7450 ETHERNET SERVICE SWITCH
7750 SERVICE ROUTER
7950 EXTENSIBLE ROUTING SYSTEM
VIRTUALIZED SERVICE ROUTER

MULTICAST ROUTING PROTOCOLS GUIDE
RELEASE 16.0.R4

3HE 14137 AAAB TQZZA 01

Issue: 01

November 2018

Table of Contents

1 Getting Started

1.1 About This Guide

This guide describes multicast routing protocols, troubleshooting, and proprietary entities and presents configuration and implementation examples.

This document is organized into functional chapters and provides concepts and descriptions of the implementation flow, as well as Command Line Interface (CLI) syntax and command usage.

The topics and commands described in this document apply to the:

- 7450 ESS
- 7750 SR
- 7950 XRS
- VSR

Table 1 lists the available chassis types for each SR OS router.

Table 1 **Supported SR OS Router Chassis Types**

7450 ESS	7750 SR	7950 XRS
• 7450 ESS-7/12 running in standard mode (not mixed-mode)	• 7450 ESS-7/12 running in mixed-mode (not standard mode) • 7750 SR-a4/a8 • 7750 SR-c4/c12 • 7750 SR-1e/2e/3e • 7750 SR-7/12 • 7750 SR-12e	• 7950 XRS-16c • 7950 XRS-20/40

For a list of unsupported features by platform and chassis, refer to the *SR OS 16.0.Rx* Software Release Notes, part number 3HE 14220 000*x* TQZZA or the *VSR Release Notes*, part number 3HE 14204 000*x* TQZZA.

Command outputs shown in this guide are examples only; actual displays may differ depending on supported functionality and user configuration.

Note: This guide generically covers Release 16.0.R*x* content and may contain some content that will be released in later maintenance loads. Please refer to the *SR OS 16.0.Rx* Software Release Notes, part number 3HE 14220 000*x* TQZZA or the *VSR Release Notes*, part number 3HE 14204 000*x* TQZZA, for information about features supported in each load of the Release 16.0.R*x* software.

1.2 Multicast Configuration Process

Table 2 lists the tasks necessary to configure multicast protocols. This guide is presented in an overall logical configuration flow. Each section describes a software area and provides CLI syntax and command usage to configure parameters for a functional area.

Table 2 **Configuration Process**

Area	Task	Section
Multicast protocol configuration	Configure Internet Group Management Protocol.	Configuring IGMP with CLI
	Configure Multicast Listener Discovery.	Configuring MLD with CLI
	Configure Protocol Independent Multicast.	Configuring PIM with CLI
	Configure Multicast Source Discovery Protocol.	Configuring MSDP with CLI
	Configure Multicast Label Distribution Protocol.	MLDP
	Configure Multicast Extensions to BGP.	Multicast Extensions to BGP
	Configure Multicast Connection Admission Control.	Configuring MCAC with CLI
Troubleshooting	Use Mtrace, Mstat, and Mrinfo, and show commands for troubleshooting.	Troubleshooting Tools

2 Introduction to Multicast

2.1 Multicast Overview

IP multicast provides an effective method of many-to-many communication. Delivering unicast datagrams is fairly simple. Normally, IP packets are sent from a single source to a single recipient. The source inserts the address of the target host in the IP header destination field of an IP datagram; intermediate routers (if present) simply forward the datagram towards the target in accordance with their respective routing tables.

Sometimes, distribution needs individual IP packets be delivered to multiple destinations (like audio or video streaming broadcasts). Multicast is a method of distributing datagrams sourced from one or more hosts to a set of receivers that may be distributed over different (sub) networks. This makes delivery of multicast datagrams significantly more complex.

Multicast sources can send a single copy of data using a single address for the entire group of recipients. The routers between the source and recipients route the data using the group address route. Multicast packets are delivered to a multicast group. A multicast group specifies a set of recipients who are interested in a particular data stream and is represented by an IP address from a specified range. Data addressed to the IP address is forwarded to the members of the group. A source host sends data to a multicast group by specifying the multicast group address in the datagram's destination IP address. A source does not have to register in order to send data to a group nor do they need to be a member of the group.

Routers and Layer 3 switches use the Internet Group Management Protocol (IGMP) to manage membership for a multicast session. When a host wants to receive one or more multicast sessions it will send a join message for each multicast group it wants to join. When a host wants to leave a multicast group, it will send a leave message.

To extend multicast to the Internet, the multicast backbone (Mbone) is used. The Mbone is layered on top of portions of the Internet. These portions, or islands, are interconnected using tunnels. The tunnels allow multicast traffic to pass between the multicast-capable portions of the Internet. As more and more routers in the Internet are multicast-capable (and scalable), the unicast and multicast routing table will converge.

The original Mbone was based on Distance Vector Multicast Routing Protocol (DVMRP) and was very limited. The Mbone is, however, converging around the following protocol set:

- IGMP
- Protocol Independent Multicast (Sparse Mode) (PIM-SM)
- Border Gateway Protocol with multi-protocol extensions (MBGP)
- Multicast Source Discovery Protocol (MSDP)

2.2 Multicast Models

This section describes the models which Nokia routers support to provide multicast.

2.2.1 Any-Source Multicast (ASM)

Any-Source Multicast (ASM) is the IP multicast service model defined in RFC 1112, *Host Extensions for IP Multicasting*. An IP datagram is transmitted to a host group, a set of zero or more end-hosts identified by a single IP destination address (224.0.0.0 through 239.255.255.255 for IPv4). End-hosts can join and leave the group any time and there is no restriction on their location or number. This model supports multicast groups with arbitrarily many senders. Any end-host can transmit to a host group even if it is not a member of that group.

To combat the vast complexity and scaling issues that ASM represents, the IETF is developing a service model called Source Specific Multicast (SSM).

2.2.2 Source Specific Multicast (SSM)

The Source Specific Multicast (SSM) service model defines a channel identified by an (S,G) pair, where S is a source address and G is an SSM destination address. In contrast to the ASM model, SSM only provides network-layer support for one-to-many delivery.

The SSM service model attempts to alleviate the following deployment problems that ASM has presented:

- Address allocation — SSM defines channels on a per-source basis. For example, the channel (S1,G) is distinct from the channel (S2,G), where S1 and S2 are source addresses, and G is an SSM destination address. This averts the problem of global allocation of SSM destination addresses and makes each source independently responsible for resolving address collisions for the various channels it creates.
- Access control — SSM provides an efficient solution to the access control problem. When a receiver subscribes to an (S,G) channel, it receives data sent only by the source S. In contrast, any host can transmit to an ASM host group. At the same time, when a sender picks a channel (S,G) to transmit on, it is automatically ensured that no other sender will be transmitting on the same channel (except in the case of malicious acts such as address spoofing). This makes it harder to spam an SSM channel than an ASM multicast group.

- Handling of well-known sources — SSM requires only source-based forwarding trees, eliminating the need for a shared tree infrastructure. In terms of the IGMP, PIM-SM, MSDP, MBGP protocol suite, this implies that neither the RP-based shared tree infrastructure of PIM-SM nor the MSDP protocol is required. Thus, the complexity of the multicast routing infrastructure for SSM is low, making it viable for immediate deployment. MBGP is still required for distribution of multicast reachability information.
- Anticipating that point-to-multipoint applications such as Internet TV will be significant in the future, the SSM model is better suited for such applications.

2.2.3 Multicast in IP-VPN Networks

Multicast can be deployed as part of IP-VPN networks. For details on multicast support in IP-VPNs, refer to the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 3 Services Guide: IES and VPRN*.

3 IGMP

3.1 IGMP Overview

Internet Group Management Protocol (IGMP) is used by IPv4 hosts and routers to report their IP multicast group memberships to neighboring multicast routers. A multicast router keeps a list of multicast group memberships for each attached network, and a timer for each membership.

Multicast group memberships include at least one member of a multicast group on a given attached network, not a list of all of the members. With respect to each of its attached networks, a multicast router can assume one of two roles, querier or non-querier. There is normally only one querier per physical network.

A querier issues two types of queries, a general query and a group-specific query. General queries are issued to solicit membership information with regard to any multicast group. Group-specific queries are issued when a router receives a leave message from the node it perceives as the last group member remaining on that network segment.

Hosts wanting to receive a multicast session issue a multicast group membership report. These reports must be sent to all multicast enabled routers.

3.1.1 IGMP Versions and Interoperability Requirements

If routers run different versions of IGMP, they will negotiate the lowest common version of IGMP that is supported on their subnet and operate in that version.

Version 1 — Specified in RFC 1112, *Host extensions for IP Multicasting*, was the first widely deployed version and the first version to become an Internet standard.

Version 2 — Specified in RFC 2236, *Internet Group Management Protocol, Version 2*, added support for “low leave latency”, that is, a reduction in the time it takes for a multicast router to learn that there are no longer any members of a particular group present on an attached network.

Version 3 — Specified in RFC 3376, *Internet Group Management Protocol, Version 3*, adds support for source filtering; that is, the ability for a system to report interest in receiving packets only from specific source addresses, as required to support Source Specific Multicast (SSM), or from all but specific source addresses, sent to a particular multicast address.

IGMPv3 must keep state per group per attached network. This group state consists of a filter-mode, a list of sources, and various timers. For each attached network running IGMP, a multicast router records the desired reception state for that network.

3.1.2 IGMP Version Transition

Nokia's routers are capable of interoperating with routers and hosts running IGMPv1, IGMPv2, and/or IGMPv3. RFC 5186, *Internet Group Management Protocol Version 3 (IGMPv3)/Multicast Listener Discovery Version 2 (MLDv2) and Multicast Routing Protocol Interaction* explores some of the interoperability issues and how they affect the various routing protocols.

IGMP version 3 specifies that if at any point a router receives an older version query message on an interface that it must immediately switch into a compatibility mode with that earlier version. Since none of the previous versions of IGMP are source aware, should this occur and the interface switch to Version 1 or 2 compatibility mode, any previously learned group memberships with specific sources (learned via the IGMPv3 specific INCLUDE or EXCLUDE mechanisms) must be converted to non-source specific group memberships. The routing protocol will then treat this as if there is no EXCLUDE definition present.

3.1.3 Source-Specific Multicast Groups

IGMPv3 permits a receiver to join a group and specify that it only wants to receive traffic for a group if that traffic comes from a particular source. If a receiver does this, and no other receiver on the LAN requires all the traffic for the group, then the designated router (DR) can omit performing a (*,G) join to set up the shared tree, and instead issue a source-specific (S,G) join only.

The range of multicast addresses from 232.0.0.0 to 232.255.255.255 is currently set aside for source-specific multicast in IPv4. For groups in this range, receivers should only issue source-specific IGMPv3 joins. If a PIM router receives a non-source-specific join for a group in this range, it should ignore it.

A Nokia router PIM router must silently ignore a received (*,G) PIM join message where G is a multicast group address from the multicast address group range that has been explicitly configured for SSM. This occurrence should generate an event. If configured, the IGMPv2 request can be translated into IGMPv3. The router allows for the conversion of an IGMPv2 (*,G) request into a IGMPv3 (S,G) request based on manual entries. A maximum of 32 SSM ranges is supported.

IGMPv3 also permits a receiver to join a group and specify that it only wants to receive traffic for a group if that traffic does not come from a specific source or sources. In this case, the DR will perform a (*,G) join as normal, but can combine this with a prune for each of the sources the receiver does not wish to receive.

