Configuration Commands

Generic Commands

shutdown

Syntax [**no**] **shutdown**

Context
config>router>igmp
config>router>igmp>interface
config>router>igmp>interface>group-interface
config>router>igmp>if>mcac>mc-constraints
config>router>pim
config>router>pim>interface
config>router>pim>rp>rp-candidate
config>router>pim>rp>bsr-candidate
config>router>pim>rp>ipv6>rp-candidate
config>router>pim>rp>ipv6>bsr-candidate
config>router>pim>if>mcac>mc-constraints
config>router>msdp
config>router>msdp>peer
config>router>msdp>group
config>router>mcac>policy>bundle
config>router>mld
config>router>mld>group-interface>mcac>mc-constraints
config>router>mld>group-interface
config>router>mld>interface

Description The **shutdown** command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command.

The **shutdown** command administratively disables an entity. The operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shut down before they may be deleted.

Unlike other commands and parameters where the default state is not indicated in the configuration file, **shutdown** and **no shutdown** are always indicated in system generated configuration files.

The **no** form of the command puts an entity into the administratively enabled state.

Default

no shutdown:	config>router>igmp config>router>igmp>interface *ip-int-name* config>router>pim config>router>pim>rp>rp-candidate
shutdown:	config>router>pim>rp>bsr-candidate

Multicast Commands

ssm-translate

Syntax **ssm-translate**

Context config>router>igmp>interface>shutdown

Description This command adds or removes ssm-translate group ranges.

source

Syntax [**no**] **source** *ip-address*

Context config>router>igmp>interface>shutdown>ssm-translate>grp-range

Description This command adds or removes source addresses for the SSM translate group range.

Parameters *ip-address* — a.b.c.d - unicast source address

grp-range

Syntax [**no**] **grp-range** *start end*

Context config>router>igmp>interface>shutdown>ssm-translate

Description This command adds or removes SSM translate group range entries.

Parameters *start* — a.b.c.d - multicast group range start address

end — a.b.c.d - multicast group range end address

description

Syntax **description** *description-string*
no description

Context config>router>mcac>policy
config>router>mcac>policy>bundle

Description This command creates a text description stored in the configuration file for a configuration context.

The **description** command associates a text string with a configuration context to help identify the context in the configuration file.

The **no** form of the command removes any description string from the context.

Default No description associated with the configuration context.

Parameters *string* — The description character string. Allowed values are any string up to 80 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

ip-fast-reroute

Syntax [**no**] **ip-fast-reroute**

Context config>router

Description This command configures IP fast reroute.

mc-maximum-routes

Syntax **mc-maximum-routes** *number* [**log-only**] [**threshold** *threshold*]
no mc-maximum-routes

Context config>router

Description This command specifies the maximum number of multicast routes that can be held within a VPN routing/forwarding (VRF) context. When this limit is reached, a log and SNMP trap are sent. If the **log-only** parameter is not specified and the maximum-routes value is set below the existing number of routes in a VRF, then no new joins will be processed.

The **no** form of the command disables the limit of multicast routes within a VRF context. Issue the **no** form of the command only when the VPRN instance is shutdown.

Default no mc-maximum-routes

Parameters *number* — Specifies the maximum number of routes to be held in a VRF context.

Values 1 — 2147483647

log-only — Specifies that if the maximum limit is reached, only log the event. **log-only** does not disable the learning of new routes.

threshold *threshold* **—** The percentage at which a warning log message and SNMP trap should be sent.

Values 0 — 100

Default 1

multicast-info

Syntax **multicast-info-policy** *policy-name*
no multicast-info-policy

Context configure>router

Description This command configures multicast information policy.

Parameters *policy-name* — Specifies the policy name.

Values 32 chars max

Router IGMP Commands

igmp

Syntax [**no**] **igmp**

Context config>router

Description This command enables the Internet Group Management Protocol (IGMP) context. When the context is created, the IGMP protocol is enabled.

The Internet Group Management Protocol (IGMP) is used by IPv4 systems (hosts and routers) to report their IP multicast group memberships to neighboring multicast routers. An IP multicast router can be a member of one or more multicast groups, in which case it performs both the "multicast router part" of the protocol which collects the membership information needed by its multicast routing protocol, and the "group member part" of the protocol which informs itself and other neighboring multicast routers of its memberships.

The **no** form of the command disables the IGMP instance. To start or suspend execution of IGMP without affecting the configuration, use the **no shutdown** command.

Default none

grp-if-query-src-ip

Syntax **grp-if-query-src-ip** *ip-address*
no grp-if-query-src-ip

Context config>router>igmp

Description This command configures the query source IP address for all group interfaces.

The **no** form of the command removes the IP address.

Default none

interface

Syntax [**no**] **interface** *ip-int-name*

Context config>router>igmp

Description This command enables the context to configure an IGMP interface. The interface is a local identifier of the network interface on which reception of the specified multicast address is to be enabled or disabled.

The **no** form of the command deletes the IGMP interface. The **shutdown** command in the **config>router>igmp>interface** context can be used to disable an interface without removing the configuration for the interface.

Default **no interface** — No interfaces are defined.

Parameters *ip-int-name* — The IP interface name. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service ies interface** commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

If the IP interface name does not exist or does not have an IP address configured an error message will be returned.

If the IP interface exists in a different area it will be moved to this area.

disable-router-alert-check

Syntax [**no**] **disable-router-alert-check**

Context config>router>igmp>if
config>router>igmp>group-interface

Description This command enables the router alert checking for IGMP messages received on this interface.

The **no** form of the command disables the IGMP router alert check option.

group-interface

Syntax [**no**] **group-interface** *ip-int-name*

Context config>router>igmp>if

Description This command enables IGMP on a group-interface in a VRF context. Activating IGMP under the group-interface is a prerequisite for subscriber replication. The group-interface is also needed so that mcac can be applied and various IGMP parameters defined.

This command can be used in a regular, wholesaler or retailer type of VRF. Note that the retailer VRF does not have the concept of group-interfaces under the subscriber-interface hierarchy. In case that this command is applied to a retailer VRF instance, the optional fwd-service command must be configured. The fwd-service command is referencing the wholesaler VRF in which the traffic is ultimately replicated. Note that redirection in the retailer VRF is supported.

This command enables IGMP on a group-interface in the Global Routing Table (GRT). The group-interface in GRT is defined under the IES service. Activating IGMP under the group-interface is a prerequisite for subscriber replication. The group-interface is also needed so that MCAC can be applied and various IGMP parameters defined.

Default none

Parameters *ip-int-name* — Specifies the name of the group interface.

import

Syntax **import** *policy-name*
no import

Context configure>router>igmp>interface
configure>router>igmp>group-interface
configure>service>vprn>igmp>interface
configure>service>vprn>igmp>group-interface
configure>subscr-mgmt>igmp-policy

Description This command applies the referenced IGMP policy (filter) to a subscriber or a group-interface. An IGMP filter is also known as a black/white list and it is defined under the **configure>router>policy-options**.

When redirection is applied, only the import policy from the subscriber will be in effect. The import policy under the group interface is applicable only for IGMP states received directly on the sap (AN in IGMP proxy mode).

The **no** form of the command removes the policy association from the IGMP instance.

Default **no import** — No import policy specified.

Parameters *policy-name* — The route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Route policies are configured in the **config>router>policy-options** context.

query-src-ip

Syntax **query-src-ip** *ip-address*
no query-src-ip

Context config>router>igmp>group-interface

Description This command configures the query source IP address for the group interface. This IP address overrides the source IP address configured at the router level.

The **no** form of the command removes the IP address.

Default none

Parameters *ip-address* — Sets the source IPv4 address for all subscriber's IGMP queries.

sub-hosts-only

Syntax [**no**] **sub-hosts-only**

Context config>router>igmp>group-interface>mcac
config>router>mld>group-interface

Description This command enables the handling of IGMP joins received from hosts that are not known in subscriber management or on which no IGMP policy is applied.

The **no** form of the command disables the command.

Default sub-hosts-only

sub-hosts-only

Syntax [**no**] **sub-hosts-only**

Context config>router>igmp>group-interface

Description This command disables processing of IGMP messages outside of the subscriber-host context. No other hosts outside of the subscriber-hosts can create IGMP states.

Disabling this command will allow creation of the IGMP states that correspond to the AN that operate in IGMP proxy mode. In this mode the AN will hide source IP addresses of IGMP messages and will source IGMP messages with its own IP address. In this case an IGMP state can be created under the sap context. This IGMP state creation under the sap is controlled via the import policy under the group-interface.

IGMP state processing for regular subscriber-hosts is unaffected by this command.

The **no** form of the command disables the command.

Default sub-hosts-only

max-groups

Syntax **max-groups** [1..16000]
no max-groups

Context config>router>igmp>if
config>router>igmp>group-interface
config>router>pim>if

Description This command specifies the maximum number of groups for which IGMP can have local receiver information based on received IGMP reports on this interface. When this configuration is changed dynamically to a value lower than the currently accepted number of groups, the groups that are already accepted are not deleted. Only new groups will not be allowed. This command is applicable for IPv4 and IPv6.

Default 0, no limit to the number of groups.

Parameters *value* — Specifies the maximum number of groups for this interface.

Values 1 — 16000

max-grp-sources

Syntax **max-grp-sources** [1..32000]
no max-grp-sources

Context config>router>igmp>interface
config>router>igmp>group-interface
config>router>mld>group-interface

Description This command configures the maximum number of group sources for which IGMP can have local receiver information based on received IGMP reports on this interface. When this configuration is changed dynamically to a value lower than currently accepted number of group sources, the group sources that are already accepted are not deleted. Only new group sources will not be allowed.

The **no** form of the command reverts to the default.

Default 0

Parameters **1 — 32000 —** Specifies the maximum number of group source.

Values 1 — 32000

max-sources

Syntax **max-sources** [1..1000]
no max-sources

Context config>router>igmp>group-interface
config>router>mld>group-interface

Description This command configures the maximum number of group sources for this group-interface.

static

Syntax **static**

Context config>router>igmp>if

Description This command tests multicast forwarding on an interface without a receiver host. When enabled, data is forwarded to an interface without receiving membership reports from host members.

Default none

group

Syntax [**no**] **group** *grp-ip-address*

Context config>router>igmp>if>static

Description This command enables the context to add a static multicast group either as a (*,G) or one or more (S,G) records. Use IGMP static group memberships to test multicast forwarding without a receiver host. When IGMP static groups are enabled, data is forwarded to an interface without receiving membership reports from host members.

When static IGMP group entries on point-to-point links that connect routers to a rendezvous point (RP) are configured, the static IGMP group entries do not generate join messages toward the RP.

Default none

Parameters *grp-ip-address* — Specifies an IGMP multicast group address that receives data on an interface. The IP address must be unique for each static group.

source

Syntax [**no**] **source** *ip-address*

Context config>router>igmp>if>static>group
config>router>igmp>ssm-translate>grp-range

Description This command specifies a IPv4 unicast address that sends data on an interface. This enables a multicast receiver host to signal a router the group to receive multicast traffic from, and from the source(s) that the traffic is expected.

The **source** command is mutually exclusive with the specification of individual sources for the same group.

The source command in combination with the group is used to create a specific (S,G) static group entry.

Use the **no** form of the command to remove the source from the configuration.

Default none

Parameters *ip-address* — Specifies the IPv4 unicast address.

starg

Syntax [**no**] **starg**

Context config>router>igmp>if>static>group

Description This command adds a static (*,G) entry. This command can only be enabled if no existing source addresses for this group are specified.

