

ip rgmp

To enable the Router-Port Group Management Protocol (RGMP) on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces, use the **ip rgmp** command in interface configuration mode. To disable RGMP on the interfaces, use the **no** form of this command.

ip rgmp

no ip rgmp

Syntax Description

This command has no arguments or keywords.

Defaults

RGMP is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(10)S	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(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

RGMP is supported only on Ethernet, Fast Ethernet, and Gigabit Ethernet interfaces.

Before you enable RGMP, the following features must be enabled on your router:

- IP routing
- IP multicast
- PIM in sparse mode, sparse-dense mode, source specific mode, or bidirectional mode

If your router is in a bidirectional group, make sure to enable RGMP only on interfaces that do not function as a designated forwarder (DF). If you enable RGMP on an interface that functions as a DF, the interface will not forward multicast packets up the bidirectional shared tree to the rendezvous point (RP).

The following features must be enabled on your switch:

- IP multicast
- IGMP snooping

Examples

The following example enables RGMP on Ethernet interface 1/0:

```
interface ethernet 1/0
 ip rgmp
```

Related Commands

Command	Description
debug ip rgmp	Logs debug messages sent by an RGMP-enabled router.
show ip igmp interface	Displays multicast-related information about an interface.

ip sap cache-timeout

To limit how long a Session Announcement Protocol (SAP) cache entry stays active in the cache, use the **ip sap cache-timeout** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip sap cache-timeout *minutes*

no ip sap cache-timeout

Syntax Description	<i>minutes</i>	Time (in minutes) that a SAP cache entry is active in the cache.
--------------------	----------------	--

Defaults	By default, session announcements remain for 1440 minutes (24 hours) in the cache.
----------	--

Command Modes	Global configuration
---------------	----------------------

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

Usage Guidelines	This command defines how long session announcements are cached by the router. Active session announcements are periodically re-sent by the originating site, refreshing the cached state in the router. The minimum interval between announcements for a single group is 5 minutes. Setting the cache timeout to a value less than 30 minutes is not recommended. Set the cache timeout to 0 to keep entries in the cache indefinitely.
------------------	---

Examples	The following example causes SAP cache entries to remain in the cache for 30 minutes:
----------	---

```
ip sap cache-timeout 30
```

Related Commands	Command	Description
	clear ip sap	Deletes a SAP cache entry or the entire SAP cache.
	show ip sap	Displays the SAP cache.

ip sap listen

To enable the Cisco IOS software to listen to session directory announcements, use the **ip sap listen** command in interface configuration mode. To disable the function, use the **no** form of this command.

ip sap listen

no ip sap listen

Syntax Description This command has no arguments or keywords.

Defaults The command is disabled.

Command Modes Interface configuration

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

Usage Guidelines Cisco IOS software can receive and store Session Description Protocol (SDP) and Session Announcement Protocol (SAP) session announcements. When the **ip sap listen** command is configured on an interface, the well-known session directory groups on that interface can receive and store session announcements. The announcements can be displayed with the **show ip sap** command. The **ip multicast rate-limit** command uses stored session announcements. To configure the period of time after which received announcements will expire, use the **ip sap cache-timeout** command.

When the **no ip multicast routing** command is configured, announcements are only stored if they are received on an interface configured with the **ip sap listen** command. When a system is configured as a multicast router, it is sufficient to configure the **ip sap listen** command on only a single multicast-enabled interface. The well-known session directory groups are handled as local joined groups after the **ip sap listen** command is first configured (see the L flag of the **show ip mroute** command). This configuration causes announcements received from all multicast-enabled interfaces to be routed and stored within the system.