3.1.4 Query Messages

The IGMP query source address is configurable at two hierarchal levels. It can be configured globally at each router instance IGMP level and can be configured at individual at the group-interface level. The group-interface level overrides the src-ip address configured at the router instance level.

By default, subscribers with IGMP policies send IGMP queries with an all zero SRC IP address (0.0.0.0). However, some systems only accept and process IGMP query messages with non-zero SRC IP addresses. This feature allows the BNG to inter-operate with such systems.

3.2 Configuring IGMP with CLI

This section provides information to configure IGMP using the command line interface.

3.2.1 IGMP Configuration Overview

The routers use IGMP to manage membership for a given multicast session. IGMP is not enabled by default. When enabled, at least one interface must be specified in the IGMP context as IGMP is an interface function. Creating an interface enables IGMP. Traffic can only flow away from the router to an IGMP interface and to and from a PIM interface. A router directly connected to a source must have PIM enabled on the interface to that source. The traffic travels in a network from PIM interface to PIM interface and arrives finally on an IGMP enabled interface.

The IGMP CLI context allows you to specify an existing IP interface and modify the interface-specific parameters. Static IGMP group memberships can be configured to test multicast forwarding without a receiver host. When IGMP static group membership is 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. When a host wants to receive multicast sessions it sends a join message for each multicast group it wants to join. Then, a leave message may be sent for each multicast group it no longer wishes to participate with.

A multicast router keeps a list of multicast group memberships for each attached network, and an interval timer for each membership. Hosts issue a Multicast Group Membership Report when they want to receive a multicast session. The reports are sent to all multicast routers.

3.2.2 Basic IGMP Configuration

Perform the following basic multicast configuration tasks:

- Enable IGMP (required)
- Configure IGMP interfaces (required)
- Specify IGMP version on the interface (optional)

- Configure static (S,G)/(*,G) (optional)
- Configure SSM translation (optional)

3.2.3 Configuring IGMP Parameters

3.2.3.1 Enabling IGMP

Use the following CLI syntax to enable IGMP.

CLI Syntax: `config>router# igmp`

The following example displays the detailed output when IGMP is enabled.

```
A:LAX>>config>router# info detail
...
#------------------------------------------
echo "IGMP Configuration"
#------------------------------------------
        igmp
            query-interval 125
            query-last-member-interval 1
            query-response-interval 10
            robust-count 2
            no shutdown
        exit
#------------------------------------------
A:LAX>>config>system#
```

3.2.3.2 Configuring an IGMP Interface

To configure an IGMP interface:

CLI Syntax:

```
config>router# igmp
      interface ip-int-name
            max-groups value
            import policy-name
            version version
            no shutdown
```

Use the following CLI syntax to configure IGMP interfaces:

Example:

```
config>router#
config>router>igmp# interface "lax-vls"
```

```
config>router>igmp>if? no shutdown
config>router>igmp>if# exit
config>router>igmp# interface "p1-ix"
config>router>igmp>if? no shutdown
config>router>igmp>if# exit
config>router>igmp# interface "lax-sjc"
config>router>igmp>if? no shutdown
config>router>igmp>if# exit
```

The following example displays the IGMP configuration:

```
A:LAX>config>router>igmp# info
----------------------------------------------
        interface "lax-sjc"
        exit
        interface "lax-vls"
        exit
        interface "p1-ix"
        exit
----------------------------------------------
A:LAX>config>router>igmp# exit
```

3.2.3.3 Configuring Static Parameters

To add an IGMP static multicast source:

CLI Syntax:

```
config>router# igmp
     interface ip-int-name
          no shutdown
          static
               group grp-ip-address
                    source ip-address
```

Use the following CLI syntax to configure static group addresses and source addresses for the SSM translate group ranges:

Example:

```
config>router>igmp# interface lax-vls
config>router>igmp>if# static
config>router>igmp>if>static# group 239.255.0.2
config>router>igmp>if>static>group# source
 172.22.184.197
config>router>igmp>if>static>group# exit
config>router>igmp>if>static# exit
config>router>igmp>if# exit
```

The following example displays the configuration:

```
A:LAX>config>router>igmp# info
```

```
----------------------------------------------
        interface "lax-sjc"
        exit
        interface "lax-vls"
            static
                group 239.255.0.2
                    source 172.22.184.197
                exit
            exit
        exit
        interface "p1-ix"
        exit
----------------------------------------------
A:LAX>config>router>igmp#
```

To add an IGMP static starg entry:

CLI Syntax:
```
config>router# igmp
      interface ip-int-name
            no shutdown
            static
                  group grp-ip-address
                        starg
```

Use the following CLI syntax to configure static group addresses and add a static (*,G) entry:

Example:
```
config>router>igmp# interface lax-sjc
config>router>igmp>if# static
config>router>igmp>if>static# group 239.1.1.1
config>router>igmp>if>static>group# starg
config>router>igmp>if>static>group# exit
config>router>igmp>if>static# exit
config>router>igmp>if# exit
config>router>igmp#
```

The following example displays the configuration:

```
A:LAX>config>router>igmp# info
----------------------------------------------
        interface "lax-sjc"
            static
                group 239.1.1.1
                    starg
                exit
            exit
        exit
        interface "lax-vls"
            static
                group 239.255.0.2
                    source 172.22.184.197
                exit
            exit
```

```
        exit
        interface "p1-ix"
        exit
----------------------------------------------
A:LAX>config>router>igmp#
```

3.2.3.4 Configuring SSM Translation

To configure IGMP parameters:

CLI Syntax:
```
config>router# igmp
      ssm-translate
            grp-range start end
                  source ip-address
```

The following example displays the command usage to configure IGMP parameters:

Example:
```
config>router# igmp
config>router>igmp# ssm-translate
config>router>igmp>ssm# grp-range 239.255.0.1 239.2.2.2
config>router>igmp>ssm>grp-range# source 10.1.1.1
```

The following example displays the SSM translation configuration:

```
A:LAX>config>router>igmp# info
----------------------------------------------
        ssm-translate
            grp-range 239.255.0.1 239.2.2.2
                source 10.1.1.1
            exit
        exit
        interface "lax-sjc"
            static
                group 239.1.1.1
                    starg
                exit
            exit
        exit
        interface "lax-vls"
            static
                group 239.255.0.2
                    source 172.22.184.197
                exit
            exit
        exit
        interface "p1-ix"
        exit
----------------------------------------------
A:LAX>config>router>igmp# exit
```

3.2.4 Disabling IGMP

Use the following CLI syntax to disable IGMP.

CLI Syntax:
```
config>router#
      igmp
            shutdown
```

The following example displays the command usage to disable multicast:

Example:
```
config>router# igmp
config>router>igmp# shutdown
config>router>igmp# exit
```

The following example displays the configuration output:

```
A:LAX>config>router# info
----------------------------------------------
...
#--------------------------------------------
echo "IGMP Configuration"
#--------------------------------------------
        igmp
            shutdown
            ssm-translate
                grp-range 239.255.0.1 239.2.2.2
                    source 10.1.1.1
                exit
            exit
            interface "lax-sjc"
                static
                    group 239.1.1.1
                        starg
                    exit
                exit
            exit
            interface "lax-vls"
                static
                    group 239.255.0.2
                        source 172.22.184.197
                    exit
                exit
            exit
            interface "p1-ix"
            exit
        exit
#--------------------------------------------
```

3.3 IGMP Configuration Command Reference

3.3.1 Command Hierarchies

- IGMP Configuration Commands

3.3.1.1 IGMP Configuration Commands

config
- — **router**
  - — [**no**] **igmp**
    - — [**no**] **group-interface** *ip-int-name*
      - — [**no**] **disable-router-alert-check**
      - — **import** *policy-name*
      - — **no import**
      - — **max-groups** *value*
      - — **no max-groups**
      - — **max-grp-sources** *value*
      - — **no max-grp-sources**
      - — **max-sources** *value*
      - — **no max-sources**
      - — **query-src-ip** *ip-address*
      - — **no query-src-ip**
      - — [**no**] **shutdown**
      - — [**no**] **sub-hosts-only**
      - — [**no**] **subnet-check**
      - — **version** *version*
      - — **no version**
    - — **grp-if-query-src-ip** *ip-address*
    - — **no grp-if-query-src-ip**
    - — [**no**] **interface** *ip-int-name*
      - — [**no**] **disable-router-alert-check**
      - — [**no**] **group-interface** *ip-int-name*
        - — [**no**] **shutdown**
      - — **import** *policy-name*
      - — **no import**
      - — **max-groups** *value*
      - — **no max-groups**
      - — **max-grp-sources** *value*
      - — **no max-grp-sources**
      - — **max-sources** *value*
      - — **no max-sources**
      - — **query-interval** *seconds*
      - — **no query-interval**
      - — **query-last-member-interval** *seconds*
      - — **no query-last-member-interval**

— **query-response-interval** *seconds*
— **no query-response-interval**
— [**no**] **redundant-multicast**
— [**no**] **shutdown**
— **ssm-translate**
    — [**no**] **grp-range** *start end*
        — [**no**] **source** *ip-address*
— **static**
    — [**no**] **group** *grp-ip-address*
    — [**no**] **group** **start** *grp-ip-address* **end** *grp-ip-address* [**step** *ip-address*]
        — [**no**] **source** *ip-address*
        — [**no**] **starg**
— [**no**] **subnet-check**
— **version** *version*
— **no version**

— **query-interval** *seconds*
— **no query-interval**
— **query-last-member-interval** *seconds*
— **no query-last-member-interval**
— **query-response-interval** *seconds*
— **no query-response-interval**
— **robust-count** *robust-count*
— **no robust-count**
— [**no**] **shutdown**
— **ssm-translate**
    — [**no**] **grp-range** *start end*
        — [**no**] **source** *ip-address*
— [**no**] **tunnel-interface** **rsvp-p2mp** *lsp-name*
— [**no**] **tunnel-interface** **ldp-p2mp** *p2mp-id* **sender** *ip-address*
    — [**no**] **shutdown**
    — **static**
        — [**no**] **group** *grp-ip-address*
            — [**no**] **source** *ip-address*
            — [**no**] **starg**

3.3.2 Command Descriptions

3.3.2.1 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.

group-interface

Syntax

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

Context

config>router>igmp
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. The retailer VRF does not have the concept of group-interfaces under the subscriber-interface hierarchy. In the 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. 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.

Parameters

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

disable-router-alert-check

Syntax

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

Context

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

Description

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

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

import

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

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

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

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, and so on), 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>igmp>group-interface
config>router>igmp>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.

The **no** form of the command sets no limit to the number of groups.

Default no max-groups

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

Values 1 to 16000

max-grp-sources

Syntax **max-grp-sources** *value*
no max-grp-sources

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

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 no max-grp-sources

Parameters *value* — Specifies the maximum number of group sources.

Values 1 to 32000

max-sources

Syntax **max-sources** *value*
no max-sources

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

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

Parameters *value* — Specifies the maximum number of group sources.

Values 1 to 1000

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.

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

shutdown

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

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

sub-hosts-only

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

Context config>router>igmp>group-interface

Description This command disables the 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 allows the 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.

The 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

subnet-check

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

Context config>router>igmp>group-interface

config>router>igmp>if

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 subnet-check

version

Syntax **version** *version*
no version

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

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, 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 version 3

Parameters *version* — Specifies the IGMP version number.

