msg.
statistics	Displays events of type statistics.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display information in the MSDP msgs event history buffer:

```
switch(config)# show ip msdp event-history msgs
```

Related Commands

Command	Description
clear ip msdp event-history	Clears the contents of the MSDP event history buffers.
ip msdp event-history	Configures the size of MSDP event history buffers.

Review Draft -- Cisco Confidential

show ip msdp mesh-group

To display information about Multicast Source Discovery Protocol (MSDP) mesh groups, use the **show ip msdp mesh-group** command.

show ip msdp mesh-group [*mesh-group*] [**vrf** {*vrf-name* | **all**}]

Syntax Description

mesh-group	(Optional) Mesh group name.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about MSDP mesh groups:

```
switch(config)# show ip msdp mesh-group
```

Review Draft -- Cisco Confidential

show ip msdp peer

To display information about Multicast Source Discovery Protocol (MSDP) peers, use the **show ip msdp peer** command.

show ip msdp peer [*peer-address*] [**vrf** {*vrf-name* | **all**}]

Syntax Description

peer-address	(Optional) IP address of an MSDP peer.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about MSDP peers:

```
switch(config)# show ip msdp peer
```

Review Draft -- Cisco Confidential

show ip msdp policy statistics sa-policy

To display information about Multicast Source Discovery Protocol (MSDP) Source-Active (SA) policies, use the **show ip msdp policy statistics sa-policy** command.

show ip msdp policy statistics sa-policy *peer-address* {**in** | **out**} [**vrf** {*vrf-name*}]

Syntax Description

peer-address	IP address of the MSDP peer for the SA policy.
in	Specifies the input policy.
out	Specifies the output policy.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about MSDP SA policies:

```
switch(config)# show ip msdp policy statistics sa-policy 192.168.1.10 in
```

Review Draft -- Cisco Confidential

show ip msdp route

To display information about the Multicast Source Discovery Protocol (MSDP) Source-Active (SA) cache, use the **show ip msdp route** command.

show ip msdp route [{*source* [*group*]} | {*group* [*source*]}] [*asn*] [**peer** *peer*] [**detail**] [**vrf** {*vrf-name* | **all**}]

Syntax Description

source	Source address for SA cache information.
group	(Optional) Group address for SA cache information.
asn	(Optional) Autonomous system (AS) number.
peer *peer*	(Optional) Specifies the IP address of a peer.
detail	(Optional) Displays detailed information.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **show ip msdp sa-cache** command is an alternative form of this command.

This command requires the LAN Base Services license.

Examples

This example shows how to display information about the MSDP SA cache:

```
switch(config)# show ip msdp route
```

Related Commands

Command	Description
clear ip msdp route	Clears routes in the MSDP Source-Active cache.
show ip msdp sa-cache	Displays information about the MSDP SA cache.

Review Draft -- Cisco Confidential

show ip msdp rpf

To display information about the Multicast Source Discovery Protocol (MSDP) next-hop autonomous system (AS) on the Border Gateway Protocol (BGP) path to a rendezvous point (RP) address, use the **show ip msdp rpf** command.

show ip msdp rpf *rp-address* [**vrf** {*vrf-name* **all**}]

Syntax Description

rp-address	IP address of the RP.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about MSDP reverse path forwarding (RPF) peers:

```
switch(config)# show ip msdp rpf 192.168.1.10
```

Review Draft -- Cisco Confidential

show ip msdp sa-cache

To display information about the Multicast Source Discovery Protocol (MSDP) Source-Active (SA) cache, use the **show ip msdp sa-cache** command.

show ip msdp sa-cache [{*source* [*group*]} | {*group* [*source*]}] [*asn*] [**peer** *peer*] [**detail**] [**vrf** {*vrf-name* | **all**}]

Syntax Description

source	Source address for SA cache information.
group	(Optional) Group address for SA cache information.
asn	(Optional) Autonomous system (AS) number.
peer *peer*	(Optional) Specifies the IP address of a peer.
detail	(Optional) Displays detailed information.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **show ip msdp route** command is an alternative form of this command.

This command requires the LAN Base Services license.

Examples

This example shows how to display information about the MSDP SA cache:

```
switch(config)# show ip msdp sa-cache
```

Related Commands

Command	Description
clear ip msdp sa-cache	Clears routes in the MSDP Source-Active cache.
show ip msdp route	Displays information about the MSDP SA cache.

Review Draft -- Cisco Confidential

show ip msdp route

To display information about the Multicast Source Discovery Protocol (MSDP) Source-Active (SA) route cache, use the **show ip msdp route** command.

show ip msdp route [{*source* [*group*]} | {*group* [*source*]}] [*asn*] [**peer** *peer*] [**detail**] [**vrf** {*vrf-name* | **all**}]

Syntax Description

source	Source address for SA cache information.
group	(Optional) Group address for SA cache information.
asn	(Optional) Autonomous system (AS) number.
peer *peer*	(Optional) Specifies the IP address of a peer.
detail	(Optional) Displays detailed information.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **show ip msdp route** command is an alternative form of this command.

This command requires the LAN Base Services license.

Examples

This example shows how to display information about the MSDP SA cache:

```
switch(config)# show ip msdp sa-cache
```

Related Commands

Command	Description
clear ip msdp sa-cache	Clears routes in the MSDP Source-Active cache.
show ip msdp route	Displays information about the MSDP SA cache.

Review Draft -- Cisco Confidential

show ip msdp sources

To display information about Multicast Source Discovery Protocol (MSDP) learned sources, use the **show ip msdp sources** command.

show ip msdp sources [**vrf** {*vrf-name* | **all**}]

Syntax Description

vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about MSDP learned sources:

```
switch(config)# show ip msdp sources
```

Review Draft -- Cisco Confidential

show ip msdp summary

To display summary information about Multicast Source Discovery Protocol (MSDP) peers, use the **show ip msdp summary** command.

show ip msdp summary [**vrf** {*vrf-name* | **all**}]

Syntax Description

vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display summary information about MSDP peers:

```
switch(config)# show ip msdp summary
```

Review Draft -- Cisco Confidential

show running-config msdp

To display information about the running-system configuration for Multicast Source Discovery Protocol (MSDP), use the **show running-config msdp** command.

show running-config msdp [**all**]

Syntax Description		
	all	(Optional) Displays configured and default information.

Command Default None

Command Modes Any command mode

Command History	Release	Modification
	6.0(2)N1(1)	This command was introduced.

Usage Guidelines This command requires the LAN Base Services license.

Examples This example shows how to display information about the MSDP running-system configuration:

Need new output[1]

```
switch(config)# show running-config msdp

!Command: show running-config msdp
!Time: Sat Apr 12 09:14:49 2008

version 5.0(3)N1(1)
feature msdp


switch(config)#
```

1.

Review Draft -- Cisco Confidential

show startup-config msdp

To display information about the startup-system configuration for Multicast Source Discovery Protocol (MSDP), use the **show startup-config msdp** command.

show startup-config msdp [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about the startup-system configuration for MSDP:

```
switch(config)# show startup-config msdp
```

Review Draft -- Cisco Confidential

PIM Commands

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

C Commands

This chapter describes the Cisco NX-OS PIM commands that begin with C.

Review Draft -- Cisco Confidential

clear ip mroute

To clear the multicast routing table, use the **clear ip mroute** command.

clear ip mroute {* | *group* [*source*] | *group-prefix*} [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

*	Specifies all routes.
group	Group address in the format *A.B.C.D*.
source	(Optional) Source (S, G) route.
group-prefix	Group prefix in the format *A.B.C.D/length*.
vrf	(Optional) Clears the virtual routing and forwarding (VRF) instance information.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies that all VRF entries be cleared from the multicast routing table.
default	Specifies that the default VRF entry be cleared from the multicast routing table.
management	Specifies that the management VRF entry be cleared from the multicast routing table.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **clear routing multicast** command is an alternative form of this command.

Examples

This example shows how to clear the multicast routing table:

```
switch(config)# clear ip mroute *
switch(config)#
```

Related Commands

Command	Description
clear routing multicast	Clears the multicast routing table
show ip mroute	Displays information about the multicast routing table.

Review Draft -- Cisco Confidential

clear ip pim event-history

To clear information in the IPv4 Protocol Independent Multicast (PIM) event history buffers, use the **clear ip pim event-history** command.

clear ip pim event-history

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to clear information in the PIM event history buffers:

```
switch(config)# clear ip pim event-history
switch(config)#
```

Related Commands

Command	Description
ip pim event-history	Configures the size of the PIM event history buffers.
show ip pim event-history	Displays information in the PIM event history buffers.

Review Draft -- Cisco Confidential

clear ip pim interface statistics

To clear Protocol Independent Multicast (PIM) counters for a specified interface, use the **clear ip pim interface statistics** command.

clear ip pim interface statistics [**ethernet** *slot/port* | **port-channel** *channel-number*[*.sub_if-number*] | **vlan** *vlan-id*]

Syntax Description

ethernet *slot/port*	(Optional) Specifies the Ethernet interface. The slot number is from 1 to 255, and the port number is from 1 to 128.
port-channel *number*	(Optional) Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
sub_if-number	(Optional) Subinterface number. The range is from 1 to 4093.
vlan *vlan-id*	(Optional) Specifies the VLAN. The range is from 1 to 4094.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to clear the PIM counters for a specified interface:

```
switch# clear ip pim interface statistics ethernet 2/1
switch#
```

Related Commands

Command	Description
show ip pim statistics	Displays PIM statistics.

Review Draft -- Cisco Confidential

clear ip pim policy statistics

To clear Protocol Independent Multicast (PIM) policy counters, use the **clear ip pim policy statistics** command.

clear ip pim policy statistics {**jp-policy** | **neighbor-policy**} {**ethernet** *slot/port* | **port-channel** *channel-number*[*.sub_if-number*] | **vlan** *vlan-id*}

clear ip pim policy statistics register-policy [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

jp-policy	Specifies statistics for the join-prune policy.
neighbor-policy	Specifies statistics for the neighbor policy.
ethernet *slot/port*	Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
port-channel *number*	Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
sub_if-number	(Optional) Subinterface number. The range is from 1 to 4093.
vlan	Specifies the VLAN.
vlan-id	VLAN number. The range is from 1 to 4094.
register-policy	Specifies statistics for the register policy.
vrf	(Optional) Clears the virtual routing and forwarding (VRF) instance information.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies that all VRF entries be cleared from the IPv4 multicast routing table.
default	Specifies that the default VRF entry be cleared from the IPv4 multicast routing table.
management	Specifies that the management VRF entry be cleared from the IPv4 multicast routing table.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to clear PIM register policy counters:

```
switch# clear ip pim policy statistics register-policy
```

Review Draft -- Cisco Confidential

```
switch#
```

Related Commands

Command	Description
show ip pim policy statistics	Displays PIM policy statistics.

Review Draft -- Cisco Confidential

clear ip pim route

To clear routes specific to Protocol Independent Multicast (PIM) for IPv4, use the **clear ip pim route** command.

clear ip pim route {* | *group* [*source*] | *group-prefix*} [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

*	Specifies all routes.
group	Group address in the format *A.B.C.D*.
source	(Optional) Source (S, G) route.
group-prefix	Group prefix in the format *A.B.C.D/length*.
vrf	(Optional) Clears the virtual routing and forwarding (VRF) instance information.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies that all VRF entries be cleared from the multicast routing table.
default	Specifies that the default VRF entry be cleared from the multicast routing table.
management	Specifies that the management VRF entry be cleared from the multicast routing table.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to clear the all the routes specific to PIM:

```
switch(config)# clear ip pim route *
switch(config)#
```

Related Commands

Command	Description
show ip pim route	Displays information about PIM specific routes.

