I Commands

ipv6 mld robustness-variable

To configure a Multicast Listener Discovery (MLD) robustness count that you can tune to reflect the expected packet loss on a congested network, use the **ipv6 mld robustness-variable** command. To reset the count to the default, use the **no** form of this command.

ipv6 [**icmp**] **mld robustness-variable** *count*
no ipv6 [**icmp**] **mld robustness-variable** *[count]*

Syntax Description

icmp	(Optional) Specifies the Internet Control Message Protocol (ICMP) designator.
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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to configure a robustness count:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ipv6 mld 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 ipv6 mld robustness-variable
switch(config-if)#
```

Related Commands

Command	Description
show ipv6 mld interface	Displays information about ICMPv6 interfaces.

ipv6 mld ssm-translate

To translate Multicast Listener Discovery (MLD) version 1 reports to create (S, G) state entries so that the router treats them as MLDv2 membership reports, use the **ipv6 mld ssm-translate** command. To remove the translation, use the **no** form of this command.

ipv6 [**icmp**] **mld ssm-translate** *group source*
no ipv6 [**icmp**] **mld ssm-translate** *group source*

Syntax Description

icmp	(Optional) Specifies the Internet Control Message Protocol (ICMP) designator.
group	IPv6 multicast group range. By default, the group prefix range is FF3x/96. To modify the IPv6 Protocol Independent Multicast (PIM6) SSM range, see the **ipv6 pim ssm range** command.
source	IPv6 multicast source address.

Command Default

None

Command Modes

Global configuration (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 requires the Enterprise Services license.

Examples

This example shows how to configure a translation:

```
switch(config)# ipv6 mld ssm-translate FF30::0/16 2001:0DB8:0:ABCD::1
```

This example shows how to remove a translation:

```
switch(config)# no ipv6 mld ssm-translate FF30::0/16 2001:0DB8:0:ABCD::1
```

Related Commands

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

ipv6 mld startup-query-count

To configure the query count used when the Multicast Listener Discovery (MLD) process starts up, use the **ipv6 mld startup-query-count** command. To reset the query count to the default, use the **no** form of this command.

ipv6 [**icmp**] **mld startup-query-count** *count*
no ipv6 [**icmp**] **mld startup-query-count** *[count]*

Syntax Description

icmp	(Optional) Specifies the Internet Control Message Protocol (ICMP) designator.
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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to configure a query count:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ipv6 mld 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 ipv6 mld startup-query-count
switch(config-if)#
```

Related Commands

Command	Description
show ipv6 mld interface	Displays information about ICMPv6 interfaces.

ipv6 mld startup-query-interval

To configure the query interval used when the Multicast Listener Discovery (MLD) process starts up, use the **ipv6 mld startup-query-interval** command. To reset the query interval to the default, use the **no** form of this command.

ipv6 [**icmp**] **mld startup-query-interval** *interval*
no ipv6 [**icmp**] **mld startup-query-interval** *[interval]*

Syntax Description

icmp	(Optional) Specifies the Internet Control Message Protocol (ICMP) designator.
interval	Query interval in seconds. The range is from 1 to 18,000. The default is 31.

Command Default

The startup query interval is 31 seconds.

Command Modes

Interface configuration (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to configure a startup query interval:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ipv6 mld 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 ipv6 mld startup-query-interval
switch(config-if)#
```

Related Commands

Command	Description
show ipv6 mld interface	Displays information about ICMPv6 interfaces.

ipv6 mld state-limit

To configure the Multicast Listener Discovery (MLD) maximum states allowed, use the **ipv6 mld state-limit** command. To remove the limit, use the **no** form of this command.

ipv6 [**icmp**] **mld state-limit** *max-states* [**reserved** *reserve-policy max-reserved*]
no ipv6 [**icmp**] **mld state-limit** *max-states* [**reserved** *reserve-policy max-reserved*]

Syntax Description

icmp	(Optional) Specifies the Internet Control Message Protocol (ICMP) designator.
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 and set the maximum number of (*, G) and (S, G) entries allowed on the interface.

Command Default

None

Command Modes

Interface configuration (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to configure a state limit:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ipv6 mld 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 ipv6 mld state-limit
switch(config-if)#
```

Related Commands

Command	Description
show ipv6 mld interface	Displays information about ICMPv6 interfaces.

ipv6 mld static-oif

To statically bind a multicast group to the outgoing interface (OIF), which is handled by the device hardware, use the **ipv6 mld static-oif** command. To remove the static OIF, use the **no** form of this command.

ipv6 [**icmp**] **mld static-oif** {*group* [**source** *source*] | **route-map** *policy-name*}
no ipv6 [**icmp**] **mld static-oif** {*group* [**source** *source*] | **route-map** *policy-name*}

Syntax Description

icmp	(Optional) Specifies the Internet Control Message Protocol (ICMP) designator.
group	Multicast group IPv6 address. If you specify only the group address, the (*, G) state is created.
source*source*	(Optional) Configures the source IPv6 address for MLDv2 and creates the (S, G) state. **Note** A source tree is built for the (S, G) state only if you enable MLDv2, which is the default.
route-map*policy-name*	Specifies the route-map policy name that defines the group prefixes where this feature is applied.

Command Default

None

Command Modes

Interface configuration (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.2(1)	Added the keyword **route-map** and argument *policy-name* .

Usage Guidelines

The **match ipv6 multicast** command is the only **match** command that is evaluated in the route map. You can specify the group prefix, group range, and source prefix to filter messages with the **match ip**v6 **multicast** command.

This command requires the Enterprise Services license.

Examples

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

```
switch(config)# interface ethernet 2/2
switch(config-if)# ipv6 mld static-oif FFFE::1
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 ipv6 mld static oif FFFE::1
switch(config-if)#
```

Related Commands

Command	Description
show ipv6 mld local-groups	Displays information about the MLD local group membership.

ipv6 mld version

To configure the Multicast Listener Discovery (MLD) version on an interface, use the **ipv6 mld version** command. To reset the version to the default, use the **no** form of this command.

ipv6 mld version *version*
no ipv6 mld version *[version]*

Syntax Description

version	Version number. The number is 1 or 2. The default is 2.

Command Default

The version number is 2.

Command Modes

Interface configuration (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to configure the MLD version:

```
switch(config)# ipv6 mld version 1
```

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

```
switch(config)# no ipv6 mld version
```

Related Commands

Command	Description
show ipv6 mld interface	Displays information about ICMPv6 interfaces.

ipv6 pim anycast-rp

To configure an IPv6 Protocol Independent Multicast (PIM6) Anycast-RP peer for the specified Anycast-RP address, use the **ipv6 pim anycast-rp** command. To remove the peer, use the **no** form of this command.

ipv6 pim anycast-rp *anycast-rp rp-addr*
no ipv6 pim anycast-rp *anycast-rp rp-addr*

Syntax Description

anycast-rp	Address for the Anycast-RP address.
rp-addr	Address of the RP in the Anycast-RP set.

Command Default

None

Command Modes

Global configuration (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

This example shows how to configure a PIM Anycast-RP peer:

```
switch(config)# ipv6 pim anycast-rp 2001:0db8:0:abcd::3 2001:0db8:0:abcd::31
```

This example shows how to remove a peer:

```
switch(config)# no ipv6 pim anycast-rp 2001:0db8:0:abcd::3 2001:0db8:0:abcd::31
```

Related Commands

Command	Description
show ipv6 pim rp	Displays information about PIM6 RPs.

ipv6 pim bidir-rp-limit

To configure the number of bidirectional (Bidir) RPs for use in IPv6 Protocol Independent Multicast (PIM6), use the **ipv6 pim bidir-rp-limit** command. To reset the number of RPs to the default, use the **no** form of this command.

ipv6 pim bidir-rp-limit *limit*
no ipv6 pim bidir-rp-limit *limit*

Syntax Description

limit	Limit for the number of Bidir RPs permitted in PIM6. The range is from 0 to 8. The default is 2.

Command Default

The Bidir RP limit is 2.

Command Modes

Global configuration (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(2)	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)# ipv6 pim bidir-rp-limit 6
```

This example shows how to reset the number of Bidir RPs to the default:

```
switch(config)# no ipv6 pim bidir-rp-limit 6
```

Related Commands

Command	Description
ip pim bidir-rp-limit	Configures the number of Bidir RPs for PIM.
show running-config	Displays information about the running-system configuration.

ipv6 pim border

To configure an interface on an IPv6 Protocol Independent Multicast (PIM6) border, use the **ipv6 pim border** command. To remove an interface from a PIM6 border, use the **no** form of this command.

ipv6 pim border
no ipv6 pim border

Syntax Description

This command has no arguments or keywords.

Command Default

The interface is not on a PIM6 border.

Command Modes

Interface configuration (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to configure an interface on a PIM6 border:

```
switch(config)# ipv6 pim border
```

This example shows how to remove an interface from a PIM6 border:

```
switch(config)# no ipv6 pim border
```

Related Commands

Command	Description
show ipv6 pim interface	Displays information about PIM6-enabled interfaces.

ipv6 pim bsr bsr-policy

To enable filtering of IPv6 Protocol Independent Multicast (PIM6) bootstrap router (BSR) messages by the BSR client routers based on a route-map policy, use the **ipv6 pim bsr bsr-policy** command. To disable filtering, use the **no** form of this command.

ipv6 pim bsr bsr-policy *policy-name*
no ipv6 pim bsr bsr-policy *[policy-name]*

Syntax Description

policy-name	Route-map policy name.

Command Default

Disabled

Command Modes

Global configuration (config)VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can specify which source addresses to filter messages from with the **match ipv6 multicast** command in a route-map policy.

This command requires the Enterprise Services license.

Examples

This example shows how to enable filtering of BSR messages:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ipv6 pim bsr bsr-policy my_bsr_policy
```

This example shows how to disable filtering:

```
switch(config)# interface ethernet 2/2no ipv6 pim bsr bsr-policy
switch(config-if)# no ipv6 pim bsr bsr-policy
```

Related Commands

Command	Description
show ipv6 pim rp	Displays information about PIM6 RPs.

ipv6 pim bsr forward

To listen to and forward IPv6 Protocol Independent Multicast (PIM6) bootstrap router (BSR) and Candidate-RP messages, use the **ipv6 pim bsr forward** command. To disable listening and forwarding, use the **no** form of this command.

ipv6 pim bsr forward [**listen**]
no ipv6 pim bsr [**forward** [**listen**]]

Syntax Description

listen	(Optional) Specifies to listen to Bootstrap and Candidate-RP messages.
forward	Specifies to forward Bootstrap and Candidate-RP messages.