Use the **no** form of the command to remove the starg entry from the configuration.

Default none

subnet-check

Syntax [**no**] **subnet-check**

Context config>router>igmp>interface
config>router>mld>group-interface
config>router>igmp>group-interface>mcac

Description This command enables subnet checking for IGMP messages received on this interface. All IGMP packets with a source address that is not in the local subnet are dropped.

Default enabled

version

Syntax **version** *version*
no version

Context config>router>igmp>if
config>router>mld>group-interface
config>router>igmp>group-interface>mcac

Description This command specifies the IGMP version. If routers run different versions of IGMP, they will negotiate the lowest common version of IGMP that is supported by hosts on their subnet and operate in that version. For IGMP to function correctly, all routers on a LAN should be configured to run the same version of IGMP on that LAN.

For IGMPv3, note that a multicast router that is also a group member performs both parts of IGMPv3, receiving and responding to its own IGMP message transmissions as well as those of its neighbors.

Default 3

Parameters *version* — Specifies the IGMP version number.

Values 1, 2, 3

Values >= 1000

query-interval

Syntax **query-interval** *seconds*
no query-interval

Context config>router>igmp

Description This command specifies the frequency that the querier router transmits general host-query messages. The host-query messages solicit group membership information and are sent to the all-systems multicast group address, 224.0.0.1.

Default 125

seconds — The time frequency, in seconds, that the router transmits general host-query messages.

Values 2 — 1024

query-last-member-interval

Syntax **query-last-member-interval** *seconds*

Context config>router>igmp

Description This command configures the frequency at which the querier sends group-specific query messages including messages sent in response to leave-group messages. The lower the interval, the faster the detection of the loss of the last member of a group.

Default 1

Parameters *seconds* — Specifies the frequency, in seconds, at which query messages are sent.

Values 1 — 1024

query-response-interval

Syntax **query-response-interval** *seconds*

Context config>router>igmp

Description This command specifies how long the querier router waits to receive a response to a host-query message from a host.

Default 10

Parameters *seconds* — Specifies the the length of time to wait to receive a response to the host-query message from the host.

Values 1 — 1023

robust-count

Syntax **robust-count** *robust-count*
no robust-count

Context config>router>igmp

Description This command configures the robust count. The robust-count variable allows tuning for the expected packet loss on a subnet. If a subnet anticipates losses, the robust-count variable can be increased.

Default 2

Parameters *robust-count* — Specify the robust count value.

Values 2 — 10

ssm-translate

Syntax **ssm-translate**

Context config>router>igmp

Description This command enables the context to configure group ranges which are translated to SSM (S,G) entries. If the static entry needs to be created, it has to be translated from a IGMPv1 IGMPv2 request to a Source Specific Multicast (SSM) join. An SSM translate source can only be added if the starg command is not enabled. An error message is generated if you try to configure the **source** command with **starg** command enabled.

grp-range

Syntax [**no**] **grp-range** *start end*

Context config>router>igmp>ssm-translate

Description This command is used to configure group ranges which are translated to SSM (S,G) entries.

Parameters *start* — An IP address that specifies the start of the group range.

end — An IP address that specifies the end of the group range. This value should always be greater than or equal to the value of the *start* value.

source

Syntax [**no**] **source** *ip-address*

Context config>router>igmp>ssm-translate>grp-range

Description This command specifies the source IP address for the group range. Whenever a (*,G) report is received in the range specified by **grp-range** *start* and *end* parameters, it is translated to an (S,G) report with the value of this object as the source address.

Parameters *ip-address* — Specifies the IP address that will be sending data.

tunnel-interface

Syntax [**no**] **tunnel-interface** {**rsvp-p2mp** *lsp-name* | **ldp-p2mp** *p2mp-id* **sender** *sender-address* [**root-node**]}

Context config>router

config>router>igmp

Description This command creates a tunnel interface associated with an RSVP P2MP LSP. IPv4 multicast packets are forwarded over the P2MP LSP at the ingress LER based on a static join configuration of the multicast group against the tunnel interface associated with the originating P2MP LSP. At the egress LER, packets of a multicast group are received from the P2MP LSP via a static assignment of the specific <S,G> to the tunnel interface associated with a terminating LSP.

At ingress LER, the tunnel interface identifier consists of a string of characters representing the LSP name for the RSVP P2MP LSP. The user can create one or more tunnel interfaces in PIM and associate each to a different RSVP P2MP LSP. P2mp-ID is required to configure LDP P2MP LSP tunnel interfaces. Sender address for a tunnel itnerface must be specified only on the leaf node.

At egress LER, the tunnel interface identifier consists of a couple of string of characters representing the LSP name for the RSVP P2MP LSP followed by the system address of the ingress LER. The LSP name must correspond to a P2MP LSP name configured by the user at the ingress LER. The LSP name string must not contain "::" (two :s) nor contain a ":" (single ":") at the end of the LSP name. However, a ":" (single ":") can appear anywhere in the string except at the end of the name.

Default none

Parameters **rsvp-p2mp** *lsp-name* — Specifies the LSP. The LSP name can be up to 32 characters long and must be unique.

p2mp-id — Identifier used for signaling mLDP P2MP LSP.

Values 1 – 4294967296 (On Leaf Node)

Values 1-8192 (On Root Node)

sender *lsp-name* — :Specifies the sender IP address: a.b.c.d

static

Syntax **static**

Context config>router>igmp>tunnel-interface

Description This command provides the context to configure static multicast receiver hosts on a tunnel interface associated with an RSVP P2MP LSP.

When enabled, data is forwarded to an interface without receiving membership reports from host members.

Default none

group

Syntax [**no**] **group** *grp-ip-address*

Context config>router>igmp>tunnel-interface>static

Description This command enables the context to add a static multicast group either as a (*,G) or one or more (S,G) records.

The user can assign static multicast group joins to a tunnel interface associated with an RSVP P2MP LSP. Note that a given <*,G> or <S,G> can only be associated with a single tunnel interface.

A multicast packet which is received on an interface and which succeeds the RPF check for the source address will be replicated and forwarded to all OIFs which correspond to the branches of the P2MP LSP. The packet is sent on each OIF with the label stack indicated in the NHLFE of this OIF. The packets will also be replicated and forwarded natively on all OIFs which have received IGMP or PIM joins for this <S,G>.

The multicast packet can be received over a PIM or IGMP interface which can be an IES interface, a spoke SDP terminated IES interface, or a network interface.

Default none

Parameters *grp-ip-address* — Specifies a multicast group address that receives data on a tunnel interface. The IP address must be unique for each static group.

source

Syntax **[no] source** *ip-address*

Context config>router>igmp>tunnel-interface>static>group

Description This command specifies a IPv4 unicast address of a multicast source. The source command is mutually exclusive with the specification of individual sources for the same group. The source command in combination with the group is used to create a specific (S,G) group entry in a static group join on a tunnel interface associated with a P2MP RSVP LSP.

The **no** form of the command removes the source from the configuration.

Default none

Parameters *ip-address* — Specifies the IPv4 unicast address.

starg

Syntax **[no] starg**

Context config>router>igmp>tunnel-interface>static>group

Description This command adds a static (*,G) group entry in a static group join on a tunnel interface associated with a P2MP RSVP LSP.

This command can only be enabled if no existing source addresses for this group are specified.

The **no** form of the command removes the starg entry from the configuration.

Default none

Router PIM Commands

pim

Syntax [**no**] **pim**

Context config>router

Description This command configures a Protocol Independent Multicast (PIM) instance.

PIM is used for multicast routing within the network. Devices in the network can receive the multicast feed requested and non-participating routers can be pruned. The router OS supports PIM sparse mode (PIM-SM).

Default not enabled

interface

Parameters [**no**] **interface** *ip-int-name*

Context config>router>pim

Description This command creates a PIM interface.

Interface names are case-sensitive and must be unique within the group of defined IP interfaces defined for **config router interface**, **config service ies interface**, and **config service ies subscriber-interface group-interface**. Interface names must not be in the dotted decimal notation of an IP address. For example, the name "1.1.1.1" is not allowed, but "int-1.1.1.1" is allowed. Show commands for router interfaces use either the interface names or the IP addresses. Ambiguity can exist if an IP address is used as an IP address and an interface name. Duplicate interface names can exist in different router instances, although this is not recommended because it may be confusing.

The **no** form of the command removes the IP interface and all the associated configurations.

Default No interfaces or names are defined within PIM.

Parameters *ip-int-name* — The name of the IP interface. Interface names must be unique within the group of defined IP interfaces for **config router interface**, **config service ies interface**, and **config service ies subscriber-interface group-interface** commands. An interface name cannot be in the form of an IP address. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

Values 1 — 32 alphanumeric characters.

If the *ip-int-name* already exists, the context is changed to maintain that IP interface. If *ip-int-name* does not exist, the interface is created and the context is changed to that interface for further command processing.

apply-to

Syntax **apply-to {ies | non-ies | all | none}**

Context config>router>pim

Description This command creates a PIM interface with default parameters.

If a manually created or modified interface is deleted, the interface will be recreated when (re)processing the **apply-to** command and if PIM is not required on a specific interface a shutdown should be executed.

The **apply-to** command is first saved in the PIM configuration structure. Then, all subsequent commands either create new structures or modify the defaults as created by the apply-to command.

Default none (keyword)

Parameters **ies —** Creates all IES interfaces in PIM.

non-ies — Non-IES interfaces are created in PIM.

all — All IES and non-IES interfaces are created in PIM.

none — Removes all interfaces that are not manually created or modified. It also removes explicit no interface commands if present.

assert-period

Syntax **assert-period** *assert-period*
no assert-period

Context config>router>pim>if

Description This command configures the period for periodic refreshes of PIM Assert messages on an interface.

The **no** form of the command removes the assert-period from the configuration.

Default no assert-period

Parameters *assert-period* — Specifies the period for periodic refreshes of PIM Assert messages on an interface.

Values 1 — 300 seconds

bfd-enable

Syntax [**no**] **bfd-enable** [**ipv4** | **ipv6**]

Context config>router>pim>interface

Description This command enables the use of IPv4 or IPv6 bi-directional forwarding (BFD) to control the state of the associated protocol interface. By enabling BFD on a given protocol interface, the state of the protocol interface is tied to the state of the BFD session between the local node and the remote node. The parameters used for the BFD are set via the BFD command under the IP interface.

The **no** form of this command removes BFD from the associated IGP protocol adjacency.

Default no bfd-enable

Parameters **ipv4 —** Enables the use of IPv4 bi-directional forwarding (BFD)

ipv6 — Enables the use of IPv6 bi-directional forwarding (BFD)

enable-mdt-spt

Syntax [**no**] **enable-mdt-spt**

Context config>router>pim

Description This command is used to enable SPT switchover for default MDT. On enable, PIM instance resets all MDTs and reinitiate setup.

The **no** form of the command disables SPT switchover for default MDT. On disable, PIM instance resets all MDTs and reinitiate setup.

Default **no enable-mdt-spt**

import

Syntax **import** {**join-policy** | **register-policy**} [*policy-name* [.. *policy-name*]]
no import {**join-policy** | **register-policy**}

Context config>router>pim

Description This command specifies the import route policy to be used. Route policies are configured in the **config>router>policy-options** context.

When an import policy is not specified, BGP routes are accepted by default. Up to five import policy names can be specified.

The **no** form of the command removes the policy association from the instance.