Review Draft -- Cisco Confidential

clear ip pim statistics

To clear Protocol Independent Multicast (PIM) statistics counters, use the **clear ip pim statistics** command.

clear ip pim statistics [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

vrf	(Optional) Clears the virtual routing and forwarding (VRF) instance information.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies that all VRF entries be cleared from the multicast routing table.
default	Specifies that the default VRF entry be cleared from the multicast routing table.
management	Specifies that the management VRF entry be cleared from the multicast routing table.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to clear PIM statistics counters:

```
switch# clear ip pim statistics
switch#
```

Related Commands

Command	Description
show ip pim statistics	Displays PIM statistics.

Review Draft -- Cisco Confidential

clear ip routing multicast event-history

To clear information in the IPv4 Multicast Routing Information Base (MRIB) event history buffers, use the **clear ip routing multicast event-history** command.

clear ip routing multicast event-history {**cli** | **mfdm-debugs** | **mfdm-events** | **mfdm-stats** | **rib** | **vrf**}

Syntax Description

cli	Clears the CLI event history buffer.
mfdm-debugs	Clears the multicast FIB distribution (MFDM) debug history buffer.
mfdm-events	Clears the MFDM events history buffer.
mfdm-stats	Clears the MFDM sum event history buffer.
rib	Clears the RIB event history buffer.
vrf	Clears the virtual routing and forwarding (VRF) event history buffer.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to clear information in the MRIB RIB event history buffer:

```
switch(config)# clear ip routing multicast event-history rib
switch(config)#
```

Related Commands

Command	Description
ip routing multicast event-history	Configures the size of the IPv4 MRIB event history buffers.
show routing ip multicast event-history	Displays information in the IPv4 MRIB event history buffers.

Review Draft -- Cisco Confidential

clear routing multicast

To clear the IPv4 multicast routing table, use the **clear routing multicast** command.

clear routing [**ip** | **ipv4**] **multicast** {* | *group* [*source*] | *group-prefix*} [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

ip	(Optional) Clears IP commands.
ipv4	(Optional) Clears IPv4 commands.
*	Specifies all routes.
group	Group address in the format *A.B.C.D*.
source	(Optional) Source (S, G) route.
group-prefix	Group prefix in the format *A.B.C.D/length*.
vrf	(Optional) Clears the virtual routing and forwarding (VRF) instance information.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies that all VRF entries be cleared from the IPv4 multicast routing table.
default	Specifies that the default VRF entry be cleared from the IPv4 multicast routing table.
management	Specifies that the management VRF entry be cleared from the IPv4 multicast routing table.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **clear ip mroute** command is an alternative form of this command.

This command does not require a license.

Examples

This example shows how to clear the IPv4 multicast routing table:

```
switch(config)# clear routing multicast *
switch(config)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
clear ip mroute	Clears the multicast routing table.
show routing ip multicast	Displays information about IPv4 multicast routes.

Review Draft -- Cisco Confidential

Review Draft -- Cisco Confidential

F Commands

This chapter describes the Cisco NX-OS PIM commands that begin with F.

Review Draft -- Cisco Confidential

feature pim

To enable Protocol Independent Multicast (PIM), use the **feature pim** command. To disable PIM, use the **no** form of this command.

feature pim

no feature pim

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode

Command History

Release	Modified
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You must enable the PIM feature before you can configure PIM.

This command requires the LAN Base Services license.

Examples

This example shows how to enable a PIM configuration:

```
switch(config)# feature pim
switch(config#
```

Related Commands

Command	Description
show running-configuration pim	Displays the PIM running configuration information.
show feature	Displays the status of features on a switch.
ip pim sparse-mode	Enables IPv4 PIM sparse mode on an interface.

Review Draft -- Cisco Confidential

H Commands

This chapter describes the Cisco NX-OS PIM commands that begin with H.

Review Draft -- Cisco Confidential

hardware profile multicast max-limit

To set the maximum number of entries in the multicast routing table, use the **hardware profile multicast max-limit** command.

hardware profile multicast max-limit *max-entries*

Syntax Description

max-entries	Maximum number of entries in the multicast routing table. The range is from 0 to 16000.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to set the maximum number of entries in the multicast routing table to 3000:

```
switch(config)# hardware profile multicast max-limit 3000
Warning!!: The multicast and /32 unicast route limits have been changed.
           Any route exceeding the limit may get dropped.
switch(config)#
```

Related Commands

Command	Description
show hardware profile status	Displays information about the multicast routing table limits.

Review Draft -- Cisco Confidential

I Commands

This chapter describes the Cisco NX-OS PIM commands that begin with I.

Review Draft -- Cisco Confidential

ip mroute

To configure multicast reverse path forwarding (RPF) static routes, use the **ip mroute** command. To remove RPF static routes, use the **no** form of this command.

ip mroute {*ip-addr ip-mask* | *ip-prefix*} {{*next-hop* | *nh-prefix*} | {**ethernet** *slot*/*port* | **loopback** *if_number* | **port-channel** *number* | **vlan** *vlan-id*}} [*pref*] [**vrf** *vrf-name*]

no ip mroute {*ip-addr ip-mask* | *ip-prefix*} {{*next-hop* | *nh-prefix*} | {**ethernet** *slot*/*port* | **loopback** *if_number* | **port-channel** *number* | **vlan** *vlan-id*}} [*pref*] [**vrf** *vrf-name*]

Syntax Description

ip-addr	IP prefix in the format i.i.i.i.
ip-mask	IP network mask in the format m.m.m.m.
ip-prefix	IP prefix and network mask length in the format x.x.x.x/m.
next-hop	IP next-hop address in the format i.i.i.i.
nh-prefix	IP next-hop prefix in the format i.i.i.i/m.
ethernet *slot*/*port*	Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	Specifies the loopback interface. The loopback interface number is from 0 to 1023.
port-channel *number*	Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
vlan *vlan-id*	Specifies the VLAN interface. The range is from 1 to 4094.
pref	(Optional) Route preference. The range is from 1 to 255. The default is 1.
vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) context name. The name can be any case-sensitive, alphanumeric string up to 32 characters.

Command Default

The route preference is 1.

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure an RPF static route:

```
switch(config)# ip mroute 192.0.2.33/24 192.0.2.1
switch(config)#
```

Review Draft -- Cisco Confidential

This example shows how to remove an RPF static route:

```
switch(config)# no ip mroute 192.0.2.33/24 192.0.2.1
switch(config)#
```

Related Commands

Command	Description
show ip mroute	Displays information about multicast routes.

Review Draft -- Cisco Confidential

ip pim anycast-rp

To configure an IPv4 Protocol Independent Multicast (PIM) Anycast-RP peer for the specified Anycast-RP address, use the **ip pim anycast-rp** command. To remove the peer, use the **no** form of this command.

ip pim anycast-rp *anycast-rp rp-addr*

no ip pim anycast-rp *anycast-rp rp-addr*

Syntax Description

anycast-rp	Anycast-RP address of the peer.
rp-addr	Address of RP in the Anycast-RP set.

Command Default

None

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Each command with the same Anycast-RP address forms an Anycast-RP set. The IP addresses of RPs are used for communication with RPs in the set.

This command requires the LAN Base Services license.

Examples

This example shows how to configure a PIM Anycast-RP peer:

```
switch# configure terminal
switch(config)# ip pim anycast-rp 192.0.2.3 192.0.2.31
```

This example shows how to remove a peer:

```
switch# configure terminal
switch(config)# no ip pim anycast-rp 192.0.2.3 192.0.2.31
```

Related Commands

Command	Description
show ip pim rp	Displays information about PIM RPs.

Review Draft -- Cisco Confidential

ip pim auto-rp

To enable Protocol Independent Multicast (PIM) listening and forwarding of Auto-RP messages, use the **ip pim auto-rp listen** and **ip pim auto-rp forward** commands. To disable the listening and forwarding of Auto-RP messages, use the **no** form of this command.

ip pim auto-rp {**listen** [**forward**] | **forward** [**listen**]}

no ip pim auto-rp [{**listen** [**forward**] | **forward** [**listen**]}]

Syntax Description

listen	Specifies to listen to Auto-RP messages.
forward	Specifies to forward Auto-RP messages.

Command Default

Disabled

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to enable listening and forwarding of Auto-RP messages:

```
switch(config)# ip pim auto-rp listen forward
```

This example shows how to disable listening and forwarding of Auto-RP messages:

```
switch(config)# no ip pim auto-rp listen forward
```

Related Commands

Command	Description
show ip pim rp	Displays information about PIM RPs.

Review Draft -- Cisco Confidential

ip pim auto-rp mapping-agent

To configure the router as an IPv4 Protocol Independent Multicast (PIM) Auto-RP mapping agent that sends RP-Discovery messages, use the **ip pim auto-rp mapping-agent** command. To remove the mapping agent configuration, use the **no** form of this command.

ip pim auto-rp mapping-agent {**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number* | **vlan** *vlan-id*} [**scope** *ttl*]

no ip pim auto-rp mapping-agent [{**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number* | **vlan** *vlan-id*}] [**scope** *ttl*]

Syntax Description

ethernet *slot/port*	Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	Specifies the loopback interface. The loopback interface number is from 0 to 1023.
port-channel *number*	Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
vlan *vlan-id*	Specifies the VLAN interface. The range is from 1 to 4094.
scope *ttl*	(Optional) Specifies the time-to-live (TTL) value for the scope of Auto-RP Discovery messages. The range is from 1 to 255. The default is 32. **Note** See the **ip pim border** command to explicitly define a router on the edge of a PIM domain rather than using the **scope** argument.

Command Default

The TTL is 32.

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **ip pim send-rp-discovery** command is an alternative form of this command.

This command requires the LAN Base Services license.

Examples

This example shows how to configure an Auto-RP mapping agent:

```
switch(config)# ip pim auto-rp mapping-agent ethernet 2/1
```

This example shows how to remove the Auto-RP mapping agent configuration:

```
switch(config)# no ip pim auto-rp mapping-agent ethernet 2/1
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
ip pim border	Configures a router to be on the edge of a PIM domain.
ip pim send-rp-discovery	Configures a router as an Auto-RP mapping agent.
show ip pim rp	Displays information about PIM RPs.

Review Draft -- Cisco Confidential

ip pim auto-rp mapping-agent-policy

To enable filtering of IPv4 IPv4 Protocol Independent Multicast (PIM) Auto-RP Discover messages, use the **ip pim auto-rp mapping-agent-policy** command. To disable filtering, use the **no** form of this command.

ip pim auto-rp mapping-agent-policy *policy-name*

no ip pim auto-rp mapping-agent-policy [*policy-name*]

Syntax Description

policy-name	Route-map policy name.

Command Default

Disabled

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command can be used on client routers where you can specify mapping agent addresses.

You can specify mapping agent source addresses to filter messages from with the **match ip multicast** command in a route-map policy.

This command requires the LAN Base Services license.

Examples

This example shows how to enable a route-map policy to filter Auto-RP Discover messages:

```
switch(config)# ip pim auto-rp mapping-agent-policy my_mapping_agent_policy
```

This example shows how to disable filtering:

```
switch(config)# no ip pim auto-rp mapping-agent-policy
```

Related Commands

Command	Description
show ip pim rp	Displays information about PIM RPs.