Command Default

Disabled

Command Modes

Global configuration (config)VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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.

This command has the same functionality as the **ipv6 pim bsr listen** command.

This command requires the Enterprise Services license.

Examples

This example shows how to listen to and forward BSR and Candidate-RP messages:

```
switch(config)# ipv6 pim bsr listen forward
```

This example shows how to disable listening and forwarding:

```
switch(config)# no ipv6 pim bsr listen forward
```

Related Commands

Command	Description
ipv6 pim bsr listen	Enables listening to and forwarding of BSR messages.
show ipv6 pim rp	Displays information about PIM6 RPs.

ipv6 pim bsr listen

To listen to and forward IPv6 Protocol Independent Multicast (PIM6) bootstrap router (BSR) and Candidate-RP messages, use the **ipv6 pim bsr listen** command. To disable listening and forwarding, use the **no** form of this command.

ipv6 pim bsr listen [**forward**]
no ipv6 pim bsr [**listen** [**forward**]]

Syntax Description

listen	(Optional) Specifies to listen to Bootstrap and Candidate-RP messages.
forward	(Optional) Specifies to forward Bootstrap and Candidate-RP messages.

Command Default

Disabled

Command Modes

Global configuration (config)VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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.

This command has the same functionality as the **ipv6 pim bsr forward** command

This command requires the Enterprise Services license.

Examples

This example shows how to listen to and forward BSR and Candidate-RP messages:

```
switch(config)# ipv6 pim bsr listen forward
```

This example shows how to disable listening and forwarding:

```
switch(config)# no ipv6 pim bsr listen forward
```

Related Commands

Command	Description
ipv6 pim bsr forward	Enables listening to and forwarding of BSR messages.
show ipv6 pim rp	Displays information about PIM6 RPs.

ipv6 pim bsr rp-candidate-policy

To filter IPv6 Protocol Independent Multicast (PIM6) bootstrap router (BSR) Candidate-RP messages that are based on a route-map policy, use the **ipv6 pim bsr rp-candidate-policy** command. To disable filtering, use the **no** form of this command.

ipv6 pim bsr rp-candidate-policy *policy-name*
no ipv6 pim bsr rp-candidate-policy *[policy-name]*

Syntax Description

policy-name	Route-map policy name.

Command Default

None

Command Modes

Global configuration (config)VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can specify the RP and group addresses and whether the type is Bidir or ASM with the **match ipv6 multicast** command in a route-map policy.

This command requires the Enterprise Services license.

Examples

This example shows how to filter Candidate-RP messages:

```
switch(config)# ipv6 pim bsr rp-candidate-policy my_bsr_rp_candidate_policy
```

This example shows how to disable message filtering:

```
switch(config)# no ipv6 pim bsr rp-candidate-policy
```

Related Commands

Command	Description
show ipv6 pim rp	Displays information about PIM6 RPs.

ipv6 pim bsr-candidate

To configure the router as an IPv6 Protocol Independent Multicast (PIM6) bootstrap router (BSR) candidate, use the **ipv6 pim bsr-candidate** command. To remove a router as a BSR candidate, use the **no** form of this command.

ipv6 pim [**bsr**] **bsr-candidate** *if-type if-number* [**hash-len** *hash-len*] [**priority** *priority*]
no ipv6 pim [**bsr**] **bsr-candidate** *if-type if-number* [**hash-len** *hash-len*] [**priority** *priority*]

Syntax Description

bsr	(Optional) Specifies the BSR protocol RP-distribution configuration.
if-type	Interface type. For more information, use the question mark (?) online help function.
if-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
hash-len*hash-len*	(Optional) Specifies the hash mask length used in BSR messages. The range is from 0 to 128. The default is 126.
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 126.The priority is 64.

Command Modes

Global configuration (config)VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to configure a router as a BSR candidate:

```
switch(config)# ipv6 pim bsr-candidate ethernet 2/2
```

This example shows how to remove a router as a BSR candidate:

```
switch(config)# no ipv6 pim bsr-candidate
```

Related Commands

Command	Description
show ipv6 pim rp	Displays information about PIM6 RPs.

ipv6 pim dr-priority

To configure the designated router (DR) priority that is advertised in IPv6 Protocol Independent Multicast (PIM6) hello messages, use the **ipv6 pim dr-priority** command. To reset the DR priority to the default, use the **no** form of this command.

ipv6 pim dr-priority *priority*
no ipv6 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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to configure the DR priority on an interface:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ipv6 pim dr-priority 5
```

This example shows how to reset the DR priority on an interface to the default:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ipv6 pim dr-priority
```

Related Commands

Command	Description
show ipv6 pim interface	Displays information about PIM6-enabled interfaces.

ipv6 pim event-history

To configure the size of the IPv6 Protocol Independent Multicast (PIM6) event history buffers, use the **ipv6 pim event-history** command. To revert to the default buffer size, use the **no** form of this command.

ipv6 pim event-history {**assert-receive** | **bidir** | **cli** | **hello** | **join-prune** | **null-register** | **packet** | **pim6-internal** | **rp** | **vrf**} **size** *buffer-size*
no ipv6 pim event-history {**assert-receive** | **bidir** | **cli** | **hello** | **join-prune** | **null-register** | **packet** | **pim6-internal** | **rp** | **vrf**} **size** *buffer-size*

Syntax Description

assert-receive	Configures the assert receive event history buffer.
bidir	Configures the Bidr 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.
pim6-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 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

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the size of the PIM6 hello event history buffer:

```
switch(config)# ipv6 pim event-history hello size medium
switch(config)#
```

Related Commands

Command	Description
clear ipv6 pim event-history	Clears information in the IPv6 PIM event history buffers.
show ipv6 pim event-history	Displays information in the IPv6 PIM event history buffers.
show running-config pim6	Displays information about the running-system PIM6 configuration.

ipv6 pim flush-routes

To remove routes when the IPv6 Protocol Independent Multicast (PIM6) process is restarted, use the **ipv6 pim flush-routes** command. To leave routes in place, use the **no** form of this command.

ipv6 pim flush-routes
no ipv6 pim flush-routes

Syntax Description

This command has no arguments or keywords.

Command Default

The routes are not flushed.

Command Modes

Global configuration (config)VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

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

```
switch(config)# ipv6 pim flush-routes
```

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

```
switch(config)# no ipv6 pim flush-routes
```

Related Commands

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

ipv6 pim hello-interval

To configure the IPv6 Protocol Independent Multicast (PIM6) hello-message interval on an interface, use the **ipv6 pim hello-interval** command. To reset the hello interval to the default, use the **no** form of this command.

ipv6 pim hello-interval *interval*
no ipv6 pim hello-interval *i[nterval]*

Syntax Description

interval	Interval in milliseconds. The range is from 1 to 4294967295. The default is 30000.

Command Default

The PIM6 hello interval is 30,000 milliseconds.