Default **no import join-policy**
no import register-policy

Parameters **join-policy —** Use this command to filter PIM join messages which prevents unwanted multicast streams from traversing the network.

register-policy — This keyword filters register messages. PIM register filters prevent register messages from being processed by the RP. This filter can only be defined on an RP. When a match is found, the RP immediately sends back a register-stop message.

policy-name — The route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Route policies are configured in the **config>router>policy-options** context.

ipv4-multicast-disable

Syntax [**no**] **ipv4-multicast-disable**

Context configure>router>pim
configure>router>pim>interface

Description This command administratively disables/enables PIM operation for IPv4.

Note that IPv4 multicast must be enabled to enable mLDP in-band signaling for IPv4 PIM joins; see p2mp-ldp-tree-join.

Default no ipv4-multicast-disable

lag-usage-optimization

Syntax [**no**] **lag-usage-optimization**

Context configure>router>pim

Description This command specifies whether the router should optimize usage of the LAG such that traffic for a given multicast stream destined to an IP interface using the LAG is sent only to the forwarding complex that owns the LAG link on which it will actually be forwarded.

Changing the value causes the PIM protocol to be restarted.

If this optimization is disabled, the traffic will be sent to all the forwarding complexes that own at least one link in the LAG.

Note that changes made for 9G multicast hashing causes Layer 4 multicast traffic to not hashed. This is independent whether **lag-usage-optimization** is enabled or disabled.

mc-ecmp-balance

Syntax [**no**] **mc-ecmp-balance**

Context configure>router>pim

Description This command enables multicast balancing of traffic over ECMP links. When enabled, each multicast stream that needs to be forwarded over an ECMP link will be re-evaluated for the total multicast bandwidth utilization. Re-evaluation occurs on the ECMP interface in question.

The **no** form of the command disables the multicast balancing.

mc-ecmp-balance-hold

Syntax **mc-ecmp-balance-hold** *minutes*
no mc-ecmp-balance-hold

Context configure>router>pim

Description This command configures the hold time for multicast balancing over ECMP links.

Parameters *minutes* — Specifies the hold time, in minutes, that applies after an interface has been added to the ECMP link.

mc-ecmp-hashing-enabled

Syntax [**no**] **mc-ecmp-hashing-enabled**

Context configure>router>pim

Description This command enables hash-based multicast balancing of traffic over ECMP links and causes PIM joins to be distributed over the multiple ECMP paths based on a hash of S and G (and possibly

next-hop IP). When a link in the ECMP set is removed, the multicast streams that were using that link are re-distributed over the remaining ECMP links using the same hash algorithm. When a link is added to the ECMP set new joins may be allocated to the new link based on the hash algorithm, but existing multicast streams using the other ECMP links stay on those links until they are pruned.

Hash-based multicast balancing is supported for both IPv4 and IPv6.

This command is mutually exclusive with the `mc-ecmp-balance` command in the same context.

The **no** form of the command disables the hash-based multicast balancing of traffic over ECMP links.

Default no mc-ecmp-hashing-enabled

multicast-fast-failover

Syntax **[no] multicast-fast-failover**

Context configure>router>pim

Description This command configures the option to enable multicast only fast failover functionality for IPv4 PIM SSM interfaces in the global routing table instance.

The **no** version of this command disables MoFRR for PIM interfaces.

Default no multicast-fast-failover

ipv6-multicast-disable

Syntax **ipv6-multicast-disable**

Context configure>router>pim
configure>router>pim>interface

Description This command administratively disables/enables PIM operation for IPv6.

Note that IPv6 multicast must be enabled to enable mLDP in-band signaling for IPv6 PIM joins; see p2mp-ldp-tree-join.

Default ipv6-multicast-disable

bsm-check-rtr-alert

Syntax [**no**] **bsm-check-rtr-alert**

Context config>router>pim>interface

Description This command enables the checking of the router alert option in the bootstrap messages received on this interface.

Default no bsm-check-rtr-alert

hello-interval

Syntax **hello-interval** *hello-interval*
no hello-interval

Context config>router>pim>interface

Description This command configures the frequency at which PIM Hello messages are transmitted on this interface.

The **no** form of this command reverts to the default value of the hello-interval.

Default **30**

Parameters *hello-interval* — Specifies the hello interval in seconds. A 0 (zero) value disables the sending of hello messages (the PIM neighbor will never timeout the adjacency).

Values 0 — 255 seconds

hello-multiplier

Syntax **hello-multiplier** *deci-units*
no hello-multiplier

Context config>router>pim>interface

Description This command configures the multiplier to determine the holdtime for a PIM neighbor on this interface.

The **hello-multiplier** in conjunction with the **hello-interval** determines the holdtime for a PIM neighbor.

Parameters *deci-units* — Specify the value, specified in multiples of 0.1, for the formula used to calculate the hello-holdtime based on the hello-multiplier:

(hello-interval * hello-multiplier) / 10

This allows the PIMv2 default timeout of 3.5 seconds to be supported.

Values 20 — 100

Default 35

improved-assert

Syntax [**no**] **improved-assert**

Context config>router>pim>interface

Description The PIM assert process establishes a forwarder for a LAN and requires interaction between the control and forwarding planes. The assert process is started when data is received on an outgoing interface meaning that duplicate traffic is forwarded to the LAN until the forwarder is negotiated among the routers.

When the **improved-assert** command is enabled, the PIM assert process is done entirely in the control plane. The advantages are that it eliminates duplicate traffic forwarding to the LAN. It also improves performance since it removes the required interaction between the control and data planes.

NOTE: improved-assert is still fully interoperable with the draft-ietf-pim-sm-v2-new-xx, *Protocol Independent Multicast - Sparse Mode (PIM-SM): Revised*, and RFC 2362, *Protocol Independent Multicast-Sparse Mode (PIM-SM)*, implementations. However, there may be conformance tests that may fail if the tests expect control-data plane interaction in determining the assert winner. Disabling the **improved-assert** command when performing conformance tests is recommended.

Default enabled

multicast-senders

Syntax **multicast-senders** {**auto** | **always** | **never**}
no multicast-senders

Context config>router>pim>interface

Description This command configures how traffic from directly-attached multicast sources should be treated on broadcast interfaces. It can also be used to treat all traffic received on an interface as traffic coming from a directly-attached multicast source. This is particularly useful if a multicast source is connected to a point-to-point or unnumbered interface.

Default auto

Parameters **auto —** Specifies that, on broadcast interfaces, the forwarding plane performs subnet-match check on multicast packets received on the interface to determine if the packet is from a directly-attached source. On unnumbered/point-to-point interfaces, all traffic is implicitly treated as coming from a remote source.

always — Treats all traffic received on the interface as coming from a directly-attached multicast source.

never — Specifies that, on broadcast interfaces, traffic from directly-attached multicast sources will not be forwarded. Note that traffic from a remote source will still be forwarded if there is a multicast state for it. On unnumbered/point-to-point interfaces, it means that all traffic received on that interface must not be forwarded.

p2mp-ldp-tree-join

Syntax [**no**] **p2mp-ldp-tree-join** [**ipv4**] [**ipv6**]

Context config>router>pim>interface

Description This command configures the option to join the P2MP LDP tree towards the multicast source. If **p2mp-ldp-tree-join** is enabled, a PIM multicast join received on an interface is processed to join the P2MP LDP LSP, using the in-band signaled P2MP tree for the same multicast flow. LDP P2MP tree is set up towards the multicast source. The route to the multicast node source is looked up from the RTM. The next-hop address for the route to source is set as the root of LDP P2MP tree.

The **no** form of the command disables joining the P2MP LDP tree for IPv4 or IPv6 or for both (if both or none is specified).

Parameters **ipv4** — Enables dynamic mLDP in-band signaling for IPv4 PIM joins. IPv4 multicast must be enabled; see ipv4-multicast-disable. For backward compatibility **p2mp-ldp-tree-join** is equivalent to **p2mp-ldp-tree-join ipv4**.

ipv6 — Enables dynamic mLDP in-band signaling for IPv6 PIM joins. IPv6 multicast must be enabled; see ipv6-multicast-disable).

Default no p2mp-ldp-tree-join

priority

Syntax **priority** *dr-priority*
no priority

Context config>router>pim>interface

Description This command sets the priority value to elect the designated router (DR). The DR election priority is a 32-bit unsigned number and the numerically larger priority is always preferred.

The **no** form of the command restores the default values.

Default **1**

Parameters *priority* — Specifies the priority to become the designated router. The higher the value, the higher the priority.

Values 1 — 4294967295

priority

Syntax **priority** *bootstrap-priority*
no priority

Context config>router>pim>rp>bsr-candidate

Description This command configures the bootstrap priority of the router. The RP is sometimes called the bootstrap router. The priority determines if the router is eligible to be a bootstrap router. In the case of a tie, the router with the highest IP address is elected to be the bootstrap router.

Default 0

Parameters *bootstrap-priority* — Specifies the priority to become the bootstrap router. The higher the value, the higher the priority. A 0 value the router is not eligible to be the bootstrap router. A value of 1 means router is the least likely to become the designated router.

Values 0 — 255

priority

Syntax **priority** *priority*
no priority

Context config>router>pim>rp>rp-candidate
config>router>pim>rp>ipv6>rp-candidate

Description This command configures the Candidate-RP priority for becoming a rendezvous point (RP). This value is used to elect RP for a group range.

Default 192

Parameters *priority* — Specifies the priority to become a rendezvous point (RP). A value of 0 is considered as the highest priority.

Values 0 — 255

sticky-dr

Syntax **sticky-dr** [**priority** *dr-priority*]
no sticky-dr

Context config>router>pim>interface

Description This command enables sticky-dr operation on this interface. When enabled, the priority in PIM hellos sent on this interface when elected as the designateed router (DR) will be modified to the value configured in *dr-priority*. This is done to avoid the delays in forwarding caused by DR recovery, when switching back to the old DR on a LAN when it comes back up.

By enabling **sticky-dr** on this interface, it will continue to act as the DR for the LAN even after the old DR comes back up.

The **no** form of the command disables sticky-dr operation on this interface.

Default disabled

Parameters **priority** *dr-priority* — Sets the DR priority to be sent in PIM Hello messages following the election of that interface as the DR, when sticky-dr operation is enabled.

Values 1 — 4294967295

three-way-hello

Syntax **three-way-hello** [**compatibility-mode**]
no three-way-hello

Context config>router>pim>interface

Description This command configures the compatibility mode to enable three-way hello. By default, the value is disabled on all interface which specifies that the standard two-way hello is supported. When enabled, the three way hello is supported.

Default no three-way-hello

tracking-support

Syntax [**no**] **tracking-support**

Context config>router>pim>interface

Description This command sets the the T bit in the LAN Prune Delay option of the Hello Message. This indicates the router's capability to enable join message suppression. This capability allows for upstream routers to explicitly track join membership.

Default no tracking-support

rp

Syntax **rp**

Context config>router>pim

Description This command enables the context to configure rendezvous point (RP) parameters. The address of the root of the group's shared multicast distribution tree is known as its RP. Packets received from a source upstream and join messages from downstream routers rendezvous at this router.

If this command is not enabled, then the router can never become the RP.

ipv6

Syntax **ipv6**

Context config>router>pim>rp

Description This command enables the conftext to configure IPv6 parameters.

anycast

Syntax [**no**] **anycast** *rp-ip-address*

Context config>router>pim>rp
config>router>pim>rp>ipv6

Description This command configures a PIM anycast protocol instance for the RP being configured. Anycast enables fast convergence when a PIM RP router fails by allowing receivers and sources to rendezvous at the closest RP.