Examples

The following example shows how to enable a router to listen to session directory announcements:

```
ip routing
interface loopback 0
 ip address 10.0.0.51 255.255.255.0
 ip pim sparse-dense mode
 ip sap listen
```

Related Commands

Command	Description
clear ip sap	Deletes a SAP cache entry or the entire SAP cache.
ip multicast rate-limit	Controls the rate a sender from the source list can send to a multicast group in the group list.
ip multicast-routing	Enables IP multicast routing or multicast distributed switching.
ip sap cache-timeout	Limits how long a SAP cache entry stays active in the cache.
show ip mroute	Displays the contents of the IP mroute routing table.
show ip sap	Displays the SAP cache.

ip sdr cache-timeout

The **ip sdr cache-timeout** command is replaced by the **ip sap cache-timeout** command. See the description of the **ip sap cache-timeout** command for more information.

ip sdr listen

The **ip sdr listen** command is replaced by the **ip sap listen** command. See the description of the **ip sap listen** command for more information.

ip service reflect

To match and rewrite multicast packets routed onto a Vif1 interface, use the **ip service reflect** command in interface configuration mode. To disable this feature, use the **no** form of this command.

ip service reflect *input-interface* **destination** *destination-address* **to** *new-destination-address*
mask-len *number* **source** *new-source-address*

no ip service reflect *input-interface* **destination** *destination-address* **to** *new-destination-address*
mask-len *number* **source** *new-source-address*

Syntax Description

<i>input-interface</i>	Interface type and number.
destination	Identifies packets with the specified destination address.
<i>destination-address</i>	Destination IP address in the packets, in A.B.C.D format.
to	Modifies the destination IP address in reflected packets to a new IP address.
<i>new-destination-address</i>	New destination address to be used, in A.B.C.D format.
mask-len <i>number</i>	Specifies the mask length of the destination address to match. The <i>number</i> argument is a value from 0 to 32.
source	Modifies the source address in reflected packets. The source address must be on the same subnet as the Vif1 interface.
<i>new-source-address</i>	New source address to be used, in A.B.C.D format.

Command Default

The multicast service reflection feature is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(33)SX14	This command was integrated into Cisco IOS Release 12.2(33)SX14.

Usage Guidelines

Use the **ip service reflect** command to match and rewrite multicast packets routed onto a Vif1 interface.

The matched and rewritten packet is sent back into Cisco multicast packet routing, where it is handled like any other packet arriving from an interface.

More than one multicast service reflection operation can be configured to match the same packet, allowing you to replicate the same received traffic to multiple destination addresses.

Examples

The following example shows how to translate any multicast packet with a destination address of 239.1.1.0/24 to a destination of 239.2.2.0/24 with a new source address of 10.1.1.2. For example, a packet with a source and destination of (10.10.10.10, 239.1.1.15) would be translated to (10.1.1.2, 239.2.2.15).

```
Router(config)# interface Vif1
Router(config-if)# ip address 10.1.1.1 255.255.255.0
Router(config-if)# ip pim sparse-mode
Router(config-if)# ip service reflect Ethernet 0/0 destination 239.1.1.0 to 239.2.2.0
mask-len 24 source 10.1.1.2
Router(config-if)# ip igmp static-group 239.1.1.0
Router(config-if)# ip igmp static-group 239.1.1.1
```

ip urd

To enable interception of TCP packets sent to the reserved URL Rendezvous Directory (URD) port 465 on an interface and processing of URD channel subscription reports, use the **ip urd** command in interface configuration mode. To disable URD on an interface, use the **no** form of this command.

ip urd [proxy]

no ip urd [proxy]

Syntax Description

proxy	(Optional) Allows an interface to accept URL requests from any TCP connection sent to that interface. If the proxy keyword is not configured, the interface will accept URL requests from TCP connections only if the requests originated from directly connected hosts. The proxy option must be enabled on an interface if it is unnumbered or if it has downstream routers configured with Internet Group Management Protocol (IGMP) proxy routing. To prevent users on the backbone from creating URD state on your router, do not enable the proxy option on a backbone interface of your router.
--------------	--

Defaults

The command is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

To use this command, you must first define a Source Specific Multicast (SSM) range of IP addresses using the **ip pim ssm** global configuration command. When URD is enabled, it is supported in the SSM range of addresses only. We recommend that you not enable URD on backbone interfaces, but only on interfaces connecting to hosts.