Review Draft -- Cisco Confidential

ip pim auto-rp rp-candidate

To configure an IPv4 Protocol Independent Multicast (PIM) Auto-RP candidate route processor (RP), use the **ip pim auto-rp rp-candidate** command. To remove an Auto-RP candidate RP, use the **no** form of this command.

ip pim auto-rp rp-candidate {**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number* | **vlan** *vlan-id*} {**group-list** *prefix*} {[**scope** *ttl*] | [**interval** *interval*] }

no ip pim auto-rp rp-candidate [{**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number* | **vlan** *vlan-id*}] [**group-list** *prefix*} {[**scope** *ttl*] | [**interval** *interval*]}

Syntax Description

ethernet *slot/port*	Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	Specifies the loopback interface. The loopback interface number is from 0 to 1023.
port-channel *number*	Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
vlan *vlan-id*	Specifies the VLAN interface. The range is from 1 to 4094.
group-list *prefix*	Specifies the group range used for the access list.
scope *ttl*	(Optional) Specifies a time-to-live (TTL) value for the scope of Auto-RP Announce messages. The range is from 1 to 255. The default is 32. **Note** See the **ip pim border** command to explicitly define a router on the edge of a PIM domain rather than using the **scope** argument.
interval *interval*	(Optional) Specifies an Auto-RP Announce message transmission interval in seconds. The range is from 1 to 65,535. The default is 60.

Command Default

The TTL is 32.
The Announce message interval is 60 seconds

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **scope** and **interval** keywords can be entered once and in any order.

The **ip pim send-rp-announce** command is an alternative form of this command.

Using a route map, you can add group ranges that this auto RP candidate-RP can serve.

Review Draft -- Cisco Confidential

Note Use the same configuration guidelines for the route-map auto-rp-range that you used when you create a route map for static RPS.

This command requires the LAN Base Services license.

Examples

This example shows how to configure a PIM Auto-RP candidate RP:

```
switch(config)# ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24
```

This example shows how to remove a PIM Auto-RP candidate RP:

```
switch(config)# no ip pim auto-rp rp-candidate ethernet 2/1 group-list 239.0.0.0/24
```

Related Commands

Command	Description
ip pim send-rp-announce	Configures a PIM Auto-RP candidate RP.
show ip pim interface	Displays information about PIM-enabled interfaces.

Review Draft -- Cisco Confidential

ip pim auto-rp rp-candidate-policy

To allow the Auto-RP mapping agents to filter IPv4 Protocol Independent Multicast (PIM) Auto-RP Announce messages that are based on a route-map policy, use the **ip pim auto-rp rp-candidate-policy** command. To disable filtering, use the **no** form of this command.

ip pim auto-rp rp-candidate-policy *policy-name*

no ip pim auto-rp rp-candidate-policy [*policy-name*]

Syntax Description

policy-name	Route-map policy name.

Command Default

Disabled

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You can specify the RP and group addresses, and whether the type is ASM with the **match ip multicast** command in a route-map policy.

This command requires the LAN Base Services license.

Examples

This example shows how to allow the Auto-RP mapping agents to filter Auto-RP Announce messages:

```
switch(config)# ip pim auto-rp rp-candidate-policy my_policy
```

This example shows how to disable filtering:

```
switch(config)# no ip pim auto-rp rp-candidate-policy
```

Related Commands

Command	Description
show ip pim rp	Displays information about PIM RPs.

Review Draft -- Cisco Confidential

ip pim bidir-rp-limit

To configure the number of bidirectional (Bidir) RPs for use in IPv4 Protocol Independent Multicast (PIM), use the **ip pim bidir-rp-limit** command. To reset the number of RPs to the default, use the **no** form of this command.

ip pim bidir-rp-limit *limit*

no ip pim bidir-rp-limit *limit*

Syntax Description

limit	Limit for the number of Bidir RPs permitted in PIM. The range is from 0 to 8. The default is 6.

Defaults

The Bidir RP limit is 6.

Command Modes

Global configuration (config)
VRF configuration (config-vrf)

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Because the maximum ordinal count of designated forwarders (DFs) is 8, the PIM and IPv6 PIM RP limits should be no more than 8.

To display the Bidir RP limit configured, use this command line:

```
switch(config)# show running-config | include bidir
```

This command requires the Enterprise Services license.

Examples

This example shows how to configure the number of Bidir RPs:

```
switch(config)# ip pim bidir-rp-limit 6
```

This example shows how to reset the number of Bidir RPs to the default:

```
switch(config)# no ip pim bidir-rp-limit 6
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
show running-config	Displays information about the running-system configuration.

Review Draft -- Cisco Confidential

ip pim border

To configure an interface on an IPv4 Protocol Independent Multicast (PIM) border, use the **ip pim border** command. To remove an interface from a PIM border, use the **no** form of this command.

ip pim border

no ip pim border

Syntax Description

This command has no arguments or keywords.

Command Default

The interface is not on a PIM border.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to configure an interface on a PIM border:

```
switch(config)# ip pim border
```

This example shows how to remove an interface from a PIM border:

```
switch(config)# no ip pim border
```

Related Commands

Command	Description
show ip pim interface	Displays information about PIM-enabled interfaces.

Review Draft -- Cisco Confidential

ip pim bsr bsr-policy

To allow the bootstrap router (BSR) client routers to filter IPv4 Protocol Independent Multicast (PIM) BSR messages that are based on a route-map policy, use the **ip pim bsr bsr-policy** command. To disable filtering, use the **no** form of this command.

ip pim bsr bsr-policy *policy-name*

no ip pim bsr bsr-policy [*policy-name*]

Syntax Description

policy-name	Route-map policy name.

Command Default

Disabled

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You can specify which source addresses to filter messages from with the **match ip multicast** command in a route-map policy.

This command requires the LAN Base Services license.

Examples

This example shows how to allow the BSR client routers to filter BSR messages:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip pim bsr bsr-policy my_bsr_policy
```

This example shows how to disable filtering:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip pim bsr bsr-policy
```

Related Commands

Command	Description
show ip pim rp	Displays information about PIM RPs.

Review Draft -- Cisco Confidential

ip pim bsr-candidate

To configure the router as an IPv4 Protocol Independent Multicast (PIM) bootstrap router (BSR) candidate, use the **ip pim bsr-candidate** command. To remove a router as a BSR candidate, use the **no** form of this command.

ip pim [**bsr**] **bsr-candidate** {**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number* | **vlan** *vlan-id*} [**hash-len** *hash-len*] [**priority** *priority*]

no ip pim [**bsr**] **bsr-candidate** [{**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number* | **vlan** *vlan-id*}] [**hash-len** *hash-len*] [**priority** *priority*]

Syntax Description

bsr	(Optional) Specifies the BSR protocol RP-distribution configuration.
ethernet *slot/port*	Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	Specifies the loopback interface. The loopback interface number is from 0 to 1023.
port-channel *number*	Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
vlan *vlan-id*	Specifies the VLAN interface. The range is from 1 to 4094.
hash-len *hash-len*	(Optional) Specifies the hash mask length used in BSR messages. The range is from 0 to 32. The default is 30.
priority *priority*	(Optional) Specifies the BSR priority used in BSR messages. The range is from 0 to 255. The default is 64.

Command Default

The hash mask length is 30.
The BSR priority is 64.

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The interface specified is used to derive the BSR source IP address used in BSR messages.

This command requires the LAN Base Services license.

Examples

This example shows how to configure a router as a BSR candidate:

```
switch(config)# ip pim bsr-candidate ethernet 2/2
```

This example shows how to remove a router as a BSR candidate:

Review Draft -- Cisco Confidential

```
switch(config)# no ip pim bsr-candidate
```

Related Commands

Command	Description
show ip pim rp	Displays information about PIM RPs.

Review Draft -- Cisco Confidential

ip pim bsr forward

To listen to and forward IPv4 Protocol Independent Multicast (PIM) bootstrap router (BSR) and Candidate-RP messages, use the **ip pim bsr forward** command. To disable listening and forwarding, use the **no** form of this command.

ip pim bsr forward [**listen**]

no ip pim bsr [**forward** [**listen**]]

Syntax Description

forward	Specifies to forward BSR and Candidate-RP messages.
listen	(Optional) Specifies to listen to BSR and Candidate-RP messages.

Command Default

Disabled

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

A router configured as either a candidate RP or a candidate BSR will automatically listen to and forward all BSR protocol messages, unless an interface is configured with the domain border feature.

The **ip pim bsr listen** command is an alternative form of this command.

This command requires the LAN Base Services license.

Examples

This example shows how to forward BSR and Candidate-RP messages:

```
switch(config)# ip pim bsr forward
```

This example shows how to disable forwarding:

```
switch(config)# no ip pim bsr forward
```

Related Commands

Command	Description
ip pim bsr listen	Enables listening to and forwarding of BSR messages.
show ip pim rp	Displays information about PIM RPs.

Review Draft -- Cisco Confidential

ip pim bsr listen

To listen to and forward IPv4 Protocol Independent Multicast (PIM) bootstrap router (BSR) and Candidate-RP messages, use the **ip pim bsr listen** command. To disable listening and forwarding, use the **no** form of this command.

ip pim bsr listen [**forward**]

no ip pim bsr [**listen** [**forward**]]

Syntax Description

listen	Specifies to listen to BSR and Candidate-RP messages.
forward	(Optional) Specifies to forward BSR and Candidate-RP messages.

Command Default

Disabled

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

A router configured as either a candidate RP or a candidate BSR will automatically listen to and forward all BSR protocol messages, unless an interface is configured with the domain border feature.

The **ip pim bsr forward** command is an alternative form of this command.

This command requires the LAN Base Services license.

Examples

This example shows how to listen to and forward BSR and Candidate-RP messages:

```
switch(config)# ip pim bsr listen forward
```

This example shows how to disable listening and forwarding:

```
switch(config)# no ip pim bsr listen forward
```

Related Commands

Command	Description
ip pim bsr forward	Enables listening to and forwarding of BSR messages.
show ip pim rp	Displays information about PIM RPs.

Review Draft -- Cisco Confidential

ip pim bsr rp-candidate-policy

To filter IPv4 Protocol Independent Multicast (PIM) bootstrap router (BSR) Candidate-RP messages that are based on a route-map policy, use the **ip pim bsr rp-candidate-policy** command. To disable filtering, use the **no** form of this command.

ip pim bsr rp-candidate-policy *policy-name*

no ip pim bsr rp-candidate-policy [*policy-name*]

Syntax Description

policy-name	Route-map policy name.

Command Default

Disabled

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You can specify the RP and group addresses, and whether the type is ASM with the **match ip multicast** command in a route-map policy.

This command requires the LAN Base Services license.

Examples

This example shows how to filter Candidate-RP messages:

```
switch(config)# ip pim bsr rp-candidate-policy my_bsr_rp_candidate_policy
```

This example shows how to disable message filtering:

```
switch(config)# no ip pim bsr rp-candidate-policy
```

Related Commands

Command	Description
show ip pim rp	Displays information about PIM RPs.

Review Draft -- Cisco Confidential

ip pim dr-priority

To configure the designated router (DR) priority that is advertised in IPv4 Protocol Independent Multicast (PIM) hello messages, use the **ip pim dr-priority** command. To reset the DR priority to the default, use the **no** form of this command.

ip pim dr-priority *priority*

no ip pim dr-priority [*priority*]

Syntax Description

priority	Priority value. The range is from 1 to 4294967295. The default is 1.

Command Default

The DR priority is 1.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to configure DR priority on an interface:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip pim dr-priority 5
```