Values 1, 2, 3

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.

Parameters *ip-address* — Sets the query source IP address.

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

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, and so on), 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.

query-interval

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

Context config>router>igmp
config>router>igmp>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 query-interval 125

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

Values 2 to 1024

query-last-member-interval

Syntax **query-last-member-interval** *seconds*
no query-last-member-interval

Context config>router>igmp
config>router>igmp>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 query-last-member-interval 1

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

Values 1 to 1023

query-response-interval

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

Context config>router>igmp
config>router>igmp>if

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

Default query-response-interval 10

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

Values 1 to 1023

redundant-multicast

Syntax [**no**] **redundant-multicast**

Context config>router>igmp>if

Description This command configures the interface as a member of a redundant pair for multicast traffic.

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

ssm-translate

Syntax **ssm-translate**

Context config>router>igmp
config>router>igmp>if

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>if>ssm-translate
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>if>ssm-translate>grp-range
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.

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.

group

Syntax [**no**] **group** *grp-ip-address*
[**no**] **group start** *grp-ip-address* **end** *grp-ip-address* [**step** *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.

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

start *grp-ip-address* — Specifies the start multicast group address.

end *grp-ip-address* — Specifies the end multicast group address.

step *ip-address* — Specifies the step increment.

source

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

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

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.

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

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 (*,G) entry from the configuration.

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 robust-count 2

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

Values 2 to 10

tunnel-interface

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

Context 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 interface 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 “::” or “:” at the end of the LSP name. However, a single “:” can be used anywhere in the string except at the end of the name.

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

ldp-p2mp *p2mp-id* — Identifier used for signaling MLDP P2MP LSP.

Values 1 to 4294967296 (on leaf node)
1 to 8192 (on root node)

sender *sender-address* — 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.

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.

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.

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.

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 (*,G) entry from the configuration.

3.4 Show, Clear, and Debug Command Reference

3.4.1 Command Hierarchies

- Show Commands
- Clear Commands
- Debug Commands

3.4.1.1 Show Commands

show
— **router**
— **igmp**
— **group** [*grp-ip-address*] [**hosts** | **interfaces** | **saps**]
— **group summary** [**hosts** | **interfaces** | **saps**]
— **group-interface** [**fwd-service** *service-id*] [*ip-int-name*] [**detail**] [**group**] [*grp-address*]
— **hosts** [**detail**] [**fwd-service** *service-id*] [**grp-interface** *ip-int-name*]
— **hosts** [**host** *ip-address*] [**group** *grp-address*] [**detail**]
— **hosts summary**
— **interface** [*ip-int-name* | *ip-address*] [**group**] [*grp-ip-address*] [**detail**]
— **mcast-reporting-statistics** *ip-address*
— **ssm-translate**
— **ssm-translate interface** *interface-name*
— **static** [*ip-int-name* | *ip-addr*]
— **statistics** [*ip-int-name* | *ip-address*]
— **statistics group-interface** [**fwd-service** *service-id*] [*ip-int-name*]
— **statistics host** [*ip-address*]
— **status**
— **tunnel-interface**

3.4.1.2 Clear Commands

clear
— **router**
— **igmp**
— **database** [**group** *grp-ip-address* [**source** *src-ip-address*]]
— **database interface** {*ip-int-name* | *ip-address*} [**group** *grp-ip-address* [**source** *src-ip-address*]]
— **database host** *ip-address* [**group** *grp-ip-address* [**source** *src-ip-address*]]
— **database host all** [**group** *grp-ip-address* [**source** *src-ip-address*]]

— **database group-interface** *interface-name* [**fwd-service** *service-id*] [**group** *grp-ip-address* [**source** *src-ip-address*]]
— **database group-interface all**
— **statistics group-interface** [**fwd-service** *service-id*] *ip-int-name*
— **statistics group-interface all**
— **statistics host** *ip-address*
— **statistics host all**
— **statistics** [**interface** *ip-int-name* | *ip-address*]
— **version group-interface** [**fwd-service** *service-id*] *ip-int-name*
— **version group-interface all**
— **version host** *ip-address*
— **version host all**
— **version** [**interface** *ip-int-name* | *ip-address*]

3.4.1.3 Debug Commands

debug
— **router**
— **igmp**
— [**no**] **group-interface** [**fwd-service** *service-id*] [*ip-int-name*]
— [**no**] **host** [*ip-address*]
— [**no**] **host** [**fwd-service** *service-id*] **group-interface** *ip-int-name*
— [**no**] **interface** [*ip-int-name* | *ip-address*]
— **mcs** [*ip-int-name*]
— **no mcs**
— [**no**] **misc**
— **packet** [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] [*ip-int-name* | *ip-address*] [**mode** {**dropped-only** | **ingr-and-dropped** | **egr-ingr-and-dropped**}]
— **packet** [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] [**mode** {**dropped-only** | **ingr-and-dropped** | **egr-ingr-and-dropped**}] **group-interface** *ip-int-name*
— **packet** [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] **host** *ip-address* [**mode** {**dropped-only** | **ingr-and-dropped** | **egr-ingr-and-dropped**}]
— **no packet** [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] [*ip-int-name* | *ip-address*]
— **no packet** [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] **group-interface** *ip-int-name*
— **no packet** [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] **host** *ip-address*

3.4.2 Command Descriptions

3.4.2.1 Show Commands

The command outputs in the following section are examples only; actual displays may differ depending on supported functionality and user configuration.

group

Syntax **group** [*grp-ip-address*] [**hosts | interfaces | saps**]
group summary [**hosts | interfaces | saps**]

Context show>router>igmp

Description This command displays the multicast group and (S,G) addresses. If no *grp-ip-address* parameters are specified, then all IGMP group, (*,G) and (S,G) addresses are displayed.

Parameters *grp-ip-address* — Displays specific multicast group addresses.

hosts — Displays hosts for the multicast group address.

interfaces — Displays interfaces for the multicast group address.

saps — Displays SAPs for the multicast group address.

Output IGMP Group Output

The following table describes the output fields for IGMP group information.

Table 3 **IGMP Group Information Output Fields**

Label	Description
IGMP Groups	Displays the IP multicast sources corresponding to the IP multicast groups.
Fwd List	Displays the list of interfaces in the forward list.
Blk List	Displays the list of interfaces in the blocked list.

Sample Output

```
*B:Dut-C# show router igmp group
===============================================================================
IGMP Interface Groups
===============================================================================
===============================================================================
IGMP Host Groups
```

```
===============================================================================
(*,239.0.0.1)
    Fwd List  : 239.112.1.2             Up Time : 0d 00:00:21
(10.11.0.1,239.0.0.1)
    Fwd List  : 239.112.1.1             Up Time : 0d 00:00:30
    Blk List  : 239.112.1.2             Up Time : 0d 00:00:21
(10.11.0.2,239.0.0.1)
    Fwd List  : 239.112.1.1             Up Time : 0d 00:00:30
(*,239.0.0.2)
    Fwd List  : 239.112.1.2             Up Time : 0d 00:00:21
(10.11.0.1,239.0.0.2)
    Blk List  : 239.112.1.2             Up Time : 0d 00:00:21
-------------------------------------------------------------------------------
(*,G)/(S,G) Entries : 5
===============================================================================
*B:Dut-C#

*B:Dut-C# show router igmp group summary
===============================================================================
IGMP Interface Groups
===============================================================================
===============================================================================
IGMP Host Groups Summary          Nbr Fwd Hosts          Nbr Blk Hosts
===============================================================================
(*,239.0.0.1)                     1                      0
(10.11.0.1,239.0.0.1)             1                      1
(10.11.0.2,239.0.0.1)             1                      0
(*,239.0.0.2)                     1                      0
(10.11.0.1,239.0.0.2)             0                      1
-------------------------------------------------------------------------------
(*,G)/(S,G) Entries : 5
===============================================================================
*B:Dut-C#

A:NYC# show router igmp group 239.24.24.24
===============================================================================
IGMP Groups
===============================================================================
(*,239.24.24.24)                        Up Time : 0d 05:23:23
    Fwd List  : nyc-vlc
-------------------------------------------------------------------------------
(*,G)/(S,G) Entries : 1
===============================================================================
A:NYC#
```

group-interface

Syntax **group-interface** [**fwd-service** *service-id*] [*ip-int-name*] [**detail**] [**group**] [*grp-address*]

Context show>router>igmp>group-interface

Description This command displays IGMP group-interface information.

Parameters *service-id* — [1..2148007980] | <svc-name:64 char max>

ip-int-name — IP interface name. A string up to 32 characters.

detail — Displays detailed information.

group — Displays information from the group IP address.

grp-address — Group IP address in format: a.b.c.d

hosts

Syntax **hosts** [**detail**] [**fwd-service** *service-id*] [**grp-interface** *ip-int-name*]
hosts [**host** *ip-address*] [**group** *grp-address*] [**detail**]
hosts summary

Context show>router>igmp

Description This command shows IGMP hosts information.

Parameters *grp-address* — Specifies the group IP address in format: a.b.c.d

service-id — [1 to 2148007980]|<svc-name: 64 characters maximum>

ip-int-name — IP interface name. A string up to 32 characters.

ip-address — IP address in format: a.b.c.d

Output The following output is an example of IGMP host information.