Command Modes

Interface configuration (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to configure the PIM6 hello-message interval on an interface:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ipv6 pim hello-interval 20000

This example shows how to reset the PIM6 hello message-interval on an interface to the
default:

switch(config)# interface ethernet 2/2
switch(config-if)# no ipv6 pim hello-interval
```

Related Commands

Command	Description
show ipv6 pim interface	Displays information about PIM6-enabled interfaces.

ipv6 pim jp-policy

To filter IPv6 Protocol Independent Multicast (PIM6) join-prune messages that are based on a route-map policy, use the **ipv6 pim jp-policy** command. To disable filtering, use the **no** form of this command.

ipv6 pim jp-policy *policy-name* [{**in** | **out**}]
no ipv6 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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.2(3)	The optional **in** and **out** parameters were added.

Usage Guidelines

Beginning with Cisco NX-OS Release 4.2(3), the **ipv6 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 arguments, that is no explicit direction, the system rejects further configurations if given with explicit direction.

You can specify group, group and source, or group and RP addresses to filter messages with the **match ipv6 multicast** command.

This command requires the Enterprise Services license.

Examples

This example shows how to filter PIM join-prune messages:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ipv6 pim jp-policy my_jp_policy
```

This example shows how to disable filtering:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ipv6 pim jp-policy
```

Related Commands

Command	Description
show ipv6 pim interface	Displays information about PIM6-enabled interfaces.

ipv6 pim log-neighbor-changes

To generate syslog messages that list the IPv6 Protocol Independent Multicast (PIM6) neighbor state changes, use the **ipv6 pim log-neighbor-changes** command. To disable messages, use the **no** form of this command.

ipv6 pim log-neighbor-changes
no ipv6 pim log-neighbor-changes

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration (config)VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to generate syslog message that list the PIM6 neighbor state changes:

```
switch(config)# ipv6 pim log-neighbor-changes
```

This example shows how to disable logging:

```
switch(config)# no ipv6 pim log-neighbor-changes
```

Related Commands

Command	Description
logging level ipv6 pim	Configures logging level of PIM6 messages.

ipv6 pim neighbor-policy

To configure a route-map policy that determines which IPv6 Protocol Independent Multicast (PIM6) neighbors should become adjacent, use the **ipv6 pim neighbor-policy** command. To reset to the default, use the **no** form of this command.

ipv6 pim neighbor-policy *policy-name*
no ipv6 pim neighbor-policy *[policy-name]*

Syntax Description

policy-name	Route-map policy name.

Command Default

Forms adjacency with all neighbors.

Command Modes

Interface configuration (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use the **match ipv6 address** command in a route-map policy to specify which groups to become adjacent to.

This command requires the Enterprise Services license.

Examples

This example shows how to configure a policy that determines which PIM6 neighbors should become adjacent:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ipv6 pim neighbor-policy
```

This example shows how to reset to the default:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ipv6 pim neighbor-policy
```

Related Commands

Command	Description
show ipv6 pim interface	Displays information about PIM6-enabled interfaces.

ipv6 pim register-policy

To filter IPv6 Protocol Independent Multicast (PIM6) Register messages that are based on a route-map policy, use the **ipv6 pim register-policy** command. To disable message filtering, use the **no** form of this command.

ipv6 pim register-policy *policy-name*
no ipv6 pim register-policy *[policy-name]*

Syntax Description

policy-name	Route-map policy name.

Command Default

Disabled

Command Modes

Global configuration (config)VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can use the **match ipv6 multicast** command in a route-map policy to specify the group or group and source addresses whose register messages that should be filtered.

To display the configured register policy, use this command line:

```
switch(config)# show running-config | include register-policy
```

This command requires the Enterprise Services license.

Examples

This example shows how to filter PIM6 Register messages:

```
switch(config)# ipv6 pim register-policy my_register_policy
```

This example shows how to disable message filtering:

```
switch(config)# no ipv6 pim register-policy
```

Related Commands

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

ipv6 pim register-rate-limit

To configure a rate limit for IPv6 Protocol Independent Multicast (PIM6) data registers, use the **ipv6 pim register-rate-limit** command. To remove a rate limit, use the **no** form of this command.

ipv6 pim register-rate-limit *rate*
no ipv6 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 (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(3)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a rate limit for PIM6 data registers:

```
switch(config)# ipv6 pim register-rate-limit 1000
```

This example shows how to remove a rate limit:

```
switch(config)# no ipv6 pim register-rate-limit
```

Related Commands

Command	Description
show ipv6 pim interface	Displays information about PIM6 interfaces.

ipv6 pim rp-address

To configure an IPv6 Protocol Independent Multicast (PIM6) static rendevous point (RP) address for a multicast group range, use the **ipv6 pim rp-address** command. To remove a static RP address, use the **no** form of this command.

ipv6 pim *rp-address* **rp-address** [{**group-list** *prefix* | **route-map** *policy-name*}] [**bidir**]
no ipv6 pim *rp-address* **rp-address** [{**group-list** *prefix* | **route-map** *policy-name*}] [**bidir**]

Syntax Description

rp-address	IPv6 address of the router, which is the RP for the group range.
group-list *prefix*	(Optional) Specifies a group range for a static RP.
route-map *prefix*	Specifies the route-map policy name.
bidir	(Optional) Specifies to handle group ranges in PIM6 bidirectional (Bidir) mode.

Command Default

The group range is treated in ASM mode.

Command Modes

Global configuration (config)VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.2(1)	Added the keyword **route-map** and argument *policy-name* .

Usage Guidelines

The **match ipv6 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 ipv6 multicast** command.

This command requires the Enterprise Services license.

Examples

This example shows how to configure a PIM6 static RP address for a group range:

```
switch(config)# ipv6 pim rp-address 2001:0db8:0:abcd::1 group-list ff1e:abcd:def1::0/96
```

This example shows how to remove a static RP address:

```
switch(config)# no ipv6 pim rp-address 2001:0db8:0:abcd::1
```

Related Commands

Command	Description
show ipv6 pim rp	Displays information about PIM6 RPs.

ipv6 pim rp-candidate

To configure the router as an IPv6 Protocol Independent Multicast (PIM6) bootstrap router (BSR) rendevous point (RP) candidate, use the **ipv6 pim rp-candidate** command. To remove the router as an RP candidate, use the **no** form of this command.

ipv6 pim [**bsr**] **rp-candidate** *if-type if-number* **group-list** *prefix* [**priority** *priority*] [**interval** *interval*] [**bidir**]
no ipv6 pim [**bsr**] **rp-candidate** *if-type if-number* **group-list** *prefix* [**priority** *priority*] [**interval** *interval*] [**bidir**]

Syntax Description

bsr	(Optional) Specifies the BSR protocol RP-distribution configuration.
if-type	Interface type. For more information, use the question mark (?) online help function.
if-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
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.
bidir	(Optional) Specifies the group range advertised in PIM6 bidirectional (Bidir) mode.

Command Default

The RP priority is 192.The BSR message interval is 60 seconds.

Command Modes

Global configuration (config)VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

We recommend that you configure the candidate RP interval to a minimum of 15 seconds.

This command requires the Enterprise Services license.

Examples

This example shows how to configure the router as a PIM6 BSR RP candidate:

```
switch(config)# ipv6 pim rp-candidate e 2/11 group-list ff1e:abcd:def1::0/24
```

This example shows how to remove the router as an RP candidate:

```
switch(config)# no ipv6 pim rp-candidate
```

Related Commands

Command	Description
show ipv6 pim rp	Displays information about PIM6 RPs.

ipv6 pim sparse-mode

To enable IPv6 Protocol Independent Multicast (PIM6) sparse mode on an interface, use the **ipv6 pim sparse-mode** command. To disable PIM6 on an interface, use the **no** form of this command.

ipv6 pim sparse-mode
no ipv6 pim [**sparse-mode**]

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to enable PIM6 sparse mode on an interface:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ipv6 pim sparse-mode
```

This example shows how to disable PIM6 on an interface:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ipv6 pim
```

Related Commands

Command	Description
show ipv6 pim interface	Displays information about PIM6-enabled interfaces.

ipv6 pim ssm range

To configure IPv6 Protocol Independent Multicast (PIM6) group ranges for Source Specific Multicast (SSM), use the **ipv6 pim ssm range** command. To reset the SSM group range to the default, use the **no** form of this command with the **none** keyword.

ipv6 pim ssm {**range** [{*groups* | **none**}] | **route-map** *policy-name*}
no ipv6 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 FF3x/96.

Command Modes

Global configuration (config)VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.1(2)	Keyword **none** was added.
4.2(1)	Added the keyword **route-map** and argument *policy-name* .

Usage Guidelines

The **match ipv6 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 ipv6 multicast** command.

This command requires the Enterprise Services license.

Examples

This example shows how to configure a PIM6 group range for SSM:

```
switch(config)# ipv6 pim ssm range FF30::0/32
```

This example shows how to reset the group range to the default:

```
switch(config)# no ipv6 pim ssm range none
```

This example shows how to remove all group ranges:

```
switch(config)# ipv6 pim ssm range none
```

Related Commands

Command	Description
show ipv6 pim group-range	Displays information about PIM6 group ranges.

ipv6 pim state-limit

To configure a maximum number of IPv6 Protocol Independent Multicast (PIM6) state entries in the current virtual routing and forwarding (VRF) instance, use the **ipv6 pim state-limit** command. To remove the limit on state entries, use the **no** form of this command.

ipv6 pim state-limit *max-states* [**reserved** *policy-name max-reserved*]
no ipv6 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 4294967295. 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.

Command Default

None

Command Modes

Global configuration (config)VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 Enterprise 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)# ipv6 pim state-limit 100000 reserved my_reserved_policy 40000
```

This example shows how to remove the limits on state entries:

```
switch(config)# no ipv6 pim state-limit
```

Related Commands

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

ipv6 pim use-shared-tree-only

To create IPv6 Protocol Independent Multicast (PIM6) (*, G) state only (where no source state is created), use the **ipv6 pim use-shared-tree-only** command. To remove the creation of shared tree state only, use the **no** form of this command.

ipv6 pim use-shared-tree-only group-list *policy-name*
no ipv6 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 (config)VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.1(2)	Keyword **group-list** was added and a route-map policy name is used to define groups.

Usage Guidelines

You can use the **match ipv6 multicast** command in a route-map policy to specify the groups where shared trees should be enforced.

This command requires the Enterprise Services license.