This example shows how to reset DR priority on an interface to the default:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip pim dr-priority
```

Related Commands

Command	Description
show ip pim interface	Displays information about PIM-enabled interfaces.

Review Draft -- Cisco Confidential

ip pim event-history

To configure the size of the IPv4 Protocol Independent Multicast (PIM) event history buffers, use the **ip pim event-history** command. To revert to the default buffer size, use the **no** form of this command.

ip pim event-history {**assert-receive** | **cli** | **hello** | **join-prune** | **null-register** | **packet** | **pim-internal** | **rp** | **vrf**} **size** *buffer-size*

no ip pim event-history {**assert-receive** | **cli** | **hello** | **join-prune** | **null-register** | **packet** | **pim-internal** | **rp** | **vrf**} **size** *buffer-size*

Syntax Description

assert-receive	Configures the assert receive event history buffer.
cli	Configures the CLI event history buffer.
hello	Configures the hello event history buffer.
join-prune	Configures the join-prune event history buffer.
null-register	Configures the null register event history buffer.
packet	Configures the packet event history buffer.
pim-internal	Configures the PIM internal event history buffer.
rp	Configures the rendezvous point (RP) event history buffer.
vrf	Configures the virtual routing and forwarding (VRF) event history buffer.
size	Specifies the size of the buffer to allocate.
buffer-size	Buffer size is one of the following values: **disabled**, **large**, **medium**, or **small**. The default buffer size is **small**.

Command Default

All history buffers are allocated as small.

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to configure the size of the PIM hello event history buffer:

```
switch(config)# ip pim event-history hello size medium
switch(config)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
clear ip pim event-history	Clears information in the IPv4 PIM event history buffers.
show ip pim event-history	Displays information in the IPv4 PIM event history buffers.
show running-config pim	Displays information about the running-system PIM configuration.

Review Draft -- Cisco Confidential

ip pim flush-routes

To remove routes when the IPv4 Protocol Independent Multicast (PIM) process is restarted, use the **ip pim flush-routes** command. To leave routes in place, use the **no** form of this command.

ip pim flush-routes

no ip pim flush-routes

Syntax Description

This command has no arguments or keywords.

Command Default

The routes are not flushed.

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

To display whether flush routes are configured, use this command line:

```
switch(config)# show running-config | include flush-routes
```

This command requires the LAN Base Services license.

Examples

This example shows how to remove routes when the PIM process is restarted:

```
switch(config)# ip pim flush-routes
```

This example shows how to leave routes in place when the PIM process is restarted:

```
switch(config)# no ip pim flush-routes
```

Related Commands

Command	Description
show running-config	Displays information about the running-system configuration.

Review Draft -- Cisco Confidential

ip pim hello-authentication ah-md5

To enable an MD5 hash authentication key in IPv4 Protocol Independent Multicast (PIM) hello messages, use the **ip pim hello-authentication ah-md5** command. To disable hello-message authentication, use the **no** form of this command.

ip pim hello-authentication ah-md5 *auth-key*

no ip pim hello-authentication ah-md5 [*auth-key*]

Syntax Description

auth-key	MD5 authentication key. You can enter an unencrypted (cleartext) key, or one of these values followed by a space and the MD5 authentication key: • 0—Specifies an unencrypted (cleartext) key • 3—Specifies a 3-DES encrypted key • 7—Specifies a Cisco Type 7 encrypted key The key can be from 1 to 16 characters.

Command Default

Disabled

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

Triple Data Encryption Standard (3-DES) is a strong form of encryption (168-bit) that allows sensitive information to be transmitted over untrusted networks. Cisco Type 7 encryption uses the algorithm from the Vigenère cipher.

This command requires the LAN Base Services license.

Examples

This example shows how to enable a 3-DES encrypted key for PIM hello-message authentication:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip pim hello-authentication-ah-md5 3 myauthkey
```

This example shows how to disable PIM hello-message authentication:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip pim hello-authentication-ah-md5
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
show ip pim interface	Displays information about PIM-enabled interfaces.

Review Draft -- Cisco Confidential

ip pim hello-interval

To configure the IPv4 Protocol Independent Multicast (PIM) hello-message interval on an interface, use the **ip pim hello-interval** command. To reset the hello interval to the default, use the **no** form of this command.

ip pim hello-interval *interval*

no ip pim hello-interval [*interval*]

Syntax Description

interval	Interval in milliseconds. The range is from 1 to 18,724,286. The default is 30000. **Note** We do not support agressive hello intervals. Any value below 30000 milliseconds is an aggressive PIM hello-interval value.

Command Default

The PIM hello interval is 30,000 milliseconds.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

At a minimum interval, VPC vs non-VPC cases, and also with single vs dual sup cases, Basically for vPC and with dual sups one needs to use default timers. the neighbor hold time is automatically set to 3.5x this value. Also it is recommended to use BFD for PIM instead of non-default timers.

This command requires the LAN Base Services license.

Examples

This example shows how to configure the PIM hello-message interval on an interface:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip pim hello-interval 20000
```

This example shows how to reset the PIM hello-message interval on an interface to the default:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip pim hello-interval
```

Related Commands

Command	Description
show ip pim interface	Displays information about PIM-enabled interfaces.

Review Draft -- Cisco Confidential

ip pim jp-policy

To filter IPv4 Protocol Independent Multicast (PIM) join-prune messages that are based on a route-map policy, use the **ip pim jp-policy** command. To disable filtering, use the **no** form of this command.

ip pim jp-policy *policy-name* [**in** | **out**]

no ip pim jp-policy [***policy-name***]

Syntax Description

policy-name	Route-map policy name.
in	Specifies that the system applies a filter only for incoming messages.
out	Specifies that the system applies a filter only for outgoing messages.

Command Default

Disabled; no filter is applied for either incoming or outgoing messages.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **ip pim jp-policy** command filters messages in both incoming and outgoing directions. To specify filtering only incoming messages, use the optional **in** keyword; to specify filtering only outgoing messages, use the optional **out** keyword. When you enter the command with no keywords, that is no explicit direction, the system rejects further configurations if given with explicit direction.

Use the **ip pim jp-policy** command to filter incoming messages. You can configure the route map to prevent state from being created in the multicast routing table.

You can specify group, group and source, or group and RP addresses to filter messages with the **match ip multicast** command.

This command requires the LAN Base Services license.

Examples

This example shows how to filter PIM join-prune messages:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip pim jp-policy my_jp_policy
```

This example shows how to disable filtering:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip pim jp-policy
```

Related Commands

Review Draft -- Cisco Confidential

Command	Description
show ip pim interface	Displays information about PIM-enabled interfaces.

Review Draft -- Cisco Confidential

ip pim log-neighbor-changes

To generate syslog messages that list the IPv4 Protocol Independent Multicast (PIM) neighbor state changes, use the **ip pim log-neighbor-changes** command. To disable messages, use the **no** form of this command.

ip pim log-neighbor-changes

no ip pim log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to generate syslog message that list the PIM neighbor state changes:

```
switch(config)# ip pim log-neighbor-changes
```

This example shows how to disable logging:

```
switch(config)# no ip pim log-neighbor-changes
```

Related Commands

Command	Description
logging level ip pim	Configures the logging level of PIM messages.

Review Draft -- Cisco Confidential

ip pim neighbor-policy

To configure a route-map policy that determines which IPv4 Protocol Independent Multicast (PIM) neighbors should become adjacent, use the **ip pim neighbor-policy** command. To reset to the default, use the **no** form of this command.

ip pim neighbor-policy *policy-name*

no ip pim neighbor-policy [*policy-name*]

Syntax Description

policy-name	Route-map policy name.

Command Default

Forms adjacency with all neighbors.

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You can use the **match ip address** command in a route-map policy to specify which groups to become adjacent to.

This command requires the LAN Base Services license.

Examples

This example shows how to configure a policy that determines which PIM neighbors should become adjacent:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip pim neighbor-policy
```

This example shows how to reset to the default:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip pim neighbor-policy
```

Related Commands

Command	Description
show ip pim interface	Displays information about PIM-enabled interfaces.

Review Draft -- Cisco Confidential

ip pim pre-build-spt

To prebuild the shortest path tree (SPT) for all known (S,G) in the routing table by triggering Protocol Independent Multicast (PIM) joins upstream, use the **ip pim pre-build-spt** command. To reset to the default, use the **no** form of this command.

ip pim pre-build-spt

no ip pim pre-build-spt

Syntax Description

This command has no arguments or keywords.

Command Default

Joins are triggered only if the OIF list is not empty.

Command Modes

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

To prebuild the SPT for all known (S,G)s in the routing table by triggering PIM joins upstream, even in the absence of any receivers, use the **ip pim pre-build-spt** command.

By default, PIM (S,G) joins are triggered upstream only if the OIF-list for the (S,G) is not empty. It is useful in certain scenarios—for example, on the virtual port-channel (vPC) nonforwarding router—to prebuild the SPTs and maintain the (S,G) states even when the system is not forwarding on these routes. Prebuilding the SPT ensures faster convergence when a vPC failover occurs.

When you are running virtual port channels (vPCs), enabling this feature causes both vPC peer switches to join the SPT, even though only one vPC peer switch actually routes the multicast traffic into the vPC domain. This behavior results in the multicast traffic passing over two parallel paths from the source to the vPC switch pair, consuming bandwidth on both paths. Additionally, when both vPC peer switches join the SPT, one or more upstream devices in the network may be required to perform additional multicast replications to deliver the traffic on both parallel paths toward the receivers in the vPC domain.

This command requires the LAN Base Services license.

Examples

This example shows how to prebuild the SPT in the absence of receivers:

```
switch(config)# vrf context Enterprise
switch(config-vrf)# ip pim pre-build-spt
switch(config-vrf)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
show ip pim context	Displays information about PIM routes.

Review Draft -- Cisco Confidential

ip pim register-policy

To filter IPv4 Protocol Independent Multicast (PIM) Register messages that are based on a route-map policy, use the **ip pim register-policy** command. To disable message filtering, use the **no** form of this command.

ip pim register-policy *policy-name*

no ip pim register-policy [*policy-name*]

Syntax Description

policy-name	Route-map policy name.

Command Default

Disabled

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You can use the **match ip multicast** command in a route-map policy to specify the group or group and source addresses whose register messages that should be filtered.

This command requires the LAN Base Services license.

Examples

This example shows how to enable filtering of PIM Register messages:

```
switch(config)# ip pim register-policy my_register_policy
```

This example shows how to disable message filtering:

```
switch(config)# no ip pim register-policy
```

Related Commands

Command	Description
show ip pim policy statistics register-policy	Displays statistics for PIM Register messages.

Review Draft -- Cisco Confidential

ip pim register-rate-limit

To configure a rate limit for IPv4 Protocol Independent Multicast (PIM) data registers, use the **ip pim register-rate-limit** command. To remove a rate limit, use the **no** form of this command.

ip pim register-rate-limit *rate*

no ip pim register-rate-limit [*rate*]

Syntax Description

rate	Rate in packets per second. The range is from 1 to 65,535.

Command Default

None

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to configure a rate limit for PIM data registers:

```
switch(config)# ip pim register-rate-limit 1000
```

This example shows how to remove a rate limit:

```
switch(config)# no ip pim register-rate-limit
```

Related Commands

Command	Description
show ip pim vrf detail	Displays information about the PIM configuration.