Sample Output

```
*B:Dut-C# show router igmp hosts
===============================================================================
IGMP Hosts
===============================================================================
Host            Oper    Oper    Fwd   GrpItf            Num    Subscriber
                State   Version Svc                     Groups
-------------------------------------------------------------------------------
239.112.1.1     Up      3       1     gi_1_1            1      sub_1
239.112.1.2     Up      3       1     gi_1_1            2      sub_1
239.112.1.3     Up      3       1     gi_1_2            0      sub_2
-------------------------------------------------------------------------------
Hosts : 3
===============================================================================
*B:Dut-C#

*B:Dut-C# show router igmp hosts detail
===============================================================================
IGMP Host 239.112.1.1
===============================================================================
Oper Status      : Up         MacAddress     : 00:00:00:00:00:01
Oper version     : 3          Subscriber     : sub_1
Num Groups       : 1          GrpItf         : gi_1_1
Max Grps Till Now: 2          IGMP-Policy    : pol1
PPPoE SessionId  : 1          Next query time: 0d 00:02:03
FwdSvcId         : 1
-------------------------------------------------------------------------------
IGMP Group
```

```
-------------------------------------------------------------------------------
Group Address    : 239.0.0.1      Up Time    : 0d 00:00:24
Expires          : Not running    Mode       : Include
V1 Host Timer    : Not running    Type       : Dynamic
V2 Host Timer    : Not running    Compat Mode: IGMP Version 3
Redir.vRtrId     : N/A            Redir.Intf : N/A
------------------------------------------------------------
Source Address     Expires        Type         Fwd/Blk
------------------------------------------------------------
10.11.0.1          0d 00:03:56    Dynamic      Fwd
10.11.0.2          0d 00:03:56    Dynamic      Fwd
===============================================================================
IGMP Host 239.112.1.2
===============================================================================
Oper Status      : Up         MacAddress     : 00:00:00:00:00:01
Oper version     : 3          Subscriber     : sub_1
Num Groups       : 2          GrpItf         : gi_1_1
Max Grps Till Now: 2          IGMP-Policy    : pol1
PPPoE SessionId  : 2          Next query time: 0d 00:02:03
FwdSvcId         : 1
-------------------------------------------------------------------------------
IGMP Group
-------------------------------------------------------------------------------
Group Address    : 239.0.0.1      Up Time    : 0d 00:00:16
Expires          : 0d 00:04:05    Mode       : Exclude
V1 Host Timer    : Not running    Type       : Dynamic
V2 Host Timer    : Not running    Compat Mode: IGMP Version 3
Redir.vRtrId     : N/A            Redir.Intf : N/A
------------------------------------------------------------
Source Address     Expires        Type         Fwd/Blk
------------------------------------------------------------
10.11.0.1          0d 00:00:00    Dynamic      Blk
-------------------------------------------------------------------------------
IGMP Group
-------------------------------------------------------------------------------
Group Address    : 239.0.0.2      Up Time    : 0d 00:00:16
Expires          : 0d 00:04:04    Mode       : Exclude
V1 Host Timer    : Not running    Type       : Dynamic
V2 Host Timer    : Not running    Compat Mode: IGMP Version 3
Redir.vRtrId     : N/A            Redir.Intf : N/A
------------------------------------------------------------
Source Address     Expires        Type         Fwd/Blk
------------------------------------------------------------
10.11.0.1          0d 00:00:00    Dynamic      Blk
===============================================================================
IGMP Host 239.112.1.3
===============================================================================
Oper Status      : Up         MacAddress     : 00:00:00:00:00:02
Oper version     : 3          Subscriber     : sub_2
Num Groups       : 0          GrpItf         : gi_1_2
Max Grps Till Now: 1          IGMP-Policy    : pol1
PPPoE SessionId  : 1          Next query time: 0d 00:00:48
FwdSvcId         : 1
-------------------------------------------------------------------------------
Hosts : 3
===============================================================================
*B:Dut-C#

*B:Dut-C# show router igmp statistics host 239.112.1.1
```

```
==================================================
IGMP Host Statistics 239.112.1.1
==================================================
Message Type        Received       Transmitted
--------------------------------------------------
Queries             0              580
Report V1           0              0
Report V2           0              0
Report V3           5              0
Leaves              0              0
-------------------------------------------------------------------------------
General Host Statistics
-------------------------------------------------------------------------------
Bad Length         : 0
Bad Checksum       : 0
Unknown Type       : 0
Bad Receive If     : 0
Rx Non Local       : 0
Rx Wrong Version   : 0
Policy Drops       : 0
No Router Alert    : 0
Rx Bad Encodings   : 0
Local Scope Pkts   : 0
Resvd Scope Pkts   : 0
MCAC Policy Drops  : 0
-------------------------------------------------------------------------------
Source Group Statistics
-------------------------------------------------------------------------------
(S,G)              : 0
(*,G)              : 0
==================================================
*B:Dut-C# show subscriber-mgmt igmp-policy
```

interface

Syntax **interface** [*ip-int-name* **|** *ip-address*] [**group**] [*grp-ip-address*] [**detail**]

Context show>router>igmp

Description This command displays IGMP interface information.

Parameters *ip-int-name* — Only displays the information associated with the specified IP interface name.

ip-address — Only displays the information associated with the specified IP address.

group *grp-ip-address* — Only displays IP multicast group address for which this entry contains information.

detail — Displays detailed IP interface information along with the source group information learned on that interface.

Output IGMP Interface Output

The following table provides IGMP field descriptions.

Table 4 **IGMP Fields**

Label	Description
Interface	Displays the interfaces that participate in the IGMP protocol.
Adm Admin Status	Displays the administrative state for the IGMP protocol on this interface.
Oper Oper Status	Displays the current operational state of IGMP protocol on the interface.
Querier	Displays the address of the IGMP querier on the IP subnet to which the interface is attached.
Querier Up Time	Displays the time since the querier was last elected as querier.
Querier Expiry Timer	Displays the time remaining before the querier ages out. If the querier is the local interface address, the value will be zero.
Cfg/Opr Version Admin/Oper version	Cfg The configured version of IGMP running on this interface. For IGMP to function correctly, all routers on a LAN must be configured to run the same version of IGMP on that LAN. Opr The operational version of IGMP running on this interface. If the cfg value is 3 but all of the routers in the local subnet of this interface use IGMP version v1 or v2, the operational version will be v1 or v2.
Num Groups	The number of multicast groups which have been learned by the router on the interface.
Policy	Displays the policy that is to be applied on the interface.
Group Address	Displays the IP multicast group address for which this entry contains information.
Up Time	Displays the time since this source group entry got created.
Last Reporter	Displays the IP address of the source of the last membership report received for this IP Multicast group address on this interface. If no membership report has been received, this object has the value 0.0.0.0.

Table 4 **IGMP Fields (Continued)**

Label	Description
Mode	The mode is based on the type of membership report(s) received on the interface for the group. In the 'include' mode, reception of packets sent to the specified multicast address is requested only from those IP source addresses listed in the source-list parameter of the IGMP membership report. In 'exclude' mode, reception of packets sent to the given multicast address is requested from all IP source addresses except those listed in the source-list parameter.
V1 Host Timer	The time remaining until the local router will assume that there are no longer any IGMP version 1 members on the IP subnet attached to this interface. Upon hearing any IGMPv1 Membership Report, this value is reset to the group membership timer. While this time remaining is non-zero, the local router ignores any IGMPv2 Leave messages for this group that it receives on this interface.
V2 Host Timer	The time remaining until the local router will assume that there are no longer any IGMP version 2 members on the IP subnet attached to this interface. Upon hearing any IGMPv2 Membership Report, this value is reset to the group membership timer. While this time remaining is non-zero, the local router ignores any IGMPv3 Leave messages for this group that it receives on this interface.
Type	Indicates how this group entry was learned. If this group entry was learned by IGMP, it will be set to “dynamic”. For statically configured groups, the value will be set to 'static'.
Compat Mode	Used in order for routers to be compatible with older version routers. IGMPv3 hosts must operate in version 1 and version 2 compatibility modes. IGMPv3 hosts must keep state per local interface regarding the compatibility mode of each attached network. A host's compatibility mode is determined from the Host Compatibility Mode variable which can be in one of three states: IGMPv1, IGMPv2 or IGMPv3. This variable is kept per interface and is dependent on the version of General Queries heard on that interface as well as the Older Version Querier Present timers for the interface.

Sample Output

```
*A:ALA-BA# show router 100 interface
===============================================================================
Interface Table (Service: 100)
===============================================================================
Interface-Name                   Adm         Opr(v4/v6)  Mode    Port/SapId
```

```
   IP-Address                                                 PfxState
-------------------------------------------------------------------------------
IGMP_to_CE                       Up          Up          VPRN    1/1/7
   10.1.1.1/24                                                n/a
system                           Up          Up          VPRN    loopback
   10.20.1.2/32                                               n/a
-------------------------------------------------------------------------------
Interfaces : 2
===============================================================================
*A:ALA-BA#

*A:ALA-BA# show router 100 interface IGMP_to_CE
===============================================================================
Interface Table (Service: 100)
===============================================================================
Interface-Name                   Adm         Opr(v4/v6)  Mode    Port/SapId
   IP-Address                                                 PfxState
-------------------------------------------------------------------------------
IGMP_to_CE                       Up          Up          VPRN    1/1/7
   10.1.1.1/24                                                n/a
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
*A:ALA-BA#

*A:ALA-BA# show router 100 igmp interface
===============================================================================
IGMP Interfaces
===============================================================================
Interface               Adm  Oper Querier         Cfg/Opr Num     Policy
                                                  Version Groups
-------------------------------------------------------------------------------
IGMP_to_CE              Up   Up   10.1.1.1        1/1     3       igmppol
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
*A:ALA-BA#

*A:ALA-BA# show router 100 igmp interface IGMP_to_CE
===============================================================================
IGMP Interface IGMP_to_CE
===============================================================================
Interface               Adm  Oper Querier         Cfg/Opr Num     Policy
                                                  Version Groups
-------------------------------------------------------------------------------
IGMP_to_CE              Up   Up   10.1.1.1        1/1     3       igmppol
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
*A:ALA-BA#

*A:ALA-BA# show router 100 igmp interface 10.1.1.1
===============================================================================
IGMP Interface 10.1.1.1
===============================================================================
Interface               Adm  Oper Querier         Cfg/Opr Num     Policy
                                                  Version Groups
-------------------------------------------------------------------------------
IGMP_to_CE              Up   Up   10.1.1.1        1/1     3       igmppol
```

```
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
*A:ALA-BA#

*A:ALA-BA# show router 100 igmp interface IGMP_to_CE group 239.1.1.1
===============================================================================
IGMP Interface IGMP_to_CE
===============================================================================
Interface              Adm  Oper Querier         Cfg/Opr Num     Policy
                                                 Version Groups
-------------------------------------------------------------------------------
IGMP_to_CE             Up   Up   10.1.1.1        1/1     3       igmppol
-------------------------------------------------------------------------------
IGMP Group
-------------------------------------------------------------------------------
Group Address : 239.1.1.1              Up Time       : 0d 00:03:52
Interface     : IGMP_to_CE             Expires       : never
Last Reporter : 0.0.0.0                Mode          : exclude
V1 Host Timer : Not running            Type          : static
V2 Host Timer : Not running            Compat Mode   : IGMP Version 3
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
*A:ALA-BA#

*A:ALA-BA# show router 100 igmp interface IGMP_to_CE group 239.1.1.1 detail
===============================================================================
IGMP Interface IGMP_to_CE
===============================================================================
Interface          : IGMP_to_CE
Admin Status       : Up                Oper Status        : Up
Querier            : 10.1.1.1          Querier Up Time    : 0d 00:04:01
Querier Expiry Time: N/A               Time for next query: 0d 00:13:42
Admin/Oper version : 1/1               Num Groups         : 3
Policy             : igmppol           Subnet Check       : Disabled
Max Groups Allowed : 16000             Max Groups Till Now: 3
MCAC Policy Name   :                   MCAC Const Adm St  : Enable
MCAC Max Unconst BW: no limit          MCAC Max Mand BW   : no limit
MCAC In use Mand BW: 0                 MCAC Avail Mand BW : unlimited
MCAC In use Opnl BW: 0                 MCAC Avail Opnl BW : unlimited
-------------------------------------------------------------------------------
IGMP Group
-------------------------------------------------------------------------------
Group Address : 239.1.1.1              Up Time       : 0d 00:04:02
Interface     : IGMP_to_CE             Expires       : never
Last Reporter : 0.0.0.0                Mode          : exclude
V1 Host Timer : Not running            Type          : static
V2 Host Timer : Not running            Compat Mode   : IGMP Version 3
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
*A:ALA-BA#
```

mcast-reporting-statistics

Syntax **mcast-reporting-statistics** *ip-address*

Context show>router>igmp

Description This command displays IGMP multicast reporting statistics.

Parameters *ip-address* — Displays the information associated with the specified IP address.

ssm-translate

Syntax **ssm-translate**
ssm-translate interface *interface-name*

Context show>router>igmp

Description This command displays IGMP SSM translate configuration information.

Parameters *interface-name* — IP interface name. A string up to 32 characters.

Output IGMP Interface Output

The following table provides IGMP field descriptions.

Table 5 **IGMP Fields**

Label	Description
Group Range	Displays the address ranges of the multicast groups for which this router can be an RP.
Source	Displays the unicast address that sends data on an interface.
SSM Translate Entries	Displays the total number of SSM translate entries.