The **no** form of the command removes the anycast instance from the configuration.

Default none

Parameters *rp-ip-address* — Configure the loopback IP address shared by all routes that form the RP set for this anycast instance. Only a single address can be configured. If another anycast command is entered with an address then the old address will be replaced with the new address. If no ip-address is entered then the command is simply used to enter the anycast CLI level.

Values Any valid loopback address configured on the node.

auto-rp-discovery

Syntax [**no**] **auto-rp-discovery**

Context config>router>pim>rp

Description This command enables Auto-RP protocol in discovery mode. In discovery mode, RP-mapping and RP-candidate messages are received and forwarded to downstream nodes. RP-mapping messages are received locally to learn about availability of RP nodes present in the network.

The **no** form of the command disables auto RP.

Default no auto-rp-discovery

rp-set-peer

Syntax [**no**] **rp-set-peer** *ip-address*

Context config>router>pim>rp>anycast
config>router>pim>rp>ipv6>anycast

Description This command configures a peer in the anycast rp-set. The address identifies the address used by the other node as the RP candidacy address for the same multicast group address range as configured on this node.

This is a manual procedure. Caution should be taken to produce a consistent configuration of an RP-set for a given multicast group address range. The priority should be identical on each node and be a higher value than any other configured RP candidate that is not a member of this rp-set.

Although there is no set maximum number of addresses that can be configured in an rp-set, up to 15 IP addresses is recommended.

The **no** form of the command removes an entry from the list.

Default None

Parameters *ip-address* — Specifies a peer in the anycast rp-set.

Values Any valid ip-address within the scope outlined above.

bsr-candidate

Syntax **bsr-candidate**

Context config>router>pim>rp
config>router>pim>rp>ipv6

Description This command enables the context to configure Candidate Bootstrap (BSR) parameters.

rp-candidate

Syntax **rp-candidate**

Context config>router>pim>rp
config>router>pim>rp>ipv6

Description This command enables the context to configure the Candidate RP parameters.

Routers use a set of available rendezvous points distributed in Bootstrap messages to get the proper group-to-RP mapping. A set of routers within a domain are also configured as candidate RPs (C-RPs); typically these will be the same routers that are configured as candidate BSRs.

Every multicast group has a shared tree through which receivers learn about new multicast sources and new receivers learn about all multicast sources. The rendezvous point (RP) is the root of this shared tree.

Default shutdown

static

Syntax **static**

Context config>router>pim>rp
config>router>pim>rp>ipv6

Description This command enables the context to configure static Rendezvous Point (RP) addresses for a multicast group range.

Entries can be created or destroyed. If no IP addresses are configured in the **config>router>pim>rp>static>address** context, then the multicast group to RP mapping is derived from the RP-set messages received from the Bootstrap Router.

address

Syntax **address** *ip-address*

Context config>router>pim>rp>bsr-candidate
config>router>pim>rp>ipv6>bsr-cand

Description This command is used to configure the candidate BSR IP address. This address is for Bootstrap router election.

Default none

Parameters *ip-address* — The *ip-address* portion of the **address** command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation.

Values 1.0.0.0 – 223.255.255.255

address

Syntax [**no**] **address** *ip-address*

Context config>router>pim>rp>rp-candidate
config>router>pim>rp>ipv6>bsr-cand

Description This command configures the local RP address. This address is sent in the RP candidate advertisements to the bootstrap router.

Default none

Parameters *ip-address* — The *ip-address.*

Values 1.0.0.0 – 223.255.255.255

address

Syntax **address** *ip-address*
no address

Context config>router>pim>rp>static
config>router>pim>rp>ipv6>static

Description This command indicates the Rendezvous Point (RP) address that should be used by the router for the range of multicast groups configured by the range command.

Default none

Parameters *ip-address* — The static IP address of the RP. The *ip-addr* portion of the **address** command specifies the IP host address that will be used by the IP interface within the subnet. This address must be unique within the subnet and specified in dotted decimal notation.

Values 1.0.0.0 – 223.255.255.255

embedded-rp

Syntax [**no**] **embedded-rp**

Context config>router>pim>rp>ipv6

Description This command enables the context to configure embedded RP parameters.

Embedded RP is required to support IPv6 inter-domain multicast because there is no MSDP equivalent in IPv6.

The detailed protocol specification is defined in RFC 3956, *Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*. This RFC describes a multicast address allocation policy in which the address of the RP is encoded in the IPv6 multicast group address, and specifies a PIM-SM group-to-RP mapping to use the encoding, leveraging, and extending unicast-prefix-based addressing. This mechanism not only provides a simple solution for IPv6 inter-domain ASM but can be used as a simple solution for IPv6 intra-domain ASM with scoped multicast addresses as well. It can also be used as an automatic RP discovery mechanism in those deployment scenarios that would have previously used the Bootstrap Router protocol (BSR).

The **no** form of the command disables embedded RP.

group-range

Syntax [**no**] **group-range** *ipv6-address/prefix-length*

Context config>router>pim>ipv6>rp>embedded-rp

Description This command defines which multicast groups can embed RP address information besides FF70::/12. Embedded RP information is only used when the multicast group is in FF70::/12 or the configured group range.

Parameters *ipv6-address/prefix-length* — Specifies the group range for embedded RP.

Values

ipv6-address:	x:x:x:x:x:x:x:x (eight 16-bit pieces) x:x:x:x:x:x:d.d.d.d x: [0..FFFF]H d: [0..255]D
prefix-length:	16 — 128

group-range

Syntax [**no**] **group-range** {*grp-ip-address/mask* | *grp-ip-address netmask*}

Context config>router>pim>rp>rp-candidate
config>router>pim>rp>static>rp>ipv6>rp-candidate

Description This command configures the address ranges of the multicast groups for which this router can be an RP.

Default none

Parameters *grp-ip-address* — The multicast group IP address expressed in dotted decimal notation.

Values 224.0.0.0 — 239.255.255.255

mask — The mask associated with the IP prefix expressed as a mask length or in dotted decimal notation; for example /16 for a sixteen-bit mask. The mask can also be entered in dotted decmial notation (255.255.0.0).

Values 4 — 32

netmask — The subnet mask in dotted decimal notation.

Values 0.0.0.0 — 255.255.255.255 (network bits all 1 and host bits all 0)

group-range

Syntax [**no**] **group-range** {*ip-prefix/mask* | *ip-prefix netmask*}

Context config>router>pim>ssm-groups

Description This command configures the address ranges of the multicast groups for this router. When there are parameters present, the command configures the SSM group ranges for IPv6 addresses and netmasks.

Default none

Parameters *ip-prefix/mask* — The IP prefix in dotted decimal notation for the range used by the ABR to advertise that summarizes the area into another area.

Values

ipv4-prefix:	a.b.c.d
ipv4-prefix-le:	0 — 32
ipv6-prefix:	x:x:x:x:x:x:x:x (eight 16-bit pieces)
	x:x:x:x:x:x:d.d.d.d
	x: [0..FFFF]H
	d: [0..255]D
ipv6-prefix-le:	0 — 128

Values 0 — 32 (mask length), 0.0.0.0 — 255.255.255.255 (dotted decimal)

netmask — The subnet mask in dotted decimal notation.

Values 0.0.0.0 — 255.255.255.255 (network bits all 1 and host bits all 0)

holdtime

Syntax **holdtime** *holdtime*
no holdtime

Context config>router>pim>rp>rp-candidate
config>router>pim>rp>ipv6>rp-candidate

Description This command configures the length of time, in seconds, that neighbors should consider the sending router to be operationally up. A local RP cannot be configured on a logical router.

Parameters *holdtime* — Specifies the hold time, in seconds.

Values 5 — 255

group-prefix

Syntax [**no**] **group-prefix** {*grp-ip-address*/*mask* | *grp-ip-address netmask*}

Context config>router>pim>rp>static>address
config>router>pim>rp>ipv6>static>address

Description This command specifies the range of multicast group addresses which should be used by the router as the Rendezvous Point (RP). The config>router>pim>rp>static>address a.b.c.d implicitly defaults to deny all for all multicast groups (224.0.0.0/4). A group-prefix must be specified for that static address. This command does not apply to the whole group range.

The **no** form of the command removes the group-prefix from the configuration.

Default none

Parameters *grp-ip-address* — The multicast group IP address expressed in dotted decimal notation.

Values 224.0.0.0 — 239.255.255.255

mask — The mask associated with the IP prefix expressed as a mask length or in dotted decimal notation; for example /16 for a sixteen-bit mask. The mask can also be entered in dotted decmial notation (255.255.0.0).

Values 4 — 32

netmask — The subnet mask in dotted decimal notation.

Values 0.0.0.0 — 255.255.255.255 (network bits all 1 and host bits all 0)

override

Syntax [**no**] **override**

Context config>router>pim>rp>static>address
config>router>pim>rp>ipv6>static>address

Description This command changes the precedence of static RP over dyanamically learned Rendezvous Point (RP).

When enabled, the static group-to-RP mappings take precedence over the dynamically learned mappings.

Default no override

non-dr-attract-traffic

Syntax [**no**] **non-dr-attract-traffic**

Context config>router>pim

Description This command specifies whether the router should ignore the designated router state and attract traffic even when it is not the designater router.

An operator can configure an interface (router or IES or VPRN interfaces) to IGMP and PIM. The interface state will be synchronized to the backup node if it is associated with the redundant peer port. The interface can be configured to use PIM which will cause multicast streams to be sent to the elected DR only. The DR will also be the router sending traffic to the DSLAM. Since it may be required to attract traffic to both routers a flag non-dr-attract-trafffic can be used in the PIM context to have the router ignore the DR state and attract traffic when not DR. Note that while using this flag the router may not send the stream down to the DSLAM while not DR.

When enabled, the designated router state is ignored. When disabled, **no non-dr-attract-traffic**, the designated router value is honored.

Default no non-dr-attract-traffic

rpf-rtm

Syntax **[no] rpf-rtm** *rtm-id* **|** *rtm-name*

Context config>router>pim

Description This command associates the specified RTM instance with the PIM protocol. This RTM will then be used to generate the RPF table for multicast.

The **no** form of this command removes the association with the specified RTM instance and will cause PIM to use the unicast RTM.

Default No default

Parameters *rtm-id* — RTM Instance ID that is to be associated with the new IS-IS topology.

Values integer: 3 — 32

rtm-name — string name given to the RTM instance.

rpf6-table

Syntax **rpf6-table** {**rtable6-m** | **rtable6-u** | **both**}
no rpf6-table

Context config>router>pim
config>router>msdp

Description This command configures the sequence of route tables used to find a Reverse Path Forwarding (RPF) interface for a particular multicast route.

By default, only the unicast route table is looked up to calculate RPF interface towards the source/ rendezvous point. However the operator can specify the following:

a) Use unicast route table only

b) Use multicast route table only or

c) Use both the route tables.

Parameters **rtable6-m —** Specifies that only the multicast route table will be used by the multicast protocol (PIM) for IPv6 RPF checks. This route table will contain routes submitted by static routes, ISIS and OSPF.

rtable6-u — Specifies only that the unicast route table will be used by the multicast protocol (PIM) for IPv6 RPF checks. This route table will contain routes submitted by all the unicast routing protocols.

both — Will always lookup first in the multicast route table and if there is a route, it will use it. If PIM does not find a route in the first lookup, it will try to find it in the unicast route table. Rtable6-m is checked before rtable6-u.