Review Draft -- Cisco Confidential

ip pim rp-address

To configure an IPv4 Protocol Independent Multicast (PIM) static route processor (RP) address for a multicast group range, use the **ip pim rp-address** command. To remove a static RP address, use the **no** form of this command.

ip pim rp-address *rp-address* [**group-list** *prefix* | **override** | **route-map** *policy-name*]

no ip pim rp-address *rp-address* [**group-list** *prefix* | **override** | **route-map** *policy-name*]

Syntax Description

rp-address	IP address of a router which is the RP for a group range.
group-list *prefix*	(Optional) Specifies a group range for a static RP.
override	(Optional) Specifies the RP address. The RP address overrides the dynamically learned RP addresses.
route-map *policy-name*	(Optional) Specifies a route-map policy name.

Command Default

The group range is treated in ASM mode.

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **match ip multicast** command is the only **match** command that is evaluated in the route map. You can the specify group prefix to filter messages with the **match ip multicast** command.

Customers can use this “override” provision, if they want the static RPs always to override the dynamic ones.

This command requires the LAN Base Services license.

Examples

This example shows how to configure a PIM static RP address for a serving group range and to override any dynamically learned (through BSR) RP addresses:

```
switch(config)# ip pim rp-address 1.1.1.1 group-list 225.1.0.0/16 override
```

This example shows how to configure a PIM static RP address for a group range:

```
switch(config)# ip pim rp-address 192.0.2.33 group-list 224.0.0.0/9
```

This example shows how to remove a static RP address:

```
switch(config)# no ip pim rp-address 192.0.2.33
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
show ip pim rp	Displays information about PIM RPs.

Review Draft -- Cisco Confidential

ip pim rp-candidate

To configure the router as an IPv4 Protocol Independent Multicast (PIM) bootstrap router (BSR) roure processor (RP) candidate, use the **ip pim rp-candidate** command. To remove the router as an RP candidate, use the **no** form of this command.

ip pim [**bsr**] **rp-candidate** {**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number*} {**group-list** *prefix*} [**priority** *priority*] [**interval** *interval*]

no ip pim [**bsr**] **rp-candidate** {**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number*} {**group-list** *prefix*} [**priority** *priority*] [**interval** *interval*]

Syntax Description

bsr	(Optional) Specifies the BSR protocol RP-distribution configuration.
ethernet *slot/port*	(Optional) Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	(Optional) Specifies the loopback interface. The loopback interface number is from 0 to 1023.
port-channel *number*	(Optional) Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
group-list *prefix*	Specifies a group range handled by the RP.
priority *priority*	(Optional) Specifies the RP priority used in candidate-RP messages. The range is from 0 to 65,535. The default is 192.
interval *interval*	(Optional) Specifies the BSR message transmission interval in seconds. The range is from 1 to 65,535. The default is 60.

Command Default

The RP priority is 192.
The BSR message interval is 60 seconds.

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

We recommend that you configure the candidate RP interval to be a minimum of 15 seconds.

Using this route map, you can add a range of group lists that this candidate-RP can serve.

Note Use the same configuration guidelines for the route-map auto-rp-range that you used when you created a route map for static RPS.

Review Draft -- Cisco Confidential

This command requires the LAN Base Services license.

Examples

This example shows how to configure the router as a PIM BSR RP candidate:

```
switch(config)# ip pim rp-candidate e 2/11 group-list 239.0.0.0/24
```

This example shows how to remove the router as an RP candidate:

```
switch(config)# no ip pim rp-candidate
```

Related Commands

Command	Description
show ip pim rp	Displays information about PIM RPs.

Review Draft -- Cisco Confidential

ip pim send-rp-announce

To configure an IPv4 Protocol Independent Multicast (PIM) Auto-RP candidate route processor (RP), use the **ip pim send-rp-announce** command. To remove an Auto-RP candidate RP, use the **no** form of this command.

ip pim send-rp-announce {**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number*} {**group-list** *prefix*} {[**scope** *ttl*] | [**interval** *interval*]}

no ip pim send-rp-announce [{**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number*} {**group-list** *prefix*} {[**scope** *ttl*] | [**interval** *interval*] }

Syntax Description

ethernet *slot/port*	(Optional) Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	(Optional) Specifies the loopback interface. The loopback interface number is from 0 to 1023.
port-channel *number*	(Optional) Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
group-list *prefix*	Specifies a group range handled by the RP.
scope *ttl*	(Optional) Specifies a time-to-live (TTL) value for the scope of Auto-RP Announce messages. The range is from 1 to 255. The default is 32. **Note** See the **ip pim border** command to explicitly define a router on the edge of a PIM domain rather than using the **scope** argument.
interval *interval*	(Optional) Specifies an Auto-RP Announce message transmission interval in seconds. The range is from 1 to 65,535. The default is 60.

Command Default

The TTL is 32.
The Auto-RP Announce message interval is 60 seconds.

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **scope**, and **interval** keywords can be entered once and in any order.

The **ip pim auto-rp rp-candidate** command is an alternative form of this command.

This command requires the LAN Base Services license.

Review Draft -- Cisco Confidential

Examples

This example shows how to configure a PIM Auto-RP candidate RP:

```
switch(config)# ip pim send-rp-announce ethernet 2/1 group-list 239.0.0.0/24
```

This example shows how to remove a PIM Auto-RP candidate RP:

```
switch(config)# no ip pim send-rp-announce ethernet 2/1 group-list 239.0.0.0/24
```

Related Commands

Command	Description
ip pim auto-rp rp-candidate	Configures a PIM Auto-RP candidate RP.
show ip pim interface	Displays information about PIM-enabled interfaces.

Review Draft -- Cisco Confidential

ip pim send-rp-discovery

To configure the router as an IPv4 Protocol Independent Multicast (PIM) Auto-RP mapping agent that sends RP-Discovery messages, use the **ip pim send-rp-discovery** command. To remove the configuration, use the **no** form of this command.

ip pim send-rp-discovery {**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number*} [**scope** *ttl*]

no ip pim send-rp-discovery [{**ethernet** *slot/port* | **loopback** *if_number* | **port-channel** *number*} [**scope** *ttl*]

Syntax Description

ethernet *slot/port*	Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
loopback *if_number*	Specifies the loopback interface. The loopback interface number is from 0 to 1023.
port-channel *number*	Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
scope *ttl*	(Optional) Specifies the time-to-live (TTL) value for the scope of Auto-RP Discovery messages. The range is from 1 to 255. The default is 32. **Note** See the **ip pim border** command to explicitly define a router on the edge of a PIM domain rather than using the **scope** argument.

Command Default

The TTL is 32.

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **ip pim auto-rp mapping-agent** command is an alternative form of this command.

This command requires the LAN Base Services license.

Examples

This example shows how to configure an Auto-RP mapping agent:

```
switch(config)# ip pim send-rp-discovery ethernet 2/1
```

This example shows how to remove an Auto-RP mapping agent:

```
switch(config)# no ip pim send-rp-discovery ethernet 2/1
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
show ip pim rp	Displays information about PIM RPs.
ip pim auto-rp mapping-agent	Configures a router as an Auto-RP mapping agent.
ip pim border	Configures a router to be on the edge of a PIM domain.

Review Draft -- Cisco Confidential

ip pim sg-expiry-timer

To adjust the (S, G) expiry timer interval for Protocol Independent Multicast sparse mode (PIM-SM) (S, G) multicast routes, use the **ip pim sg-expiry-timer** command. To reset to the default values, use the **no** form of the command.

ip pim [**sparse**] **sg-expiry-timer** *seconds* [**sg-list** *route-map*]

no ip pim [**sparse**] **sg-expiry-timer** *seconds* [**sg-list** *route-map*]

Syntax Description

sparse	(Optional) Specifies sparse mode.
seconds	Expiry-timer interval. The range is from 181 to 57600 seconds.
sg-list *route-map*	(Optional) Specifies S,G values to which the timer applies. The route map name can be a maximum of 100 alphanumeric characters.

Command Default

The default expiry time is 180 seconds.
The timer applies to all (S, G) entries in the routing table.

Command Modes

VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to configure the expiry interval to 300 seconds for all (S, G) entries:

```
switch(config)# vrf context Enterprise
switch(config-vrf)# ip pim sg-expiry-timer 300
switch(config-vrf)#
```

Related Commands

Command	Description
show ip pim context	Displays information about the PIM configuration.

Review Draft -- Cisco Confidential

ip pim sparse-mode

To enable IPv4 Protocol Independent Multicast (PIM) sparse mode on an interface, use the **ip pim sparse-mode** command. To disable PIM on an interface, use the **no** form of this command.

ip pim sparse-mode

no ip pim [**sparse-mode**]

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to enable PIM sparse mode on an interface:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ip pim sparse-mode
```

This example shows how to disable PIM on an interface:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ip pim
```

Related Commands

Command	Description
show ip pim interface	Displays information about PIM-enabled interfaces.

Review Draft -- Cisco Confidential

ip pim ssm policy

To configure group ranges for Source Specific Multicast (SSM) using a route-map policy, use the **ip pim ssm policy** command. To remove the SSM group range policy, use the **no** form of this command.

ip pim ssm policy *policy-name*

no ip pim ssm policy *policy-name*

Syntax Description

policy-name	Route-map policy name that defines the group prefixes where this feature is applied.

Command Default

The SSM range is 232.0.0.0/8.

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to configure a group range for SSM:

```
switch(config)# ip pim ssm policy my_ssm_policy
```

This example shows how to reset the group range to the default:

```
switch(config)# no ip pim ssm policy my_ssm_policy
```

Related Commands

Command	Description
show ip pim group-range	Displays information about PIM group ranges.

Review Draft -- Cisco Confidential

ip pim ssm

To configure group ranges for Source Specific Multicast (SSM), use the **ip pim ssm range** command. To reset the SSM group range to the default, use the **no** form of this command with the **none** keyword.

ip pim ssm {**range** {*groups* | **none**} | **route-map** *policy-name*}

no ip pim ssm {**range** {*groups* | **none**} | **route-map** *policy-name*}

Syntax Description

groups	List of up to four group range prefixes.
none	Removes all group ranges.
route-map *policy-name*	Specifies the route-map policy name.

Command Default

The SSM range is 232.0.0.0/8.

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

The **match ip multicast** command is the only **match** command that is evaluated in the route map. You can specify the group prefix to filter messages with the **match ip multicast** command.

This command requires the LAN Base Services license.

Examples

This example shows how to configure a group range for SSM:

```
switch(config)# ip pim ssm range 239.128.1.0/24
```

This example shows how to reset the group range to the default:

```
switch(config)# no ip pim ssm range none
```

This example shows how to remove all group ranges:

```
switch(config)# ip pim ssm range none
```

Related Commands

Command	Description
show ip pim group-range	Displays information about PIM group ranges.

Review Draft -- Cisco Confidential

ip pim state-limit

To configure a maximum number of IPv4 Protocol Independent Multicast (PIM) state entries in the current virtual routing and forwarding (VRF) instance, use the **ip pim state-limit** command. To remove the limit on state entries, use the **no** form of this command.

ip pim state-limit *max-states* [**reserved** *policy-name max-reserved*]

no ip pim state-limit [*max-states* [**reserved** *policy-name max-reserved*]]

Syntax Description

max-states	Maximum number of (*, G) and (S, G) entries allowed in this VRF. The range is from 1 to 429,496,7295. The default is no limit.
reserved	(Optional) Specifies that a number of state entries are to be reserved for the routes specified in a policy map.
policy-name	(Optional) Route-map policy name.
max-reserved	(Optional) Maximum reserved (*, G) and (S, G) entries allowed in this VRF. Must be less than or equal to the maximum states allowed. The range is from 1 to 429,496,7295.