Examples

This example shows how to create the PIM6 (*, G) state only for the group prefixes defined in my_group_policy:

```
switch(config)# ipv6 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 ipv6 pim use-shared-tree-only
```

Related Commands

Command	Description
show ipv6 pim rp	Displays information about PIM6 RPs.

ipv6 routing multicast event-history

To configure the size of the IPv6 Multicast Routing Information Base (M6RIB) event history buffers, use the **ipv6 routing multicast event-history** command. To revert to the default buffer size, use the **no** form of this command.

ipv6 routing multicast event-history {**cli** | **mfdm-debugs** | **mfdm-events** | **mfdm-stats** | **rib** | **vrf**} **size** *buffer-size*
no ipv6 routing multicast event-history {**cli** | **mfdm-debugs** | **mfdm-stats** | **rib** | **vrf**} **size** *buffer-size*

Syntax Description

cli	Configures the CLI event history buffer.
mfdm-debugs	Configures the multicast FIB distribution (MFDM) 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

Any command mode

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.
4.2(1)	Added the keyword **mfdm-events**. Changed the keyword **mfdm** to **mfdm-debugs**.

Usage Guidelines

To display configured buffer sizes, use this command line:

```
switch(config)# show running-config | include "ipv6 routing"
```

This command does not require a license.

Examples

This example shows how to configure the size of the M6RIB MFDM event history buffer:

```
switch(config)# ipv6 routing multicast event-history mfdm size large
switch(config)#
```

Related Commands

Command	Description
clear ipv6 routing multicast event-history	Clears information in the IPv6 M6RIB event history buffers.
show routing ipv6 multicast event-history	Displays information in the IPv6 M6RIB event history buffers.
show running-config	Displays information about the running-system configuration.

ipv6 routing multicast holddown

To configure the IPv6 multicast routing initial holddown period, use the **ipv6 routing multicast holddown** command. To revert to the default holddown period, use the **no** form of this command.

ipv6 routing multicast holddown *holddown-period*
no ipv6 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 (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.2(1)	This command was introduced.

Usage Guidelines

To display the holddown period configuration, use this command line:

```
switch(config)# show running-config | include "ipv6 routing multicast holddown"
```

This command does not require a license.

Examples

This example shows how to configure the routing holddown period:

```
switch(config)# ipv6 routing multicast holddown 100
switch(config)#
```

Related Commands

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

ipv6 routing multicast software-replicate

To enable software replication of IPv6 Protocol Independent Multicast (PIM) Any Source Multicast (ASM) packets that are leaked to the software for state creation, use the **ipv6 routing multicast software-replicate** command. To reset to the default, use the **no** form of this command.

ipv6 routing multicast software-replicate
no ipv6 routing multicast software-replicate

Syntax Description

This command has no arguments or keywords.

Command Default

No software replication.

Command Modes

Global configuration (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.2(3)	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 IPv6 PIM ASM packets:

```
switch(config)# ipv6 routing multicast software-replicate
switch(config)#
```

Related Commands

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

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.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 requires the Enterprise Services 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.

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 (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.1(2)	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.

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 {**clis** | **errors** | **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** | **errors** | **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.
errors	Configures the error 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

Supported User Roles

network-admin

network-operator

vdc-admin

vdc-operator

Command History

Release	Modification
4.1(2)	This command was introduced.
4.1(3)	Replaced the buffer type keywords **debug** and **event** with keywords **group-debugs**, **group-events**, **interface-debugs**, and **interface-events**.

Usage Guidelines

This command does not require a license.

Examples

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

```
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.

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 (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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.

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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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.

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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.1(3)	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.

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.

Command Default

None

Command Modes

Interface configuration (config-if) Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.2(1)	Added the keyword **route-map** and argument *policy-name* .

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.

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

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.

Beginning with Cisco NX-OS Release 5.2, if ip igmp join-group is configured under any interface, other interfaces will be removed from the outgoing interface list (OIL) resulting in multicast packet loss. The command ip igmp join-group must be only used for testing and must not be present on a production device. Use the ip igmp static-oif command instead.

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:

```
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.
ip igmp static-oif	Statically binds a multicast group to the OIF.

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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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.

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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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.

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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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.

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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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.

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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure a query 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 query 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
show ip igmp interface	Displays IGMP information about the interface.

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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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.

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 policy name is case sensitive alphanumeric, maximum size is 32 characters.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 a 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.

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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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.

ip igmp snooping (Global)

To enable IGMP snooping for the current virtual device context (VDC), use the **ip igmp snooping** command. To disable IGMP snooping for the current VDC, 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 (config) Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

If the global configuration of IGMP snooping is disabled, 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 for the current VDC:

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

This example shows how to disable IGMP snooping for the current VDC:

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

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

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 (config-vlan) mode (until Cisco NX-OS Release 5.1)

Configure VLAN (config-vlan-config) mode (Since Cisco NS-OS Release 5.1(1). You cannot configure this command in the VLAN configuration mode in Cisco Release NX-OS 5.1 and higher.)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
NX-OS 5.1(1)	The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.
4.0(1)	This command was introduced.

Usage Guidelines

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

See the Layer2 Command Reference Guide for information on entering the Configure VLAN mode by using the vlan configuration command.

This command does not require a license.

Examples

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

```
switch(config)# vlan configuration 10
switch(config-vlan-config)# ip igmp snooping
switch(config-vlan-config)# ]
```

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

```
switch(config)#vlan configuration 10
switch(config-vlan)#no ip igmp snooping
switch(config-vlan-config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

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

Syntax Description

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 Forwarding Distribution Module (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-event 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 Supported User Roles

network-admin

network-operato

rvdc-admin

vdc-operator

Command History

Release	Modification
4.1(2)	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)#
```

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.

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 (config-vlan) (until Cisco NX-OS Release 5.1)

Configure VLAN (config-vlan-config) mode (Since Cisco NS-OS Release 5.1(1). You cannot configure this command in the VLAN configuration mode in Cisco Release NX-OS 5.1 and higher).

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
NX-OS 5.1(1)	The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

See the Layer2 Command Reference Guide for information on entering the Configure VLAN mode by using the vlan configuration command.

Examples

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

```
switch(config)#vlan configuration 10
switch(config-vlan-config)#ip igmp snooping explicit-tracking
switch(config-vlan-config)#
```

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

```
switch(config)#vlan configuration 10
switch(config-vlan-config)#no ip igmp snooping explicit-tracking
switch(config-vlan-config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

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 (config-vlan) mode (until Cisco NX-OS Release 5.1)

Configure VLAN (config-vlan-config) mode (Since Cisco NS-OS Release 5.1(1). You cannot configure this command in the VLAN configuration mode in Cisco Release NX-OS 5.1 and higher).

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
NX-OS 5.1(1)	The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.
4.0(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.

See the Layer2 Command Reference Guide for information on entering the Configure VLAN mode by using the vlan configuration command.

This command does not require a license.

Examples

This example shows how to enable support of IGMPv2 hosts:

```
switch(config)#vlan configuration 10
switch(config-vlan-config)#ip igmp snooping fast-leave
switch(config-vlan-config)#
```

This example shows how to disable support of IGMPv2 hosts:

```
switch(config)#vlan configuration 10
switch(config-vlan-config)#no ip igmp snooping fast-leave
switch(config-vlan-config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping group-timeout

To configure group membership timeout in all VLANs, use the **ip igmp snooping group-timeout** command. To return to the default settings, use the **no** form of this command.

{**ip igmp snooping group-timeout** *timeout* | **never**}
no ip igmp snooping group-timeout *timeout*

Syntax Description

timeout	Timeout in minutes. The range is from 1 to 10080.
never	Never expire ports from group membership.

Command Default

None

Command Modes

Global Configuration mode

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure group membership timeout in all VLANs:

```
switch(config)#ip igmp snooping group-timeout 100
switch(config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping group-timeout (VLAN)

To configure group membership timeout in all VLANs, use the **ip igmp snooping group-timeout** command. To return to the default settings, use the **no** form of this command.

{**ip igmp snooping group-timeout** *timeout* | **never**}
no ip igmp snooping group-timeout *timeout*

Syntax Description

timeout	Timeout in minutes. The range is from 1 to 10080.
never	Never expire ports from group membership.

Command Default

None

Command Modes

VLAN configuration (config-vlan) mode (until Cisco NX-OS Release 5.1)

Configure VLAN (config-vlan-config) mode (Since Cisco NS-OS Release 5.1(1). You cannot configure this command in the VLAN configuration mode in Cisco Release NX-OS 5.1 and higher).

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
NX-OS 5.1(1)	The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.
4.1(2)	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.

See the Layer2 Command Reference Guide for information on entering the Configure VLAN mode by using the vlan configuration command.

This command does not require a license.

Examples

This example shows how to configure group membership timeout in all VLANs:

```
switch(config)#ip igmp snooping group-timeout 100
switch(config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

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 (config-vlan) until Cisco NX-OS Release 5.1. Configure VLAN (config-vlan-config) since Cisco NS-OS Release 5.1(1). You cannot configure this command in the VLAN configuration mode in Cisco Release NX-OS 5.1 and higher.

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
NX-OS 5.1(1)	The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

See the Layer2 Command Reference Guide for information on entering the Configure VLAN mode by using the vlan configuration command.