Default rtable-u

rpfv

Syntax **rpfv core**
rpfv mvpn
rpfv core mvpn
no rpfv [core] [mvpn]

Context config>router>pim

Description This command enables RPF Vector processing for Inter-AS Rosen MVPN Option-B and Option-C. The rpfv must be enabled on every node for Inter-AS Option B/C MVPN support.

Parameters **mvpn —** Enables mvpn RPF vector processing for Inter-AS Option B/C MVPN based on RFC 5496 and RFC6513. If a core RPF vector is received, it will be dropped before a message is processed.

core — Enables core RPF vector (no RD) processing for Inter-AS Option B/C MVPN, which allows SROS interoperability as P-router with third-party vendors that do not encode RD in the RPF vector for Inter-AS MVPN.

core mvpn — Enables core RPF vector (no RD) processing for Inter-AS Option B/C MVPN, which allows SROS interoperability as P-router with third-party vendors that do not encode RD in the RPF vector for Inter-AS MVPN.

The **no** version of this command disables RPF Vector processing. If RPF vector is received in a PIM join message, the vector will be removed before local processing of PIM message starts.

Default no rpfv

sa-timeout

Syntax **sa-timeout** *seconds*
no sa-timeout

Context config>router>msdp

Description This command configures the value for the SA entries in the cache. If these entries are not refreshed within the timeout value then they are removed from the cache. Normally the entries are refreshed at least once a minute. But under high load with many of MSDP peers the refresh cycle could be incomplete. A higher timeout value (more then 90) could be useful to prevent unstabilities in the MSDP cache.

Default 90

Parameters *seconds* — Specifies the time, in seconds, to wait for a response from the peer before declaring the peer unavailable.

Values 90 — 600

spt-switchover-threshold

Syntax **spt-switchover-threshold** {*grp-ip-address/mask* | *grp-ip-address netmask*} s*pt-thres*hold
no spt-switchover-threshold {*grp-ip-address/mask* | *grp-ip-address netmask*}

Context config>router>pim

Description This command configures shortest path (SPT) tree switchover thresholds for group prefixes.

PIM-SM routers with directly connected routers receive multicast traffic initially on a shared tree rooted at the Rendezvous Point (RP). Once the traffic arrives on the shared tree and the source of the traffic is known, a switchover to the SPT tree rooted at the source is attempted.

For a group that falls in the range of a prefix configured in the table, the corresponding threshold value determines when the router should switch over from the shared tree to the source specific tree. The switchover is attempted only if the traffic rate on the shared tree for the group exceeds the configured threshold.

In the absence of any matching prefix in the table, the default behavior is to switchover when the first packet is seen. In the presence of multiple prefixes matching a given group, the most specific entry is used.

Parameters *grp-ip-address* — The multicast group IP address expressed in dotted decimal notation.

Values 224.0.0.0 — 239.255.255.255

spt-threshold — Specifies the configured threshold in kilobits per second (kbps) for a group prefix. A switchover is attempted only if the traffic rate on the shared tree for the group exceeds this configured threshold.

Values 1 — 4294967294 | infinity

mask — The mask associated with the IP prefix expressed as a mask length or in dotted decimal notation; for example /16 for a sixteen-bit mask. The mask can also be entered in dotted decmial notation (255.255.0.0).

Values 4 — 32

infinity — When the **infinity** keyword is specified, no switchover will occur at any time, regardless of the traffic level is detected. The threshold, in kilobits per second (KBPS), value is 4294967295.

ssm-groups

Syntax [**no**] **ssm-groups**

Context config>router>pim

Description This command enables the context to enable an ssm-group configuration instance.

bootstrap-export

Syntax **bootstrap-export** *policy-name* [*..policy-name*]

Context config>router>pim>rp

Description Use this command to apply export policies to control the flow of bootstrap messages from the RP, and apply them to the PIM configuration. Up to 5 policy names can be specified.

Default no bootstrap-export

Parameters *policy-name* — Specify the export policy name up to 32 characters in length.

bootstrap-import

Syntax **bootstrap-import** *policy-name* [*..policy-name*]

Context config>router>pim>rp

Description Use this command to apply import policies to control the flow of bootstrap messages to the RP, and apply them to the PIM configuration. Up to 5 policy names can be specified.

Default no bootstrap-import

Parameters *policy-name* — Specify the import policy name up to 32 characters in length.

hash-mask-len

Syntax **hash-mask-len** *hash-mask-length*
no hash-mask-len

Context config>router>pim>rp>bsr-candidate
config>router>pim>rp>ipv6>bsr-candidate

Description This command is used to configure the length of a mask that is to be combined with the group address before the hash function is called. All groups with the same hash map to the same RP. For example, if this value is 24, only the first 24 bits of the group addresses matter. This mechanism is used to map one group or multiple groups to an RP.

Parameters *hash-mask-length* — The hash mask length.

Values 0 — 32

Router Multicast Source Discovery Protocol (MSDP) Commands

msdp

Syntax [**no**] **msdp**

Context config>router

Description This command enables a Multicast Source Discovery Protocol (MSDP) instance. When an MSDP instance is created, the protocol is enabled. To start or suspend execution of the MSDP protocol without affecting the configuration, use the [**no**] **shutdown** command.

The **no** form of the command deletes the MSDP protocol instance removing all associated configuration parameters.

Default no msdp

Interactions: In order for the MSDP protocol to function at least one peer must be configured.

When MSDP is configured and started an appropriate event message should be generated.

When **the** no form of the command is executed all sessions must be terminated and an appropriate event message should be generated.

When all peering sessions are terminated an event message per peer is not required.

active-source-limit

Syntax **active-source-limit** *number*
no active-source-limit

Context config>router>msdp
config>router>msdp>group
config>router>msdp>group>peer

Description This option controls the maximum number of active source messages that will be accepted by Multicast Source Discovery Protocol (MSDP). This effectively controls the number of active sources that can be stored on the system.

The **no** form of this command reverts the number of source message limit to default operation

Default No limit is placed on the number of source active records

Parameters *number* — This parameter defines how many active sources can be maintained by MSDP.

Values 0 — 1000000

receive-msdp-msg-rate

Syntax **receive-msg-rate** *number* **interval** *seconds* [**threshold** *number*]
no receive-msg-rate

Context config>router>msdp
config>router>msdp>peer
config>router>msdp>group
config>router>msdp>source

Description This command limits the number of Multicast Source Discovery Protocol (MSDP) messages that are read from the TCP session. It is possible that an MSDP/ RP router may receive a large number of MSDP protocol message packets in a particular source active message.

The **no** form of this command reverts this active-source limit to default operation

Default No limit is placed on the number of MSDP and source active limit messages will be accepted.

Parameters *number* — Defines the number of MSDP messages (including source active messages) that are read from the TCP session per the number of seconds.

Values 10 — 10000

Default 0

interval *seconds* **—** This defines the time that together with the *number* parameter defines the number of MSDP messages (including source active messages) that are read from the TCP session within the configured number of seconds.

Values 1 — 600

Default 0

threshold *number* — This number reflects the number of MSDP messages can be processed before the MSDP message rate limiting function described above is activated; this is of use in particular during at system startup and initialization.

Values 1 — 1000000

Default 0

Interactions: Once the number of MSDP packets (including source active messages) defined in the threshold have been processed the rate of all other MSDP packets is rate limited by no longer accepting messages from the TCP session until the time (seconds) has elapsed.

authentication-key

Syntax **authentication-key** [*authentication-key*|*hash-key*] [**hash**|**hash2**]
no authentication-key

Context config>router>msdp>peer
config>router>msdp>group>peer

Description This command configures a Message Digest 5 (MD5) authentication key to be used with a specific Multicast Source Discovery Protocol (MSDP) peering session. The authentication key must be configured per peer as such no global or group configuration is possible.

Default Authentication-key. All MSDP messages are accepted and the MD5 signature option authentication key is disabled.

Parameters *authentication-key* — The authentication key. Allowed values are any string up to 16 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

hash-key — The hash key. The key can be any combination of ASCII characters up to 33 characters in length (encrypted). If spaces are used in the string, enclose the entire string in quotation marks (“ ”).

This is useful when a user must configure the parameter, but, for security purposes, the actual unencrypted key value is not provided.

hash — Specifies the key is entered in an encrypted form. If the **hash** parameter is not used, the key is assumed to be in a non-encrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** parameter specified.

hash2 — Specifies the key is entered in a more complex encrypted form. If the **hash2** parameter is not used, the less encrypted **hash** form is assumed.

data-encapsulation

Syntax **[no] data-encapsulation**

Context config>router>msdp

Description This command configures a rendezvous point (RP) using Multicast Source Discovery Protocol (MSDP) to encapsulate multicast data received in MSDP register messages inside forwarded MSDP source-active messages.

Default data-encapsulation

default-peer

Syntax **default-peer**
no default-peer

Context config>router>msdp>peer
config>router>msdp>group>peer

Description Using the default peer mechanism a peer can be selected as the default Multicast Source Discovery Protocol (MSDP) peer, as a result all source-active messages from the peer will be accepted without the usual peer-reverse-path-forwarding (RPF) check.

The MSDP peer-RPF check is different from the normal multicast RPF checks. The peer-RPF check is used to stop source-active messages from looping. A router validates source-active messages originated from other routers in a deterministic fashion.

A set of rules is applied in order to validate received source-active messages, and the first rule that applies determines the peer-RPF neighbor. All source-active messages from other routers are rejected. The rules applied to source-active messages originating at Router S received at Router R from Router N are as follows:

- If Router N and router S are one and the same, then the message is originated by a direct peer-RPF neighbor and will be accepted.
- If Router N is a configured peer, or a member of the Router R mesh group then its source-active messages are accepted.
- If Router N is the Border Gateway Protocol (BGP) next hop of the active multicast RPF route toward Router S then Router N is the peer-RPF neighbor and its source-active messages are accepted.
- If Router N is an external BGP peer of Router R and the last autonomous system (AS) number in the BGP AS-path to Router S is the same as Router N's AS number, then Router N is the peer-RPF neighbor, and its source-active messages are accepted.
- If Router N uses the same next hop as the next hop to Router S, then Router N is the peer-RPF neighbor, and its source-active messages are accepted.
- If Router N fits none of the above rules, then Router N is not a peer-RPF neighbor, and its source-active messages are rejected.

Default No default peer is established and all active source messages must be RPF checked.

export

Syntax **export** *policy-name* [*policy-name*...(up to 5 max)]
no export

Context config>router>msdp
config>router>msdp>peer
config>router>msdp>group
config>router>msdp>group>peer

Description This command specifies the policies to export source active state from the source active list into Multicast Source Discovery Protocol (MSDP).

The **no** form of the command removes all policies from the configuration.

Default No export policies are applied and all SA entries are announced.

Parameters *policy-name* — Specifies the export policy name. Up to five policy-name arguments can be specified.

Interactions: If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple export commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

If you configure an export policy at the global level, each individual peer inherits the global policy. If you configure an export policy at the group level, each individual peer in a group inherits the group's policy. If you configure an export policy at the peer level then policy only applies to the peer where it is configured.

group

Syntax [**no**] **group** *group-name*

Context config>router>msdp

Description This command enables access to the context to create or modify a Multicast Source Discovery Protocol (MSDP) group. To configure multiple MSDP groups, include multiple group statements.