Command Default

None

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

To display commands where state limits are configured, use this command line:

```
switch(config)# show running-config | include state-limit
```

This command requires the LAN Base Services license.

Examples

This example shows how to configure a state entry limit with a number of state entries reserved for routes in a policy map:

```
switch(config)# ip pim state-limit 100000 reserved my_reserved_policy 40000
```

Review Draft -- Cisco Confidential

This example shows how to remove the limits on state entries:

```
switch(config)# no ip pim state-limit
```

Related Commands

Command	Description
show running-config	Displays information about the running-system configuration.

Review Draft -- Cisco Confidential

ip pim use-shared-tree-only

To create the IPv4 Protocol Independent Multicast (PIM) (*, G) state only (where no source state is created), use the **ip pim use-shared-tree-only** command. To remove the creation of the shared tree state only, use the **no** form of this command.

ip pim use-shared-tree-only group-list *policy-name*

no ip pim use-shared-tree-only [**group-list** *policy-name*]

Syntax Description

policy-name	Route-map policy name that defines the group prefixes where this feature is applied.

Command Default

None

Command Modes

Global configuration mode
VRF configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

You can use the **match ip multicast** command in a route-map policy to specify the groups where shared trees should be enforced.

This command requires the LAN Base Services license.

Examples

This example shows how to create the PIM (*, G) state only for the group prefixes defined in my_group_policy:

```
switch(config)# ip pim use-shared-tree-only group-list my_group_policy
```

This example shows how to remove the creation of the (*, G) state only:

```
switch(config)# no ip pim use-shared-tree-only
```

Related Commands

Command	Description
show ip pim rp	Displays information about PIM RPs.

Review Draft -- Cisco Confidential

ip routing multicast event-history

To configure the size of the IPv4 Multicast Routing Information Base (MRIB) event history buffers, use the **ip routing multicast event-history** command. To revert to the default buffer size, use the **no** form of this command.

ip routing multicast event-history {**cli** | **mfdm-debugs** | **mfdm-events** | **mfdm-stats** | **rib** | **vrf**} **size** *buffer-size*

no ip routing multicast event-history {**cli** | **mfdm** | **mfdm-stats** | **rib** | **vrf**} **size** *buffer-size*

Syntax Description

cli	Configures the CLI event history buffer.
mfdm-debugs	Configures the multicast FIB distribution (MFDM) debug event history buffer.
mfdm-events	Configures the multicast FIB distribution (MFDM) non-periodic events event history buffer.
mfdm-stats	Configures the MFDM sum event history buffer.
rib	Configures the RIB event history buffer.
vrf	Configures the virtual routing and forwarding (VRF) event history buffer.
size	Specifies the size of the buffer to allocate.
buffer-size	Buffer size is one of the following values: **disabled**, **large**, **medium**, or **small**. The default buffer size is **small**.

Command Default

All history buffers are allocated as small.

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

To display configured buffer sizes, use this command line:

```
switch(config)# show running-config | include "ip routing"
```

Examples

This example shows how to configure the size of the MRIB MFDM event history buffer:

```
switch(config)# ip routing multicast event-history mfdm size large
switch(config)#
```

Review Draft -- Cisco Confidential

Related Commands

Command	Description
clear ip routing multicast event-history	Clears information in the IPv4 MRIB event history buffers.
show routing ip multicast event-history	Displays information in the IPv4 MRIB event history buffers.
show running-config	Displays information about the running-system configuration.

Review Draft -- Cisco Confidential

ip routing multicast holddown

To configure the IPv4 multicast routing initial holddown period, use the **ip routing multicast holddown** command. To revert to the default holddown period, use the **no** form of this command.

[**ip** | **ipv4**] **routing multicast holddown** *holddown-period*

no [**ip** | **ipv4**] **routing multicast holddown** *holddown-period*

Syntax Description

holddown-period	Initial route holddown period in seconds. The range is from 90 to 210. Specify 0 to disable the holddown period. The default is 210.

Command Default

The holddown period is 210 seconds.

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

To display the holddown period configuration, use this command line:

```
switch(config)# show running-config | include "ip routing multicast holddown"
```

This command does not require a license.

Examples

This example shows how to configure the routing holddown period:

```
switch(config)# ip routing multicast holddown 100
switch(config)#
```

Related Commands

Command	Description
show running-config	Displays information about the running-system configuration.

Review Draft -- Cisco Confidential

ip routing multicast software-replicate

To enable software replication of IPv4 Protocol Independent Multicast (PIM) Any Source Multicast (ASM) packets that are leaked to the software for state creation, use the **ip routing multicast software-replicate** command. To reset to the default, use the **no** form of this command.

ip routing multicast software-replicate

no ip routing multicast software-replicate

Syntax Description

This command has no arguments or keywords.

Command Default

No software replication.

Command Modes

Global configuration mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

By default, these packets are used by the software only for (S,G) state creation and then dropped.

This command does not require a license.

Examples

This example shows how to enable software replication of IPv4 PIM ASM packets:

```
switch(config)# ip routing multicast software-replicate
switch(config)#
```

Related Commands

Command	Description
show running-config	Displays information about the running-system configuration.

Review Draft -- Cisco Confidential

Show Commands

This chapter describes the Cisco NX-OS PIM **show** commands.

Review Draft -- Cisco Confidential

show ip mroute

To display information about IPv4 multicast routes, use the **show ip mroute** command.

show ip mroute {*group* | {*source group*} | {*group* [*source*]}} [**summary** [**software-forwarded**]] [**vrf** {*vrf-name* | **all**}]

Syntax Description

group	Group address for route.
source	Source address for route.
summary	(Optional) Displays route counts and packet rates.
software-forwarded	(Optional) Displays software-switched route counts only.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about IPv4 multicast routes:

```
switch(config)# show ip mroute
IP Multicast Routing Table for VRF "default"

(*, 232.0.0.0/8), uptime: 04:18:55, pim ip
  Incoming interface: Null, RPF nbr: 0.0.0.0
  Outgoing interface list: (count: 0)

switch(config)#
```

Related Commands

Command	Description
show ip mroute summary	Displays summary information about IPv4 multicast routes.

Review Draft -- Cisco Confidential

show ip mroute summary

To display summary information about IPv4 multicast routes, use the **show ip mroute summary** command.

show ip mroute summary [**count** | **software-forwarded**] [**vrf** {*vrf-name* | **all**}]

show ip mroute [*group*] **summary** [**software-forwarded**] [**vrf** {*vrf-name* | **all**}]

Syntax Description

count	(Optional) Displays only route counts.
software-forwarded	(Optional) Displays software-switched route counts only.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.
group	(Optional) Specifies a group address for a route.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display summary information about IPv4 multicast routes:

```
switch(config)# show ip mroute summary
IP Multicast Routing Table for VRF "default"

Total number of routes: 1
Total number of (*,G) routes: 0
Total number of (S,G) routes: 0
Total number of (*,G-prefix) routes: 1
Group count: 0, rough average sources per group: 0.0

Group: 232.0.0.0/8, Source count: 0
Source          packets      bytes           aps   pps       bit-rate     oifs
(*,G)           0            0               0     0         0.000   bps  0

switch(config)#
```

This example shows how to display the number of IPv4 multicast routes:

Review Draft -- Cisco Confidential

```
switch# show ip mroute summary count
IP Multicast Routing Table for VRF "default"

Total number of routes: 2
Total number of (*,G) routes: 1
Total number of (S,G) routes: 0
Total number of (*,G-prefix) routes: 1
Group count: 1, rough average sources per group: 0.0
switch#
```

Related Commands

Command	Description
show ip mroute	Displays information about IPv4 multicast routes.

Review Draft -- Cisco Confidential

show ip pim event-history

To display information in the IPv4 Protocol Independent Multicast (PIM) event history buffers, use the **show ip pim event-history** command.

show ip pim event-history {**errors** | **msgs** | **statistics**}

Syntax Description

errors	Displays events of type error.
msgs	Displays events of type msg.
statistics	Displays events of type statistics.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display information in the IPv4 PIM msgs event history buffer:

```
switch(config)# show ip pim event-history msgs

Msg events for PIM Process
1) Event:E_DEBUG, length:38, at 165671 usecs after Sat Apr 12 08:35:02 2008
    [100] : nvdb: transient thread created

2) Event:E_DEBUG, length:38, at 165018 usecs after Sat Apr 12 08:35:02 2008
    [100] : nvdb: create transcient thread

3) Event:E_DEBUG, length:79, at 165014 usecs after Sat Apr 12 08:35:02 2008
    [100] : comp-mts-rx opc - from sap 3061 cmd pim_show_internal_event_hist_com
mand
4) Event:E_DEBUG, length:35, at 63168 usecs after Sat Apr 12 08:34:25 2008
    [100] : nvdb: terminate transaction

5) Event:E_DEBUG, length:46, at 62809 usecs after Sat Apr 12 08:34:25 2008
    [100] : nvdb: pim_show_df_command returned 0x0

6) Event:E_DEBUG, length:38, at 62676 usecs after Sat Apr 12 08:34:25 2008
    [100] : nvdb: transient thread created

7) Event:E_DEBUG, length:38, at 61971 usecs after Sat Apr 12 08:34:25 2008
    [100] : nvdb: create transcient thread

8) Event:E_DEBUG, length:62, at 61966 usecs after Sat Apr 12 08:34:25 2008
    [100] : comp-mts-rx opc - from sap 3055 cmd pim_show_df_command
9) Event:E_DEBUG, length:50, at 771336 usecs after Sat Apr 12 06:14:41 2008
    [100] : nvdb: _cli_send_my_if_command returned 0x0
```

Review Draft -- Cisco Confidential

```
10) Event:E_DEBUG, length:63, at 771105 usecs after Sat Apr 12 06:14:41 2008
    [100] : comp-mts-rx opc - from sap 0 cmd _cli_send_my_if_command
<--Output truncated-->
switch(config)#
```

Related Commands

Command	Description
clear ip pim event-history	Clears the contents of the PIM event history buffers.
ip pim event-history	Configures the size of PIM event history buffers.