Examples

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

```
switch(config)#vlan configuration 10
switch(config-vlan-config)#ip igmp snooping last-member-query-interval 3
switch(config-vlan-config)#
```

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

```
switch(config)#vlan configuration 10
switch(config-vlan-config)#no ip igmp snooping last-member-query-interval
switch(config-vlan-config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

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 (config)

VLAN configuration (config-vlan) until Cisco NX-OS Release 5.1.

Configure VLAN (config-vlan-config) since Cisco NS-OS Release 5.1(1). You cannot configure this command in the VLAN configuration mode in Cisco Release NX-OS 5.1 and higher.

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
NX-OS 5.1(1)	The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

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

See the Layer2 Command Reference Guide for information on entering the Configure VLAN mode by using the vlan configuration command.

Examples

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

```
switch(config)#vlan configuration 10
switch(config-vlan-config)#ip igmp snooping link-local-groups-suppression
switch(config-vlan-config)#
```

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

```
switch(config)#vlan configuration 10
switch(config-vlan-config)#no ip igmp snooping link-local-groups-suppression
switch(config-vlan-config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping max-gq-miss

To configure the maximum number of general query misses permitted for IGMP snooping, use the **ip igmp snooping max-gq-miss** command. To remove the default settings, use the **no** form of this command.

ip igmp snooping max-gq-miss count
no ip igmp snooping max-gq-miss *count*

Syntax Description

count	Specifies the IGMP snooping count. The range is from 3 to 5 queries. The default is 3 queries.

Command Default

3

Command Modes

Global configuration mode.

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
6.2(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the maximum number of general query misses permitted for IGMP snooping:

```
switch(config)#config t
switch(config)#ip igmp snooping max-gq-miss 5
switch(config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

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 *if-type if-number*
no ip igmp snooping mrouter interface *if-type if-number*

Syntax Description

if-type	Interface type. For more information, use the question mark (?) online help function.
if-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

None

Command Modes

VLAN configuration (config-vlan) until Cisco NX-OS Release 5.1.

Configure VLAN (config-vlan-config) since Cisco NS-OS Release 5.1(1). You cannot configure this command in the VLAN configuration mode in Cisco Release NX-OS 5.1 and higher.

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
NX-OS 5.1(1)	The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

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

See the Layer2 Command Reference Guide for information on entering the Configure VLAN mode by using the vlan configuration command.

Examples

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

```
switch(config)#vlan configuration 10
switch(config-vlan-config)#ip igmp snooping mrouter interface ethernet 2/1
switch(config-vlan-config)#
```

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

```
switch(config)#vlan configuration 10
switch(config-vlan-config)#no ip igmp snooping mrouter interface ethernet 2/1
switch(config-vlan-config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping optimised-multicast-flood

To configure Optimized Multicast Flood (OMF) on the VLAN, use the **ip igmp snooping optimised-multicast flood** command. To return to the default settings, use the **no** form of this command.

ip igmp snooping optimised-multicast-flood
no ip igmp snooping optimised-multicast-flood

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

VLAN configuration (config-vlan) until Cisco NX-OS Release 5.1.

Configure VLAN (config-vlan-config) since Cisco NS-OS Release 5.1(1). You cannot configure this command in the VLAN configuration mode in Cisco Release NX-OS 5.1 and higher.

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
NX-OS 5.1(1)	The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

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

See the Layer2 Command Reference Guide for information on entering the Configure VLAN mode by using the vlan configuration command.

Examples

This example shows how to configure OMF on the VLAN:

```
switch(config)# vlan configuration 10
switch(config-vlan-config)# ip igmp snooping optimised-multicast-flood
switch(config-vlan-config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping proxy

To configure IGMP snooping proxy, use the **ip igmp snooping proxy** command. To return to the default settings, use the **no** form of this command.

ip igmp snooping proxy general-queries
no ip igmp snooping proxy general-queries

Syntax Description

general-queries	Specifies proxy for general queries.

Command Default

None

Command Modes

Global Configuration mode

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure proxy for general queries:

```
switch(config)#ip igmp snooping proxy general-queries
switch(config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping proxy (VLAN)

To configure IGMP snooping proxy, use the **ip igmp snooping proxy** command. To return to the default settings, use the **no** form of this command.

ip igmp snooping proxy general-queries
no ip igmp snooping proxy general-queries

Syntax Description

general-queries	Specifies proxy for general queries.

Command Default

None

Command Modes

VLAN configuration (config-vlan) until Cisco NX-OS Release 5.1.

Configure VLAN (config-vlan-config) since Cisco NS-OS Release 5.1(1). You cannot configure this command in the VLAN configuration mode in Cisco Release NX-OS 5.1 and higher.

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
NX-OS 5.1(1)	The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a license.

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

See the Layer2 Command Reference Guide for information on entering the Configure VLAN mode by using the vlan configuration command.

Examples

This example shows how to configure proxy for general queries:

```
switch(config)# ip igmp snooping proxy general-queries
switch(config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping querier

To configure a snooping querier on an interface when you do not enable Protocol Independent Multicast (PIM) because the 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 (config-vlan) until Cisco NX-OS Release 5.1.

Configure VLAN (config-vlan-config) since Cisco NS-OS Release 5.1(1). You cannot configure this command in the VLAN configuration mode in Cisco Release NX-OS 5.1 and higher.

network-adminvdc-admin

Command History

Release	Modification
NX-OS 5.1(1)	The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

See the Layer2 Command Reference Guide for information on entering the Configure VLAN mode by using the vlan configuration command.

Examples

This example shows how to configure a snooping querier:

```
switch(config)#vlan configuration 10
switch(config-vlan-config)#ip igmp snooping querier 172.20.52.106
switch(config-vlan-config)#
```

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

```
switch(config)#vlan configuration 10
switch(config-vlan-config)#no ip igmp snooping querier
switch(config-vlan-config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping querier-timeout

To configure the querier timeout for IGMPv2, use the **ip igmp snooping querier-timeout** command. To remove the snooping querier, use the **no** form of this command.

ip igmp snooping querier-timeout *sec*
no ip igmp snooping querier-timeout *sec*

Syntax Description

sec	Time in seconds. The range is from 1to 65535.

Command Default

255 seconds

Command Modes

VLAN configuration (config-vlan)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the querier timeout for IGMPv2:

```
switch(config)#vlan configuration 10
switch(config-vlan-config)#ip igmp snooping querier-timeout 3
switch(config-vlan-config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping query-interval

To configure the interval between query transmission, use the **ip igmp snooping query-interval** command. To remove the snooping querier, use the **no** form of this command.

ip igmp snooping query-interval *sec*
no ip igmp snooping query-interval *sec*

Syntax Description

sec	Interval in seconds. The range is from 1 to 18000.

Command Default

125 seconds

Command Modes

VLAN configuration (config-vlan)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the interval between query transmission:

```
switch(config)#vlan configuration 10
switch(config-vlan-config)#ip igmp snooping query-interval 3
switch(config-vlan-config)# er than mrt, configure query-max-response-time
first
switch(config-vlan-config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping query-max-response-time

To configure the MRT for query messages, use the **ip igmp snooping query-max-response-time** command. To return to the default settings, use the **no** form of this command.

ip igmp snooping query-max-response-time *sec*
no ip igmp snooping query-max-response-time *sec*

Syntax Description

sec	Time in seconds. The range is from 1 to 25.

Command Default

10 seconds

Command Modes

VLAN configuration (config-vlan)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the MRT for query messages:

```
switch(config)#vlan configuration 10
switch(config-vlan-config)# ip igmp snooping query-max-response-time 20
switch(config-vlan-config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

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 (config)VLAN configuration (config-vlan) until Cisco NX-OS Release 5.1.

Configure VLAN (config-vlan-config) since Cisco NS-OS Release 5.1(1). You cannot configure this command in the VLAN configuration mode in Cisco Release NX-OS 5.1 and higher.

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
NX-OS 5.1(1)	The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.
4.0(1)	This command was introduced.
4.0(3)	Global configuration mode was added.

Usage Guidelines

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

See the Layer2 Command Reference Guide for information on entering the Configure VLAN mode by using the vlan configuration command.

This command does not require a license.

Examples

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

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

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

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

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping robustness-variable

To configure the RFC defined robustness variable, use the **ip igmp snooping robustness-variable** command. To return to the default settings, use the **no** form of this command.

ip igmp snooping robustness-variable *value*
no ip igmp snooping robustness-variable *value*

Syntax Description

value	Count value. The range is from 1 to 7.

Command Default

2

Command Modes

VLAN configuration (config-vlan)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the configure the RFC defined robustness variable:

```
switch(config)#vlan configuration 10
switch(config-vlan-config)#ip igmp snooping robustness-variable 4
switch(config-vlan-config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping startup-query-count

To configure the number of queries sent at startup, use the **ip igmp snooping startup-query-count** command. To return to the default settings, use the **no** form of this command.

ip igmp snooping startup-query-count *value*
no ip igmp snooping startup-query-count *value*

Syntax Description

value	Count value. The range is from 1 to 10.

Command Default

None

Command Modes

VLAN configuration (config-vlan)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
NX-OS 5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the number of queries sent at startup:

```
switch(config)#vlan configuration 10
switch(config-vlan-config)#ip igmp snooping startup-query-count 4
switch(config-vlan-config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping startup-query-interval

To configure the query interval at startup, use the **ip igmp snooping startup-query-interval** command. To return to the default settings, use the **no** form of this command.

ip igmp snooping startup-query-interval *sec*
no ip igmp snooping startup-query-interval *sec*

Syntax Description

sec	Interval in seconds. The range is from 1 to 18000.

Command Default

None

Command Modes

VLAN configuration (config-vlan)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
NX-OS 5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure the query interval at startup:

```
switch(config)#vlan configuration 10
switch(config-vlan-config)#ip igmp snooping startup-query-interval 4
switch(config-vlan-config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

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** *if-type if-number*
no ip igmp snooping static-group *group* [**source** *source*] **interface** *if-type 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.
if-type	Interface type. For more information, use the question mark (?) online help function.
if-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

None

Command Modes

VLAN configuration (config-vlan) until Cisco NX-OS Release 5.1.