By default, the group's options are inherited from the global MSDP options. To override these global options, group-specific options within the group statement can be configured.

In order for a group to be of use at least one peer must be configured.

Default no group

Parameters *group-name* — Species a unique name for the MSDP group.

Interactions: If the group name provided is already configured then this command only provides the context to configure the options pertaining to this group.

If the group name provided is not already configured, then the group name must be created and the context to configure the parameters pertaining to the group should be provided. In this case the $ prompt to indicate that a new entity (group) is being created should be used.

import

Syntax **import** *policy-name* [*policy-name*...(up to 5 max)]
no import

Context config>router>msdp
config>router>msdp>peer
config>router>msdp>group
config>router>msdp>group>peer

Description This command specifies the policies to import source active state from Multicast Source Discovery Protocol (MSDP) into source active list.

The no form of the command removes all policies from the configuration.

Default No import policies are applied and all source active messages are allowed.

Parameters *policy-name* — Specifies the import policy name. Up to five policy-name arguments can be specified.

Interactions: If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If multiple import commands are issued, the last command entered will override the previous command. A maximum of five policy names can be specified.

If you configure an import policy at the global level, each individual peer inherits the global policy.

If you configure an import policy at the group level, each individual peer in a group inherits the groupís policy.

If you configure an import policy at the peer level then policy only applies to the peer where it is configured.

local-address

Syntax **local-address** *address*
no local-address

Context config>router>msdp
config>router>msdp>peer
config>router>msdp>group
config>router>msdp>group>peer

Description This command configures the local end of a Multicast Source Discovery Protocol (MSDP) session. In order for MSDP to function at least one peer must be configured. When configuring a peer, you must include this local-address command to configure the local end of the MSDP session. This address must be present on the node and is used to validate incoming connections to the peer and to establish connections to the remote peer.

The no local address format of this command removes the local-address from the configuration.

Default No local address is configured.

Parameters ***address*** **—** Specifies an existing address on the node.

Interactions: If the user enters this command then the address provided is validated and will be used as the local address for MSDP peers from that point. If a subsequent local-address command is entered it will replace the existing configuration and existing session(s) will be terminated.

Similarly when the no form of this command is entered the existing local-address will be removed from the configuration and the existing session(s) will be terminated.

Whenever a session is terminated all information pertaining to and learned from that peer and will be removed.

Whenever a new peering session is created or a peering session is lost an event message should be generated.

mode

Syntax **mode** {**mesh-group** | **standard**}

Context config>router>msdp>group

Description This command configures groups of peers in a full mesh topology to limit excessive flooding of source-active messages to neighboring peers.

Multicast Source Discovery Protocol (MSDP) peers can be configured grouped in a full-mesh topology that prevents excessive flooding of source-active messages to neighboring peers.

Default standard (non-meshed)

Parameters **mesh-group —** Specifies that source-active message received from a mesh group member are always accepted but are not flooded to other members of the same mesh group. These source-active messages are only flooded to non-mesh group peers or members of other mesh groups.

standard — Specifies a non-meshed mode.

Interactions: In a meshed configuration all members of the group must have a peer connection with every other mesh group member. If this rule is not adhered to then unpredictable results may occur.

peer

Syntax [**no**] **peer** *peer-address*

Context config>router>msdp
config>router>msdp>group

Description This command configures peer parameters. Multicast Source Discovery Protocol (MSDP) must have at least one peer configured. A peer is defined by configuring a local-address that can be used by this node to set up a peering session and the address of a remote MSDP router, It is the address of this remote peer that is configured in this command and it identifies the remote MSDP router address.

After peer relationships are established, the MSDP peers exchange messages to advertise active multicast sources. It may be required to have multiple peering sessions in which case multiple peer statements should be included in the configurations.

By default the options applied to a peer are inherited from the global or group-level. To override these inherited options, include peer-specific options within the peer statement.

At least one peer must be configured for MSDP to function.

Default none

Parameters *peer-address* — The address configured in this statement must identify the remote MSDP router that the peering session must be established with.

Interactions: If the peer address provided is already a configured peer then this command only provides the context to configure the parameters pertaining to this peer.

If the peer address provided is not already a configured peer, then the peer instance must be created and the context to configure the parameters pertaining to this peer should be provided. In this case the $ prompt to indicate that a new entity (peer) is being created should be used.

The peer address provided will be validated and assuming it is valid it will be used as the remote address for an MSDP peering session.. When the no form of this command is entered the existing peering address will be removed from the configuration and the existing session will be terminated. Whenever a session is terminated all source active information pertaining to and learned from that peer and will be removed. Whenever a new peering session is created or a peering session is lost an event message should be generated.

source

Syntax [**no**] **source** *ip-prefix/mask*

Context config>router>msdp

Description This command limits the number of active source messages the router accepts from sources in the specified address range.

The **no** form of this message removes the source active rate limiter for this source address range.

Default None. The source active **msdp** messages are not rate limited based on the source address range.

Interactions: If the prefix and mask provided is already a configured then this command only provides the context to configure the parameters pertaining to this active source-message filter.

If the prefix and mask provided is not already a configured, then the source node instance must be created and the context to configure the parameters pertaining to this node should be provided. In this case the $ prompt to indicate that a new entity (source) is being created should be used.

Parameters *ip-prefix* — The IP prefix in dotted decimal notation for the range used by the ABR to advertise that summarizes the area into another area.

Values ip-prefix/mask: ip-prefix a.b.c.d (host bits must be 0)

mask — The subnet mask for the range expressed as a decimal integer mask length or in dotted decimal notation.

Values 0 — 32 (mask length), 0.0.0.0 — 255.255.255.255 (dotted decimal)

Multicast CAC Policy Configuration Commands

mcac

Parameters **mcac**

Context config>router
config>router>pim>if
config>router>mld>group-interface

Description This command enables the context to configure multicast CAC parameters.

Default none

policy

Syntax **policy** *mcac-policy-name*
no policy *mcac-policy-name*

Context configure>router>igmp>interface>mcac
configure>service>vprn>igmp>interface >mcac

Description This command references the global channel bandwidth definition policy that is used for (H)mcac and HQoS Adjust.

HQoS Adjustment is supported only with redirection enabled. In other words, the policy from the redirected interface is used for HQoS Adjustment.

Hierarchical mcac (Hmcac) is supported only with redirection enabled. In Hmcac, the subscriber is checked first against its bandwidth limits followed by the check on the redirected interface against the bandwidth limits defined under the redirected interface. In the Hmcac case the channel definition policy must be referenced under the redirected interface level.

Parameters *mcac-policy-name* — Specifies the name of the global mcac channel definition policy defined under the hierarchy configure>router>mcac>policy.

Default No policy is referenced.

bundle

Parameters [**no**] **bundle** *bundle-name*

Context config>router>mcac>policy

Description This command creates the context that enables the grouping of MCAC group addresses into bundles.

When a number of multicast groups or BTV channels are grouped into a single bundle, then policing, if a join for a particular MC-group (BTV channel), can depend on whether:

1. There is enough physical bandwidth on the egress interface.
2. The given channel is a mandatory or optional channel.

– If optional, is there sufficient bandwidth according to the policy settings for the relevant interface.

– If optional, is there sufficient bandwidth within the bundle.

The **no** form of the command removes the named bundle from the configuration.

Default none

Parameters *bundle-name* — Specifies the multicast bundle name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

bandwidth

Syntax **bandwidth** *bandwidth*
no bandwidth

Context config>router>mcac>policy>bundle

Description This command configures the MCAC policy bundle maximum bandwidth.

Parameters *bandwidth* — Specifies the MCAC policy bandwidth.

channel

Syntax **channel** *start-address end-address* **bw** *bandwidth* [**class** {**high** | **low**}] [**type** {**mandatory** | **optional**}] [**source** *source-prefix*]
no channel *start-address end-address* [**source** *source-prefix*]

Context config>router>mcac>policy>bundle

Description This command creates a multicast channel within the bundle where it is configured. A join for a particular multicast channel can be accepted if:

1) Mandatory channels:

A sufficient bandwidth exists on the interface according to the policy settings for the interface. Note, there is always sufficient BW available on the bundle level, as mandatory channels get BW pre-reserved.

2) Optional channels:

A sufficient BW exists on both interface and bundle level.

A channel definition can be either IPv4 (*start-address, end-address, source-address* are IPv4 addresses) or IPv6. A single bundle can have either IPv4 or IPv6 or IPv6 and IPv4 channel definitions. A single policy can mix any of those bundles.

Overlapping channels are not allowed. Two channels overlap if they contain same groups and the same source address prefix (or both do not specify source address prefix). Two channels with same groups and different source prefixes (including one of the channels having no source configured or one of the channels having more specific prefix than the other) do not overlap and are treated as separate channels.

When joining a group from multiple sources, MCAC accounts for that only once when no source address is specified or a prefix for channel covers both sources. Channel BW should be adjusted accordingly or source-aware channel definition should be used if that is not desired.

If a bundle is removed, the channels associated are also removed and every multicast group that was previously policed (because it was in the bundle that contained the policy) becomes free of constraints.

When a new bundle is added to a MCAC policy, the bundle's established groups on a given interfaces are accounted by the policy. Even if this action results in exceeding the bundle's constrain, no active multicast groups are removed. When a leave message is received for an existing optional channel, then the multicast stream is pruned and subsequent new joins may be denied in accordance with the policy. It is possible that momentarily there may be insufficient bandwidth, even for mandatory channels, in this bundle.

Default No channels are specified as part of a bundle on default.

Parameters *start-address end-address* — Specifies the beginning and ending multicast IP addresses that identifies a multicast stream (BTV channel). Both addresses have to be either IPv4 or IPv6.

Values This must be a valid IPv4 or IPv6 multicast group address

source *source-prefix* — Specifies the source of the multicast IP stream. This must be a valid IPv4 or IPv6 multicast source address prefix.

Values address-prefix/prefix-length

address-prefix is valid IPv4/IPv6 multicast source IP address prefix (local scope excluded)

prefix-length [0..32] for IPv4 [0..128] for IPv6

bw *bandwidth* — Specifies the bandwidth required by this channel in kbps. If this bandwidth is configured for a mandatory channel then this bandwidth is reserved by subtracting the amount from the total available bandwidth for all potential egress interfaces and the bundle.

If this bandwidth is configured as an optional channel then this bandwidth must be available for both the bundle and the egress interface requesting the channel to be added. Once the channel has been added the available bandwidth for the bundle and the interface must be reduced by the configured bandwidth of channel.

Values 10 — 10000 kbps

class {high | low} — Provides deeper classification of channels used in the algorithm when LAG ports change state.

Default low

type {mandatory | optional} — Specifies the channel to be either mandatory or optional.

mandatory — When the **mandatory** keyword is specified, then the bandwidth is reserved by subtracting it from the total available for all the potential egress interfaces and the bundle.

optional — When the **optional** keyword is specified then the bandwidth must be available on both the bundle and the egress interface that requests the channel to be added. Once the channel has been added the available bandwidth for the bundle and the interface must be reduced by the configured bandwidth of channel.

Default optional

mc-constraints

Syntax **mc-constraints**

Context config>router>mcac>policy>bundle
config>router>igmp>group-interface>mcac
config>router>mld>group-interface

Description This command enables the context to configure the level and its associated bandwidth for a bundle or a logical interface.