Review Draft -- Cisco Confidential

show ip pim group-range

To display information about the group ranges for IPv4 Protocol Independent Multicast (PIM), use the **show ip pim group-range** command.

show ip pim group-range [*group*] [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

group	(Optional) Group address.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies that all VRF entries be cleared from the IPv4 multicast routing table.
default	Specifies that the default VRF entry be cleared from the IPv4 multicast routing table.
management	Specifies that the management VRF entry be cleared from the IPv4 multicast routing table.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about IPv4 PIM group ranges:

```
switch(config)# show ip pim group-range
PIM Group-Range Configuration for VRF "default"
Group-range        Mode      RP-address       Shared-tree-only range
232.0.0.0/8        SSM       -                -
switch(config)#
```

Review Draft -- Cisco Confidential

show ip pim interface

To display information about the enabled interfaces for IPv4 Protocol Independent Multicast (PIM), use the **show ip pim interface** command.

show ip pim interface [**brief**] [**vrf** {*vrf-name* | **all** | **default** | **management**}]

show ip pim interface ethernet {*slot/port* | **port-channel** *channel-number*[.*sub_if-number*] | **vlan** *vlan-id*}

Syntax Description

brief	(Optional) Specifies a brief format for display.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.
default	Specifies the default VRF.
management	Specifies the management VRF.
ethernet *slot/port*	Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
port-channel *number*	Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
sub_if-number	(Optional) Subinterface number. The range is from 1 to 4093.
vlan *vlan-id*	Specifies the VLAN. The range is from 1 to 4094.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display brief information about IPv4 PIM-enabled interfaces:

```
switch# show ip pim interface brief
PIM Interface Status for VRF "default"
Interface            IP Address      PIM DR Address  Neighbor  Border
                                                     Count     Interface
Vlan100              192.0.2.252     192.0.2.252     0         no
port-channel2000     192.0.2.1       192.0.2.1       1         no
port-channel2001     192.0.2.8       192.0.2.8       1         no
```

Review Draft -- Cisco Confidential

```
Ethernet1/26         192.0.2.2       192.0.2.2       1         no
Ethernet2/5          192.0.2.3       192.0.2.3       1         no
Ethernet2/6          192.0.2.4       192.0.2.4       1         no
Ethernet2/7          192.0.2.5       192.0.2.5       1         no
Ethernet3/11         192.0.2.6       192.0.2.6       1         no
Ethernet3/12         192.0.2.7       192.0.2.7       1         no
switch#
```

This example shows how to display information about PIM-enabled interfaces:

```
switch# show ip pim interface ethernet 2/5
PIM Interface Status for VRF "default"
Ethernet2/5, Interface status: protocol-up/link-up/admin-up
  IP address: 192.0.2.3, IP subnet: 192.0.2.0/24
  PIM DR: 192.0.2.3, DR's priority: 1
  PIM neighbor count: 1
  PIM hello interval: 30 secs, next hello sent in: 00:00:20
  PIM neighbor holdtime: 105 secs
  PIM configured DR priority: 1
  PIM border interface: no
  PIM GenID sent in Hellos: 0x36a7d6d1
  PIM Hello MD5-AH Authentication: disabled
  PIM Neighbor policy: none configured
  PIM Join-Prune inbound policy: none configured
  PIM Join-Prune outbound policy: none configured
  PIM BFD enabled: no
  PIM Interface Statistics, last reset: never
    General (sent/received):
      Hellos: 454/453, JPs: 4/0, Asserts: 0/0
      Grafts: 0/0, Graft-Acks: 0/0
      DF-Offers: 0/0, DF-Winners: 0/0, DF-Backoffs: 0/0, DF-Passes: 0/0
    Errors:
      Checksum errors: 0, Invalid packet types/DF subtypes: 0/0
      Authentication failed: 0
      Packet length errors: 0, Bad version packets: 0, Packets from self: 0
      Packets from non-neighbors: 0
      JPs received on RPF-interface: 0
      (*,G) Joins received with no/wrong RP: 0/0
      (*,G)/(S,G) JPs received for SSM/Bidir groups: 0/0
      JPs filtered by inbound policy: 0
      JPs filtered by outbound policy: 0
switch#
```

Review Draft -- Cisco Confidential

show ip pim neighbor

To display information about IPv4 Protocol Independent Multicast (PIM) neighbors, use the **show ip pim neighbor** command.

show ip pim neighbor {[**ethernet** *slot/port* | **port-channel** *channel-number*[.*sub_if-number*] | **vlan** *vlan-id*] | [*neighbor-addr*]} [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

ethernet *slot/port*	(Optional) Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
port-channel *number*	(Optional) Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
sub_if-number	(Optional) Subinterface number. The range is from 1 to 4093.
vlan *vlan-id*	Specifies the VLAN. The range is from 1 to 4094.
neighbor-addr	(Optional) IP address of a neighbor.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies that all VRF entries be cleared from the IPv4 multicast routing table.
default	Specifies that the default VRF entry be cleared from the IPv4 multicast routing table.
management	Specifies that the management VRF entry be cleared from the IPv4 multicast routing table.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about PIM neighbors:

```
switch(config)# show ip pim neighbor
PIM Neighbor Status for VRF "default"
Neighbor        Interface            Uptime    Expires   DR       Bidir-  BFD
                                                         Priority Capable State
192.0.2.2       port-channel2000     03:43:40  00:01:21  1        no     n/a
192.0.2.9       port-channel2001     03:43:41  00:01:35  1        no     n/a
192.0.2.1       Ethernet1/26         03:43:44  00:01:33  1        no     n/a
192.0.2.2       Ethernet2/5          03:43:45  00:01:34  1        no     n/a
```

Review Draft -- Cisco Confidential

```
192.0.2.3       Ethernet2/6          03:43:45  00:01:19  1        no     n/a
192.0.2.4       Ethernet2/7          03:43:45  00:01:39  1        no     n/a
192.0.2.5       Ethernet3/11         03:43:46  00:01:35  1        no     n/a
192.0.2.6       Ethernet3/12         03:43:46  00:01:34  1        no     n/a
switch(config)#
```

Review Draft -- Cisco Confidential

show ip pim oif-list

To display information about IPv4 Protocol Independent Multicast (PIM) interfaces for a group, use the **show ip pim oif-list** command.

show ip pim oif-list *group* [*source*] [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

group	Group address.
source	(Optional) Source address.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies that all VRF entries be cleared from the IPv4 multicast routing table.
default	Specifies that the default VRF entry be cleared from the IPv4 multicast routing table.
management	Specifies that the management VRF entry be cleared from the IPv4 multicast routing table.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display IPv4 PIM interfaces for a group:

```
switch(config)# show ip pim oif-list 232.0.0.0
PIM OIF-List for VRF default
(*, 232.0.0.0/8)
  Incoming interface: Null0, RPF nbr 0.0.0.0
  Timeout interval: 66 secs left
  Oif-list (count: 0):
  Timeout-list (count: 0):
  Immediate-list (count: 0):
  Immediate-timeout-list (count: 0):
  Assert-lost-list (count: 0):
switch(config)#
```

Review Draft -- Cisco Confidential

show ip pim policy statistics auto-rp

To display information about the Auto-RP policy statistics for IPv4 Protocol Independent Multicast (PIM), use the **show ip pim policy statistics auto-rp** command.

show ip pim policy statistics auto-rp {**rp-candidate-policy** | **mapping-agent-policy**} [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

rp-candidate-policy	Specifies candidate-RP messages.
mapping-agent-policy	Specifies mapping agent messages.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies that all VRF entries be cleared from the IPv4 multicast routing table.
default	Specifies that the default VRF entry be cleared from the IPv4 multicast routing table.
management	Specifies that the management VRF entry be cleared from the IPv4 multicast routing table.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about IPv4 PIM policy statistics:

```
switch(config)# show ip pim policy statistics auto-rp rp-candidate-policy
```

Review Draft -- Cisco Confidential

show ip pim policy statistics bsr

To display information about the bootstrap router (BSR) policy statistics for IPv4 Protocol Independent multicast (PIM), use the **show ip pim policy statistics bsr** command.

show ip pim policy statistics bsr {**bsr-policy** | **rp-candidate-policy**} [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

bsr-policy	Specifies BSR messages.
rp-candidate-policy	Specifies candidate-RP messages.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies that all VRF entries be cleared from the IPv4 multicast routing table.
default	Specifies that the default VRF entry be cleared from the IPv4 multicast routing table.
management	Specifies that the management VRF entry be cleared from the IPv4 multicast routing table.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about IPv4 PIM policy statistics:

```
switch(config)# show ip pim policy statistics bsr bsr-policy
```

Review Draft -- Cisco Confidential

show ip pim policy statistics jp-policy

To display information about the join-prune policy statistics for IPv4 Protocol Independent Multicast (PIM), use the **show ip pim policy statistics jp-policy** command.

show ip pim policy statistics jp-policy {**ethernet** *slot/port* | **port-channel** *channel-number*[*.sub_if-number*] | **vlan** *vlan-id*}

Syntax Description

ethernet *slot/port*	Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
port-channel *number*	Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
sub_if-number	(Optional) Subinterface number. The range is from 1 to 4093.
vlan *vlan-id*	Specifies the VLAN. The range is from 1 to 4094.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about PIM policy statistics:

```
switch(config)# show ip pim policy statistics jp-policy ethernet 2/12
```

Review Draft -- Cisco Confidential

show ip pim policy statistics neighbor-policy

To display information about the neighbor policy statistics for IPv4 Protocol Independent Multicast (PIM), use the **show ip pim policy statistics neighbor-policy** command.

show ip pim policy statistics neighbor-policy {**ethernet** *slot*/*port* | **port-channel** *channel-number*[.*sub_if-number*] | **vlan** *vlan-id*}

Syntax Description

ethernet *slot*/*port*	Specifies the Ethernet interface and the slot number and port number. The slot number is from 1 to 255, and the port number is from 1 to 128.
port-channel *number*	Specifies the EtherChannel interface and EtherChannel number. The range is from 1 to 4096.
sub_if-number	(Optional) Subinterface number. The range is from 1 to 4093.
vlan *vlan-id*	Specifies the VLAN. The range is from 1 to 4094.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about IPv4 PIM policy statistics:

```
switch(config)# show ip pim policy statistics neighbor-policy ethernet 2/12
```

Review Draft -- Cisco Confidential

show ip pim policy statistics register-policy

To display information about the register policy statistics for IPv4 Protocol Independent Multicast (PIM), use the **show ip pim policy statistics register-policy** command.

show ip pim policy statistics register-policy [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.
default	Specifies the default VRF.
management	Specifies the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about PIM policy statistics:

```
switch(config)# show ip pim policy statistics register-policy vrf all
```

Review Draft -- Cisco Confidential

show ip pim route

To display information about the routes for IPv4 Protocol Independent Multicast (PIM), use the **show ip pim route** command.

show ip pim route {*source group* | *group* [*source*]} [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

source	Source address.
group	Group address.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies that all VRF entries be cleared from the IPv4 multicast routing table.
default	Specifies that the default VRF entry be cleared from the IPv4 multicast routing table.
management	Specifies that the management VRF entry be cleared from the IPv4 multicast routing table.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display IPv4 PIM routes:

```
switch(config)# show ip pim route 232.0.0.0
PIM Routing Table for VRF "default" - 1 entries

(*, 232.0.0.0/8), expires 00:02:15
  Incoming interface: Null0, RPF nbr 0.0.0.0
  Oif-list:       (0) 00000000, timeout-list: (0) 00000000
  Immediate-list: (0) 00000000, timeout-list: (0) 00000000
  Timeout-interval: 3, JP-holdtime round-up: 3

switch(config)#
```

Review Draft -- Cisco Confidential

show ip pim rp

To display information about the rendezvous points (RPs) for IPv4 Protocol Independent Multicast (PIM), use the **show ip pim rp** command.

show ip pim rp [*group*] [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

group	(Optional) Group address.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.
default	Specifies the default VRF.
management	Specifies the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about IPv4 PIM RPs:

```
switch(config)# show ip pim rp
PIM RP Status Information for VRF "default"
BSR disabled
Auto-RP disabled
BSR RP Candidate policy: None
BSR RP policy: None
Auto-RP Announce policy: None
Auto-RP Discovery policy: None

switch(config)#
```

Review Draft -- Cisco Confidential

show ip pim rp-hash

To display information about the RP-hash values for IPv4 Protocol Independent Multicast (PIM), use the **show ip pim rp-hash** command.

show ip pim rp-hash *group* [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

group	Group address for RP lookup.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.
default	Specifies the default VRF.
management	Specifies the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about IPv4 PIM RP-hash values:

```
switch(config)# show ip pim rp-hash 224.1.1.1
```

Review Draft -- Cisco Confidential

show ip pim statistics

To display information about the packet counter statistics for IPv4 Protocol Independent Multicast (PIM), use the **show ip pim statistics** command.