Configure VLAN (config-vlan-config) since Cisco NS-OS Release 5.1(1). You cannot configure this command in the VLAN configuration mode in Cisco Release NX-OS 5.1 and higher.

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
NX-OS 5.1(1)	The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.
4.0(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

See the Layer2 Command Reference Guide for information on entering the Configure VLAN mode by using the vlan configuration command.

Examples

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

```
switch(config)#vlan configuration 10
switch(config-vlan-config)#ip igmp snooping static-group 230.0.0.1 interface ethernet 2/1
switch(config-vlan-config)#
```

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

```
switch(config)#vlan configuration 10
switch(config-vlan-config)#no ip igmp snooping static-group 230.0.0.1 interface ethernet
2/1
switch(config-vlan-config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

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 (config) Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(3)	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.

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 (config-vlan) until Cisco NX-OS Release 5.1.

Configure VLAN (config-vlan-config) since Cisco NS-OS Release 5.1(1). You cannot configure this command in the VLAN configuration mode in Cisco Release NX-OS 5.1 and higher.

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
NX-OS 5.1(1)	The mode to configure this command on a VLAN changed to the configure VLAN mode (config-vlan-config)#. You can no longer configure this command in the VLAN configuration mode (config-vlan)#.
4.0(3)	This command was introduced.

Usage Guidelines

If this setting is disabled for the device, which is the default value, 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.

See the Layer2 Command Reference Guide for information on entering the Configure VLAN mode by using the vlan configuration command.

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

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

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

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

ip igmp snooping version

To configure the IGMP version number for VLAN, use the **ip igmp snooping version** command. To return to the default settings, use the **no** form of this command.

ip igmp snooping version *value*
no ip igmp snooping version *value*

Syntax Description

value	Version number value. The range is from 2 to 3.

Command Default

None

Command Modes

VLAN configuration (config-vlan)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
5.1(1)	This command was introduced.

Usage Guidelines

This command does not require a license.

Examples

This example shows how to configure IGMP version number for VLAN:

```
switch(config-vlan-config)#ip igmp snooping version 3
switch(config-vlan-config)#
```

Related Commands

Command	Description
show ip igmp snooping	Displays IGMP snooping information.

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 (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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(config)#ip igmp ssm-translate 232.0.0.0/8 10.1.1.1
```

This example shows how to remove a translation:

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

Related Commands

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

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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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.

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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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.

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 and set the maximum number of (*, G) and (S, G) entries allowed on the interface.

Command Default

None

Command Modes

Interface configuration (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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.

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.

Command Default

None

Command Modes

Interface configuration (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.2(1)	Added the keyword **route-map** and argument *policy-name* .

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, group range, and source prefix to filter messages with the **match ip multicast** 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)#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 ip igmp static oif 230.0.0.0
switch(config-if)#
```

Related Commands

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

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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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.

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-maskip-prefix*} {{*next-hopnh-prefix*} | *if-type if-number*} [*pref*] [**vrf** *vrf-name*]
no ip mroute {*ip-addr ip-maskip-prefix*} {{*next-hopnh-prefix*} | *if-type if-number*} [*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.
if-type	Interface type. For more information, use the question mark (?) online help function.
if-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
pref	(Optional) Route preference. The range is from 1 to 255. The default is 1.
vrf *vrf-name*	(Optional) Applies to the specified virtual routing and forwarding (VRF) instance.

Command Default

The route preference is 1.

Command Modes

Global configuration (config)

network-adminvdc-admin

Command History

Release	Modification
4.0(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 192.168.1.0/24 192.168.2.0/24
switch(config)#
```

This example shows how to remove an RPF static route:

```
switch(config)#no ip mroute 192.168.1.0/24 192.168.2.0/24
switch(config)#
```

Related Commands

Command	Description
show ip mroute	Displays information about multicast routes.

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 (config)

network-adminvdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise 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.

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

Supported User Roles

network-admin

network-operator

vdc-admin

vdc-operator

Command History

Release	Modification
4.1(2)	This command was introduced.
4.1(3)	Changed the buffer type arguments to required.

Usage Guidelines

This command does not require a 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.
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.

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 (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 Enterprise 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 leave routes in place 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.

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 (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise 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.

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 (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise 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.

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 the mesh group.

Command Default

None

Command Modes

Global configuration (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise 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.

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 *if-type if-number*
no ip msdp originator-id [*if-type if-number*]

Syntax Description

if-type	Interface type. For more information, use the question mark (?) online help function.
if-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

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

Command Modes

Global configuration (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

We recommend that you use a loopback interface for the RP address.

This command requires the Enterprise 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.

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 (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise 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.

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** *if-type if-number* [**remote-as** *asn*]
no ip msdp peer *peer-address* **connect-source** *if-type if-number* [**remote-as** *asn*]

Syntax Description

peer-address	IP address of the MSDP peer.
connect-source	Configures a local IP address for a TCP connection.
if-type	Interface type. For more information, use the question mark (?) online help function.
if-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
remote-as *asn*	(Optional) Configures a remote autonomous system (AS) number.

Command Default

None

Command Modes

Global configuration (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.0(3)	The remote AS number was made an optional argument.

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 Enterprise 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
```

Related Commands

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

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 (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise 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.

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 (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 Enterprise 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.

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 (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise 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.

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 (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise 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.

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 (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise 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.

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 (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise 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.

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 (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 Enterprise Services license.

Examples

This example shows how to configure a PIM Anycast-RP peer:

```
switch(config)#
ip pim anycast-rp 192.0.2.3 192.0.2.31
```

This example shows how to remove a peer:

```
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.

ip pim auto-rp listen

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 (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise 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.

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 *if-type if-number* [**scope** *ttl*]
no ip pim auto-rp mapping-agent [*if-type if-number*] [**scope** *ttl*]

Syntax Description

if-type	Interface type. For more information, use the question mark (?) online help function.
if-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
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 (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 Enterprise 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
```

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.

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 (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 Enterprise 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.

ip pim auto-rp rp-candidate

To configure an IPv4 Protocol Independent Multicast (PIM) Auto-RP candidate rendevous point (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 *if-type if-number* **group-list** *prefix* {[**scope** *ttl*] | [**interval** *interval*] | [**bidir**]}
no ip pim auto-rp rp-candidate *if-type if-number* **group-list** *prefix* {[**scope** *ttl*] | [**interval** *interval*] | [**bidir**]}

Syntax Description

if-type	Interface type. For more information, use the question mark (?) online help function.
if-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
group-list *prefix*	Specifies the group range used for the access list.
priority *priority*	(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.
bidir	(Optional) Specifies that the group range is advertised in PIM bidirectional (Bidir) mode.

Command Default

The TTL is 32.The Announce message interval is 60 seconds.

Command Modes

Global configuration (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **scope**, **interval**, and **bidir** 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.

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 Enterprise 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.

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 (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can specify the RP and group addresses, and whether the type is Bidir or ASM with the **match ip multicast** command in a route-map policy.

This command requires the Enterprise 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.

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.

Command Default

The Bidir RP limit is 6.

Command Modes

Global configuration (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(2)	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
```

Related Commands

Command	Description
ipv6 pim bidir-rp-limit	Configures the number of Bidir RPs for PIM6.

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

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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise 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.

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 (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 Enterprise 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.

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 (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 Enterprise 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.

Command	Description
show ip pim rp	Displays information about PIM RPs.

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 (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 Enterprise 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.

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 (config)VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

You can specify the RP and group addresses and whether the type is Bidir or ASM with the **match ip multicast** command in a route-map policy.

This command requires the Enterprise 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.

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** *if-type if-number* [*hash-len* **hash-len**] [**priority** *priority*]
no ip pim [**bsr**] **bsr-candidate** [*if-type if-number*] [**hash-len** *hash-len*] [**priority** *priority*]

Syntax Description

bsr	(Optional) Specifies the BSR protocol RP-distribution configuration.
if-type	Interface type. For more information, use the question mark (?) online help function.
if-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
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 (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 Enterprise 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:

```
switch(config)#
no ip pim bsr-candidate
```

Related Commands

Command	Description
show ip pim rp	Displays information about PIM RPs.

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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to configure the 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 the 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.

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** | **bidir** | **cli** | **hello** | **join-prune** | **null-register** | **packet** | **pim-internal** | **rp** | **vrf**} **size** *buffer-size*
no ip pim event-history {**assert-receive** | **bidir** | **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.
bidir	Configures the Bidir 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

Supported User Roles

network-admin

network-operator

vdc-admin

vdc-operator

Command History

Release	Modification
4.1(2)	This command was introduced.

Usage Guidelines

This command does not require a 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)#
```

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.

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 (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 Enterprise 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.

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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 Enterprise 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
```

Related Commands

Command	Description
show ip pim interface	Displays information about PIM-enabled interfaces.