Sample Output

```
=================================================================
IGMP SSM Translate Entries
=================================================================
Group Range                Source                    Interface
-----------------------------------------------------------------
<239.1.1.1 - 239.1.1.2>   10.1.1.1                    -

<239.1.1.1 - 239.1.1.5>   00.1.1.2                    ies-abc
-----------------------------------------------------------------
```

static

Syntax **static** [*ip-int-name* | *ip-addr*]

Context show>router>igmp

Description This command displays static IGMP, (*,G) and (S,G) information.

Parameters *ip-int-name* — Only displays the information associated with the specified IP interface name.

ip-addr — Only displays the information associated with the specified IP address.

Output Static IGMP Output

The following table provides static IGMP field descriptions.

Table 6 **IGMP Static Fields**

Label	Description
Source	Displays entries which represents a source address from which receivers are interested/not interested in receiving multicast traffic.
Group	Displays the IP multicast group address for which this entry contains information.
Interface	Displays the interface name.

Sample Output

```
*A:ALA-BA# show router 100 igmp static
==================================================================
IGMP Static Group Source
==================================================================
Source           Group            Interface
------------------------------------------------------------------
10.11.11.11      239.136.22.3     IGMP_to_CE
*                239.1.1.1        IGMP_to_CE
10.22.22.22      239.255.255.255  IGMP_to_CE
------------------------------------------------------------------
Static (*,G)/(S,G) Entries : 3
==================================================================
*A:ALA-BA#
```

statistics

Syntax **statistics** [*ip-int-name* | *ip-address*]
statistics group-interface [**fwd-service** *service-id*] [*ip-int-name*]
statistics host [*ip-address*]

Context show>router>igmp

Description This command displays IGMP statistics information.

Parameters *ip-int-name* — Only displays the information associated with the specified IP interface name.

ip-address — Only displays the information associated with the specified IP address.

Output IGMP Statistics Output

The following table provides statistical IGMP field descriptions.

Table 7 **IGMP Statistics Fields**

Label	Description
IGMP Interface Statistics	Lists the IGMP statistics for a particular interface.
Message Type	Queries The number of IGMP general queries transmitted or received on this interface.
	Report The total number of IGMP V1, V2, or V3 reports transmitted or received on this interface.
	Leaves The total number of IGMP leaves transmitted on this interface.
Received	Displays the total number of IGMP packets received on this interface.
Transmitted	Displays the total number of IGMP packets transmitted from this interface.
General Interface Statistics	Lists the general IGMP statistics.
Bad Length	Displays the total number of IGMP packets with bad length received on this interface.
Bad Checksum	Displays the total number of IGMP packets with bad checksum received on this interface.
Unknown Type	Displays the total number of IGMP packets with unknown type received on this interface.
Drops	Displays the total number of IGMP packets dropped on this interface.

Table 7 IGMP Statistics Fields (Continued)

Label	Description
Rx Non Local	Displays the total number of IGMP packets received from a non-local sender.
Rx Wrong Version	Displays the total number of IGMP packets with wrong versions received on this interface.
Policy Drops	Displays the total number of IGMP packets dropped by import policies on this interface.
No Router Alert	Displays the total number of IGMPv3 packets received on this interface which did not have the router alert flag set.
Rx Bad Encodings	Displays the total number of IGMP packets with bad encodings received on this interface.
Rx Pkt Drops	Displays the total number of IGMP receive packet drops on this interface.
Local Scope Pkts	Displays the total number of IGMP packets with local scope received on this interface.
Resvd Scope Pkts	Displays the total number of IGMP packets with reserved scope received on this interface.
MCAC Policy Drops	Displays the total number of IGMP packets dropped by MCAC policies on this interface.

Sample Output

```
*A:ALA-BA# show router igmp interface "IGMP_to_CE"
==================================================
IGMP Interface IGMP_to_CE Statistics
==================================================
Message Type        Received       Transmitted
--------------------------------------------------
Queries             0              0
Report V1           0              0
Report V2           0              0
Report V3           0              0
Leaves              0              0
--------------------------------------------------
Interface General Statistics
--------------------------------------------------
Bad Length         : 0
Bad Checksum       : 0
Unknown Type       : 0
Drops              : 0
Rx Non Local       : 0
Rx Wrong Version   : 0
Policy Drops       : 0
No Router Alert    : 0
Rx Bad Encodings   : 0
```

```
Local Scope Pkts  : 0
Resvd Scope Pkts  : 0
MCAC Policy Drops : 0
--------------------------------------------------
Interface Source Group Statistics
--------------------------------------------------
(S,G)             : 0
(*,G)             : 0
==================================================
*A:ALA-BA#

*B:Dut-C# show router igmp statistics host
==================================================
IGMP Host Statistics
==================================================
Message Type        Received       Transmitted
--------------------------------------------------
Queries             0              1739
Report V1           0              0
Report V2           0              0
Report V3           10             0
Leaves              0              0
--------------------------------------------------------------------------------
General Host Statistics
--------------------------------------------------------------------------------
Bad Length        : 0
Bad Checksum      : 0
Unknown Type      : 0
Bad Receive If    : 0
Rx Non Local      : 0
Rx Wrong Version  : 0
Policy Drops      : 0
No Router Alert   : 0
Rx Bad Encodings  : 0
Local Scope Pkts  : 0
Resvd Scope Pkts  : 0
MCAC Policy Drops : 0
==================================================
*B:Dut-C#
```

status

Syntax **status**

Context show>router>igmp

Description This command displays IGMP status information.

If IGMP is not enabled, the following message appears:

```
A:NYC# show router igmp status
MINOR: CLI IGMP is not configured.
A:NYC#
```

Output IGMP Status Output

The following table provides IGMP status field descriptions.

Table 8 **IGMP Status Fields**

Label	Description
Admin State	Displays the administrative status of IGMP.
Oper State	Displays the current operating state of this IGMP protocol instance on this router.
Query Interval	The frequency at which IGMP query packets are transmitted.
Last Member Query Interval	The maximum response time inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages.
Query Response Interval	The maximum query response time advertised in IGMPv2 queries.
Robust Count	Displays the number of times the router will retry a query.

Sample Output

```
*A:ALA-BA# show router 100 igmp status
===============================================================================
IGMP Status
===============================================================================
Admin State                          : Up
Oper State                           : Up
Query Interval                       : 1024
Last Member Query Interval           : 1024
Query Response Interval              : 1023
Robust Count                         : 10
===============================================================================
*A:ALA-BA#
```

tunnel-interface

Syntax **tunnel-interface**

Context show>router>igmp

Description This command displays tunnel interface information.

Output

Output Sample

```
*A:Dut-C# show router igmp tunnel-interface
===============================================================================
IGMP Tunnel-Interfaces
```

```
===============================================================================
LSP/LDP         Type        SenderAddr      IfIndex          AdmState  OperState
-------------------------------------------------------------------------------
1               ldp         10.20.1.3       74218            Up        Up
2               ldp         10.20.1.3       74219            Up        Up
3               ldp         10.20.1.3       74220            Up        Up
4               ldp         10.20.1.3       74221            Up        Up
5               ldp         10.20.1.3       74222            Up        Up
-------------------------------------------------------------------------------
Interfaces : 5
===============================================================================
```

3.4.2.2 Clear Commands

database

Syntax **database** [**group** *grp-ip-address*] [**source** *src-ip-address*]

database interface {*ip-int-name* **|** *ip-address*} [**group** *grp-ip-address*] [**source** *src-ip-address*]

database host *ip-address* [**group** *grp-ip-address*] [**source** *src-ip-address*]

database host all [**group** *grp-ip-address*] [**source** *src-ip-address*]

database group-interface *interface-name* [**fwd-service** *service-id*] [**group** *grp-ip-address*] [**source** *src-ip-address*]

database group-interface all

Context clear>router>igmp

Description This command clears IGMP or PIM database statistics on a specified interface or IP address.

Parameters **group** *grp-ip-address* — Clears the multicast group address (IPv4/IPv6) or zero in the specified address group.

source *src-ip-address* — Clears the IGMP database from the specified source IP address.

interface *ip-int-name* — Clears the IGMP database on the specified interface.

interface *ip-address* — Clears the IGMP database on the specified IP address.

host *ip-address* — Clears the IGMP database on the specified host.

host all — Clears the IGMP database on all hosts.

group-interface *interface-name* — Clears the IGMP database on the specified group interface.

group-interface all — Clears the IGMP database on all group interfaces.

statistics

Syntax **statistics group-interface** [**fwd-service** *service-id*] *ip-in-name*
statistics group-interface all
statistics host *ip-address*
statistics host all
statistics [**interface** *ip-int-name* | *ip-address*]

Context clear>router>igmp

Description This command clears IGMP statistics on a specified interface or IP address.

Note: Interface and group/source cannot be specified at the same time.

Parameters **group-interface** *interface-name* — Clears the IGMP statistics on the specified group interface.

group-interface all — Clears the IGMP statistics on all group interfaces.

fwd-service *service-id* — [1to 2148007980] | <svc-name:64 char max>

host *ip-address* — Clears the IGMP statistics on the specified host.

host all — Clears the IGMP statistics on all hosts.

interface *ip-int-name* — Clears the IGMP statistics on the specified interface.

interface *ip-address* — Clears the IGMP statistics on the specified IP address.

version

Syntax **version group-interface** [**fwd-service** *service-id*] *ip-in-name*
version group-interface all
version host *ip-address*
version host all
version [**interface** *ip-int-name* | *ip-address*]

Context clear>router>igmp

Description This command clears the IGMP version on a specified interface or IP address.

Parameters **group-interface** *interface-name* — Clears the IGMP version on the specified group interface.

group-interface all — Clears the IGMP version on all group interfaces.

fwd-service *service-id* — [1to 2148007980] | <svc-name:64 char max>

host *ip-address* — Clears the IGMP version on the specified host.

host all — Clears the IGMP version on all hosts.

interface *ip-int-name* — Clears the IGMP version on the specified interface.

interface *ip-address* — Clears the IGMP version on the specified IP address.

3.4.2.3 Debug Commands

group-interface

Syntax [**no**] **group-interface** [**fwd-service** *service-id*] [*ip-int-name*]

Context debug>router>igmp

Description This command enables debugging for IGMP group-interface.

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

Parameters **fwd-service** *service-id* — [1 to 2148007978]|<svc-name: 64 characters maximum>

ip-int-name — Debugs the information associated with the specified IP interface name.

Values IP interface address

host

Syntax [**no**] **host** [*ip-address*]
[**no**] **host** [**fwd-service** *service-id*] **group-interface** *ip-int-name*

Context debug>router>igmp

Description This command enables debugging for the IGMP host.

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

Parameters *ip-address* — Debugs the information associated with the specified IP address.

fwd-service *service-id* — [1 to 2148007978]|<svc-name: 64 characters maximum>

group-interface *ip-int-name* — Debugs the information associated with the specified IP interface name.

Values IP interface address

interface

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

Context debug>router>igmp

Description This command enables debugging for IGMP interfaces.

The **no** form of the command disables the IGMP interface debugging for the specifies interface name or IP address.

Parameters *ip-int-name* — Debugs the information associated with the specified IP interface name.

Values IP interface address

ip-address — Debugs the information associated with the specified IP address.

mcs

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

Context debug>router>igmp

Description This command enables debugging for IGMP multicast servers (MCS).