show ip pim statistics [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.
default	Specifies the default VRF.
management	Specifies the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about IPv4 PIM statistics (if PIM is not in vPC mode, the vPC statistics are not displayed):

```
switch(config)# show ip pim statistics
PIM Global Counter Statistics for VRF:default, last reset: never
  Register processing (sent/received):
    Registers: 0/0, Null registers: 0/0, Register-Stops: 0/0
    Registers received and not RP: 0
    Registers received for SSM groups: 0
  BSR processing (sent/received):
    Bootstraps: 0/0, Candidate-RPs: 0/0
    BSs from non-neighbors: 0, BSs from border interfaces: 0
    BS length errors: 0, BSs which RPF failed: 0
    BSs received but not listen configured: 0
    Cand-RPs from border interfaces: 0
    Cand-RPs received but not listen configured: 0
  Auto-RP processing (sent/received):
    Auto-RP Announces: 0/0, Auto-RP Discoveries: 0/0
    Auto-RP RPF failed: 0, Auto-RP from border interfaces: 0
    Auto-RP invalid type: 0, Auto-RP TTL expired: 0
    Auto-RP received but not listen configured: 0
  General errors:
    Control-plane RPF failure due to no route found: 0
```

Review Draft -- Cisco Confidential

```
    Data-plane RPF failure due to no route found: 0
    Data-plane no multicast state found: 0
    Data-plane create route state count: 0
  vPC packet stats:
    assert requests sent: 0
    assert requests received: 0
    assert request send error: 0
    assert response sent: 0
    assert response received: 0
    assert response send error: 0
    assert stop sent: 0
    assert stop received: 0
    assert stop send error: 0
    rpf-source metric requests sent: 0
    rpf-source metric requests received: 0
    rpf-source metric request send error: 0
    rpf-source metric response sent: 0
    rpf-source metric response received: 0
    rpf-source metric response send error: 0
    rpf-source metric rpf change trigger sent: 0
    rpf-source metric rpf change trigger received: 0
    rpf-source metric rpf change trigger send error: 0
switch(config)#
```

Review Draft -- Cisco Confidential

show ip pim vrf

To display information about IPv4 Protocol Independent Multicast (PIM) by virtual routing and forwarding (VRF) instance, use the **show ip pim vrf** command.

show ip pim vrf [*vrf-name* | **all** | **default** | **detail** | **management**]

Syntax Description

vrf-name	(Optional) VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	(Optional) Specifies all VRFs.
default	(Optional) Specifies the default VRF.
detail	(Optional) Displays detailed PIM VRF information.
management	(Optional) Specifies the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about IPv4 PIM by VRF:

```
switch(config)# show ip pim vrf
PIM Enabled VRF
VRF Name              VRF      Table       Interface  BFD
                      ID       ID          Count      Enabled
default               1        0x00000001  1          no
switch(config)#
```

This example shows how to display the detailed information about IPv4 PIM by VRF:

```
switch# show ip pim vrf detail
PIM Enabled VRF
VRF Name              VRF      Table       Interface  BFD
                      ID       ID          Count      Enabled
default               1        0x00000001  1          no
  State Limit: None
  Register Rate Limit: none
  Shared tree ranges: none
  (S,G)-expiry timer: not configured
    (S,G)-list policy: none
    (S,G)-expiry timer config version 0, active version 0
```

Review Draft -- Cisco Confidential

```
  Pre-build SPT for all (S,G)s in VRF: disabled
switch#
```

Review Draft -- Cisco Confidential

show ip static-route

To display static routes from the unicast Routing Information Base (RIB), use the **show ip static-route** command.

show ip static-route [**vrf** {*vrf-name* | **all** | **default** | **management**}]

Syntax Description

vrf *vrf-name*	(Optional) Specifies the virtual routing and forwarding (VRF) context name. The name can be any case-sensitive, alphanumeric string up to 32 characters.
all	(Optional) Specifies all VRF instances.
default	(Optional) Specifies the default VRF.
management	(Optional) Specifies the management VRF.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display the static routes:

```
switch(config)# show ip static-route
Static-route for VRF "default"(1)

IPv4 Unicast Static Routes:

Total number of routes: 0, unresolved: 0
switch(config)#
```

Related Commands

Command	Description
ip route	Configures a static route.

Review Draft -- Cisco Confidential

show routing ip multicast event-history

To display information in the IPv4 Multicast Routing Information Base (MRIB) event history buffers, use the **show routing ip multicast event-history** command.

show routing ip multicast event-history {**cli** | **errors** | **mfdm-debugs** | **mfdm-stats** | **msgs** | **rib** | **statistics** | **vrf**}

Syntax Description

cli	Displays the event history buffer of type CLI.
errors	Displays the event history buffer of type errors.
mfdm-debugs	Displays the event history buffer of type multicast FIB distribution (MFDM).
mfdm-stats	Displays the event history buffer of type MFDM sum.
msgs	Displays the event history buffer of type msgs.
rib	Displays the event history buffer of type RIB.
statistics	Displays information about the event history buffers.
vrf	Displays the event history buffer of type virtual routing and forwarding (VRF).

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Examples

This example shows how to display information in the MRIB msgs event history buffer:

```
switch(config)# show routing ip multicast event-history msgs

Msg events for MRIB Process
1) Event:E_DEBUG, length:38, at 932956 usecs after Sat Apr 12 09:09:41 2008
    [100] : nvdb: transient thread created

2) Event:E_DEBUG, length:38, at 932269 usecs after Sat Apr 12 09:09:41 2008
    [100] : nvdb: create transcient thread

3) Event:E_DEBUG, length:75, at 932264 usecs after Sat Apr 12 09:09:41 2008
    [100] : comp-mts-rx opc - from sap 3210 cmd mrib_internal_event_hist_command
4) Event:E_MTS_RX, length:60, at 362578 usecs after Sat Apr 12 09:08:51 2008
    [RSP] Opc:MTS_OPC_MFDM_V4_ROUTE_STATS(75785), Id:0X000F217E, Ret:SUCCESS
    Src:0x00000101/214, Dst:0x00000101/1203, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x000F217B, Sync:NONE, Payloadsize:148
    Payload:
    0x0000:  01 00 00 00 05 00 01 00 00 04 00 00 00 00 00 00
5) Event:E_MTS_RX, length:60, at 352493 usecs after Sat Apr 12 09:07:51 2008
    [RSP] Opc:MTS_OPC_MFDM_V4_ROUTE_STATS(75785), Id:0X000F188B, Ret:SUCCESS
    Src:0x00000101/214, Dst:0x00000101/1203, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x000F1888, Sync:NONE, Payloadsize:148
```

Review Draft -- Cisco Confidential

```
    Payload:
    0x0000:  01 00 00 00 05 00 01 00 00 04 00 00 00 00 00 00
6) Event:E_MTS_RX, length:60, at 342641 usecs after Sat Apr 12 09:06:51 2008
    [RSP] Opc:MTS_OPC_MFDM_V4_ROUTE_STATS(75785), Id:0X000F0DF0, Ret:SUCCESS
    Src:0x00000101/214, Dst:0x00000101/1203, Flags:None
    HA_SEQNO:0X00000000, RRtoken:0x000F0DED, Sync:NONE, Payloadsize:148
    Payload:
    0x0000:  01 00 00 00 05 00 01 00 00 04 00 00 00 00 00 00
7) Event:E_MTS_RX, length:60, at 332954 usecs after Sat Apr 12 09:05:51 2008
    [RSP] Opc:MTS_OPC_MFDM_V4_ROUTE_STATS(75785), Id:0X000F0493, Ret:SUCCESS
<--Output truncated-->
switch(config)#
```

Related Commands

Command	Description
ip routing multicast event-history	Configures the size of the IPv4 MRIB event history buffers.
clear ip routing multicast event-history	Clears information in the IPv4 MRIB event history buffers.

Review Draft -- Cisco Confidential

show routing multicast

To display information about IPv4 multicast routes, use the **show routing multicast** command.

show routing [**ip** | **ipv4**] **multicast** [**vrf** {*vrf-name* | **all** | **default** | **management**}]
{{*source group*} | {*group* [*source*]}}

Syntax Description

ip	(Optional) Specifies IPv4 routes.
ipv4	(Optional) Specifies IPv4 routes.
vrf	(Optional) Applies to a virtual routing and forwarding (VRF) instance.
vrf-name	VRF name. The name can be a maximum of 32 alphanumeric characters and is case sensitive.
all	Specifies all VRFs.
default	Specifies the default VRF.
management	Specifies the management VRF.
source	Source address for routes.
group	Group address for routes.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about IPv4 multicast routes:

```
switch(config)# show routing multicast
IP Multicast Routing Table for VRF "default"

(*, 232.0.0.0/8), uptime: 05:11:19, pim ip
  Incoming interface: Null, RPF nbr: 0.0.0.0
  Outgoing interface list: (count: 0)

switch(config)#
```

Review Draft -- Cisco Confidential

show routing multicast clients

To display information about IPv4 multicast routing clients, use the **show routing multicast clients** command.

show routing [**ip** | **ipv4**] **multicast clients** [*client-name*]

Syntax Description

ip	(Optional) Specifies IPv4 multicast clients.
ipv4	(Optional) Specifies IPv4 multicast clients.
client-name	(Optional) One of the following multicast routing client names: • mrib • igmp • static • msdp • ip • pim

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about IPv4 multicast clients:

```
switch(config)# show routing multicast clients pim
IP Multicast Routing Client information

Client: pim, client-id: 5, pid: 5296, mts-sap: 310
  Shared-memory: pim, Notifications: joins prunes rpf delete repopulate
  Protocol is ssm owner, bidir owner, shared-only mode owner,
  Join notifications:         sent 1, fail 0, ack rcvd 1
  Prune notifications:        sent 0, fail 0, ack rcvd 0
  RPF notifications:          sent 0, fail 0, ack rcvd 0
  Delete notifications:       sent 0, fail 0, ack rcvd 0
  Repopulate notifications:   sent 0, fail 0, ack rcvd 0
  Clear mroute notifications: sent 0, fail 0
  Add route requests:         rcvd 2, ack sent 2, ack fail 0
  Delete route requests:      rcvd 0, ack sent 0, ack fail 0
  Update route requests:      rcvd 0, ack sent 0, ack fail 0
```

Review Draft -- Cisco Confidential

```
  MTS update route requests:  rcvd 0, ack sent 0, ack fail 0
   Per VRF notification markers: 1

switch(config)#
```

Review Draft -- Cisco Confidential

show running-config pim

To display information about the running-system configuration for IPv4 Protocol Independent Multicast (PIM), use the **show running-config pim** command.

show running-config pim [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about the IPv4 PIM running-system configuration:

Need new output[1]

```
switch(config)# show running-config pim

!Command: show running-config pim
!Time: Sat Apr 12 09:15:11 2008

version 5.0(3)N1(1)
feature pim

ip pim ssm range 232.0.0.0/8

interface Vlan20
  ip pim sparse-mode

switch(config)#
```

1.

Review Draft -- Cisco Confidential

show startup-config pim

To display information about the startup-system configuration for IPv4 Protocol Independent Multicast (PIM), use the **show startup-config pim** command.

show startup-config pim [**all**]

Syntax Description

all	(Optional) Displays configured and default information.

Command Default

None

Command Modes

Any command mode

Command History

Release	Modification
6.0(2)N1(1)	This command was introduced.

Usage Guidelines

This command requires the LAN Base Services license.

Examples

This example shows how to display information about the startup-system configuration for IPv4 PIM:

```
switch(config)# show startup-config pim
```