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 1000 to 18724286. The default is 30000. **Note** We do not support aggressive 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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
5.2	Changed the minimum value from 1 millisecond to 1000 milliseconds and maximum value from 4294967295 to 18724286.
4.0(1)	This command was introduced.

Usage Guidelines

We recommend that you use BFD for PIM instead of non-default timers.

.This command requires the Enterprise 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.

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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.2(3)	The optional **in** and **out** parameters were added.

Usage Guidelines

Beginning with Cisco NX-OS Release 4.2(3), the **ip pim jp-policy** command filters messages in both incoming and outgoing directions. To specify filtering on only incoming messages, use the optional **in** keyword; to specify filtering on only outgoing messages, use the optional **out** keyword.

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 Enterprise 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

Command	Description
show ip pim interface	Displays information about PIM-enabled interfaces.

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 (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to generate a syslog message that lists 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.

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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 Enterprise 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.

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 (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.2(3)	This command was introduced.

Usage Guidelines

To prebuild the SPT for all known (S,G)s joins 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 Enterprise 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)#
```

Related Commands

Command	Description
show ip pim context	Displays information about PIM routes.

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 (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 Enterprise 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.

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 (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(3)	This command was introduced.

Usage Guidelines

This command does not require a 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.

ip pim register-until-stop

To configure the device to continue to send PIM data registers from the first-hop router until a PIM register-stop message is received, use the ip pim register-until-stop command. To return to default setting, use the no form of this command.

ip pim register-until-stop
no ip pim register-until-stop

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
5.2(1)	This command was introduced.

Usage Guidelines

Must have PIM enabled.

This command does not require a license.

Examples

This example shows how to configure send data registers till register stop is received:

```
switch(config)#
ip pim register-until-stop
```

Related Commands

Command	Description
show running-config pim	Displays the current operating information about the PIM configuration.

ip pim rp-address

To configure an IPv4 Protocol Independent Multicast (PIM) static rendezvous point (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*}] [**bidir**]
no ip pim *rp-address* **rp-address** [{**group-list** *prefix* | **override** | **route-map** *policy-name*}] [**bidir**]

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.
bidir	(Optional) Specifies to handle a group range in PIM bidirectional (Bidir) mode.

Command Default

The group range is treated in ASM mode.

Command Modes

Global configuration (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
5.1(1)	Added the keyword override.
4.0(1)	This command was introduced.
4.2(1)	Added the keyword **route-map** and argument *policy-name* .

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.

You can use this override provision, if you want the static RPs always to override the dynamic ones.

This command requires the Enterprise 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)# i
p 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
```

Related Commands

Command	Description
show ip pim rp	Displays information about PIM RPs.

ip pim rp-candidate

To configure the router as an IPv4 Protocol Independent Multicast (PIM) bootstrap router (BSR) rendezvous point (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** *if-type if-number* **group-list** *prefix* [**priority** *priority*] [**interval** *interval*] [**bidir**]
no ip pim [**bsr**] **rp-candidate** [*if-type if-number*] **group-list** *prefix* [**priority** *priority*] [**interval** *interval*] [**bidir**]

Syntax Description

bsr	(Optional) Specifies the BSR protocol RP-distribution configuration.
if-type	Interface type. For more information, use the question mark (?) online help function.
if-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
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.
bidir	(Optional) Specifies the group range advertised in PIM bidirectional (Bidir) mode.

Command Default

The RP priority is 192.The BSR message interval is 60 seconds.

Command Modes

Global configuration (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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.

This command requires the Enterprise Services license.

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.

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.

ip pim send-rp-announce

To configure an IPv4 Protocol Independent Multicast (PIM) Auto-RP candidate rendevous point (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 *if-type if-number* **group-list** *prefix* {[**scope** *ttl*] | [**interval** *interval*] | [**bidir**]}
no ip pim send-rp-announce [*if-type if-number*] [**group-list** *prefix*] {[**scope** *ttl*] | [**interval** *interval*] | [**bidir**]}

Syntax Description

if-type	Interface type. For more information, use the question mark (?) online help function.
if-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
group-list *prefix*	Specifies a group range handled by the RP.
priority *priority*	(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.
bidir	(Optional) Specifies that the group range is advertised in PIM bidirectional (Bidir) mode.

Command Default

The TTL is 32.The Auto-RP Announce message interval is 60 seconds.

Command Modes

Global configuration (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **scope**, **interval**, and **bidir** 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 Enterprise Services license.

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.

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 *if-type if-number* [**scope** *ttl*]
no ip pim send-rp-discovery [*if-type if-number*] [**scope** *ttl*]

Syntax Description

if-type	Interface type. For more information, use the question mark (?) online help function.
if-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
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 (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 Enterprise 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
```

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.

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 180 to 57600 seconds.
sg-list *route-map*route-map	(Optional) Specifies S,G values to which the timer applies.

Command Default

The default is 180 seconds.

The timer applies to all (S,G) multicast routes in the routing table.

Command Modes

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.2(2)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to configure the expiry interval to 300 seconds for all (S,G) multicast routes:

```
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.

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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise 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.

ip pim spt-threshold infinity

To create the IPv4 Protocol Independent Multicast (PIM) (*, G) state only (where no source state is created), use the **ip pim spt-threshold infinity** command. To remove the creation of the shared tree state only, use the **no** form of this command.

ip pim spt-threshold infinity group-list *route-map-name*
no ip pim spt-threshold infinity [**group-list** *route-map-name*]

Syntax Description

route-map-name	Route-map name that defines the group prefixes where this feature is applied.

Command Default

None

Command Modes

Global configuration (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.1(2)	Keyword **group-list** was added and a route-map name is used to define groups.

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.

You must have enabled PIM before you can use this command.

Note This command is not supported for virtual port channels (vPCs).

Note Prior to Cisco NX-OS Release 5.2(3), the route map specified by the **ip pim spt-threshold infinity group-list** *route-map* command was limited to 50 sequence lines. Starting in Cisco NX-OS Release 5.2(3), the number of sequence lines in the route map has increased to 500. If you specify more than 500 sequence lines in a route map, they are not functional.

This command requires the Enterprise Services license.

Examples

This example shows how to create the PIM (*, G) state only for the group prefixes defined in my_group_map:

```
switch(config)#
ip pim spt-threshold infinity group-list my_group_map
```

This example shows how to remove the creation of the (*, G) state only:

```
switch(config)#
no ip pim spt-threshold infinity
```

Related Commands

Command	Description
show ip pim rp	Displays information about PIM RPs.

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 (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise 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.

ip pim ssm range

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 (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.1(2)	The keyword **none** was added.
4.2(1)	Added the keyword **route-map** and argument *policy-name* .

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 Enterprise 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.

ip pim ssm route-map

To configure route-map policy name for SSM range, use the **ip pim ssm route-map** command. To remove the prefix-list, use the **no** form of this command.

ip pim ssm route-map *word*
no ip pim ssm route-map *route-map name*

Syntax Description

route-map name	Specifies route-map policy name for SSM range. The policy name can be maximum up to 63 characters.

Command Modes

Global configuration (config)

VRF configuration (config-vrf)

ip pim ssm prefix-list

To configure prefix-list policy name for SSM range, use the **ip pim ssm prefix-list** command. To remove the prefix-list, use the **no** form of this command.

ip pim ssm prefix-list *word*
no ip pim ssm prefix-list *prefix-list name*

Syntax Description

prefix-list name	Specifies a prefix-list policy name for the SSM range.

Command Modes

Global configuration (config)

VRF configuration (config-vrf)

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 4294967295. 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.

Command Default

None

Command Modes

Global configuration (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(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 Enterprise 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
```

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.

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 (config)

VRF configuration (config-vrf)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.1(2)	The keyword **group-list** was added and a route-map policy name was used to define groups.

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.

You must have enabled PIM before you can use this command.

Note This command is not supported for virtual port channels (vPCs).

This command requires the Enterprise 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.

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 Forwarding Distribution Module (MFDM) debug event history buffer.
mfdm-events	Configures the (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 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 (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.1(2)	This command was introduced.
4.2(1)	Added the keyword **mfdm-events**. Changed the keyword **mfdm** to **mfdm-debugs**.

Usage Guidelines

To display configured buffer sizes, use this command line:

```
switch(config)# show running-config | include "ip routing"
```

This command does not require a license.

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)#
```

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.

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

ipv4	(Optional)
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 (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.2(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.

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 (config)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.2(3)	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.

ipv6 mld access-group

To enable a Multicast Listener Discovery (MLD) route-map policy to control the multicast groups that hosts on a subnet serviced by an interface can join, use the **ipv6 mld access-group** command. To disable the route-map policy, use the **no** form of this command.

ipv6 [**icmp**] **mld access-group** *policy-name*
no ipv6 [**icmp**] **mld access-group** *[policy-name]*

Syntax Description

icmp	(Optional) Specifies the Internet Control Message Protocol (ICMP) designator.
policy-name	Specifies the route-map policy name.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to enable an MLD route-map policy:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ipv6 mld 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 ipv6 mld access-group
switch(config-if)#
```

Related Commands

Command	Description
show ipv6 mld interface	Displays information about ICMPv6 interfaces.

ipv6 mld group-timeout

To configure the Multicast Listener Discovery (MLD) group membership timeout, use the **ipv6 mld group-timeout** command. To reset to the default, use the **no** form of this command.

ipv6 [**icmp**] **mld group-timeout** *time*
no ipv6 [**icmp**] **mld group-timeout** *[time]*

Syntax Description

icmp	(Optional) Specifies the Internet Control Message Protocol (ICMP) designator.
time	Time 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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to configure a group membership timeout:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ipv6 mld 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 ipv6 mld group-timeout
switch(config-if)#
```

Related Commands

Command	Description
show ipv6 mld interface	Displays information about ICMPv6 interfaces.

ipv6 mld immediate-leave

To enable the device to remove the group entry from the IPv6 multicast routing table immediately upon receiving a leave message for the group, use the **ipv6 mld immediate-leave** command. To disable the immediate leave option, use the **no** form of this command.

ipv6 [**icmp**] **mld immediate-leave**
no ipv6 [**icmp**] **mld immediate-leave**

Syntax Description

icmp	(Optional) Specifies the Internet Control Message Protocol (ICMP) designator.

