ipv6 pim through senders

ipv6 pim

To reenable IPv6 Protocol Independent Multicast (PIM) on a specified interface, use the **ipv6 pim**command in interface configuration mode. To disable PIM on a specified interface, use the **no** form of the command.

ipv6 pim
no ipv6 pim

Syntax Description

This command has no arguments or keywords.

Command Default

PIM is automatically enabled on every interface.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

After a user has enabled the **ipv6 multicast-routing** command, PIM is enabled to run on every interface. Because PIM is enabled on every interface by default, use the **no** form of the **ipv6 pim** command to disable PIM on a specified interface. When PIM is disabled on an interface, it does not react to any host membership notifications from the Multicast Listener Discovery (MLD) protocol.

Examples

The following example turns off PIM on Fast Ethernet interface 1/0:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# no ipv6 pim
```

Related Commands

Command	Description
ipv6 multicast-routing	Enables multicast routing using PIM and MLD on all IPv6-enabled interfaces of the router and enables multicast forwarding.

ipv6 pim accept-register

To accept or reject registers at the rendezvous point (RP), use the **ipv6 pim accept-register**command in global configuration mode. To return to the default value, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **accept-register list** *access-list* | **route-map** *map-name*
no ipv6 pim [**vrf** *vrf-name*] **accept-register list** *access-list* | **route-map** *map-name*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
list *access-list*	Defines the access list name.
route-map *map-name*	Defines the route map.

Command Default

All sources are accepted at the RP.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use the **ipv6 pim accept-register**command to configure a named access list or route map with match attributes. When the permit conditions as defined by the *access-list* and *map-name* arguments are met, the register message is accepted. Otherwise, the register message is not accepted, and an immediate register-stop message is returned to the encapsulating designated router.

Examples

The following example shows how to filter on all sources that do not have a local multicast Border Gateway Protocol (BGP) prefix:

```
ipv6 pim accept-register route-map reg-filter
route-map reg-filter permit 20
 match as-path 101
ip as-path access-list 101 permit
```

ipv6 pim allow-rp

To enable the PIM Allow RP feature for all IP multicast-enabled interfaces in an IPv6 device, use the **ip pim allow-rp** command in global configuration mode. To return to the default value, use the **no** form of this command.

ipv6 pim allow-rp [**group-list** *access-list* | **rp-list** *access-list* [**group-list** *access-list*]]
no ipv6 pim allow-rp

Syntax Description

group-list	(Optional) Identifies an access control list (ACL) of allowed group ranges for PIM Allow RP.
rp-list	(Optional) Specifies an ACL for allowed rendezvous-point (RP) addresses for PIM Allow RP.
access-list	(Optional) Unique number or name of a standard ACL.

Command Default

PIM Allow RP is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(4)S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.3(1)T	This command was integrated into Cisco IOS Release 15.3(1)T.

Usage Guidelines

Use this command to enable the receiving device in an IP multicast network to accept a (*, G) Join from an unexpected (different) RP address.

Before enabling PIM Allow RP, you must first use the **ipv6 pim rp-address** command to define an RP.

Examples

NEED CONFIG EXAMPLE HERE

Related Commands

Command	Description
ipv6 pim rp-address	Statically configures the address of a PIM RP for multicast groups.

ipv6 pim anycast-RP

To configure the address of the Protocol-Independent Multicast (PIM) rendezvous point (RP) for an anycast group range, use the **ipv6 pim anycast-RP** command in global configuration mode. To remove an RP address for an anycast group range, use the **no** form of this command.

ipv6 pim anycast-RP {*rp-address peer-address*}
no ipv6 pim anycast-RP

Syntax Description

anycast-rp-address	Anycast RP set for the RP assigned to the group range. This is the address that first-hop and last-hop PIM routers use to register and join.
peer-address	The address to which register messages copies are sent. This address is any address assigned to the RP router, not including the address assigned using the *anycast-rp-address* variable.

Command Default

No PIM RP address is configured for an anycast group range.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.2(3)T	This command was integrated into Cisco IOS XE Release 15.2(3)T.
15.1(1)SY	This command was integrated into Cisco IOS XE Release 15.1(1)SY.

Usage Guidelines

The anycast RP feature is useful when interdomain connection is not required. Use this command to configure the address of the PIM RP for an anycast group range.

Examples

```
Router# ipv6 pim anycast-rp 2001:DB8::1:1 2001:DB8::3:3
```

Related Commands

Command	Description
show ipv6 pim anycast-RP	Verifies IPv6 PIM RP anycast configuration.

ipv6 pim bsr border

To configure a border for all bootstrap message (BSMs) of any scope on a specified interface, use the **ipv6 pim bsr border**command in interface configuration mode. To remove the border, use the **no** form of this command.

ipv6 pim bsr border
no ipv6 pim bsr border

Syntax Description

This command has no argument or keywords.

Command Default

No border is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The **ipv6 pim bsr border** command is used to configure a border to all global and scoped BSMs. The command filters incoming or outgoing BSMs, preventing the BSMs from being forwarded or accepted on the interface on which the **ipv6 pim bsr border** command is configured.

Examples

The following example configures a BSR border on Ethernet interface 1/0:

```
Router(config)# interface Ethernet1/0
 Router(config-if)# ipv6 pim bsr border
 Router(config-if)# end
Router# show running-config interface e1/0
 Building configuration...
 Current configuration :206 bytes
 !
 interface Ethernet1/0
 ipv6 address 2:2:2::2/64
 ipv6 enable
 ipv6 rip test enable
```

```
ipv6 pim bsr border
no cdp enable
end
```

Related Commands

Command	Description
ipv6 pim bsr candidate bsr	Configures a router as a candidate BSR.
ipv6 pim bsr candidate rp	Sends PIM RP advertisements to the BSR.

ipv6 pim bsr candidate bsr

To configure a device to be a candidate bootstrap device (BSR), use the **ipv6 pim bsr candidate bsr**command in global configuration mode. To remove this device as a candidate BSR, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*] [**scope**] [**accept-rp-candidate** *acl-name*]
no ipv6 pim [**vrf** *vrf-name*] **bsr candidate bsr** *ipv6-address* [*hash-mask-length*] [**priority** *priority-value*] [**scope**] [**accept-rp-candidate** *acl-name*]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
ipv6-address	The IPv6 address of the device to be configured as a candidate BSR. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
hash-mask-length	(Optional) The length (in bits) of the mask to use in the BSR hash function. The default value is 126.
priority	(Optional) Priority of the candidate BSR.
priority-value	(Optional) Integer from 0 through 192. The BSR with the larger priority is preferred. If the priority values are the same, the device with the larger IPv6 address is the BSR. The default value is 0.
scope	(Optional) BSR will originate bootstrap messages (BSMs), including the group range associated with the scope, and accept candidate RP (C-RP) announcements only if they are for groups that belong to the given scope.
accept-rp-candidate *acl-name*	(Optional) BSR C-RP advertisements will be filtered at the BSR using the named access list (*acl-name*) for the RP candidates.

Command Default

Device is not enabled as a BSR.

Command Modes

Global configuration

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.2(18)SXE	The **scope** keyword and *scope-value* argument were added.
12.4	The **scope** keyword and *scope-value* argument are no longer available in syntax.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.

Release	Modification
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(1)SY	This command was integrated into Cisco IOS Release 15.0(1)SY.
15.2(1)S	This command was modified. The **accept-rp-candidate** keyword was added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

This command is used to configure a device as a candidate BSR; however, the device becomes a candidate only if the address belongs to a PIM-enabled interface. When a device is configured, it will participate in BSR election. If elected BSR, this device will periodically originate BSR messages advertising the group-to-RP mappings it has learned through candidate-RP-advertisement messages.

If the **scope** keyword is enabled, the BSR will originate BSMs, including the group range associated with the scope, and accept C-RP announcements only if they are for groups that belong to the given scope. If no scope is configured, all scopes are used.

The **accept-rp-candidate** *acl-name* keyword and argument will restrict the C-RP candidates accepted. If the **accept-rp-candidate** keyword is not configured, BSR C-RP advertisements at the BSR are not filtered.

Examples

The following example configures the device with the IPv6 address 2001:0DB8:3000:3000::42 as the candidate BSR, with a hash mask length of 124 and a priority of 10:

```
ipv6 pim bsr candidate bsr 2001:0DB8:3000:3000::42 124 priority 10
```

The following example will restrict the C-RP advertisements accepted. The ACL, crp, is used to filter the advertisements.

```
ipv6 pim bsr candidate bsr 194::1:1:2 priority 150 accept-rp-candidate crp
acl crp with
permit ipv6 host 192::1:1:1 any log
deny ipv6 any any log
```

Related Commands

Command	Description
ipv6 pim bsr border	Configures a border for all bootstrap message BSMs of any scope.
ipv6 pim bsr candidate rp	Sends PIM RP advertisements to the BSR.

ip pim cache rpf-oif

To cache the information from an outgoing interface that became the incoming (RPF) interface for PIM sparse mode on a Protocol Independent Multicast (PIM) router, use the **ip pim cache rpf-oif** command in the global configuration mode. To stop caching this information, use the **no** form of this command

ip pim [**vrf** *vrf-name*] **cache rpf-oif**
noip pim [**vrf** *vrf-name*] **cache rpf-oif**

Syntax Description

vrf *vrf-name*	(Optional) Specifies support for multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance. This parameter indicates the name assigned to a VRF.

Command Default

The caching information from an outgoing interface that became the incoming (RPF) interface is disabled on PIM routers that are running a Cisco IOS software

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Polaris 16.9.3	This command was introduced.

Usage Guidelines

Configuring this command may sometimes improve convergence in a network by restoring cached interface (provided it exists and is still valid) to an outgoing interface list (OIL), when the interface stops being the incoming (RPF) interface. The command is disabled by default to avoid potential minor side effects such as asserts upon restoring outgoing interface.

Examples

The following example shows how to cache information from outgoing interface that becomes the incoming (RPF) interface

```
ip pim cache vrf vrf123 rpf-oif
```

Related Commands

Command	Description
show ip pim mroute verbose	The **show ip pim mroute verbose** command shows the cached interface information as 'OIL RPF interface'

ipv6 pim bsr candidate rp

To configure the candidate rendezvous point (RP) to send Protocol Independent Multicast (PIM) RP advertisements to the bootstrap device (BSR), use the **ipv6 pim bsr candidate rp** command in global configuration mode. To disable PIM RP advertisements to the BSR, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**]
no ipv6 pim [**vrf** *vrf-name*] **bsr candidate rp** *ipv6-address* [**group-list** *access-list-name*] [**priority** *priority-value*] [**interval** *seconds*] [**scope** *scope-value*] [**bidir**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
ipv6-address	The IPv6 address of the device to be advertised as the candidate RP (C-RP). This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
group-list	(Optional) List of group prefixes. When the **bidir** keyword is not enabled, the **group-list** keyword with the *access-list-name* argument is advertised in the sparse range. If no access list is specified, all valid multicast nonsource-specific multicast (SSM) address ranges are advertised in association with the specified RP address.
access-list-name	(Optional) Name of the IPv6 access list containing group prefixes that will be advertised in association with the RP address. Names cannot contain a space or quotation mark, or begin with a numeral. When the **bidir** keyword is not enabled, the **group-list** keyword with the *access-list-name* argument is advertised in the sparse range. If the access list contains any group address ranges that overlap the assigned SSM group address range (FF3x::/96), a warning message is displayed, and the overlapping address ranges are ignored.
priority	(Optional) Priority of the candidate BSR.
priority-value	(Optional) Integer from 0 through 192 that specifies the priority. The RP with the higher priority is preferred. If the priority values are the same, the device with the higher IPv6 address is the RP. The default value is 192.
interval	(Optional) Configures the C-RP advertisement interval.
seconds	(Optional) Advertisement interval in number of seconds.
scope	(Optional) Device advertises itself as the C-RP only to the BSR for the specified scope.
scope-value	(Optional) Integer from 3 through 15 that specifies the scope.
bidir	(Optional) Device advertises itself as the C-RP for the **group-list** *access-list-name* in the bidirectional range.

Command Default

Device is not enabled as a candidate RP. If no scope is configured, all scopes are advertised.

Command Modes

Global configuration

Command History

Release	Modification
12.0(28)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T.
12.2(18)SXE	The **scope** and **bidir** keywords were added. The *scope-value* argument was added.
12.4	The **scope** keyword and *scope-value* argument are no longer available in syntax.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SRE	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Use this command to send PIM RP advertisements to the BSR. The PIM RP advertisement becomes a candidate only if the address belongs to a PIM-enabled interface.

The group prefixes defined by the *access-list-name* argument will also be advertised in association with the RP address. If a group prefix in the access list is denied, it will not be included in the C-RP advertisement.

If the **priority***priority-value* keyword and argument are specified, then the device will announce itself to be a candidate RP with the specified priority.

If the **scope** keyword is used, the device advertises itself as the C-RP only to the BSR for the specified scope. If the **group-list**keyword is specified along with the scope, then only prefixes in the *access-list-name* argument with the same scope as the scope configured will be advertised. If no scope is configured, all scopes are advertised.

Examples

The following example configures the device with the IPv6 address 2001:0DB8:3000:3000::42 to be advertised as the candidate RP, with a priority of 0:

```
Device(config)# ipv6 pim bsr candidate rp 2001:0DB8:3000:3000::42 priority 0
```

The following example configures the device with the IPv6 address 2001:0DB8:1:1:1 as the candidate RP for scope 6 for the group ranges specified in the access list named list1:

```
Device(config)# ipv6 pim bsr candidate rp 2001:0DB8:1:1:1 group-list list1 scope 6
```

Related Commands

Command	Description
ipv6 pim bsr candidate bsr	Configures a device as a candidate BSR.
ipv6 pim bsr border	Configures a border for all BSMs of any scope.

ipv6 pim dr-priority

To configure the designated router (DR) priority on a Protocol Independent Multicast (PIM) router, use the **ipv6 pim dr-priority** command in interface configuration mode. To restore the default value, use the **no** form of this command.

ipv6 pim dr-priority *value*
no ipv6 pim dr-priority

Syntax Description

value	An integer value to represent DR priority. Value range is from 0 to 4294967294. The default value is 1.

Command Default

Default value is 1.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.

Usage Guidelines

The **ipv6 pim dr-priority** command configures the neighbor priority used for PIM DR election. The router with the highest DR priority on an interface becomes the PIM DR. If several routers have the same priority, then the router with the highest IPv6 address on the interface becomes the DR.

If a router does not include the DR priority option in its hello messages, then the router is considered to be the highest-priority router and becomes the DR. If several routers do not include the DR priority option in their hello messages, then the router with the highest IPv6 address becomes the DR.

Examples

The following example configures the router to use DR priority 3:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 pim dr-priority 3
```

Related Commands

Command	Description
ipv6 pim hello-interval	Configures the frequency of PIM hello messages on an interface.

ipv6 pim hello-interval

To configure the frequency of Protocol Independent Multicast (PIM) hello messages on an interface, use the **ipv6 pim hello-interval** command in interface configuration mode. To return to the default interval, use the **no** form of this command.

ipv6 pim hello-interval *seconds*
no ipv6 pim hello-interval *seconds*

Syntax Description

seconds	Interval, in seconds, at which PIM hello messages are sent.

Command Default

Hello messages are sent at 30-second intervals with small random jitter.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Periodic hello messages are sent out at 30-second intervals with a small jitter. The **ipv6 pim hello-interval**command allows users to set a periodic interval.

Examples

The following example sets the PIM hello message interval to 45 seconds:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 pim hello-interval 45
```

Related Commands

Command	Description
ipv6 mld query-interval	Configures the frequency at which the Cisco IOS software sends MLD host-query messages.
ipv6 pim dr-priority	Configures the DR priority on a PIM router.
show ipv6 pim neighbor	Displays the PIM neighbors discovered by the Cisco IOS software.

ipv6 pim join-prune-interval

To configure periodic join and prune announcement intervals for a specified interface, use the **ipv6 pim join-prune-interval**command in interface configuration mode. To return to the default value, use the **no** form of the command.

ipv6 pim join-prune-interval *seconds*
no ipv6 pim join-prune-interval *seconds*

Syntax Description

seconds	The join and prune announcement intervals, in number of seconds. The default value is 60 seconds.

Command Default

The default is 60 seconds.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.4(1)S	This command was implemented on the Cisco ASR 901 series routers.

Usage Guidelines

Periodic join and prune announcements are sent out at 60-second intervals. The **ipv6 pim join-prune-interval** commandallows users to set a periodic interval.

Examples

The following example sets the join and prune announcement intervals to 75 seconds:

```
Router(config)# interface FastEthernet 1/0
Router(config-if)# ipv6 pim join-prune-interval 75
```

ipv6 pim maximum group-mappings

To configure the maximum number of number of group to active rendezvous points (RPs) mappings that can be created for BSR, use the **ipv6 pim maximum group-mappings** command in global configuration mode. To return to the default, use the **no** form of this command.

ipv6 pim maximum group-mappingsbsr *max-mappings*
no ipv6 pim maximum group-mappingsbsr

Syntax Description

bsr	Specifies that PIM group mappings are learned from BSR.
max-mappings	Maximum number of PIM group mappings. The range is from 1 to 1000.

Command Default

No limit is configured for PIM group mappings.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)S	This command was introduced.

Usage Guidelines

Use this command to limit the number of group-to-RP mappings that can be created. When the specified maximum number of mappings is reached, existing mappings are updated but new mappings cannot be created.

Use the **show ipv6 pim range-list** command to display the count and limit for mappings when this command is configured and there are mappings created.

Examples

```
Router(config)# ipv6 pim maximum group-mappings bsr 5
Router (config)# exit
Router# show running-config | inc max
ipv6 pim maximum group-mappings bsr 5
```

Related Commands

Command	Description
show ipv6 pim range-list	Displays the mappings for the PIM group to the active rendezvous points.

ipv6 pim neighbor-filter list

To filter Protocol Independent Multicast (PIM) neighbor messages from specific IPv6 addresses, use the **ipv6 pim neighbor-filter** command in the global configuration mode. To return to the router default, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **neighbor-filter list** *access-list*
no ipv6 pim [**vrf** *vrf-name*] **neighbor-filter list** *access-list*

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
access-list	Name of an IPv6 access list that denies PIM hello packets from a source.

Command Default

PIM neighbor messages are not filtered.

Command Modes

Global configuration

Command History

Release	Modification
12.4(2)T	This command was introduced.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

The **ipv6 pim neighbor-filter list**command is used to prevent unauthorized routers on the LAN from becoming PIM neighbors. Hello messages from addresses specified in this command are ignored.

Examples

The following example causes PIM to ignore all hello messages from IPv6 address FE80::A8BB:CCFF:FE03:7200:

```
Router(config)# ipv6 pim neighbor-filter list nbr_filter_acl
Router(config)# ipv6 access-list nbr_filter_acl
Router(config-ipv6-acl)# deny ipv6 host FE80::A8BB:CCFF:FE03:7200 any
Router(config-ipv6-acl)# permit any any
```

ipv6 pim passive

To enable the Protocol Independent Multicast (PIM) passive feature on a specific interface, use the **ipv6 pim passive**command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 pim passive
no ipv6 pim passive

Syntax Description

This command has no arguments or keywords.

Command Default

PIM passive mode is not enabled on the router.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

Use the **ipv6 pim passive**command to configure IPv6 PIM passive mode on an interface.

A PIM passive interface does not send or receive any PIM control messages. However, a PIM passive interface acts as designated router (DR) and designated forwarder (DF)-election winner, and it can accept and forward multicast data.

Examples

The following example configures IPv6 PIM passive mode on an interface:

```
Router(config)# interface gigabitethernet 1/0/0
Router(config-if)# ipv6 pim passive
```

Related Commands

Command	Description
ipv6 multicast pim-passive-enable	Enables the PIM passive feature on an IPv6 router.

ipv6 pim rp embedded

To enable embedded rendezvous point (RP) support in IPv6 Protocol Independent Multicast (PIM), use the **ipv6 pim rp-embedded**command in global configuration mode. To disable embedded RP support, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **rp embedded**
no ipv6 pim [**vrf** *vrf-name*] **rp embedded**

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.

Command Default

Embedded RP support is enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(26)S	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.

Usage Guidelines

Because embedded RP support is enabled by default, users will generally use the **no** form of this command to turn off embedded RP support.

The **ipv6 pim rp embedded**command applies only to the embedded RP group ranges ff7X::/16 and fffX::/16. When the router is enabled, it parses groups in the embedded RP group ranges ff7X::/16 and fffX::/16, and extracts the RP to be used from the group address.

Examples

The following example disables embedded RP support in IPv6 PIM:

```
no ipv6 pim rp embedded
```

ipv6 pim rp-address

To configure the address of a Protocol Independent Multicast (PIM) rendezvous point (RP) for a particular group range, use the **ipv6 pim rp-address** command in global configuration mode. To remove an RP address, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **rp-address** *ipv6-address* [*group-access-list*] [**bidir**]
no ipv6 pim rp-address *ipv6-address* [*group-access-list*] [**bidir**]

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
ipv6-address	The IPv6 address of a router to be a PIM RP. The *ipv6-address*argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
group-access-list	(Optional) Name of an access list that defines for which multicast groups the RP should be used. If the access list contains any group address ranges that overlap the assigned source-specific multicast (SSM) group address range (FF3x::/96), a warning message is displayed, and the overlapping ranges are ignored. If no access list is specified, the specified RP is used for all valid multicast non-SSM address ranges. To support embedded RP, the router configured as the RP must use a configured access list that permits the embedded RP group ranges derived from the embedded RP address. Note that the embedded RP group ranges need not include all the scopes (for example, 3 through 7).
bidir	(Optional) Indicates that the group range will be used for bidirectional shared-tree forwarding; otherwise, it will be used for sparse-mode forwarding. A single IPv6 address can be configured to be RP only for either bidirectional or sparse-mode group ranges. A single group-range list can be configured to operate either in bidirectional or sparse mode.

Command Default

No PIM RPs are preconfigured. Embedded RP support is enabled by default when IPv6 PIM is enabled (where embedded RP support is provided). Multicast groups operate in PIM sparse mode.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	Embedded RP support was added.
12.3(7)T	The **bidir** keyword was added to Cisco IOS Release 12.3(7)T.

Release	Modification
12.2(25)S	The **bidir** keyword was added to Cisco IOS Release 12.2(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.

Usage Guidelines

When PIM is configured in sparse mode, you must choose one or more routers to operate as the RP. An RP is a single common root of a shared distribution tree and is statically configured on each router.

Where embedded RP support is available, only the RP needs to be statically configured as the RP for the embedded RP ranges. No additional configuration is needed on other IPv6 PIM routers. The other routers will discover the RP address from the IPv6 group address. If these routers want to select a static RP instead of the embedded RP, the specific embedded RP group range must be configured in the access list of the static RP.

The RP address is used by first-hop routers to send register packets on behalf of source multicast hosts. The RP address is also used by routers on behalf of multicast hosts that want to become members of a group. These routers send join and prune messages to the RP.

If the optional *group-access-list* argument is not specified, the RP is applied to the entire routable IPv6 multicast group range, excluding SSM, which ranges from FFX[3-f]::/8 to FF3X::/96. If the *group-access-list* argument is specified, the IPv6 address is the RP address for the group range specified in the *group-access-list* argument.

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

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

Examples

The following example shows how to set the PIM RP address to 2001::10:10 for all multicast groups:

```
Router(config)# ipv6 pim rp-address 2001::10:10
```

The following example sets the PIM RP address to 2001::10:10 for the multicast group FF04::/64 only:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# permit ipv6 any ff04::/64
Router(config)# ipv6 pim rp-address 2001::10:10 acc-grp-1
```

The following example shows how to configure a group access list that permits the embedded RP ranges derived from the IPv6 RP address 2001:0DB8:2::2:

```
Router(config)# ipv6 pim rp-address 2001:0DB8:2::2 embd-ranges
```

```
Router(config)# ipv6 access-list embd-ranges
Router(config-ipv6-acl)# permit ipv6 any ff73:240:2:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff74:240:2:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff75:240:2:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff76:240:2:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff77:240:2:2:2::/96
Router(config-ipv6-acl)# permit ipv6 any ff78:240:2:2:2::/96
```

The following example shows how to enable the address 100::1 as the bidirectional RP for the entries multicast range FF::/8:

```
ipv6 pim rp-address 100::1 bidir
```

In the following example, the IPv6 address 200::1 is enabled as the bidirectional RP for the ranges permitted by the access list named bidir-grps. The ranges permitted by this list are ff05::/16 and ff06::/16.

```
Router(config)# ipv6 access-list bidir-grps
Router(config-ipv6-acl)# permit ipv6 any ff05::/16
Router(config-ipv6-acl)# permit ipv6 any ff06::/16
Router(config-ipv6-acl)# exit
Router(config)# ipv6 pim rp-address 200::1 bidir-grps bidir
```

Related Commands

Command	Description
debug ipv6 pim df-election	Displays debug messages for PIM bidirectional DF-election message processing.
ipv6 access-list	Defines an IPv6 access list and places the router in IPv6 access list configuration mode.
show ipv6 pim df	Displays the DF -election state of each interface for each RP.
show ipv6 pim df winner	Displays the DF-election winner on each interface for each RP.

ipv6 pim spt-threshold infinity

To configure when a Protocol Independent Multicast (PIM) leaf router joins the shortest path tree (SPT) for the specified groups, use the **ipv6 pim spt-threshold infinity**command in global configuration mode. To restore the default value, use the **no** form of this command.

ipv6 pim [**vrf** *vrf-name*] **spt-threshold infinity** [**group-list** *access-list-name*]
no ipv6 pim spt-threshold infinity

Syntax Description

vrf *vrf-name*	(Optional) Specifies a virtual routing and forwarding (VRF) configuration.
group-list *access-list-name*	(Optional) Indicates to which groups the threshold applies. Must be a standard IPv6 access list name. If the value is omitted, the threshold applies to all groups.

Command Default

When this command is not used, the PIM leaf router joins the SPT immediately after the first packet arrives from a new source. Once the router has joined the SPT, configuring the **ipv6 pim spt-threshold infinity**command will not cause it to switch to the shared tree.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
15.1(4)M	The **vrf** *vrf-name* keyword and argument were added.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.

Usage Guidelines

Using the **ipv6 pim spt-threshold infinity**command enables all sources for the specified groups to use the shared tree. The **group-list** keyword indicates to which groups the SPT threshold applies.

The *access-list-name*argument refers to an IPv6 access list. When the *access-list-name*argument is specified with a value of 0, or the **group-list** keyword is not used, the SPT threshold applies to all groups. The default setting (that is, when this command is not enabled) is to join the SPT immediately after the first packet arrives from a new source.

Examples

The following example configures a PIM last-hop router to stay on the shared tree and not switch to the SPT for the group range ff04::/64.:

```
Router(config)# ipv6 access-list acc-grp-1
Router(config-ipv6-acl)# permit ipv6 any FF04::/64
Router(config-ipv6-acl)# exit
Router(config)# ipv6 pim spt-threshold infinity group-list acc-grp-1
```

manager

To specify the interface that is to act as the Manager for Multicast Routing Monitor (MRM), and to specify the multicast group address the Test Receiver will listen to, use the **manager**command in MRM manager configuration mode. To remove the Manager or group address, use the **no** form of this command.

manager *interface-type interface-number* **group** *ip-address*
no manager *interface-type interface-number* **group** *ip-address*

Syntax Description

interface-type interface-number	Interface type and number of the Manager. The IP address associated with this interface is the source address of the Manager.
group *ip-address*	Specifies the IP multicast group address that the Test Receiver will listen to.

Command Default

There is no MRM Manager configured.

Command Modes

MRM manager configuration (config-mrm-manager)

Command History

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

Usage Guidelines

This command identifies the interface that acts as the Manager, and therefore is required in order to run MRM.

Examples

The following example shows how to configure Ethernet interface 0 as the Manager and the Test Receiver to listen to multicast group 239.1.1.1:

```
ip mrm manager test1
 manager ethernet 0 group 239.1.1.1
```

Related Commands

Command	Description
beacon (multicast routing monitor)	Changes the frequency, duration, or scope of beacon messages that the Manager sends to Test Senders and Test Receivers during an MRM test.
ip mrm accept-manager	Configures a Test Sender or Test Receiver to accept requests only from Managers that pass an access list.
show ip mrm manager	Displays test information for MRM.

mdt auto-discovery pim

To enable a device to originate Border Control Protocol (BGP) MVPN Subsequence-Address Family (SAFI) auto-discovery (AD) routes for a VRF address-family and process received BGP customer (C) routes, use the **mdt auto-discovery pim** command in address family configuration mode. To return to the default, use the **no** form of this command.

mdt auto-discovery pim pim-tvl-announce
no mdt auto-discovery pim pim-tvl-announce

Syntax Description

pim	Specifies the core MVPN transport (PIM GRE) to be advertised by multicast for BGP Intras-AS I-PMSI (Type 1) and S-PMSI (Type 3) A-D routes.
pim-tvl-announce	Enables device to originate periodic UDP TLV messages for data Multicast Distribution Trees (MDTs) in addition to S-PMSI A-D routes advertised via BGP.

Command Default

The device will not originate BGP MVPN SAFI AD routes for a VRF address-family and will not process received BGP C routes.

Command Modes

Address family configuration (config-vrf-af)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Usage Guidelines

Use this command to enable a device to originate BGP AD advertisements from multicast for a VRF address family and to process multicast BGP C routes received at a router.

Configure this command to enable a device to perform the following tasks:

- Originate Type-1 I-PMSIs routes and the MVPN core transports (GRE) advertised in these routes.
- Originate Type-3 S-PMSIs routes and the transport (GRE) advertised in these routes.
- Originate BGP Source Active AD routes (Type 5).
- Originate periodic UDP data MDT TLVs.
- Allow customer multicast flows to be transported over the GRE/IP-IP MVPN core transport.
- Process received Type 6 and Type 7 routes, create a multicast PIM state for the VRF address family, and add the appropriate transport interface (GRE MDT tunnel) to the forwarding interface.

If this command is not configured, the device will not originate BGP MVPN SAFI auto-discovery routes for the VRF address-family and will not process received MVPN BGP customer routes.

Examples

```
!
vrf definition vrf1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 !
```

```
 address-family ipv4
  mdt auto-discovery pim pim-tlv-announce
  mdt default 239.0.0.1
 exit-address-family
!

!
vrf definition vrf1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 !
 address-family ipv6
  mdt auto-discovery pim pim-tlv-announce
  mdt default 2001:DB8::/24
 exit-address-family
!
```

Related Commands

Command	Description
address-family ipv4 (BGP)	Enters address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 4 address prefixes.
address-family ipv6	Enters address family configuration mode for configuring routing sessions such as BGP, RIP, or static routing sessions that use standard IP Version 6 address prefixes.

mdt data

To specify a range of addresses to be used in the data multicast distribution tree (MDT) pool, use the **mdt data** command in VRF configuration or VRF address family configuration mode. To disable this function, use the **no** form of this command.

mdt data *group-address-range wildcard-bits* [**threshold** *kb/s*] [**list** *access-list*]
no mdt data *group-address-range wildcard-bits* [**threshold** *kb/s*] [**list** *access-list*]

Syntax Description

group-address-range	Multicast group address range. The range is from 224.0.0.1 to 239.255.255.255.
wildcard-bits	Wildcard bits to be applied to the multicast group address range.
threshold *kb/s*	(Optional) Defines the bandwidth threshold value in kilobits per second (kb/s). The range is from 1 to 4294967.
list *access-list*	(Optional) Limits the creation of the data MDT to the particular (S,G) Multicast Virtual Private Network (MVPN) entries defined in the access list specified for the *access-list* argument.

Command Default

A data MDT pool is not configured.

Command Modes

VRF address family configuration (config-vrf-af)

VRF configuration (config-vrf)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was added on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

A data MDT can include a maximum of 256 multicast groups per MVPN. Multicast groups used to create the data MDT are dynamically chosen from a pool of configured IP addresses.

Use the **mdt data** command to specify a range of addresses to be used in the data MDT pool. Because these are multicast group addresses (Class D addresses), there is no concept of a subnet; therefore, you can use all addresses in the mask (wildcard) range. The threshold is specified in kb/s. Using the optional **list** keyword and *access-list* argument, you can define the (S, G) MVPN entries to be used in a data MDT pool, which would further limit the creation of a data MDT pool to the particular (S, G) MVPN entries defined in the access list specified for the *access-list*argument.

You can access the **mdt data**command by using the **ip vrf** global configuration command. You can also access the **mdt data**command by using the **vrf definition**global configuration command followed by the **address-family ipv4**VRF configuration command.

Examples

The following example shows how to configure the range of group addresses for the MDT data pool. In this example, the mask 0.0.0.15 allows the range 239.192.20.32 to 239.192.20.47 to be used as the address pool. In addition, a threshold of 1 kb/s has been set, which means that if a multicast stream exceeds 1 kb/s, then a data MDT is created.

```
ip vrf vrf1
 rd 10:27
 route-target export 10:27
 route-target import 10:27
 mdt default 232.0.0.1
 mdt data 232.0.1.0 0.0.0.255 threshold 500 list 101
!
.
.
.
!
ip pim ssm default
ip pim vrf vrf1 accept-rp auto-rp
!
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address family configuration mode.
mdt default	Configures a default MDT group for a VPN VRF.
mdt preference	Specifies a preference for a particular MDT type.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

mdt data mpls mldp

To configure a VRF to support data Multicast Distribution Trees (MDTs), use the **mdt data mpls mldp** command in the VRF address family configuration or VRF configuration mode. To return to the default, use the **no** form of this command

mdt data mpls mldp*num_tree* [**list** *acl*] [**scope** *scope_id*][**immediate-switch**]
no mdt data mpls mldp*num_tree* **list** *acl* [**scope** *scope_id*][**immediate-switch**]

Syntax Description

num_tree	Number of data MDTs to be supported. The maximum number of data MDTs supported per VRF is the sum of the number of data MDTs configured for the VRF. The range is 0 to 5000 and 0 equals the default MDT.
list *acl*	(Optional) Limits the creation of the data MDT to the (S,G) Multicast Virtual Private Network (MVPN) entries defined in the specified extended access list (ACL). The default is that all (S,G) MVPN entries can use this data MDT.
scope *scope_id*	(Optional) Specifies value to be encoded into the higher 16 bits of the 32-bit tree number. The default is 0.
immediate-switch	(Optional) Specifies that once the data MDT switch happens, packets are no longer sent over the default MDT. The default is that packets continue to be sent over the default MDT for 3 seconds after the data MDT switch happens.

Command Default

Traffic flows on the default MDT.

Command Modes

VRF address family configuration (config-vrf-af)

VRF configuration (config-vrf)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(3)S	This command was modified. The **immediate-switch** keyword and the **list** *acl* and **scope** *scope_id* keyword and argument combinations were added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

The Multicast Distribution Tree (MDT) tree number is a 32 bit integer. Use the **scope** *scope-id* keyword and argument combination to encode the specified scope ID into the higher 16 bits of the 32-bit MDT tree number. The lower order 16 bits is the tree ID number.

Use the **list** *acl* keyword and argument combination to define the (S, G) MVPN entries to be used in a data MDT pool. The data MDT pool is limited to the (S, G) MVPN entries in the specified ACL.

Use the **immediate-switch** keyword to define whether traffic should flow on the default MDT or be switched immediately to the data MDT after the (S,G) state is created on the ingress Provider Edge (PE) router. Immediate switch works for source specific-multicast (SSM) groups in the VRF only if the MDT data threshold is 0. As long as the (S,G) SSM state exists on the ingress PE router, it will stay on the data MDT.

If you configure the **immediate-switch** keyword for a non-SSM group range, the MDT join and switch is sent to the data MDT after 3 seconds. Immediate switch can cause a delay in receiving traffic when the first receiver joins because the ingress PE does not send traffic on the default MDT while the P2MP tree is being built.

Examples

In the following partial sample output from the **show running config** command shows the following: At the ingress PE for a given VRF (blue), group range 232.1.1.0/24 is confined within local scope 1 with traffic switching immediately to the data MDT. Group range 232.1.2.0/24 is confined to regional scope 2, also with an immediate switch to the data MDT.