URD functionality is available for multicast process switching, fast switching, and distributed fast-switching paths.

Examples

The following example shows how to configure URD on Ethernet interface 3/3:

```
interface ethernet 3/3
 ip urd
```

Related Commands

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

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

<i>interface-type</i> <i>interface-number</i>	Interface type and number of the Manager. The IP address associated with this interface is the source address of the Manager.
group <i>ip-address</i>	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 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] | mpls mldp
number-of-data-mdts}
```

```
no mdt data {group-address-range wildcard-bits [threshold kb/s] [list access-list] | mpls mldp
number-of-data-mdts}
```

Syntax Description

<i>group-address-range</i>	Multicast group address range. The range is from 224.0.0.1 to 239.255.255.255.
<i>wildcard-bits</i>	Wildcard bits to be applied to the multicast group address range.
threshold <i>kb/s</i>	(Optional) Defines the bandwidth threshold value in kilobits per second (kb/s). The range is from 1 to 4294967.
list <i>access-list</i>	(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 <i>access-list</i> argument.
mpls mldp <i>number-of-data-mdts</i>	Specifies the number of data MDTs created using Multicast Label Distribution Protocol (MLDP) Label Switched Path (LSP).

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.
15.0(1)S	This command was modified. The keywords mpls mldp were added.

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 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

<i>group-address</i>	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 <i>root-address</i>	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.

Defaults

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.

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 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.

Defaults The command is disabled.

Command Modes VRF configuration

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.

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

Examples The following example shows how to enable MDT log reuse:

```
mdt log-reuse
```

Related Commands	Command	Description
	mdt data	Configures the multicast group address range for data MDT groups.
	mdt default	Configures a default MDT group for a VPN VRF.

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.

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.

Command	Description
mdt default	Configures a default MDT group for a VPN VRF.
vrf definition	Configures a VRF routing table instance and enters VRF configuration mode.

mls ip multicast (global configuration)



Note

Effective with Cisco IOS Release 12.2(33)SRE, the **mls ip multicast(global configuration)** command is not available in Cisco IOS software.

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.

Defaults

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.
	12.2(33)SRE	This command was removed.

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.

Defaults 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 rendezvous point, use the **mls ip multicast bidir gm-scan-interval** command in global configuration mode. To disable the RPF scan interval for the Bidir rendezvous 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	<i>interval</i>	RPF scan interval for the Bidir rendezvous point; valid values are from 1 to 1000 seconds.
---------------------------	-----------------	--

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

Examples This example shows how to set the RPF scan interval for the Bidir rendezvous 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.

Defaults 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 Release 12.2(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.
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 <i>seconds</i>	(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 <i>count-number</i>	(Optional) Specifies the maximum number of prefixes to check per scan; valid values are from 2 to 500.
period <i>seconds</i>	(Optional) Specifies the period between scans; valid values are from 2 to 3600 seconds.

Defaults

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

Defaults	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** | **fast**} *time*

no mls ip multicast non-rpf aging {**global** | **fast**}

Syntax Description	global <i>time</i>	fast <i>time</i>
	Specifies the global aging time interval. Valid values are 1 to 180; by default the time is set to 20 seconds.	Specifies the fast aging time interval. Valid values are 2 to 10; by default the time is set to 2 seconds.

Defaults 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.

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

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 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#
```

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.

Defaults

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	This 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 <i>time</i>	Specifies the maximum time to wait for protocol convergence; valid values are from 0 to 3600 seconds.
leak interval <i>seconds</i>	Specifies the packet-leak interval; valid values are from 0 to 3600 seconds.
leak percent <i>percentage</i>	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.

Defaults 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
<code>show mls ip multicast</code>	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.