The **no** form of the command disables the IGMP interface debugging for the specifies interface name.

Parameters *ip-int-name* — Debugs the information associated with the specified IP interface name.

Values IP interface address

misc

Syntax [**no**] **misc**

Context debug>router>igmp

Description This command enables debugging for IGMP miscellaneous.

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

Output

Sample Output

```
A:ALA-CA# debug router 100 igmp misc
*A:ALA-CA# show debug
debug
    router "100"
        igmp
            misc
        exit
    exit
```

```
exit
*A:ALA-CA#
```

packet

Syntax

packet [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] [*ip-int-name* | *ip-address*] [**mode** {**dropped-only** | **ingr-and-dropped** | **egr-ingr-and-dropped**}]

packet [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] [**mode** {**dropped-only** | **ingr-and-dropped** | **egr-ingr-and-dropped**}] **group-interface** *ip-int-name*

packet [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] **host** *ip-address* [**mode** {**dropped-only** | **ingr-and-dropped** | **egr-ingr-and-dropped**}]

no packet [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] [*ip-int-name* | *ip-address*]

no packet [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] **group-interface** *ip-int-name*

no packet [**query** | **v1-report** | **v2-report** | **v3-report** | **v2-leave**] **host** *ip-address*

Context debug>router>igmp

Description This command enables/disables debugging for IGMP packets.

Parameters

query — Specifies to log the IGMP group- and source-specific queries transmitted and received on this interface.

v1-report — Specifies to debug IGMP V1 reports transmitted and received on this interface.

v2-report — Specifies to debug IGMP V2 reports transmitted and received on this interface.

v3-report — Specifies to debug IGMP V3 reports transmitted and received on this interface.

v2-leave — Specifies to debug the IGMP Leaves transmitted and received on this interface.

ip-int-name — Debugs the information associated with the specified IP interface name.

Values IP interface address

ip-address — Debugs the information associated with the specified IP address.

4 MLD

4.1 MLD Overview

Multicast Listener Discovery (MLD) is the IPv6 version of IGMP and belongs to the Source Specific Multicast (SSM) service model (see IPv6 PIM models for more information). The purpose of MLD is to allow each IPv6 router to discover the presence of multicast listeners on its directly attached links, and to discover specifically which multicast groups are of interest to those neighboring nodes.

MLD is a sub-protocol of ICMPv6. MLD message types are a subset of the set of ICMPv6 messages, and MLD messages are identified in IPv6 packets by a preceding Next Header value of 58. All MLD messages are sent with a link-local IPv6 source address, a Hop Limit of 1, and an IPv6 Router Alert option in the Hop-by-Hop Options header.

4.1.1 MLDv1

Similar to IGMPv2, MLDv1 reports only include the multicast group addresses that listeners are interested in, and do not include the source addresses. In order to work with the PIM-SSM model, a similar SSM translation function is required when MLDv1 is used.

SSM translation allows an IGMPv2 device to join an SSM multicast network through the router that provides such a translation capability. Currently SSM translation can done at a box level, but this does not allow a per-interface translation to be specified. SSM translation per interface offers the ability to have a same (*,G) mapped to two different (S,G) on two different interfaces to provide flexibility.

4.1.2 MLDv2

MLDv2 is backward compatible with MLDv1 and adds the ability for a node to report interest in listening to packets with a particular multicast group only from specific source addresses or from all sources except for specific source addresses.

4.2 Configuring MLD with CLI

This section provides information to configure MLD using the command line interface.

4.2.1 MLD Configuration Overview

The routers use MLD to manage membership for a given multicast session. MLD is not enabled by default. When enabled, at least one interface must be specified in the MLD context as MLD is an interface function. Creating an interface enables MLD. Traffic can only flow away from the router to an MLD interface and to and from a PIM interface. A router directly connected to a source must have PIM enabled on the interface to that source. The traffic travels in a network from PIM interface to PIM interface and arrives finally on an MLD enabled interface.

The MLD CLI context allows you to specify an existing IP interface and modify the interface-specific parameters. Static MLD group memberships can be configured to test multicast forwarding without a receiver host. When MLD static group membership is 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. When a host wants to receive multicast sessions it sends a join message for each multicast group it wants to join. Then, a leave message may be sent for each multicast group it no longer wishes to participate with.

A multicast router keeps a list of multicast group memberships for each attached network, and an interval timer for each membership. Hosts issue a Multicast Group Membership Report when they want to receive a multicast session. The reports are sent to all multicast routers.

4.2.2 Basic MLD Configuration

Perform the following basic multicast configuration tasks:

- Enable MLD (required)
- Configure MLD interfaces (required)
- Specify MLD version on the interface (optional)

- Configure static (S,G)/(*,G) (optional)
- Configure SSM translation (optional)

4.2.3 Configuring MLD Parameters

4.2.3.1 Enabling MLD

Use the following CLI syntax to enable MLD.

CLI Syntax: `config>router# mld`

The following example displays the detailed output when MLD is enabled:

```
A:LAX>config>router>mld# info detail
----------------------------------------------
        no grp-if-query-src-ip
        query-interval 125
        query-last-listener-interval 1
        query-response-interval 10
        robust-count 2
        no shutdown
----------------------------------------------
A:LAX>config>router>mld#
```

4.2.3.2 Configuring an MLD Interface

To configure an MLD interface:

CLI Syntax:

```
config>router# mld
      interface ip-int-name
           import policy-name
           max-groups value
           version version
           no shutdown
```

Use the following CLI syntax to configure MLD interfaces:

Example:

```
config>router#
config>router>mld# interface "lax-vls"
config>router>mld>if? no shutdown
config>router>mld>if# exit
config>router>mld# interface "p1-ix"
```

```
config>router>mld>if? no shutdown
config>router>mld>if# exit
config>router>mld# interface "lax-sjc"
config>router>mld>if? no shutdown
config>router>mld>if# exit
```

The following example displays the MLD configuration:

```
A:LAX>config>router>mld# info
----------------------------------------------
        interface "lax-sjc"
        exit
        interface "lax-vls"
        exit
        interface "p1-ix"
        exit
----------------------------------------------
A:LAX>config>router>mld# exit
```

4.2.3.3 Configuring Static Parameters

To add an MLD static multicast source:

```
config>router# mld
interface ip-int-name
no shutdown
static
group grp-ipv6-address
source ipv6-address
```

Use the following CLI syntax to configure static group addresses and source addresses for the SSM translate group ranges:

Example:

```
config>router>mld# interface lax-vls
config>router>mld>if# static
config>router>mld>if>static# group ff05:db8:1
config>router>mld>if>static>group# source
 2001:db8:2016:10ff::4
```

The following example displays the configuration:

```
A:LAX>config>router>mld# info
----------------------------------------------
        interface "lax-sjc"
        exit
        interface "lax-vls"
            static
                group ff05:db8:1ff05:db8:1
                    source 2001:db8:2016:10ff::4
```

```
                exit
            exit
        exit
        interface "p1-ix"
        exit
----------------------------------------------
A:LAX>config>router>mld#
```

To add an MLD static starg entry:

CLI Syntax:
```
config>router# mld
      interface ip-int-name
            no shutdown
            static
                  group grp-ipv6-address
                        starg
```

Use the following CLI syntax to configure static group addresses and add a static (*,G) entry:

Example:
```
config>router>mld# interface lax-sjc
config>router>mld>if# static
config>router>mld>if>static# group ff06:db8:1
config>router>mld>if>static>group# starg
```

The following example displays the configuration:

```
A:LAX>config>router>mld# info
----------------------------------------------
        interface "lax-sjc"
            static
                group ff06:db8:1
                    starg
                exit
            exit
        exit
        interface "lax-vls"
            static
                group ff05:db8:1
                    source 2001:db8:2016:10ff::4
                exit
            exit
        exit
        interface "p1-ix"
        exit
----------------------------------------------
A:LAX>config>router>mld#
```

4.2.3.4 Configuring SSM Translation

To configure MLD parameters:

CLI Syntax:
```
config>router# mld
      ssm-translate
            grp-range start end
                  source ipv6-address
```

The following example displays the command usage to configure MLD parameters.

Note: The group range will not be created until the source is specified.

Example:
```
config>router# mld
config>router>mld# ssm-translate
config>router>mld>ssm# grp-range ff0e::db8:9 ff0e::db8:c
config>router>mld>ssm>grp-range# source 2001:db8::1
```

The following example displays the SSM translation configuration:

```
A:LAX>config>router>mld# info
----------------------------------------------
        ssm-translate
            grp-range ff0::db8:9 ff0e:db8:c
                source 2001:db8::1
            exit
        exit
        interface "lax-sjc"
            static
                group ff0:db8:1
                    starg
                exit
            exit
        exit
        interface "lax-vls"
            static
                group ff0:db8:1
                    source 2001:db8:2016:10ff::4
                exit
            exit
        exit
        interface "p1-ix"
        exit
----------------------------------------------
A:LAX>config>router>mld# exit
```

4.2.4 Disabling MLD

Use the following CLI syntax to disable MLD.

CLI Syntax:
```
config>router#
     mld
          shutdown
```

The following example displays the command usage to disable MLD.

Example:
```
config>router# mld
config>router>mld# shutdown
```

4.3 MSDP Configuration Command Reference

4.3.1 Command Hierarchies

- Configuration Commands

4.3.1.1 Configuration Commands

config
- **— router**
  - **—** [**no**] **msdp**
    - **—** [**no**] **active-source-limit** *number*
    - **—** [**no**] **data-encapsulation**
    - **— export** *policy-name* [*policy-name*]
    - **— no export**
    - **—** [**no**] **group** *group-name*
      - **— active-source-limit** *number*
      - **— no active-source-limit**
      - **— export** *policy-name* [*policy-name*]
      - **— no export**
      - **— import** *policy-name* [*policy-name*]
      - **— no import**
      - **— local-address** *address*
      - **— no local-address**
      - **— mode** {**mesh-group** | **standard**}
      - **—** [**no**] **peer** *peer-address*
        - **— active-source-limit** *number*
        - **— no active-source-limit**
        - **— authentication-key** [*authentication-key* | *hash-key*] [**hash** | **hash2**]
        - **— no authentication-key**
        - **—** [**no**] **default-peer**
        - **— export** *policy-name* [*policy-name*]
        - **— no export**
        - **— import** *policy-name* [*policy-name*]
        - **— no import**
        - **— local-address** *address*
        - **— no local-address**
        - **— receive-msdp-msg-rate** *number* **interval** *seconds* [**threshold** *number*]
        - **— no receive-msdp-msg-rate**
        - **—** [**no**] **shutdown**
      - **— receive-msdp-msg-rate** *number* **interval** *seconds* [**threshold** *number*]
      - **— no receive-msdp-msg-rate**
      - **—** [**no**] **shutdown**
    - **— import** *policy-name* [*policy-name*]

— **no import**
— **local-address** *address*
— **no local-address**
— [**no**] **peer** *peer-address*
  — **active-source-limit** *number*
  — **no active-source-limit**
  — **authentication-key** [*authentication-key* | *hash-key*] [**hash** | **hash2**]
  — **no authentication-key**
  — [**no**] **default-peer**
  — **export** *policy-name* [*policy-name*]
  — **no export**
  — **import** *policy-name* [*policy-name*]
  — **no import**
  — **local-address** *address*
  — **no local-address**
  — **receive-msdp-msg-rate** *number* **interval** *seconds* [**threshold** *number*]
  — **no receive-msdp-msg-rate**
  — [**no**] **shutdown**
— **receive-msdp-msg-rate** *number* **interval** *seconds* [**threshold** *number*]
— **no receive-msdp-msg-rate**
— **rpf-table** {**rtable-m** | **rtable-u** | **both**}
— **no rpf-table**
— **sa-timeout** *seconds*
— **no sa-timeout**
— [**no**] **shutdown**
— [**no**] **source** *prefix/mask*
    — **active-source-limit** *number*
    — **no active-source-limit**

4.3.2 Command Descriptions

4.3.2.1 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.