```
Router# show running config
.
.
.
access-list 100 permit ip any 232.1.1.0 0.0.0.255
access-list 101 permit ip any 232.1.2.0 0.0.0.255
.
.
.
ip vrf blue
mdt data mpls mldp 100 list 100 scope 1 immediate-switch
mdt data mpls mldp 200 list 101 scope 2 immediate-switch
```

Related Commands

Command	Description
access-list	Configures an ACL.
mdt data	Specifies the address range to be used in a data multicast distribution tree (MDT) pool.
mdt default	Configures a default MDT for a VPN VRF.

mdt default

To configure a default multicast distribution tree (MDT) group for a Virtual Private Network (VPN) routing and forwarding (VRF) instance, use the **mdt default** command in VRF configuration or VRF address family configuration mode. To disable this function, use the **no** form of this command.

mdt default*group-address* | **mpls mldp** *root-address*
no mdt default*group-address* | **mpls mldp** *root-address*

Syntax Description

group-address	IP address of the default MDT group. This address serves as an identifier for the community in that provider edge (PE) routers configured with the same group address become members of the group, allowing them to receive packets sent by each other.
mpls mldp *root-address*	Specifies the multipoint-to-multipoint (MP2MP) Label Switched Path (LSP) root address of the default MDT group, which was created using Multicast Label Distribution Protocol (MLDP) LSP.

Command Default

The command is disabled.

Command Modes

VRF address family configuration (config-vrf-af) VRF configuration (config-vrf)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
15.0(1)S	This command was modified. The **mpls mldp** keywords were added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.3(1)S	This command was integrated into Cisco IOS Release 15.13(1)S.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

The default MDT group must be the same group configured on all PE routers that belong to the same VPN.

If Source Specific Multicast (SSM) is used as the protocol for the default MDT, the source IP address will be the address used to source the Border Gateway Protocol (BGP) sessions.

A tunnel interface is created as a result of this command. By default, the destination address of the tunnel header is the *group-address* argument.

You can access the **mdt default**command by using the **ip vrf** global configuration command. You can also access the **mdt default**command by using the **vrf definition**global configuration command followed by the **address-family ipv4**VRF configuration command.

Examples

In the following example, Protocol Independent Multicast (PIM) SSM is configured in the backbone. Therefore, the default and data MDT groups are configured within the SSM range of IP addresses. Inside the VPN, PIM sparse mode (PIM-SM) is configured and only Auto-RP announcements are accepted.

```
!
ip vrf vrf1
 rd 1:1
 route-target export 1:1
 route-target import 1:1
 mdt default 232.0.0.1
 mdt data 232.0.1.0 0.0.0.255 threshold 500 list 101
!
.
.
.
!
ip pim ssm default
ip pim vrf vrf1 accept-rp auto-rp
!
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address family configuration mode.
mdt data	Configures the multicast group address range for data MDT groups.
mdt preference	Specifies a preference for a particular MDT type.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

mdt log-reuse

To enable the recording of data multicast distribution tree (MDT) reuse, use the **mdt log-reuse**command in VRF configuration or in VRF address family configuration mode. To disable this function, use the **no** form of this command.

mdt log-reuse
no mdt log-reuse

Syntax Description

This command has no arguments or keywords.

Command Default

The command is disabled.

Command Modes

VRF address family configuration (config-vrf-af) VRF configuration (config-vrf)

Command History

Release	Modification
12.0(23)S	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **mdt log-reuse** command generates a syslog message whenever a data MDT is reused.

You can access the **mdt log-reuse**command by using the **ip vrf** global configuration command. You can also access the **mdt log-reuse**command by using the **vrf definition**global configuration command followed by the **address-family ipv4**VRF configuration command.

Examples

The following example shows how to enable MDT log reuse:

```
mdt log-reuse
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address-family configuration mode.
mdt data	Configures the multicast group address range for data MDT groups.
mdt default	Configures a default MDT group for a VPN VRF.

Command	Description
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

mdt preference

To specify a preference for a particular multicast distribution tree (MDT) type, use the **mdt preference**command in VRF configuration or VRF address family configuration mode. To disable this function, use the **no** form of this command.

mdt preference mldp | **pim**
no mdt preference mldp | **pim**

Syntax Description

mldp	Specifies the creation of MDTs using Multicast Label Distribution Protocol (MLDP).
pim	Specifies the creation of MDTs using Protocol Independent Multicast (PIM).

Command Default

MDTs are created using PIM.

Command Modes

VRF address family configuration (config-vrf-af) VRF configuration (config-vrf)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

In order to support the Multicast Virtual Private Network (MVPN) migration strategy, MLDP MDTs can be configured in conjunction with PIM MDTs. In order to influence the path selection in the mroute table, this command can be used to specify a preference for a certain tree type. If the command is not configured, PIM is preferred to MLDP. The order in which the keywords **pim** and **mldp** are entered gives the preference. The keyword entered first has the higher preference.

You can also access the **mdt preference**command by using the **vrf definition** global configuration command followed by the **address-family ipv4** VRF configuration command.

Examples

The following example shows how to specify the creation of MDTs using MLDP:

```
ip vrf vrf1
 mdt preference mldp
```

Related Commands

Command	Description
address-family (VRF)	Selects an address family type for a VRF table and enters VRF address family configuration mode.
mdt data	Configures the multicast group address range for data MDT groups.
mdt default	Configures a default MDT group for a VPN VRF.

Command	Description
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

mls ip multicast (global configuration)

To enable MLS IP and configure the hardware switching globally, use the mls ip multicast command in global configuration mode . To disable MLS IP, use the **no** form of this command.

mls ip multicast [**capability**]
mls ip multicast [**vrf** *name*] [**connected** | **egress local** | **mfd** | **refresh-state** | **shared-tree-mfd** | **syslog** | **threshold** *ppsec*]
no mls ip multicast [**vrf**]

Syntax Description

capability	(Optional) Exports the information about the egress capability from the switch processor to the route processor.
vrf *name*	(Optional) Specifies the VRF name.
connected	(Optional) Installs the interface/mask entries for bridging directly connected sources to the internal router.
egress local	(Optional) Populates the multicast expansion table with local Layer 3-routed interfaces.
mfd	(Optional) Enables complete hardware switching.
refresh-state	(Optional) Refreshes the expiration time of the (S,G) entry or the (*,G) entry with NULL OIF.
shared-tree-mfd	(Optional) Enables the complete shortcut for (*,G) flows.
syslog	(Optional) Enables the display of multicast related syslog messages on console.
threshold *ppsec*	(Optional) Sets the minimum traffic rate; below this rate, the flow is software-switched instead of hardware-switched. Valid values are from 10 to 10000 seconds.

Command Default

The defaults are as follows:

- Multicast is disabled.
- Hardware switching is allowed for all eligible multicast routes.
- **connected** is enabled.
- **egress local** is disabled.
- **mfd** is enabled.
- **refresh-state** is enabled.
- **shared-tree-mfd** is enabled.
- **syslog** is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command was changed to include the **capability** keyword.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXF	This command was changed to include the **egress local**keywords.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	Support for the syslog feature was added.

Usage Guidelines

Note After you enter the **mls ip multicast egress local** command, you must perform a system reset for the configuration to take effect.

Egress multicast replication is not supported on systems that are configured with a Supervisor Engine 32

When entering the **mls ip multicast egress local** command, ensure that IPv6 multicast is not enabled. Since the egress multicast replication performance enhancement feature cannot separately turn on or turn off IPv4 and IPv6, you cannot have IPv4 and IPv6 multicast enabled when this feature is turned on.

These optional keywords are supported only on systems that are configured with a Supervisor Engine 720 with a PFC3:

- **threshold**
- **connected**
- **refresh-state**
- **shared-tree-mfd**
- **mfd**

The **threshold** *ppsec* optional keyword and argument do not impact flows that are already populated in the hardware cache.

The expiration time refresh is updated when flow statistics are received (indicating that the traffic is received from the RPF interface).

Examples

This example shows how to enable the MLS IP shortcuts:

```
Router(config)#
mls ip multicast
```

This example shows how to enable the hardware switching on a specific multicast route:

```
Router(config)#
mls ip multicast vrf test1
```

This example shows how to export the information about egress capability from the switch processor to the route processor:

```
Router(config)#
mls ip multicast capability
```

This example shows how to populate the multicast expansion table with local Layer 3-routed interfaces:

```
Router(config)#
mls ip multicast egress local
```

Related Commands

Command	Description
mls rp ip (global configuration mode)	Enables external systems to establish IP shortcuts to the MSFC.
show mls ip multicast	Displays the MLS IP information.

mls ip multicast (interface configuration)

To enable MLS IP shortcuts on the interface, use the **mls ip multicast** command in interface configuration mode. To disable MLS IP shortcuts on the interface, use the **no** form of this command.

mls ip multicast
no mls ip multicast

Syntax Description

This command has no arguments or keywords.

Command Default

Multicast is disabled.

Command Modes

Interface configuration

Command History

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

Examples

This example shows how to enable the MLS IP shortcuts:

```
Router(config-if)#
mls ip multicast
```

Related Commands

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

mls ip multicast bidir gm-scan-interval

To set the RPF scan interval for the Bidir rendevous point, use the **mls ip multicast bidir gm-scan-interval**command in global configuration mode . To disable the RPF scan interval for the Bidir rendevous point, use the **no** form of this command.

mls ip multicast bidir gm-scan-interval *interval*
no mls ip multicast bidir gm-scan-interval

Syntax Description

interval	RPF scan interval for the Bidir rendevous point ; valid values are from 1 to 1000 seconds.

Command Default

10 seconds

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

When you set the RPF scan interval for the Bidir rendevous point, you set the time that the periodic scan timer updates the RPF in the DF table for all Bidir rendevous points in the hardware.

Examples

This example shows how to set the RPF scan interval for the Bidir rendevous point:

```
Router(config)#
mls ip multicast bidir gm-scan-interval 30
```

Related Commands

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

mls ip multicast connected

To enable the downloading of directly connected subnets globally, use the **mls ip multicast connected** command in global configuration mode . To disable the downloading of directly connected subnets globally, use the **no** form of this command.

mls ip multicast connected
no mls ip multicast connected

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Do not create directly connected subnets for the following cases:

- To make more room available in the FIB TCAM
- The switch is the first-hop router for a source
- The entries are for Bidir, SSM, and DM mode groups

In these cases, if you enable the downloading of directly connected subnets, the directly connected source hits the MMLS (*,G) entry and is switched using the MMLS (*,G) entry. The registers are not sent to the route processor (in the case of PIM-SM), and the (S,G) state is not created on the first hop (in the case of PIM-DM).

The subnet entry is installed in the TCAM entries with a shorter mask to catch directly connected sources before they hit such entries. You can punt traffic from directly connected sources to the MSFC. Once the MSFC sees this traffic, it can install an MMLS (S,G) entry for this source, which gets installed before the subnet entry in the TCAM. New packets from this source are now switched with the (S,G) entry.

Examples

This example shows how to enable the downloading of directly connected subnets:

```
Router(config)#
mls ip multicast connected
```

Related Commands

Command	Description
mls ip multicast (global configuration)	Enables MLS IP and configures the hardware switching globally.

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

mls ip multicast consistency-check

To enable and configure the hardware-shortcut consistency checker, use the **mls ip multicast consistency-check** command in global configuration mode. To disable the consistency checkers, use the **no** form of this command.

mls ip multicast consistency-check[**auto-repair** | **error-message** | **settle-time** *seconds* | **type rp-sp**[**table** | **vrf**] | **scan-mroute**[**count** *count-number* | **settle-time** *seconds* | **period** *seconds*]]
no mls ip multicast consistency-check

Syntax Description

auto-repair	(Optional) Specifies the automatic repair for the consistency checker.
error-message	(Optional) Specifies the error message for the consistency checker.
settle-time *seconds*	(Optional) Specifies the settle time for the consistency checker; valid values are from 2 to 3600 seconds.
type rp-sp	(Optional) Specifies the type of consistency check as a MLSM route switch processor.
table	(Optional) Specifies the VRF multicast table to check. Valid values are 0 to 65535.
vrf	(Optional) Specifies the VPN routing/forwarding instance to check.
type scan-mroute	(Optional) Specifies the type of consistency check as a scan check of the mroute table.
count *count-number*	(Optional) Specifies the maximum number of prefixes to check per scan; valid values are from 2 to 500.
period *seconds*	(Optional) Specifies the period between scans; valid values are from 2 to 3600 seconds.

Command Default

The defaults are as follows:

- Consistency check is enabled.
- **count** *count-number* is **20**
- **period** *seconds* is **2** seconds.
- **settle-time** *seconds* is **60** seconds.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The consistency checker scans the mroute table and assures that the multicast-hardware entries are consistent with the mroute table. Whenever an inconsistency is detected, the inconsistency is automatically corrected.

To display the inconsistency error, use the **show mls ip multicast consistency-check** command.

Examples

This example shows how to enable the hardware-shortcut consistency checker:

```
Router(config)#
mls ip multicast consistency-check
```

This example shows how to enable the hardware-shortcut consistency checker and configure the scan check of the mroute table:

```
Router(config)#
mls ip multicast consistency-check type scan-mroute count 20 period 35
```

This example shows how to enable the hardware-shortcut consistency checker and specify the period between scans :

```
Router(config)#
mls ip multicast consistency-check type scan-mroute period 35
```

Related Commands

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

mls ip multicast flow-stat-timer

To set the time interval between two consecutive batches of flow-statistics messages from the switch processor to the route processor, use the **mls ip multicast flow-stat-timer** command in global configuration mode . To return to the default settings, use the **no** form of this command.

mls ip multicast flow-stat-timer *num*
no mls ip multicast flow-stat-timer

Syntax Description

num	Time interval between two consecutive batches of flow-statistics messages from the switch processor to the route processor.

Command Default

25 seconds

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to configure the time interval between two consecutive batches of flow-statistics messages from the switch processor to the route processor:

```
Router(config)#
mls ip multicast flow-stat-timer 10
```

Related Commands

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

mls ip multicast non-rpf aging

To enable rate-limiting of non-RPF traffic, use the **mls ip multicast non-rpf aging**command in global configuration mode . To return to the default settings, use the **no** form of this command.

mls ip multicast non-rpf aging global [**msec**] *time* | **fast** [**msec**] *time* | **incremental** *time* **percent** *percent* **total-vlan** | **nf-table** *time*
no mls ip multicast non-rpf aging global *time* | **fast** [**msec**] *time* | **incremental** *time* **percent** *percent* **total-vlan** | **nf-table** *time*

Syntax Description

global *time*	Specifies the global aging time interval in seconds or with the optional **msec** keyword, in milliseconds. Valid values are 1 to 180 seconds or 2000 to 10,000 milliseconds. The default is 20 seconds.
msec	(Optional) Specifies the global aging time interval in milliseconds.
fast *time*	Specifies the fast aging time interval in seconds or with the optional **msec** keyword, in milliseconds. Valid values are 2 to 10 seconds or 500 to 180,000 milliseconds. The default is 2 seconds.
msec	(Optional) Specifies the fast aging time interval in milliseconds.
incremental *time*	Specifies the incremental timeout.
percent *percent*	Specifies the percentage of total VLANs or NetFlow table.
total-vlan	Specifies the total VLANs allowed in the NetFlow table.
nf-table	Specifies when to purge the NetFlow table.

Command Default

The fast aging time default is 2 seconds and the global aging time default is 20 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced for the Supervisor Engine 720.
12.2SXH	This command was modified. The **no** and **default** forms of this command will return the command to the default settings.
12.2(33)SXJ1	This command was modified. Support for the **msec**, **incremental**, **percent**, **total-vlan**, and **nf-table** keywords was added.

Usage Guidelines

You should not configure ACL-based filtering of RPF failures.

For Cisco IOS Release 12.2SXH and later versions: This command was modified to support the return to the default settings if you use either the **no** or **default** form of this command.

Prior to Cisco IOS Release 12.2SXH, the **no** and **default** forms of this command disabled non-RPF aging, and did not return the command to the default settings. To return to the default settings after using this command to specify values for the **global** or **fast** keywords, configure the **mls ip multicast non-rpf aging global 20** command or the **mls ip multicast non-rpf aging fast 2** command, respectively.

If the configured global timeout cannot accommodate all of the configured incremental timeouts, a warning message is displayed and the command is aborted.

If the global timeout is not properly configured to accommodate the total incremental purge cycle, the following error message is displayed:

```
Global time out should be large enough to accommodate the incremental purge cycle.
```

For example, if the incremental purge timeout is set at 1000 milliseconds and the purge percent is set to 10 percent, and you configure the global purge timeout to 5000 milliseconds, the timeout is not enough to accommodate the incremental cycle. The minimum time needed is calculated by using the "purge_percent"*"purge_time" equation (which would be 10*1000 in this example).

Examples

This example shows how to enable rate-limiting of non-RPF traffic:

```
Router(config)#
mls ip multicast non-rpf aging global 90
```

This example shows how to enable fast rate-limiting of non-RPF traffic in milliseconds:

```
Router(config)# mls ip multicast non-rpf aging fast msec 1000
```

This example shows how to display the multicast configuration of the router:

```
Router# show running | incl mls ip multicast
mls ip multicast non-rpf aging global 90
mls ip multicast non-rpf aging fast 4
Router#
```

This example shows how to set the incremental purge to 500 seconds and purge on 10 percent of the total VLANs basis:

```
Router# mls ip multicast non-rpf aging incremental 500 percent 10 total-vlan
```

Related Commands

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

mls ip multicast replication-mode

To enable and specify the replication mode, use the **mls ip multicast replication-mode**command in global configuration mode. To restore the system to automatic detection mode, use the **no** form of this command.

mls ip multicast replication-mode egress | ingress
no mls ip multicast replication-mode egress | ingress

Syntax Description

egress	Forces the system to the egress mode of replication.
ingress	Forces the system to the ingress mode of replication.

Command Default

The Supervisor Engine 720 automatically detects the replication mode based on the module types that are installed in the system. If all modules are capable of egress replication, the system uses egress-replication mode. If the supervisor engine detects the modules that are not capable of egress replication, the replication mode automatically switches to ingress replication.

If the system is functioning in the automatic-detection egress mode, and you install a module that cannot perform egress replication, the following occurs:

- The Cisco 7600 series router reverts to ingress mode.
- A system log is generated.
- A system reload occurs to revert to the old configuration.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXF	Thic command was changed to support the **egress** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Note During the change from egress- to ingress-replication mode, traffic interruptions may occur because the shortcuts are purged and reinstalled. To avoid interruptions in traffic forwarding, enter the **mls ip multicast replication-mode ingress** command.

If you enter the **no mls ip multicast replication-mode egress** command, only the forced-egress mode resets and not the forced-ingress mode.

If you enter the **no mls ip multicast replication-mode ingress** command, only the forced-ingress mode resets and not the forced-egress mode.

Examples

This example shows how to enable the ingress-replication mode:

```
Router(config)#
mls ip multicast replication-mode ingress
```

This example shows how to enable the egress-replication mode:

```
Router(config)#
mls ip multicast replication-mode egress
```

This example shows how to disable the current egress-replication mode and return to automatic detection mode:

```
Router(config)#
no
mls ip multicast replication-mode egress
```

Related Commands

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

mls ip multicast sso

To configure the stateful switchover (SSO) parameters, use the **mls ip multicast sso** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mls ip multicast sso convergence-time *time* | **leak interval** *seconds* | **percent** *percentage*
no mls ip multicast sso convergence-time *time* | **leak interval** *seconds* | **percent** *percentage*

Syntax Description

convergence-time *time*	Specifies the maximum time to wait for protocol convergence; valid values are from 0 to 3600 seconds.
leak interval *seconds*	Specifies the packet-leak interval; valid values are from 0 to 3600 seconds.
leak percent *percentage*	Specifies the percentage of multicast packets leaked to the router during switchover so that protocol convergence can take place; valid values are from 1 to 100 percent.

Command Default

The defaults are as follows:

- **convergence-time** *time* --20 seconds
- **leak** *interval* --60 seconds
- **leak** *percentage* --10 percent

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to set the maximum time to wait for protocol convergence to 300 seconds:

```
Router(config)#
mls ip multicast sso convergence-time 300
Router(config)#
```

This example shows how to set the packet-leak interval to 200 seconds:

```
Router(config)#
mls ip multicast sso leak interval 200
Router(config)#
```

This example shows how to set the packet-leak percentage to 55 percent:

```
Router(config)#
```

```
mls ip multicast sso leak percent 55
Router(config)#
```

Related Commands

Command	Description
show mls ip multicast sso	Displays information about multicast high-availability SSO.

mls ip multicast stub

To enable the support for non-RPF traffic drops for PIM sparse-mode stub networks, use the **mls ip**multicast stub command in interface configuration mode. To disable support for non-RPF traffic drops for PIM sparse-mode stub networks, use the **no** form of this command.

mls ip multicast stub
no mls ip multicast stub

Syntax Description

This command has no arguments or keywords.

Command Default

Multicast is disabled.

Command Modes

Interface configuration

Command History

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

Usage Guidelines

When you enable the ACL-based method of filtering RPF failures by entering the **mls ip multicast stub** command on the redundant router, the following ACLs automatically download to the PFC and are applied to the interface that you specify:

- access-list 100 permit ip A.B.C.0 0.0.0.255 any
- access-list 100 permit ip A.B.D.0 0.0.0.255 any
- access-list 100 permit ip any 224.0.0.0 0.0.0.255
- access-list 100 permit ip any 224.0.1.0 0.0.0.255
- access-list 100 deny ip any 224.0.0.0 15.255.255.255

The ACLs filter the RPF failures and drop them in the hardware so that they are not forwarded to the router.

Use the ACL-based method of filtering the RPF failures only in sparse-mode stub networks where there are no downstream routers. For dense-mode groups, the RPF failure packets have to be seen on the router for the PIM-assert mechanism to function properly. Use CEF-or NetFlow-based rate limiting to rate limit the RPF failures in dense-mode networks and sparse-mode transit networks.

Examples

This example shows how to enable the support for the non-RPF traffic drops for the PIM sparse-mode stub networks:

```
Router(config-if)#
mls ip multicast stub
```

Related Commands

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

mls ip multicast threshold

To configure a threshold rate for installing hardware shortcuts, use the **mls ip multicast threshold** command in global configuration mode. To deconfigure the threshold rate, use the **no** form of this command.

mls ip multicast threshold *pps*
no mls ip multicast threshold

Syntax Description

pps	Threshold in packets per seconds. Valid values are from 10 to 10000.

Command Default

This command has no default settings.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use this command to prevent creation of MLS entries for short-lived multicast flows such as join requests.

If multicast traffic drops below the configured multicast rate threshold, all multicast traffic is routed by the MSFC.

This command does not affect already installed routes. For example, if you enter this command and the shortcuts are already installed, the shortcuts are not removed if they are disqualified. To apply the threshold to existing routes, clear the route and let it reestablish.

Examples

This example shows how to configure the IP MLS threshold to 10 packets per second:

```
Router(config)#
mls ip multicast threshold 10
```

Related Commands

Command	Description
mls rp ip (global configuration)	Enables external systems to establish IP shortcuts to the MSFC.
show mls ip multicast	Displays the MLS IP information.

mode bypass

To enable Virtual Multipoint Interfaces (VMI) to support multicast traffic, use the **mode bypass** command in interface configuration mode. To return the interface to the default mode of aggregate, use the **no** form of this command.

mode [**aggregate** | **bypass**]
no mode bypass

Syntax Description

aggregate	Sets the mode to aggregate. All virtual-access interfaces created by PPPoE sessions are logically aggregated under the VMI.
bypass	Sets the mode to bypass.

Command Default

No mode

Command Modes

Interface configuration

Command History

Release	Modification
12.4(15)XF	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T to support multicast traffic on Virtual Multipoint Interfaces (VMIs).

Usage Guidelines

Use the mode bypass command when you need to support multicast traffic in router-to-radio configurations.

Aggregate Mode

The default mode for operation of the VMI is **aggregate** mode. In aggregate mode, all of the virtual-access interfaces created by PPPoE sessions are logically aggregated under the VMI. As such, applications above Layer 2, such as, EIGRP and OSPFv3, should be defined on the VMI interface only. Packets sent to the VMI will be correctly forwarded to the correct virtual-access interface.

Bypass Mode

Using **bypass** mode is recommended for multicast applications.

In **bypass** mode, the virtual-access interfaces are directly exposed to applications running above Layer2. In bypass mode, definition of a VMI is still required because the VMI will continue to manage presentation of cross-layer signals, such as, neighbor up, neighbor down, and metrics. However, applications will still be aware on the actual underlying virtual-access interfaces and send packets to them directly.

Using **bypass** mode can cause databases in the applications to be larger because knowledge of more interfaces are required for normal operation.

After you enter the **mode bypass** command, Cisco recommends that you copy the running configuration to NVRAM. because the default mode of operation for VMI is to logically aggregate the virtual-access interfaces.

Examples

The following example sets the interface mode to bypass:

```
Router# enable
Router# configure terminal
Router(config)# interface vmi1
Router(config-if)# mode bypass
```

Related Commands

Command	Description
interface vmi	Creates a VMI interface.

mpls mldp

To enable Cisco Multicast Label Distribution Protocol (MLDP) on an interface on which MLDP was previously disabled, use the **mpls mldp** in interface configuration mode. To disable MLDP on an interface, use the **no** form of this command.

mpls mldp
no mpls mldp

Syntax Description

This command has no arguments or keywords.

Command Default

MLDP is enabled on all interfaces on which Multiprotocol Label Switching (MPLS) forwarding of packets along normally routed paths is enabled.

Command Modes

Interface configuration mode (config-if)

Command History

Release	Modification
15.1(3)S	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **no mpls mldp** command to prevent an interface from being used in path selection even if it is advertised as a path by route watch.

The **no mpls mldp** command must be configured on all routers that are connected to one another on a particular interface. If a router receives a label mapping on an interface on which MPLS MDLP is disabled, the router installs the label mapping and builds a tree upstream.

This command will not work with a Virtual LAN (VLAN) that does not have an interface descriptor block (IDB) configured.

Examples

```
PE2(config)# interface gigabitethernet 1/1
PE2(config-if)# no mpls mldp
PE2(config-if)# end
PE2#
*Aug  8 12:36:56.144: %SYS-5-CONFIG_I: Configured from console by console
PE2# show mpls mldp interface
Interface            IP         mLDP
EOBC0/0              Disabled   Disabled
EOBC0/2              Disabled   Disabled
GigabitEthernet1/1   Enabled    Disabled
.
.
.
PE2(config)# interface gigabitethernet 1/1
PE2(config-if)# mpls mldp
PE2(config-if)# end
PE2#
*Aug  8 12:40:48.988: %SYS-5-CONFIG_I: Configured from console by console
PE2# show mpls mldp interface
Interface            IP         mLDP
EOBC0/0              Disabled   Disabled
EOBC0/2              Disabled   Disabled
```

```
GigabitEthernet1/1   Enabled    Enabled
.
.
.
```

Related Commands

Command	Description
mpls ip	Enables Multiprotocol Label Switching (MPLS) forwarding of packets along normally routed paths.

mpls mldp fec

To define a Forward Equivalence Class (FEC) ID for filtering Multicast Label Distribution Protocol (MLDP), use the **mpls mldp fec** command in global configuration mode. To remove the FEC ID, use the **no** form of this command.

mpls mldp fec*fec_idopaque-type* **vpn-id** *vpn_id* | **anyscope** *scope_id* | **any**
no mpls mldp fec*fec_idopaque-type* **vpn-id** *vpn_id* | **anyscope** *scope_id* | **any**

Syntax Description

fec_id	Unique identifier for this FEC definition. The range is 1 to 99.
opaque-type	Opaque value for this FEC. The following keyword is valid for this argument: **mdt**
vpn-id *vpn_id*	Specifies that the FEC is being defined for a VPN, and the unique VPN ID for which the FEC is being defined, in RFC 2685 format.
scope *scope-id*	Specifies that the FEC is being defined for MDT path labels, and the unique ID (of the path) for which the FEC is being defined. The range is from 0 to 65535.
any	Specifies all VPNs or all scopes, depending upon the corresponding keyword (**vpn** or **scope**).

Command Default

No MLDP FEC is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)S	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Examples

In the following partial sample output from the **show running config** command shows the following:

- Peer P4 will be denied for all FECs (matches FEC 1).
- For FECs having VPN id 1:1 and any scope, peers P4 (matches FEC 1) and P2 (matches FEC 2) will be denied. Additionally peer P3 will be denied if FEC VPN id is 1:1 and scope 2 (matchesFEC 4).
- For FECs having VPN id 2:2 and scope 1, peers P4 (matches FEC 1) and P2 (matches FEC 3) will be denied. Additionally peer P3 will be denied if FEC VPN id is 2:2 and scope 2 (matches FEC 4).
- For FECs having any VPN id and scope 2, peers P4 (matches FEC 1) and P3 (matches FEC 4) will be denied.
- Peer P4 will be denied for FEC with VPN id 3:3 and scope 3.

```
Router# show running config
.
```

```
.
.
access-list 50 deny   4.4.4.4
access-list 50 permit any
access-list 51 deny   2.2.2.2
access-list 51 permit any
access-list 52 deny   3.3.3.3
access-list 52 permit any
.
.
.
mpls mldp fec 1 opaque-type mdt vpn-id any scope any
mpls mldp fec 2 opaque-type mdt vpn-id 1:1 scope any
mpls mldp fec 3 opaque-type mdt vpn-id 2:2 scope 1
mpls mldp fec 4 opaque-type mdt vpn-id all scope 2

mpls mldp filter 1 peer-list 50
mpls mldp filter 2 peer-list 51
mpls mldp filter 3 peer-list 51
mpls mldp filter 4 peer-list 52
```

Related Commands

Command	Description
mpls mldp filter	Filters MLDP flows in the core.

mpls mldp filter

To filter all Multicast Label Distribution Protocol (MLDP) trees that match a Forward Equivalence Class (FEC) definition, use the **mpls mldp filter** command in global configuration mode. To return to the default, use the **no** form of his command.

mpls mldp filter *fec_id* **peer-list** *acl*
no mpls mldp filter *fec_id* **peer-list** *acl*

Syntax Description

fec-id	Unique ID of an already configured FEC definition.
peer-list *acl*	Specifies that a peer list is to be filtered if the MLDP FEC matches any of the following values for the *acl* argument: • Number of the acess list (ACL). The range of 1 to 99 (standard IP access list) or 1300 to 1999 (extended IP access list). • Name of the ACL. Names cannot contain a space or quotation mark, and must begin with an alphabetic character.

Command Default

MLDP flows are not filtered.

Command Modes

Global configuration mode (config-term)

Command History

Release	Modification
15.1(3)S	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use this command to configure MLDP Filtering and prevent MLDP traffic from traversing interconnections. The filtering feature uses FEC (Forward Equivalence Class) definitions to filter specified FECs on a per-peer basis. The list of peers for which a FEC is to be filtered is defined in an access control list (ACL). If an MLDP stream is denied by the filter, then the router will not advertise label mappings to the filtered peer.

Examples

In the following partial sample output from the **show running config** command shows the following:

- Peer P4 will be denied for all FECs (matches FEC 1).
- For FECs having VPN id 1:1 and any scope, peers P4 (matches FEC 1) and P2 (matches FEC 2) will be denied. Additionally peer P3 will be denied if FEC VPN id is 1:1 and scope 2 (matchesFEC 4).
- For FECs having VPN id 2:2 and scope 1, peers P4 (matches FEC 1) and P2 (matches FEC 3) will be denied. Additionally peer P3 will be denied if FEC VPN id is 2:2 and scope 2 (matches FEC 4).
- For FECs having any VPN id and scope 2, peers P4 (matches FEC 1) and P3 (matches FEC 4) will be denied.

- Peer P4 will be denied for FEC with VPN id 3:3 and scope 3.