Defaults

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	Command	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 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.

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.

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.

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-address | interface] [host-name | host-address]
```

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

Defaults 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 <i>route-name</i> 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 mrouterd 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 (barnet-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

<i>test-name</i>	Name of the MRM test to start or stop.
start	Starts the MRM test specified for the <i>test-name</i> argument.
stop	Stops the MRM test specified for the <i>test-name</i> 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-name | source-address } | { source-name | source-address }
      [destination-name | destination-address] [group-name | group-address] }
```

Syntax Description

vrf <i>route-name</i>	Specifies the VPN routing or forwarding instance.
<i>source-name</i> <i>source-address</i>	Domain Name System (DNS) name or the IP address of the multicast-capable source.
<i>destination-name</i> <i>destination-address</i>	(Optional) DNS name or address of the destination. If omitted, the command uses the system at which the command is typed.
<i>group-name</i> <i>group-address</i>	(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).

Defaults

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 <i>route-name</i> 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

```

Table 2 describes the significant fields shown in the display.

Table 2 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-name | source-address } [destination-name | destination-address]
          [group-name | group-address] [trace-time] | { source-name | source-address } [destination-name
          | destination-address] [group-name | group-address] [trace-time] }
```

Syntax Description

vrf <i>route-name</i>	Specifies the VPN routing or forwarding instance.
<i>source-name</i> <i>source-address</i>	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.
<i>destination-name</i> <i>destination-address</i>	(Optional) DNS name or address of the unicast destination. If omitted, the mtrace starts from the system at which the command is typed.
<i>group-name</i> <i>group-address</i>	(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.
<i>trace-time</i>	(Optional) The duration for which the multicast trace request must remain active. The range is from 1 to 255 router hops.

Defaults

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 <i>route-name</i> 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
```

[Table 3](#) describes the significant fields shown in the display.

Table 3 *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.

receivers

To establish Test Receivers for Multicast Routing Monitor (MRM) tests or modify the parameters of Test Receivers, use the **receivers** command in MRM manager 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	
<i>access-list</i>	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 <i>access-list</i>	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 <i>milliseconds</i> keyword and argument of that senders command are used in this command. Otherwise, the <i>packet-delay</i> argument is required in this receivers command.
<i>packet-delay</i>	(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 <i>milliseconds</i> keyword and argument of that senders command are used in this command. Otherwise, the <i>packet-delay</i> argument is required in this receivers command.
window <i>seconds</i>	(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 <i>seconds</i>	(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 <i>percentage</i>	(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

To enable the router guard for switch ports that are connected to multicast routers, use the **router-guard ip multicast** command in interface configuration mode. To disable the router guard on switch ports that are connected to multicast routers, use the **no** form of this command.

router-guard ip multicast [**vlan** *vlan-id*]

no router-guard ip multicast [**vlan** *vlan-id*]

Syntax Description

vlan <i>vlan-id</i>	(Optional) Specifies the Layer 2 VLAN identification.
----------------------------	---

Command Default

The router guard for switch ports that are connected to multicast routers is disabled by default.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

You can enter the **vlan** *vlan-id* keyword and argument if the port is a trunk port.

You cannot enter a range or multiple VLANs in a single command.

For the router guard to work on switch ports, you must enter the **router-guard ip multicast switchports** global configuration command before entering the **router-guard ip multicast** interface configuration command.

Examples

This example shows how to enable the router guard on an interface:

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

This example shows how to disable router guard on an interface:

```
Router(config-if)# no router-guard ip multicast vlan 100
```

Related Commands

Command	Description
clear router-guard ip multicast statistics	Clears the router guard statistical information.
router-guard ip multicast switchports	Enables or disables the router guard on all switch ports.

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

<i>access-list</i>	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 <i>milliseconds</i>	(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.
<i>proxy-src</i>	(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
<code>receivers</code>	Establishes Test Receivers for MRM.