Default none

policy

Syntax **policy** *policy-name*
no policy

Context configure>router>igmp>interface>mcac
configure>router>igmp>group-interface>mcac
configure>service>vprn>igmp>interface>mcac
config>router>mld>group-interface
configure>service>vprn>igmp>group-interface>mcac

Description This command references the global channel bandwidth definition policy that is used for (H)mcac and HQoS Adjust.

Within the scope of HQoS Adjustment, the channel definition policy under the group-interface is used if redirection is disabled. In such case HQoS Adjustment can be applied to IPoE subscribers in per-sap replication mode.

In case that redirection is enabled, the channel bandwidth definition policy applied under the Layer 3 redirected interface is in effect.

Hierarchical mcac (Hmcac) is supported on two levels simultaneously:

subscriber level and redirected interface in case that redirection is enabled

subscriber level and group-interface level in case that redirection is disabled.

In Hmcac, the subscriber is first checked against its bandwidth limits followed by the check on the redirected interface (or group-interface) against the bandwidth limits there.

In the case that the redirection is enabled but the policy is referenced ONLY under the group-interface, no admission control will be executed (Hmcac or Mcac).

Default No policy is referenced.

Parameters *policy-name* — Specifies the name of the global mcac channel definition policy defined under the hierarchy **configure>router>mcac>policy.**

lag-port-down

Syntax **lag-port-down** *lag-id* **number-down** *number-lag-port-down* **level** *level-id*
no lag-port-down *lag-id* **number-down** *number-lag-port-down*

Context config>router>mcac>policy>bundle>mc-constraints

Description This command configures the bandwidth available both at the interface and bundle level when a specific number of ports in a LAG group fail.

Default none

Parameters *lag-id* — When the number of ports available in the LAG link is reduced by the number of ports configured in this context then the *level-id* specified here must be applied.

number-down *number-lag-port-down* — If the number of ports available in the LAG is reduced by the number of ports configured in this command here then bandwidth allowed for bundle and/or interface will be as per the levels configured in this context.

Values 1 — 64 (for 64-link LAG)
1 — 32 (for other LAGs)

level *level-id* — Specifies the amount of bandwidth available within a given bundle for MC traffic for a specified level.

number-down

Syntax **number-down** *number-lag-port-down* **level** *level-id*
no number-down *number-lag-port-down*

Context config>router>pim>if>mcac>mc-constraints

Description This command configures the number of ports down along with level for multicast cac policy on this interface.

Default none

Parameters **number-down** *number-lag-port-down* — If the number of ports available in the LAG is reduced by the number of ports configured in this command here then bandwidth allowed for bundle and/or interface will be as per the levels configured in this context.

Values 1 — 64 (for 64-link LAG)
1 — 32 (for other LAGs)

level *level-id* **—** Specifies the amount of bandwidth available within a given bundle for MC traffic for a specified level.

level

Syntax **level** *level* **bw** *bandwidth*
no level *level*

Context config>router>mcac>policy>bundle>mc-constraints

Description This command configures the amount of bandwidth available within a given bundle for MC traffic for a specified level. The amount of allowable BW for the specified level is expressed in kbps and this can be defined for up to eight different levels.

The **no** form of the command removes the level from the configuration.

Default none (If no bandwidth is defined for a given level then no limit is applied.)

Parameters *level* — Specifies the bandwidth for a given level. Level 1 has the highest priority. Level 8 has the lowest priority.

Values 1 — 8

bw *bandwidth* **—** Specifies the bandwidth, in kbps, for the level.

Values 1 — 2147483647 kbps

Default 1

number-down

Syntax **number-down** *number-lag-port-down* **level** *level-id*
no number-down *number-lag-port-down*

Context config>router>igmp>mcac>mc-constraints

Description This command configures the number of ports down along with level for the MCAC policy.

Parameters *number-lag-port-down* — Specifies the number of ports down along with level for the MCAC policy.

Values 1 — 64

level *level-id* **—** Specifies the bandwidth for a given level. Level 1 has the highest priority. Level 8 has the lowest priority.

Values 1 — 8

unconstrained-bw

Syntax **unconstrained-bw** *bandwidth* **mandatory-bw** *mandatory-bw*
no unconstrained-bw

Context configure>router>igmp>interface>mcac
configure>router>igmp>group-interface>mcac
configure>service>vprn>igmp>interface >mcac
config>router>mld>group-interace>mcac
configure>service>vprn>igmp>group-interface >mcac
configure>subscr-mgmt>sub-mcac-policy

Description This command enables Mcac (or Hmcac) function on the corresponding level (subscriber, group-interface or redirected interface). When Mcac (or Hmcac) is enabled and a channel definition policy is referenced, admission control is performed. The allocated bandwidth for optional channels should not exceed the unconstrained-bw minus the mandatory-bw. The mandatory channels have to stay below the specified value for the mandatory-bw.

In Hmcac, the subscriber is checked first against its bandwidth limits followed by the check on the redirected interface or the group-interface against the bandwidth limits defined there.

In case that redirection is enabled and Hmcac enabled, the channel definition policy must be referenced under the redirected interface level. If it is referenced under the group-interface level, it will be ignored.

Subscriber Mcac (only subscriber is checked for available resources) is supported only with direct subscriber replication (no redirection). In this case the channel definition policy must be referenced under the group-interface.

In the case that the redirection is enabled but the policy is referenced ONLY under the group-interface, no admission control will be executed (Hmcac or Mcac).

Default none

Parameters *bandwidth* — Specifies the unconstrained bandwidth in kbps for the MCAC policy.

Values 0 — 2147483647

mandatory-bw *mandatory-bw* — Specifies the mandatory bandwidth in kbps for the MCAC policy.

Values 0 — 2147483647

use-lag-port-weight

Syntax **use-lag-port-weight**
no use-lag-port-weight

Context config>router>igmp>interface>mcac>mc-constraints
config>router>mld>interface>mcac>mc-constraints
config>router>pim>interface>mcac>mc-constraints
config>router>mcac>policy>bundle>mc-constraints

Description This command enables port weight to be used when determining available bandwidth per level when LAG ports go down/come up. The command is required for proper operation on mixed port-speed LAGs and can be used for non-mixed port-speed LAGs as well.

Default **no use-lag-port-weight —** port number is used when determining available BW per level when LAG ports go down/come up

default-action

Syntax **default-action** {**accept** | **discard**}

Context config>router>mcac>policy

Description This command specifies the action to be applied to multicast streams (channels) when the streams do not match any of the multicast addresses defined in the MCAC policy.

When multiple default-action commands are entered, the last command will overwrite the previous command.

Default discard (all multicast stream not defined in a MCAC policy will be discarded)

Parameters **accept —** Specifies multicast streams (channels) not defined in the MCAC policy will be accepted.

discard — Specifies multicast streams (channels) not defined in the MCAC policy will be dropped.

shutdown

Syntax [**no**] **shutdown**

Context config>router>mcac>policy>bundle

Description This command administratively disables the entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics. Many entities must be explicitly enabled using the **no shutdown** command.

When an entity is shutdown, the operational state of the entity is disabled as well as the operational state of any entities contained within. Many objects must be shutdown before they may be deleted.

Unlike other commands and parameters where the default state is not indicated in the configuration file, shutdown and no shutdown are always indicated in system generated configuration files.

The **no** form of the command puts an entity into the administratively enabled state.

When a shutdown is performed then all constraints placed on either a bundle or an interface are removed and multicast can potentially take up the full bandwidth of the interface. Furthermore, when a **no shutdown** command is executed then policing of the policy must be in a gradual fashion. No active multicast groups may be removed. When a leave message is received for an optional channel then the multicast stream should be pruned and subsequent new joins can be denied in accordance with the policy. This may mean that for a period of time insufficient bandwidth is available even for mandatory channels.

MLD Commands

mld

Syntax [**no**] **mld**

Context config>router

Description This command enables the context to configure Multicast Listener Discovery (MLD) parameters.

The **no** form of the command disables MLD.

Default no mld

group-interface

Syntax [**no**] **group-interface** *ip-int-name*

Context config>router>mld

Description This command creates and enables the context to configure MLD group interface parameters.

Parameters *ip-int-name* — The IP interface name. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service ies interface** commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

grp-if-query-src-ip

Syntax **grp-if-query-src-ip** *ipv6-address*
no grp-if-query-src-ip

Context config>router>mld>group-interface

Description This command configures the query source IPv6 address for all group interfaces.

The **no** form of the command removes the IP address.

Default none

Parameters *ipv6-address* — Sets the source IPv6 address for all group interfaces. The address can be up to 64 characters.

query-src-ip

Syntax **query-src-ip** *ipv6-address*

no query-src-ip

Context config>router>mld>group-interface

Description This command configures the query source IPv6 address for the group interface. This IP address overrides the source IP address configured at the router level.

The **no** form of the command removes the IPv6 address.

Default none

Parameters *ipv6-address* — Sets the source IPv6 address for all subscriber's IGMP queries.

interface

Syntax [**no**] **interface** *ip-int-name*

Context config>router>mld

Description This command enables the context to configure an Multicast Listener Discovery (MLD) interface. The interface is a local identifier of the network interface on which reception of the specified multicast address is to be enabled or disabled.

The **no** form of the command deletes the MLD interface. The **shutdown** command in the **config>router>mld>interface** context can be used to disable an interface without removing the configuration for the interface.

Default **no interface** — No interfaces are defined.

Parameters *ip-int-name* — The IP interface name. Interface names must be unique within the group of defined IP interfaces for **config router interface** and **config service ies interface** commands. An interface name cannot be in the form of an IP address. Interface names can be any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes.

If the IP interface name does not exist or does not have an IP address configured an error message will be returned.

If the IP interface exists in a different area it will be moved to this area.

disable-router-alert-check

Syntax [**no**] **disable-router-alert-check**

Context config>router>mld>if

Description This command enables router alert checking for MLD messages received on this interface.

The no form of the command disables the router alert checking.

Default none

import

Syntax **import** *policy-name*
no import

Context config>router>mld>if

Description This command specifies the import route policy to be used for determining which membership reports are accepted by the router. Route policies are configured in the **config>router>policy-options** context.

When an import policy is not specified, all the MLD reports are accepted.

The **no** form of the command removes the policy association from the MLD instance.

Default **no import** — No import policy specified.

Parameters *policy-name* — The route policy name. Allowed values are any string up to 32 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, etc.), the entire string must be enclosed within double quotes. Route policies are configured in the **config>router>policy-options** context.

max-groups

Syntax **max-groups** *value*
no max-groups

Context config>router>mld>if

Description This command specifies the maximum number of groups for which MLD can have local receiver information based on received MLD reports on this interface. When this configuration is changed dynamically to a value lower than the currently accepted number of groups, the groups that are already accepted are not deleted. Only new groups will not be allowed.

Default 0, no limit to the number of groups.

Parameters *value* — Specifies the maximum number of groups for this interface.

Values 1 — 16000

query-interval

Syntax **query-interval** *seconds*
no query-interval

Context config>router>mld
config>router>mld>if

Description This command specifies the frequency that the querier router transmits general host-query messages. The host-query messages solicit group membership information and are sent to the all-systems multicast group address, 224.0.0.1.

Default 125

Parameters *seconds* — The time frequency, in seconds, that the router transmits general host-query messages.

Values 2 — 1024

query-last-member-interval

Syntax **query-last-member-interval** *seconds*

Context config>router>mld
config>router>mld>if

Description This command configures the frequency at which the querier sends group-specific query messages including messages sent in response to leave-group messages. The lower the interval, the faster the detection of the loss of the last member of a group.