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.

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

Default no msdp

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), effectively controlling the number of active sources that can be stored on the system.

The **no** form of this command sets no limit on the number of source active records.

Default no active-source-limit

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

Values 0 to 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>group>peer

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.

After 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.

The **no** form of this command sets no limit on the number of MSDP and source active limit messages that will be accepted.

Default no receive-msdp-msg-rate

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 to 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 to 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 particularly of use during at system startup and initialization.

Values 1 to 1000000

Default 0

shutdown

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

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

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 and 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

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.

The **no** form of the command configures acceptance of all MSDP messages and disables the MD5 signature option authentication key.

Default no authentication-key

Parameters *authentication-key* — The authentication key. Allowed values are any string up to 256 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), enclose the entire string in quotation marks (“ ”).

hash-key — The hash key. The key can be any combination of ASCII characters up to 451 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** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

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*]
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).

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.

The **no** form of the command applies no export policies and all SA entries are announced.

Default no export

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

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.

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.

import

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

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.

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 group's policy.

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

The **no** form of the command applies no import policies and all source active messages are allowed.

Default no import

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

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. 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.

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 sessions 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 sessions will be terminated.

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

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

The **no** form 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.

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.

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.

Default mode standard

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.

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.

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, if valid, 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 will be removed. Whenever a new peering session is created or a peering session is lost, an event message should be generated.

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.

rpf-table

Syntax **rpf-table** {**rtable-m | rtable-u | both**}
no rpf-table

Context 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 one of the following options:

- use the unicast route table only
- use the multicast route table only
- use both the route tables

Default rpf-table rtable-u

Parameters **rtable6-m** — Specifies that only the multicast route table will be used by the multicast protocol (PIM) for IPv4 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 IPv4 RPF checks. This route table will contain routes submitted by all the unicast routing protocols.

both — Will always look up 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. Rtable-m is checked before rtable6-u.

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, 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 than 90) could be useful to prevent instabilities 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 to 600

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.

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.

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.

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 to 32 (mask length), 0.0.0.0 to 255.255.255.255 (dotted decimal)

4.4 Show, Clear, and Debug Command Reference

4.4.1 Command Hierarchies

- Show Commands
- Clear Commands

4.4.1.1 Show Commands

show
- **— router**
  - **— mld**
    - **— group** [*grp-ipv6-address*] [**hosts** | **interfaces** | **saps**]
    - **— group summary** [**hosts** | **interfaces** | **saps**]
    - **— group-interface** [**fwd-service** *service-id*] [*ip-int-name*] [**detail**] [**group**] [*grp-ipv6-address*]
    - **— hosts** [**detail**] [**fwd-service** *service-id*] [**grp-interface** *ip-int-name*]
    - **— hosts** [**host** *ipv6-address*] [**group** *grp-ipv6-address*] [**detail**]
    - **— hosts summary**
    - **— interface** [*ip-int-name* | *ip-address*] [**group**] [*grp-ipv6-address*] [**detail**]
    - **— ipsec-interface**
    - **— ipsec-interface** *ip-int-name* [**group** *grp-ipv6-address*]
    - **— ipsec-interface gateway-name** *gw-name* [**remote-address** *ip-address* | *ipv6-address*] [**port** *port-id*] [**sa-id** *sa-id*]
    - **— ipsec-interface static-tunnel-name** *tunnel-name* [**sa-id** *sa-id*]
    - **— ssm-translate** *interface-name*
    - **— static** [*ip-int-name* | *ipv6-address*]
    - **— statistics** [*ip-int-name* | *ipv6-address*]
    - **— statistics** [**ipsec-interface** *ip-int-name*]
      - **— group-interface** [**fwd-service** *service-id*] [*ip-int-name*]
      - **— host** [*ipv6-address*]
    - **— status**

4.4.1.2 Clear Commands

clear
- **— router**
  - **— mld**
    - **— database** [**group** *grp-ipv6-address* [**source** *src-ip-address*]]
    - **— database interface** {*ip-int-name* | *ipv6-address*} [**group** *grp-ipv6-address* [**source** *src-ipv6-address*]]
    - **— database ipsec-interface** *ip-int-name* [**group** *grp-ipv6-address* [**source** *src-ipv6-address*]]
    - **— database host** *ipv6-address* [**group** *grp-ipv6-address* [**source** *src-ipv6-address*]]
    - **— database host all** [**group** *grp-ipv6-address* [**source** *src-ipv6-address*]]
    - **— database group-interface** *interface-name* [**fwd-service** *service-id*] [**group** *grp-ipv6-address* [**source** *src-ipv6-address*]]
    - **— database group-interface all**
    - **— statistics group-interface** [**fwd-service** *service-id*] *ip-int-name*
    - **— statistics group-interface all**
    - **— statistics host** *ipv6-address*
    - **— statistics host all**
    - **— statistics** [**interface** *ip-int-name* | *ipv6-address*]
    - **— statistics ipsec-interface** *ip-int-name*
    - **— version group-interface** [**fwd-service** *service-id*] *ip-int-name*
    - **— version group-interface all**
    - **— version host** *ipv6-address*
    - **— version host all**
    - **— version** [**interface** *ip-int-name* | *ip-address*]

4.4.2 Command Descriptions

4.4.2.1 Show Commands

The command outputs in the following section are examples only; actual displays may differ depending on supported functionality and user configuration.

mld

Syntax **mld**

Context show>router

Description This command enables the context to show MLD entities.

group

Syntax **group** [*grp-ipv6-address*] [**hosts | interfaces | saps**]
group summary [**hosts | interfaces | saps**]

Context show>router>mld

Description This command displays the multicast group and (S,G) addresses. If no *grp-ipv6-address* parameters are specified, then all MLD group, (*,G) and (S,G) addresses are displayed.

Parameters *grp-ipv6-address* — Displays specific multicast group addresses.

hosts — Displays hosts for the multicast group address.

interfaces — Displays interfaces for the multicast group address.

saps — Displays SAPs for the multicast group address.

Output MLD Group Output

Sample Output

```
*A:Dut-A# show router mld group
===============================================================================
MLD Interface Groups
===============================================================================
(*,ff04:db8:224:100:0:0)                                      UpTime: 0d
00:10:09
     Fwd List  : intf_to_ixia
(*,ff04:db8:224:100:0:1)                                      UpTime: 0d
00:10:09
     Fwd List  : intf_to_ixia
(*,ff04:db8:224:100:0:2)                                      UpTime: 0d
00:10:09
     Fwd List  : intf_to_ixia
(*,ff04:db8:224:100:0:3)                                      UpTime: 0d
00:10:09
     Fwd List  : intf_to_ixia
(*,ff04:db8:224:100:0:4)                                      UpTime: 0d
00:10:09
     Fwd List  : intf_to_ixia
-------------------------------------------------------------------------------
Entries : 5
===============================================================================
MLD Host Groups
===============================================================================
No Matching Entries
===============================================================================
MLD SAP Groups
===============================================================================
No Matching Entries
===============================================================================
*A:Dut-A#

*A:Dut-A# show router mld group summary
===============================================================================
MLD Interface Groups Summary                               Nbr Fwd    Nbr Blk
```

```
===============================================================================
(*,ff04:db8:224:100:0:0) 1          0
(*,ff04:db8:224:100:0:1) 1          0
(*,ff04:db8:224:100:0:2) 1          0
(*,ff04:db8:224:100:0:3) 1          0
(*,ff04:db8:224:100:0:4) 1          0
-------------------------------------------------------------------------------
Entries : 5
===============================================================================
MLD Host Groups Summary                                  Nbr Fwd    Nbr Blk
===============================================================================
No Matching Entries
===============================================================================
MLD SAP Groups Summary                                   Nbr Fwd    Nbr Blk
===============================================================================
No Matching Entries
===============================================================================
*A:Dut-A#

*A:Dut-A# show router mld group ff04:db8:224:100:0:0
===============================================================================
MLD Interface Groups
===============================================================================
(*,ff04:db8:224:100:0:0)                                    UpTime: 0d
00:10:24
     Fwd List  : intf_to_ixia
-------------------------------------------------------------------------------
Entries : 1
===============================================================================
MLD Host Groups
===============================================================================
No Matching Entries
===============================================================================
MLD SAP Groups
===============================================================================
No Matching Entries
===============================================================================
*A:Dut-A#
```

Table 9 describes the output fields for MLD group information.

Table 9 MLD Group Information Output Fields

Label	Description
MLD Groups	Displays the IP multicast sources corresponding to the IPv6 multicast groups.
Fwd List	Displays the list of interfaces in the forward list.
Blk List	Displays the list of interfaces in the blocked list.

group-interface

Syntax **group-interface** [**fwd-service** *service-id*] [*ip-int-name*] [**detail**] [**group**] [*grp-ipv6-address*]

Context show>router>mld

Description This command displays MLD group-interface information.

Parameters **fwd-service** *service-id* — [1 to 2148007980] | <svc-name:64 char max>

ip-int-name — IP interface name. A string up to 32 characters.

detail — Displays detailed information.

group — Displays information from the group IPv6 address.

grp-ipv6-address — Group IPv6 address.

hosts

Syntax **hosts** [**detail**] [**fwd-service** *service-id*] [**grp-interface** *ip-int-name*]
hosts [**host** *ipv6-address*] [**group** *grp-ipv6-address*] [**detail**]
hosts summary

Context show>router>mld

Description This command shows MLD hosts information.

Parameters *grp-ipv6-address* — Specifies the group IPv6 address.

service-id — [1 to 2148007980]| <svc-name: 64 characters maximum>

ip-int-name — IP interface name. A string up to 32 characters.

ipv6-address — IPv6 address.

Output The following output is an example of MLD host information.