```
Router# show running config
.
.
.
access-list 50 deny   4.4.4.4
access-list 50 permit any
access-list 51 deny   2.2.2.2
access-list 51 permit any
access-list 52 deny   3.3.3.3
access-list 52 permit any
.
.
.
mpls mldp fec 1 opaque-type mdt vpn-id any scope any
mpls mldp fec 2 opaque-type mdt vpn-id 1:1 scope any
mpls mldp fec 3 opaque-type mdt vpn-id 2:2 scope 1
mpls mldp fec 4 opaque-type mdt vpn-id all scope 2

mpls mldp filter 1 peer-list 50
mpls mldp filter 2 peer-list 51
mpls mldp filter 3 peer-list 51
mpls mldp filter 4 peer-list 52
```

Related Commands

Command	Description
access-list	Configures an ACL.
mpls mldp fec	Defines an FEC for MLDP.

mpls mldp forwarding recursive

To enable Multicast Label Distribution Protocol (MLDP) recursive forwarding over a point-to-multipoint (P2MP) Label Switched Path (LSP), use the **mpls mldp forwarding recursive**command in global configuration mode. To disable MLDP recursive forwarding over a P2MP LSP, use the **no** form of this command.

mpls mldp forwarding recursive
no mpls mldp forwarding recursive

Syntax Description

This command has no arguments or keywords.

Command Default

MLDP recursive forwarding is enabled on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

MLDP has two ways to resolve the next-hop that is used for forwarding labeled packets. Without this command enabled, MLDP resolves the outgoing interface based on the next hop to the downstream label switched router (LSR). If this command is enabled, the outgoing interface is resolved by Multicast Forwarding Information (MFI) using point-to-point (P2P) LSPs. The MLDP uses recursive forwarding over a P2P LSP. This means that a P2P LSP for the next hop needs to be available in the MFI. This configuration needs to be enabled to make MLDP Fast Re-route (FRR) backup over a traffic engineering (TE) tunnel possible.

Examples

The following example shows how to enable MLDP recursive forwarding on routers configured with MLDP P2MP functionality:

```
Router(config)# mpls mldp forwarding recursive
```

Related Commands

Command	Description
show mpls mldp database	Displays MLDP information.

mpls mldp logging notifications

To enable Multicast Label Distribution Protocol (MLDP) system log notifications, use the **mpls mldp logging notifications**command in global configuration mode. To disable this function, use the **no** form of this command.

mpls mldp logging notifications
no mpls mldp logging notifications

Syntax Description

This command has no arguments or keywords.

Command Default

MLDP logging notifications are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use the **mpls mldp logging notifications**command to generate syslog messages when internal errors occur in MLDP.

Examples

The following example shows how to enable MLDP logging notifications:

```
Router(config)# mpls mldp logging notifications
```

Related Commands

Command	Description
show mpls mldp database	Displays MLDP information.

mpls mldp path

To configure Multicast Label Distribution Protocol (MLDP) path options, use the **mpls mldp path**command in global configuration mode. To disable this configuration, use the **no** form of this command.

mpls mldp path multipath downstream | **upstream** | **traffic-eng**
no mpls mldp path multipath downstream | **upstream** | **traffic-eng**

Syntax Description

multipath downstream	Enables MLDP multipath for downstream Label Distribution Protocol (LDP) neighbors.
multipath upstream	Enables MLDP multipath for upstream LDP neighbors.
traffic-eng	Allows MLDP to use Traffic Engineering (TE) tunnels.

Command Default

MLDP path options are not configured on the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)S	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

If there are multiple downstream paths available to reach an LDP peer, load balancing of the branches of the LSPs over these paths occurs.

The assignment of the downstream paths to the label switched paths (LSPs) is done in a circular way. If this command is disabled, the path with the highest next-hop IP address is used to reach an LDP peer.

If there are multiple paths available to reach the root of a multiprotocol LSP, an algorithm based on the Forwarding Equivalence Class (FEC) length of the LSP is used to determine the path. If this command is disabled, the path with the highest next-hop IP address is used to reach the root.

If point-to-point MPLS TE tunnels are present in the unicast routing table, and LDP sessions exist with the destinations, then MLDP will consider TE tunnels as valid paths towards an mLDP neighbor. This command is disabled by default. If this command is not enabled and TE tunnels are present in the unicast routing table then the Interior Gateway Protocol (IGP) command **mpls traffic-eng multicast-intact**must be used to preserve the non-TE tunnel routes for use with MLDP path selection

Examples

The following example shows how to enable load balancing of different LSPs over the paths available to reach a downstream LDP peer:

```
Router(config)# mpls mldp path multicast downstream
```

Related Commands

Command	Description
show mpls mldp database	Displays MLDP information.

mrinfo

To query which neighboring multicast routers are acting as peers with the local router, use the **mrinfo**command in user EXEC or privileged EXEC mode.

mrinfo **vrf** *route-name*[*source-addressinterface*][*host-namehost-address*]

Syntax Description

vrf *route-name*	Specifies the VPN routing or forwarding instance.
source-address	(Optional) Source address used on multicast routing information (mrinfo) requests. If omitted, the source is based on the outbound interface for the destination.
interface	(Optional) Source interface used on mrinfo requests. If omitted, the source is based on the outbound interface for the destination.
host-name | *host-address*	(Optional) The Domain Name System (DNS) name or IP address of the multicast router to query. If omitted, the router queries itself.

Command Default

The command is disabled.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **vrf**and *route-name* keyword and argument pair was added.

Usage Guidelines

The **mrinfo** command is the original tool of the multicast backbone (MBONE) to determine which neighboring multicast routers are peering with a multicast router. Cisco routers have supported responding to mrinfo requests since Cisco IOS Release 10.2.

You can query a multicast router using the **mrinfo**command. The output format is identical to the multicast routed version of the Distance Vector Multicast Routing Protocol (DVMRP). (The mrouted software is the UNIX software that implements DVMRP.)

Examples

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

```
Router# mrinfo
 vrf 192.0.1.0
192.31.7.37 (barrnet-gw.cisco.com) [version cisco 11.1] [flags: PMSA]:
  192.31.7.37 -> 192.31.7.34 (sj-wall-2.cisco.com) [1/0/pim]
```

```
192.31.7.37 -> 192.31.7.47 (dirtylab-gw-2.cisco.com) [1/0/pim]
192.31.7.37 -> 192.31.7.44 (dirtylab-gw-1.cisco.com) [1/0/pim]
```

The flags indicate the following:

- P: prune-capable
- M: mtrace-capable
- S: Simple Network Management Protocol (SNMP)-capable
- A: Auto-Rendezvous Point (RP)-capable

mrm

To start or stop a Multicast Routing Monitor (MRM) test, use the **mrm** command in privileged EXEC mode.

mrm *test-name* **start** | **stop**

Syntax Description

test-name	Name of the MRM test to start or stop.
start	Starts the MRM test specified for the *test-name* argument.
stop	Stops the MRM test specified for the *test-name* argument.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

You must use this command to run an MRM test. When the test runs, the Test Sender sends User Datagram Protocol (UDP) or UDP/Real-Time Transport Protocol (RTP) packets (depending on the **senders** command) to the Test Receiver.

Examples

The following example shows how to start an MRM test. In this example, the MRM test named test1 is started.

```
Router# mrm test1 start
```

Related Commands

Command	Description
ip mrm manager	Identifies an MRM test and enters the mode in which you specify the test parameters.
senders	Configures Test Sender parameters used in MRM.
show ip mrm status-report	Displays the status reports in the MRM status report cache.

mstat

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

mstat vrf *route-name source-namesource-address* | *source-namesource-address* [*destination-namedestination-address*] [*group-namegroup-address*]

Syntax Description

vrf *route-name*	Specifies the VPN routing or forwarding instance.
source-name | *source-address*	Domain Name System (DNS) name or the IP address of the multicast-capable source.
destination-name | *destination-address*	(Optional) DNS name or address of the destination. If omitted, the command uses the system at which the command is typed.
group-name | *group-address*	(Optional) DNS name or multicast address of the group to be displayed. Default address is 224.2.0.1 (the group used for multicast backbone [MBONE] Audio).

Command Default

The command is disabled.

Command Modes

User EXEC (>) Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **vrf** *route-name* keyword and argument pair was added.

Usage Guidelines

If no arguments are entered, the router will interactively prompt you for them.

This command is a form of UNIX mtrace that reports packet rate and loss information.

Examples

The following is sample output from the **mstat** command in user EXEC mode:

```
Router> mstat lwei-home-ss2 172.16.0.1 224.0.255.255
Type escape sequence to abort.
Mtrace from 172.16.0.0 to 172.16.0.10 via group 224.0.255.255
>From source (lwei-home-ss2.cisco.com) to destination (lwei-ss20.cisco.com)
Waiting to accumulate statistics......
Results after 10 seconds:
  Source        Response Dest    Packet Statistics For    Only For Traffic
172.16.0.0      172.16.0.10 All Multicast Traffic     From 172.16.0.0
     |       __/  rtt 48   ms   Lost/Sent = Pct  Rate     To 224.0.255.255
```

```
     v      /     hop 48   ms   ---------------------     --------------------
172.16.0.1      lwei-cisco-isdn.cisco.com
     |     ^      ttl   1
     v     |      hop 31   ms    0/12 = 0%      1 pps    0/1 = --%  0 pps
172.16.0.2
172.16.0.3      eng-frmt12-pri.cisco.com
     |     ^      ttl   2
     v     |      hop -17  ms    -735/12 = --%      1 pps    0/1 = --%  0 pps
172.16.0.4
172.16.0.5      eng-cc-4.cisco.com
     |     ^      ttl   3
     v     |      hop -21  ms    -678/23 = --%      2 pps    0/1 = --%  0 pps
172.16.0.6
172.16.0.7      eng-ios-2.cisco.com
     |     ^      ttl   4
     v     |      hop 5    ms    605/639 = 95%      63 pps    1/1 = --%  0 pps
172.16.0.8
172.16.0.9      eng-ios-f-5.cisco.com
     |      \__   ttl   5
     v         \  hop 0    ms        4         0 pps           0    0 pps
172.16.0.0      172.16.0.10
  Receiver      Query Source
```

The table below describes the significant fields shown in the display.

Table 1: mstat Field Descriptions

Field	Description
Source	Traffic source of packet.
Response Dest	Place where the router sends the results of the **mstat** command.
ttl	Number of hops required from the traffic source to the current hop.
hop	Number of milliseconds of delay.
Only For Traffic From	0 packets dropped out of 2 packets received. If, for example, -2/2 was indicated, then there are 2 extra packets, which could indicate a loop condition.

Related Commands

Command	Description
mtrace	Traces the path from a source to a destination branch for a multicast distribution tree.

mtrace

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

mtrace vrf *route-name source-namesource-address* [*destination-namedestination-address*] [*group-namegroup-address*] [*trace-time*] | *source-namesource-address* [*destination-namedestination-address*] [*group-namegroup-address*] [*trace-time*]

Syntax Description

vrf *route-name*	Specifies the VPN routing or forwarding instance.
source-name | *source-address*	Domain Name System (DNS) name or the IP address of the multicast-capable source. This is a unicast address of the beginning of the path to be traced.
destination-name | *destination-address*	(Optional) DNS name or address of the unicast destination. If omitted, the mtrace starts from the system at which the command is typed.
group-name | *group-address*	(Optional) DNS name or multicast address of the group to be traced. Default address is 224.2.0.1 (the group used for multicast backbone [MBONE] Audio). When address 0.0.0.0 is used, the software invokes a weak mtrace. A weak mtrace is one that follows the Reverse Path Forwarding (RPF) path to the source, regardless of whether any router along the path has multicast routing table state.
trace-time	(Optional) The duration for which the multicast trace request must remain active. The range is from 1 to 255 router hops.

Command Default

The command is disabled.

Command Modes

User EXEC (<) Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **vrf** *route-name*keyword and argument pair was added.

Usage Guidelines

The trace request generated by the **mtrace** command is multicast to the multicast group to find the last hop router to the specified destination. The trace then follows the multicast path from the destination to the source by passing the mtrace request packet via unicast to each hop. Responses are unicast to the querying router by the first hop router to the source. This command allows you to isolate multicast routing failures.

If no arguments are entered, the router will interactively prompt you for them.

This command is identical in function to the UNIX version of **mtrace**.

Examples

The following is sample output from the **mtrace** command in user EXEC mode:

```
Router> mtrace 172.16.0.0 172.16.0.10 239.254.254.254
Type escape sequence to abort.
Mtrace from 172.16.0.0 to 172.16.0.10 via group 239.254.254.254
From source (?) to destination (?)
Querying full reverse path...
 0  172.16.0.10
-1  172.16.0.8 PIM  thresh^ 0  0 ms
-2  172.16.0.6 PIM  thresh^ 0  2 ms
-3  172.16.0.5 PIM  thresh^ 0  894 ms
-4  172.16.0.3 PIM  thresh^ 0  893 ms
-5  172.16.0.2 PIM  thresh^ 0  894 ms
-6  172.16.0.1 PIM  thresh^ 0  893 ms
```

The table below describes the significant fields shown in the display.

Table 2: mtrace Field Descriptions

Field	Description
Mtrace from 172.16.0.0 to 172.16.0.10 via group 239.254.254.254	Name and address of the source, destination, and group for which routes are being traced.
-3 172.16.0.5	Hops away from the destination (-3) and address of the intermediate router.
PIM thresh^ 0	Multicast protocol in use on this hop, and time-to-live (TTL) threshold.
893 ms	Time taken for the trace to be forwarded between hops.

Related Commands

Command	Description
mstat	Displays IP multicast packet rate and loss information.

platform multicast oce flag suppress

To suppress the use of the Negate Signal (NS) flag set by the Multicast Forwarding Information Base (MFIB) on an Output Chain Element (OCE) interface to check the activity of PIM-SM (S,G) Accept Input Interfaces (IIFs), use the platform multicast oce flag suppress command in global configuration mode. To enable the use of the NS flag to check the activity of PIM-SM (S,G) Accept IIFs, use the **no** form of the command.

platform multicast oce flag suppress
no platform multicast oce flag suppress

Syntax Description

This command has no arguments or keywords.

Command Default

The use of the NS flag in the MFIB to check the activity of PIM-SM (S,G) Accept IIFs is suppressed.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)XNE	This command was introduced. This command was implemented on Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

This command suppresses use of the NS flag set by the MFIB on an OCE interface to check the activity of PIM-SM (S,G) IIFs. OCE is a term referring to an interface belonging to MFIB's forwarding entries for a given mroute. Each OCE interface has MFIB flag states associated with it. These include the NS flag state. This command suppresses the NS flag state set by MFIB on a given OCE interface when programming the hardware forwarding. Rather than using the NS flag, MFIB will instead use the multicast packet forwarding rate to check the activity of PIM-SM (S,G) Accept IIFs. This is the recommended mode of operation. All other PIM modes and Forwarding Output Interfaces (OIFs) do not suppress the NS flag. For more information on MFIB flags, see the chapter "Verifying IPv4 Multicast Forwarding using MFIB" in the *Cisco IOS IP Multicast Configuration Guide.*

Examples

This example shows how to suppress the use of the NS flag in the MFIB to check the activity of PIM-SM (S,G) Accept IIFs:

```
Router(config)# platform mpls oce flag suppress
```

Related Commands

Command	Description
show ip mfib	Displays the forwarding entries and interfaces in the IPv4 MFIB.
show platform software ip fp active mfib	Displays the platform IP multicast forwarding information.
show platform software mlist fp active mfib	Displays the platform multicast list information.

receivers

To establish Test Receivers for Multicast Routing Monitor (MRM) tests or modify the parameters of Test Receivers, use the **receivers**commandinMRMmanager configuration mode. To restore the default values, use the **no** form of this command.

Form of the Command to Establish Test Receivers
receivers *access-list* **sender-list** *access-list* [*packet-delay*]
no receivers *access-list*

Form of the Command to Modify the Parameters of Test Receivers
receivers *access-list* [**window** *seconds*] [**report-delay** *seconds*] [**loss** *percentage*] [**no-join**] [**monitor** | **poll**]
no receivers *access-list*

Syntax Description

access-list	IP named or numbered access list that establishes the Test Receivers. Only these Test Receivers are subject to the other keywords and arguments specified in this command.
sender-list *access-list*	Specifies the sources that the Test Receiver should monitor. If the named or numbered access list matches any access list specified in the **senders** command, the associated **packet-delay** *milliseconds* keyword and argument of that **senders** command are used in this command. Otherwise, the *packet-delay* argument is required in this **receivers**command.
packet-delay	(Optional) Specifies the delay between test packets (in milliseconds). The range is from 50 to 10000. If the **sender-list** access list matches any access list specified in a **senders** command, the associated **packet-delay** *milliseconds* keyword and argument of that **senders** command are used in this command. Otherwise, the *packet-delay* argument is required in this **receivers**command.
window *seconds*	(Optional) Specifies the duration (in seconds) of a test period. This is a sliding window of time in which the packet count is collected, so that the loss percentage can be calculated. The range is from 1 to 10. The default is 5 seconds.
report-delay *seconds*	(Optional) Specifies the delay (in seconds) between status reports. The delay prevents multiple Test Receivers from sending status reports to the Manager at the same time for the same failure. This value is relevant only if there are multiple Test Receivers. The range is from 1 to 60. The default is 1 second.
loss *percentage*	(Optional) Specifies the threshold percentage of packet loss required before a status report is triggered. The range is from 0 to 100. The default is 0 percent, which means that a status report is sent for any packet loss. (This value is not applied to packet duplication; a fault report is sent for any duplicated packets.) Loss percentage calculation is explained in the “Usage Guidelines” section of this command.
no-join	(Optional) Specifies that the Test Receiver does not join the monitored group. The default is that the Test Receiver joins the monitored group.

monitor poll	(Optional) Specifies whether the Test Receiver monitors the test group or polls for receiver statistics. The **monitor** keyword means the Test Receiver reports only if the test criteria are met. The **poll** keyword means the Test Receiver sends status reports regularly, whether test criteria are met or not. The default is the behavior set with the **monitor** keyword.

Command Default

No Test Receivers are configured for MRM tests.

Command Modes

MRM manager configuration (config-mrm-manager)

Command History

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

Usage Guidelines

This command is required for MRM to work; the **receivers** *access-list* and **sender-list** *access-list* keyword-argument pairs must be specified.

Note The Cisco IOS CLI parser accepts the command entered without the required **sender-list** *access-list* keyword-argument pair. This keyword-argument pair, however, is not optional. For an MRM test to work, you must specify the sources that the Test Receiver should monitor using the **sender-list** keyword and *access-list* argument.

Optionally, you can use the **receivers** command to modify the parameters for Test Receivers.

Loss percentage is calculated based on the **packet-delay**value of the **senders** command, which defaults to 200 milliseconds, or 5 packets per second. If the **window** keyword defaults to 5 seconds, then the Test Receiver expects 5 packets per second for 5 seconds = 25 packets. If the Test Receiver receives only 15 packets, then 25 - 15 = 10 lost packets. Lost packets divided by packets expected equals loss percentage; 10/25 equals a loss percentage of 40 percent.

Examples

The following example shows how to establish a Test Receiver for an MRM test:

```
ip mrm manager test1
 manager Ethernet0/0 group 239.1.1.1
 senders 1
 receivers 2 sender-list 1
!
access-list 1 permit 10.1.1.2
access-list 2 permit 10.1.4.2
!
```

Related Commands

Command	Description
senders	Establishes Test Senders for MRM.

router-guard ip multicast efps

To enable the router guard for Ethernet Flow Points (EFPs), use the **router-guard ip multicast efps** command in global configuration mode. To disable the router guard for EFPs, use the **no** form of this command.

router-guard ip multicast efps
no router-guard ip multicast efps

Syntax Description

This command has no arguments or keywords.

Command Default

The router guard is disabled for EFPs.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Use this command in global configuration mode to enable the router guard for EFPs.

The following packet types are discarded, and the statistics are updated indicating that packets are being dropped by the router guard, if received on an EFP that has router guard enabled:

- Internet Group Management Protocol (IGMP) query messages
- IPv4 Peripheral Interface Manager version 2 messages
- IGMP PIM messages (PIMv1)
- IGMP Distance Vector Multicast Routing Protocol (DVMRP) messages
- Router-port Group Management Protocol (RGMP) messages
- Cisco Group Multicast Protocol (CGMP) messages

You must configure this command before you can configure an EFP for a bridge domain.

Examples

This example shows how to enable the router guard on all EFPs:

```
Router(config)# router-guard ip multicast efps
```

This example shows how to disable the router guard on all EFPs:

```
Router(config)# no router-guard ip multicast efps
```

Related Commands

Command	Description
clear router-guard ip multicast statistics	Clears the router guard statistical information.
router-guard ip multicast	Enables or disables the router guard for an EFP that is connected to a bridge domain interface.

Command	Description
show router-guard	Displays the router guard status and configuration information.

router-guard ip multicast switchports

To enable the router guard on all switch ports, use the **router-guard ip multicast switchports** command in global configuration mode. To disable the router guard on all switch ports, use the **no** form of this command.

router-guard ip multicast switchports
no router-guard ip multicast switchports

Syntax Description

This command has no arguments or keywords.

Command Default

The router guard is disabled on all switch ports.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

If received on a port that has router guard enabled, the following packet types are discarded and the statistics are updated indicating that packets are being dropped by the router guard:

- Internet Group Management Protocol (IGMP) query messages
- IPv4 Peripheral Interface Manager version 2 messages
- IGMP PIM messages (PIMv1)
- IGMP Distance Vector Multicast Routing Protocol (DVMRP) messages
- Router-port Group Management Protocol (RGMP)messages
- Cisco Group Multicast Protocol (CGMP)messages

Examples

This example shows how to enable the router guard on all switch ports:

```
Router(config)#
router-guard ip multicast switchports
```

This example shows how to disable the router guard on all switch ports:

```
Router(config)#
no router-guard ip multicast switchports
```

Related Commands

Command	Description
clear router-guard ip multicast statistics	Clears the router guard statistical information.
router-guard ip multicast	Enables or disables the router guard for switch ports that are connected to multicast routers.
show router-guard	Displays the router guard status and configuration information.

senders

To configure Test Sender parameters used for a Multicast Routing Monitor (MRM) test, use the **senders**command in MRM manager configuration mode. To restore the default settings, use the **no** form of this command.

senders *access-list* [**packet-delay** *milliseconds*] [**rtp** | **udp**] [**target-only** | **all-multicasts** | **all-test-senders**] [*proxy-src*]
no senders *access-list*

Syntax Description

access-list	IP named or numbered access list that defines which Test Senders are involved in the test and which Test Senders these parameters apply to.
packet-delay *milliseconds*	(Optional) Specifies the delay between test packets (in milliseconds). The range is from 50 to 10000. The default is 200 milliseconds, which results in 5 packets per second.
rtp | **udp**	(Optional) Specifies the encapsulation of test packets, either Real-Time Transport Protocol (RTP)-encapsulated or User Datagram Protocol (UDP)-encapsulated. By default, test packets are RTP-encapsulated.
target-only	(Optional) Specifies that test packets are sent out on the targeted interface only (that is, the interface with the IP address that is specified in the Test Sender request target field). By default, test packets are sent out on all interfaces that are enabled with IP multicast.
all-multicasts	(Optional) Specifies that the test packets are sent out on all interfaces that are enabled with IP multicast. This is the default method for sending test packets.
all-test-senders	(Optional) Specifies that test packets are sent out on all interfaces that have test-sender mode enabled. By default, test packets are sent out on all interfaces that are enabled with IP multicast.
proxy-src	(Optional) Source IP address for which the Test Sender will proxy test packets. Enter an address if you want to test, for a specific source, whether the multicast distribution tree is working.

Command Default

No test senders are configured to be involved in MRM tests.

Command Modes

MRM manager configuration (config-mrm-manager)

Command History

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

Usage Guidelines

Use this command to specify which Test Senders are involved in the test and are affected by these parameters.

Examples

The following example shows how to configure a Test Sender for an MRM test:

```
ip mrm manager test1
 manager Ethernet0/0 group 239.1.1.1
 senders 1
 receivers 2 sender-list 1
!
access-list 1 permit 10.1.1.2
access-list 2 permit 10.1.4.2
```

Related Commands

Command	Description
receivers	Establishes Test Receivers for MRM.