Default 1

Parameters *seconds* — Specifies the frequency, in seconds, at which query messages are sent.

Values 1 — 1024

query-response-interval

Syntax **query-response-interval** *seconds*

Context config>router>mld
config>router>mld>if

Description This command specifies how long the querier router waits to receive a response to a host-query message from a host.

Default 10

Parameters *seconds* — Specifies the the length of time to wait to receive a response to the host-query message from the host.

Values 1 — 1023

static

Syntax **static**

Context config>router>mld>if

Description This command tests multicast forwarding on an interface without a receiver host. When enabled, data is forwarded to an interface without receiving membership reports from host members.

Default none

group

Syntax [**no**] **group** *ipv6-address*

Context config>router>mld>if>static

Description This command enables the context to add a static multicast group either as a (*,G) or one or more (S,G) records. Use MLD static group memberships to test multicast forwarding without a receiver host. When MLD static groups are enabled, data is forwarded to an interface without receiving membership reports from host members.

When static MLD group entries on point-to-point links that connect routers to a rendezvous point (RP) are configured, the static MLD group entries do not generate join messages toward the RP.

The **no** form of the command removes the IPv6 address from the configuration.

Default none

Parameters *ipv6-address* — Specifies an MLD multicast group address that receives data on an interface. The IP address must be unique for each static group.

source

Syntax [**no**] **source** *ipv6-address*

Context config>router>mld>if>static>group
config>router>mld>ssm-translate>grp-range

Description This command specifies an IPv6 unicast address that sends data on an interface. This enables a multicast receiver host to signal a router the group to receive multicast traffic from, and from the source(s) that the traffic is expected.

The **source** command is mutually exclusive with the specification of individual sources for the same group.

The source command, in combination with the group, is used to create a specific (S,G) static group entry.

The **no** form of the command removes the source from the configuration.

Default none

Parameters *ip-address* — Specifies the IPv6 unicast address.

starg

Syntax [**no**] **starg**

Context config>router>mld>if>static>group

Description This command adds a static (*,G) entry. This command can only be enabled if no existing source addresses for this group are specified.

Use the **no** form of the command to remove the starg entry from the configuration.

Default none

subnet-check

Syntax [**no**] **subnet-check**

Context config>router>mld>interface

Description This command enables subnet checking for MLD messages received on this interface. All MLD packets with a source address that is not in the local subnet are dropped.

Default enabled

version

Syntax **version** *version*
no version

Context config>router>mld>if

Description This command specifies the MLD version. If routers run different versions, they will negotiate the lowest common version of MLD that is supported by hosts on their subnet and operate in that version. For MLD to function correctly, all routers on a LAN should be configured to run the same version of MLD on that LAN.

Default 1

Parameters *version* — Specifies the MLD version number.

Values 1, 2

robust-count

Syntax **robust-count** *robust-count*
no robust-count

Context config>router>mld

Description This command configures the robust count. The robust-count variable allows tuning for the expected packet loss on a subnet. If a subnet anticipates losses, the robust-count variable can be increased.

Default 2

Parameters *robust-count* — Specify the robust count value.

Values 2 — 10

ssm-translate

Syntax **ssm-translate**

Context config>router>mld

Description This command enables the context to configure group ranges which are translated to SSM (S,G) entries. If the static entry needs to be created, it has to be translated from a IGMPv1 IGMPv2 request to a Source Specific Multicast (SSM) join. An SSM translate source can only be added if the starg command is not enabled. An error message is generated if you try to configure the **source** command with **starg** command enabled.

grp-range

Syntax [**no**] **grp-range** *start end*

Context config>router>mld>ssm-translate

Description This command is used to configure group ranges which are translated to SSM (S,G) entries.

Parameters *start* — An IP address that specifies the start of the group range.

end — An IP address that specifies the end of the group range. This value should always be greater than or equal to the value of the *start* value.

source

Syntax [**no**] **source** *ip-address*

Context config>router>mld>ssm-translate>grp-range

Description This command specifies the source IP address for the group range. Whenever a (*,G) report is received in the range specified by **grp-range** *start* and *end* parameters, it is translated to an (S,G) report with the value of this object as the source address.

Parameters *ip-address* — Specifies the IP address that will be sending data.

Operational Commands

mrinfo

Syntax **mrinfo** *ip-address* [**router** *router-name*|*service*]

Context <GLOBAL>

Description This command is used to display relevant multicast information from the target multicast router. Information displayed includes adjacency information, protocol, metrics, thresholds, and flags from the target multicast router. This information can be used by network operators to determine whether bi-directional adjacencies exist.

Parameters *ip-address* — Specify the IP address of the multicast capable target router should be entered.

router *router-name* — Specify the router instance that this command applies to.

Default management Base

service — Specify the service instance that this command applies to.

Values 1 — 2147483647

Mrinfo Output Fields — The following table describes the output fields:

Label	Description
General flags	
version	Indicates software version on queried router.
prune	Indicates that router understands pruning.
genid	Indicates that router sends generation IDs.
mtrace	Indicates that the router handles mtrace requests.
Neighbors flags	
1	Metric
0	Threshold (multicast time-to-live)
pim	PIM enabled on interface.
down	Operational status of interface.
disabled	Administrative status of interface.
leaf	No downstream neighbors on interface.
querier	Interface is IGMP querier.
tunnel	Neighbor reached via tunnel.

```
A:dut-f# mrinfo 10.1.1.2

10.1.1.2  [version 3.0,prune,genid,mtrace]:
  10.1.1.2 -> 10.1.1.1 [1/0/pim]
  16.1.1.1 -> 0.0.0.0 [1/0/pim/down/disabled]
  17.1.1.1 -> 0.0.0.0 [1/0/pim/querier/leaf]
  200.200.200.3 -> 200.200.200.5 [1/0/tunnel/pim]...
```

mstat

Syntax **mstat source** *ip-address* **group** *grp-ip-address* [**destination** *dst-ip-address*] [**hop** *hop*] [**router** *router-name*|*service*] [**wait-time** *wait-time*]

Context <GLOBAL>

Description This command traces a multicast path from a source to a receiver and displays multicast packet rate and loss information. The **mstat** command adds the capability to show the multicast path in a limited graphic display and provide drops, duplicates, TTLs, and delays at each node. This information is useful to network operators because it identifies nodes with high drop and duplicate counts. Duplicate counts are shown as negative drops.

Parameters **source** *ip-address* **—** Specify the IP address of the multicast-capable source. This is a unicast address of the beginning of the path to be traced.

group *group-ip-address* **—** Specify the multicast address that will be used.

destination *dst-ip-address* **—** Specify the IP address of the unicast destination. If this parameter is omitted, the IP address of the system where the command is entered is used. The destination parameter can also be used to specify a local interface address as the destination address to send the trace query.

Default The default address for the destination address is the incoming IETF format for that (S,G)

hop *hop* **—** Specify the maximum number of hops that will be traced from the receiver back toward the source.

Values 1 — 255

Default 32 (infinity for the DVMRP routing protocol).

router *router-name* **—** Specify the router instance that this command applies to.

service — Specify the service instance that this command applies to.

Values 1 — 2147483647

wait-time *wait-time* **—** Specify the number of seconds to wait for the response.

Values 1 — 60

Default 10

Mstat Output Fields — The following table describes the output fields:

Label	Description
hop	Number of hops from the source to the listed router.
router name	Name of the router for this hop or "?" when not reverse DNS translated.
address	Address of the router for this hop.
protocol	Protocol used.
ttl	Forward TTL threshold. TTL that a packet is required to have before it will be forwarded over the outgoing interface.
forwarding code	Forwarding information/error code for this hop.

For each interface between 2 nodes a line is printed, following the same layout as other routers with an implementation derived from mrouted. Note the following:

- The forwarding information/error code is only displayed when different from "No Error".
- "?" means the there is no reverse DNS translation.
- There is no "Overall Mcast Pkt Rate" available in the PE for the VPRN case.

```
  Source         Response Dest    Overall     Packet Statistics For Traffic From
10.10.16.9       10.20.1.6       Mcast Pkt    10.10.16.9 To 224.5.6.7
     |        __/  rtt   29 ms     Rate       Lost/Sent = Pct  Rate
     v      /                     -------     --------------------
10.10.16.3
10.10.2.3        ?
     |     ^      ttl    2          1 pps        0/0    = --     0 pps
     v     |
10.10.2.1
10.10.1.1        ?
     |     ^      ttl    3          0 pps        0/0    = --     0 pps
     v     |
10.10.1.2
10.10.4.2        ?              Reached RP/Core
     |     ^      ttl    4          0 pps        0/0    = --     0 pps
     v     |
10.10.4.4
10.10.6.4        ?
     |     ^      ttl    5          0 pps        0/0    = --     0 pps
     v     |
10.10.6.5
10.10.10.5       ?
     |      \__   ttl    6          0 pps        0/0    = --     0 pps
     v         \
10.10.10.6       10.20.1.6
  Receiver       Query Source
```

mtrace

Syntax **mtrace source** *ip-address* **group** *grp-ip-address* [**destination** *dst-ip-address*] [**hop** *hop*] [**router** *router-name*|*service*] [**wait-time** *wait-time*]

Context <GLOBAL>

Description This command traces the multicast path from a source to a receiver by passing a trace query hop-by-hop along the reverse path from the receiver to the source. At each hop, information such as the hop address, routing error conditions, and packet statistics are gathered and returned to the requestor. A network administrator can determine where multicast flows stop and verify the flow of the multicast stream.

Parameters **source** *ip-address* — Specify the IP address of the multicast-capable source. This is a unicast address of the beginning of the path to be traced.

group *group-ip-address* — Specify the multicast address that will be used.

destination *dst-ip-address* — Specify the IP address of the unicast destination. If this parameter is omitted, the IP address of the system where the command is entered is used. The destination parameter can also be used to specify a local interface address as the destination address to send the trace query.

Default The default address for the desination address is the incoming IETF format for that (S,G)

hop *hop* — Specify the maximum number of hops that will be traced from the receiver back toward the source.

Values 1 — 255

Default **32 hops** (infinity for the DVMRP routing protocol).

router *router-name* — Specify the router instance that this command applies to.

service — Specify the service instance that this command applies to.

Values 1 — 2147483647

wait-time *wait-time* — Specify the number of seconds to wait for the response.

Values 1 — 60

Default 10

Mtrace Output Fields — The following table describes the output fields:

Label	Description
hop	Number of hops from the source to the listed router.
router name	Name of the router for this hop. If a DNS name query is not successful a "?" displays.
address	Address of the router for this hop.
protocol	Protocol used.
ttl	Forward TTL threshold. TTL that a packet is required to have before it will be forwarded over the outgoing interface.
forwarding code	Forwarding information/error code for this hop.

```
A:Dut-F# mtrace source 10.10.16.9 group 224.5.6.7

Mtrace from 10.10.16.9 via group 224.5.6.7
Querying full reverse path...

  0  ? (10.10.10.6)
 -1  ? (10.10.10.5)  PIM  thresh^ 1  No Error
 -2  ? (10.10.6.4)  PIM  thresh^ 1  No Error
 -3  ? (10.10.4.2)  PIM  thresh^ 1  Reached RP/Core
 -4  ? (10.10.1.1)  PIM  thresh^ 1  No Error
 -5  ? (10.10.2.3)  PIM  thresh^ 1  No Error
 -6  ? (10.10.16.9)
Round trip time 29 ms; total ttl of 5 required.
```