Command Default

The immediate leave feature is disabled.

Command Modes

Interface configuration (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.1(3)	This command was introduced.

Usage Guidelines

Use the **ipv6 mld 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)# ipv6 mld immediate-leave
```

This example shows how to disable the immediate leave feature:

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ipv6 mld immediate-leave
```

Related Commands

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

ipv6 mld join-group

To statically bind a multicast group to an interface, use the **ipv6 mld join-group** command. To remove a group binding, use the **no** form of this command.

ipv6 [**icmp**] **mld join-group** {*group* [**source** *source*] | **route-map** *policy-name*}
no ipv6 [**icmp**] **mld join-group** {*group* [**source** *source*] | **route-map** *policy-name*}

Syntax Description

icmp	(Optional) Specifies the Internet Control Message Protocol (ICMP) designator.
group	Multicast group IPv6 address.
source *source*	(Optional) Specifies a source IP address for an MLDv2 (S, G) channel.
route-map *policy-name*	Specifies the route-map policy name that defines the group prefixes where this feature is applied.

Command Default

None

Command Modes

Interface configuration (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.
4.2(1)	Added the keyword **route-map** and argument *policy-name*.

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.

The **match ipv6 multicast** command is the only **match** command that is evaluated in the route map. You can specify the group prefix, group range, and source prefix to filter messages with the **match ipv6 multicast** command.

Note A source tree is built for the (S, G) state only if you enable MLDv2, which is the default.

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

This command requires the Enterprise Services license.

Examples

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

```
switch(config)# interface ethernet 2/2
switch(config-if)# ipv6 mld join-group FFFE::1
switch(config-if)#
```

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

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ipv6 mld join-group FFFE::1
switch(config-if)#
```

Related Commands

Command	Description
show ipv6 mld interface	Displays information about ICMPv6 interfaces.

ipv6 mld last-member-query-count

To configure the number of times that the software sends a Multicast Listener Discovery (MLD) query in response to a host leave message, use the **ipv6 mld last-member-query-count** command. To reset the query interval to the default, use the **no** form of this command.

ipv6 [**icmp**] **mld last-member-query-count** *count*
no ipv6 [**icmp**] **mld last-member-query-count** *[count]*

Syntax Description

icmp	(Optional) Specifies the Internet Control Message Protocol (ICMP) designator.
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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to configure a query count:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ipv6 mld 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 ipv6 mld last-member-query-count
switch(config-if)#
```

Related Commands

Command	Description
show ipv6 mld interface	Displays information about ICMPv6 interfaces.

ipv6 mld 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 **ipv6 mld last-member-query-response-time** command. To reset the interval to the default, use the **no** form of this command.

ipv6 [**icmp**] **mld last-member-query-response-time** *interval*
no ipv6 [**icmp**] **mld last-member-query-response-time** *[interval]*

Syntax Description

icmp	(Optional) Specifies the Internet Control Message Protocol (ICMP) designator.
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

Interface configuration (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to configure a query interval:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ipv6 mld 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 ipv6 mld last-member-query-response-time
switch(config-if)#
```

Related Commands

Command	Description
show ipv6 mld interface	Displays information about ICMPv6 interfaces.

ipv6 mld querier-timeout

To configure the Multicast Listener Discovery (MLD) querier timeout for MLDv1, use the **ipv6 mld querier-timeout** command. To reset the timeout to the default, use the **no** form of this command.

ipv6 [**icmp**] **mld querier-timeout** *timeout*
no ipv6 [**icmp**] **mld querier-timeout** *[timeout]*

Syntax Description

icmp	(Optional) Specifies the Internet Control Message Protocol (ICMP) designator.
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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **ipv6 mld query-timeout** command is an alternative form of this command.

This command requires the Enterprise Services license.

Examples

This example shows how to configure a querier timeout:

```
switch(config)#interface ethernet 2/2
switch(config-if)# ipv6 mld 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 ipv6 mld querier-timeout
switch(config-if)#
```

Related Commands

Command	Description
ipv6 mld query-timeout	Configures a querier timeout.
show ipv6 mld interface	Displays information about ICMPv6 interfaces.

ipv6 mld query-interval

To configure the Multicast Listener Discovery (MLD) interval between query transmissions, use the **ipv6 mld query-interval** command. To reset the interval to the default, use the **no** form of this command.

ipv6 [**icmp**] **mld query-interval** *interval*
no ipv6 [**icmp**] **mld query-interval** *[interval]*

Syntax Description

icmp	(Optional) Specifies the Internet Control Message Protocol (ICMP) designator.
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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

This example shows how to configure a query interval:

```
switch(config)# interface ethernet 2/2ipv6 mld query-interval 100
switch(config-if)# ipv6 mld 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 ipv6 mld query-interval
switch(config-if)#
```

Related Commands

Command	Description
show ipv6 mld interface	Displays information about ICMPv6 interfaces.

ipv6 mld query-max-response-time

To configure the Multicast Listener Discovery (MLD) maximum response time for query messages, use the **ipv6 mld query-max-response-time** command. To reset the response time to the default, use the **no** form of this command.

ipv6 [**icmp**] **mld query-max-response-time** *time*
no ipv6 [**icmp**] **mld query-max-response-time** *[time]*

Syntax Description

icmp	(Optional) Specifies the Internet Control Message Protocol (ICMP) designator.
time	Time in seconds. The range is from 1 to 8387. The default is 10.

Command Default

The maximum query response time is 10 seconds.

Command Modes

Interface configuration (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

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

```
switch(config)# interface ethernet 2/2
switch(config-if)# ipv6 mld 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 ipv6 mld query-max-response-time
switch(config-if)#
```

Related Commands

Command	Description
show ipv6 mld interface	Displays information about ICMPv6 interfaces.

ipv6 mld query-timeout

To configure the Multicast Listener Discovery (MLD) querier timeout for MLDv1, use the **ipv6 mld query-timeout** command. To reset the timeout to the default, use the **no** form of this command.

ipv6 [**icmp**] **mld query-timeout** *timeout*
no ipv6 [**icmp**] **mld query-timeout** *[timeout]*

Syntax Description

icmp	(Optional) Specifies the Internet Control Message Protocol (ICMP) designator.
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 (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

The **ipv6 mld querier-timeout** command is an alternative form of this command.

This command requires the Enterprise Services license.

Examples

This example shows how to configure a querier timeout:

```
switch(config)# interface ethernet 2/2
switch(config-if)# ipv6 mld 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 ipv6 mld query-timeout
switch(config-if)#
```

Related Commands

Command	Description
ipv6 mld querier-timeout	Configures a querier timeout.
show ipv6 mld interface	Displays information about ICMPv6 interfaces.

ipv6 mld report-link-local-groups

To enable Multicast Listener Discovery (MLD) to send reports for link-local groups, use the **ipv6 mld report-link-local-groups** command. To disable sending reports to link-local groups, use the **no** form of this command.

ipv6 [**icmp**] **mld report-link-local-groups**
no ipv6 [**icmp**] **mld report-link-local-groups**

Syntax Description

icmp	(Optional) Specifies the Internet Control Message Protocol (ICMP) designator.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

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

```
switch(config)# interface ethernet 2/2
switch(config-if)# ipv6 mld 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 ipv6 mld report-link-local-groups
switch(config-if)#
```

Related Commands

Command	Description
show ipv6 mld interface	Displays information about ICMPv6 interfaces.

ipv6 mld report-policy

To enable an access policy that is based on a route-map policy for Multicast Listener Discovery (MLD) reports, use the **ipv6 mld report-policy** command. To disable the route-map policy, use the **no** form of this command.

ipv6 [**icmp**] **mld report-policy** *policy-name*
no ipv6 [**icmp**] **mld report-policy** *[policy-name]*

Syntax Description

icmp	(Optional) Specifies the Internet Control Message Protocol (ICMP) designator.
policy-name	Route-map policy name.

Command Default

Disabled

Command Modes

Interface configuration (config-if)

Supported User Roles

network-admin

vdc-admin

Command History

Release	Modification
4.0(1)	This command was introduced.

Usage Guidelines

This command requires the Enterprise Services license.

Examples

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

```
switch(config)# interface ethernet 2/2
switch(config-if)# ipv6 mld report-policy my_report_policy
switch(config-if)#
```

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

```
switch(config)# interface ethernet 2/2
switch(config-if)# no ipv6 mld report-policy
switch(config-if)#
```

Related Commands

Command	Description
show ipv6 mld interface	Displays information about ICMPv6 interfaces.