Sample Output

```
A:Dut-C# show router mld hosts
===============================================================================
MLD Hosts
===============================================================================
Host                                          Subscriber
   Oper-State Oper-Ver Fwd-Svc Num-Groups Group-Interface
-------------------------------------------------------------------------------
192:168:9::1                                  oli_1
   Up         2        1       0               grp-1-2-1
192:168:9::2                                  oli_1
   Up         2        1       0               grp-1-2-1
-------------------------------------------------------------------------------
Hosts : 2
===============================================================================
A:Dut-C#
```

```
A:Dut-C# show router mld hosts detail
===============================================================================
MLD Host 192:168:9::1
===============================================================================
Oper Status      : Up         MacAddress     : 00:00:11:00:00:01
Oper Version     : 2          Subscriber     : oli_1
NumGrps          : 0          GrpItf         : grp-1-2-1
MaxGrps Till Now : 0          MLD Policy     : oli1
PPPoE SessionId  : N/A        Next Query Time: 0d 00:00:06
FwdSvcId         : 1          MaxSrcs Allowed: No Limit
MaxGrps Allowed  : No Limit   MaxGrpSrcs All*: No Limit
Qry Interval     : 125        Qry Last Lstnr*: 1
Qry Resp Interval: 10         Router Alert C*: Enabled
Bonding Conn Idx : 0          Bonding Id     : None
===============================================================================
MLD Host 192:168:9::2
===============================================================================
Oper Status      : Up         MacAddress     : 00:00:11:00:00:02
Oper Version     : 2          Subscriber     : oli_1
NumGrps          : 0          GrpItf         : grp-1-2-1
MaxGrps Till Now : 0          MLD Policy     : oli1
PPPoE SessionId  : N/A        Next Query Time: 0d 00:00:06
FwdSvcId         : 1          MaxSrcs Allowed: No Limit
MaxGrps Allowed  : No Limit   MaxGrpSrcs All*: No Limit
Qry Interval     : 125        Qry Last Lstnr*: 1
Qry Resp Interval: 10         Router Alert C*: Enabled
Bonding Conn Idx : 0          Bonding Id     : None
-------------------------------------------------------------------------------
Hosts : 2
===============================================================================
* indicates that the corresponding row element may have been truncated.
A:Dut-C#
```

interface

Syntax **interface** [*ip-int-name* | *ipv6-address*] [**group**] [*grp-ipv6-address*] [**detail**]

Context show>router>mld

Description This command displays MLD interface information.

Parameters *ip-int-name* — Displays the information associated with the specified IPv6 interface name.

ipv6-address — Displays the information associated with the specified IPv6 address.

group *grp-ipv6-address* — Displays IPv6 multicast group address for which this entry contains information.

detail — Displays detailed IPv6 interface information along with the source group information learned on that interface.

Output MLD Interface Output

Table 10 displays MLD field descriptions.

Table 10 **MLD Fields**

Label	Description
Interface	Displays the interfaces that participate in the MLD protocol.
Adm Admin Status	Displays the administrative state for the MLD protocol on this interface.
Oper Oper Status	Displays the current operational state of MLD protocol on the interface.
Querier	Displays the address of the MLD querier on the IP subnet to which the interface is attached.
Querier Up Time	Displays the time since the querier was last elected as querier.
Querier Expiry Timer	Displays the time remaining before the querier ages out. If the querier is the local interface address, the value will be zero.
Cfg/Opr Version Admin/Oper version	Cfg — The configured version of MLD running on this interface. For MLD to function correctly, all routers on a LAN must be configured to run the same version of MLD on that LAN. Opr — The operational version of MLD running on this interface.
Num Groups	The number of multicast groups which have been learned by the router on the interface.
Policy	Displays the policy that is to be applied on the interface.
Group Address	Displays the IP multicast group address for which this entry contains information.

Sample Output

```
*A:Dut-A# show router mld interface
===============================================================================
MLD Interfaces
===============================================================================
Interface              Adm  Oper Cfg/Opr          Num Policy
    Querier                       Version          Groups
-------------------------------------------------------------------------------
intf_to_ixia           Up   Up   2/2              5 none
    fe0:db8:4403:1ff:fe01:3
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
*A:Dut-A#
```

ipsec-interface

Syntax **ipsec-interface**
ipsec-interface *ip-int-name* [**group** *grp-ipv6-address*]
ipsec-interface gateway-name *gw-name* [**remote-address** *ip-address* | *ipv6-address*] [**port** *port-id*] [**sa-id** *sa-id*]
ipsec-interface static-tunnel-name *tunnel-name* [**sa-id** *sa-id*]

Context show>router>mld

Description This command displays information about the MLD states over IPsec tunnels.

Parameters *ip-int-name* — Specifies the dynamic name for the MLD-enabled child_SA.

grp-ipv6-address — Displays IPv6 multicast group address for which this entry contains information.

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
- multicast group IPv6 address

gw-name — Specifies the IPsec gateway name up to 32 characters.

ip-address — Displays the information associated with the specified IP address.

ipv6-address — Displays the information associated with the specified IPv6 address.

port-id — Specifies the peer's UDP port.

Values 0 to 4294967295

sa-id — Specifies the child_SA ID.

Values 0 to 4294967295

tunnel-name — Specifies the IPsec static tunnel name up to 32 characters.

Output The following output displays an example of MLD IPsec interface information. The interface name in the output is the dynamic name for an MLD-enabled child_sa. There is a corresponding MLD interface name in the **show>ipsec>gateway** *name* **tunnel** *tunnel* output

Sample Output

```
*A:DUT-A# show router 40 mld ipsec-interface "ipsec-if-1583392"
===============================================================================
mld ipsec dynamic tunnel interfaces detail
===============================================================================
name          : ipsec_gw_1040_1
remote-address: 3ffe::900:1
port          : 500                     sa-id         : 1
index         : 1583392                 state         : in-service
version       : 2                       group count   : 0
querier up    : 11384                   querier expiry: 0
```

```
next query    : 56                      interface name: ipsec-if-1583392
querier       : fe80::6e:9c56:9651:5829
===============================================================================
```

ssm-translate

Syntax **ssm-translate**
ssm-translate interface *interface-name*

Context show>router>mld

Description This command displays MLD SSM translate configuration information.

Parameters *interface-name* — Specifies the IP interface name up to 32 characters in length.

Output MLD Interface Output

The following table provides MLD field descriptions.

Table 11 **MLD Fields**

Label	Description
Start Address End Address	Displays the address ranges of the multicast groups for which this router can be an RP.
Source Address	Displays the unicast address that sends data on an interface.
Interface	Displays the interface name.
SSM Translate Entries	Displays the total number of SSM translate entries.

Sample Output

```
*A:ALA-BA# show router mld static
===============================================================================
MLD SSM Translate Entries
===============================================================================
Start Address       : ff0e::db8:9
End Address         : ff0e::db8:c
   Source Address   : 2001:db8::1

Start Address       : ff04:db8:2
End Address         : ff04:db8:10
   Source Address   : 2001:db8:3:4:5:6:7:8
       Interface    : lax-vls

Start Address       : ff0e:db8:db8:9
End Address         : ff0e:db8:db8:c
   Source Address   : 2001:db8::1
       Interface    : lax-vls
-------------------------------------------------------------------------------
```

```
SSM Translate Entries : 3
===============================================================================
*A:ALA-BA#
```

static

Syntax **static** [*ip-int-name* | *ipv6-address*]

Context show>router>mld

Description This command displays static MLD, (*,G) and (S,G) information.

Parameters *ip-int-name* — Only displays the information associated with the specified IP interface name.

ipv6-address — Only displays the information associated with the specified IPv6 address.

Output Static MLD Output

The following table provides static MLD field descriptions.

Table 12 **MLD Static Fields**

Label	Description
Source	Displays entries which represents a source address from which receivers are interested/not interested in receiving multicast traffic.
Group	Displays the IPv6 multicast group address for which this entry contains information.
Interface	Displays the interface name.

Sample Output

```
*A:ALA-BA# show router mld static
===============================================================================
Rtr Base MLD Static Group Sources
===============================================================================
Source                                    Interface
  Group Start                             [Group Step]
  [Group End]                             [Group Count]
-------------------------------------------------------------------------------
2001:db8:2016:10ff::4                     lax-vls
  ff05:db8:1
*                                         lax-vls
  ff06:db8:1
*                                         lax-vls
  ff01:db8:1                                 ::4:0
  ff01:db8:100:0                             64
3::1                                      lax-vls
```

```
  ff05:db8:1                               ::1
  ff05:db8:20                              32
*                                        lax-vls
  ff05:db8:2:1                             ::1
  ff05:db8:2:3ff                           1023
3::1                                     lax-vls
  ff05:db8:3:0                             ::64
  ff05:db8:4:0                             656
3::2                                     lax-vls
  ff05:db8:3:0                             ::64
  ff05:db8:4:0                             656
4::1                                     flax-vlsoo
  ff05:db8:3:0                             ::64
  ff05:db8:4:0                             656
5::1                                     lax-vls
  ff05:db8:3:0                             ::64
  ff05:db8:4:0                             656
-------------------------------------------------------------------------------
Static (*,G)/(S,G) Entries : 9
===============================================================================
*A:ALA-BA#
```

statistics

Syntax **statistics** [*ip-int-name* | *ipv6-address*]
statistics ipsec-interface *ip-int-name*

Context show>router>mld

Description This command displays MLD statistics information.

Parameters *ip-int-name* — Displays information associated with the specified IP interface name up to 32 characters.

ipv6-address — Displays information associated with the specified IPv6 address.

ipsec-interface *ip-int-name* — Displays information associated with the specified dynamic name for the MLD-enabled child_SA.

Output MLD Statistics Output

Sample Output

```
*A:ALA-BA# show router mld statistics
==================================================
MLD Interface Statistics
==================================================
Message Type        Received       Transmitted
--------------------------------------------------
Queries             0              9
Report V1           0              0
Report V2           0              0
Dones               0              0
-------------------------------------------------------------------------------
General Interface Statistics
```

```
-------------------------------------------------------------------------------
Bad Length         : 0
Bad Checksum       : 0
Unknown Type       : 0
Bad Receive If     : 0
Rx Non Local       : 0
Rx Wrong Version   : 0
Policy Drops       : 0
No Router Alert    : 0
Rx Bad Encodings   : 0
Rx Pkt Drops       : 0
Local Scope Pkts   : 0
Resvd Scope Pkts   : 0
MCAC Policy Drops  : 0
-------------------------------------------------------------------------------
Source Group Statistics
-------------------------------------------------------------------------------
(S,G)              : 0
(*,G)              : 5
==================================================
*A:Dut-A#
```

The following table provides statistical MLD field descriptions.

Table 13 **MLD Statistics Fields**

Label	Description
MLD Interface Statistics	Lists the MLD statistics for a particular interface.
Message Type	Queries — The number of MLD general queries transmitted or received on this interface. Report — The total number of MLD V1 or V2 reports transmitted or received on this interface. Dones — The total number of MLD dones transmitted on this interface.
Received	Displays the total number of MLD packets received on this interface.
Transmitted	Displays the total number of MLD packets transmitted from this interface.
General Interface Statistics	Lists the general MLD statistics.
Bad Length	Displays the total number of MLD packets with bad length received on this interface.
Bad Checksum	Displays the total number of MLD packets with bad checksum received on this interface.

Table 13 **MLD Statistics Fields (Continued)**

Label	Description
Unknown Type	Displays the total number of MLD packets with unknown type received on this interface.
Bad Receive If	Displays the total number of MLD packets incorrectly received on this interface.
Rx Non Local	Displays the total number of MLD packets received from a non-local sender.
Rx Wrong Version	Displays the total number of MLD packets with wrong versions received on this interface.
Policy Drops	Displays the total number of MLD packets dropped by import policies on this interface.
No Router Alert	Displays the total number of MLD packets received on this interface which did not have the router alert flag set.
Rx Bad Encodings	Displays the total number of MLD packets with bad encodings received on this interface.
Rx Pkt Drops	Displays the total number of MLD receive packet drops on this interface.
Local Scope Pkts	Displays the total number of MLD packets with local scope received on this interface.
Resvd Scope Pkts	Displays the total number of MLD packets with reserved scope received on this interface.
MCAC Policy Drops	Displays the total number of MLD packets dropped by MCAC policies on this interface.

group-interface

Syntax **group-interface** [**fwd-service** *service-id*] [*ip-int-name*]

Context show>router>mld>statistics

Description This command displays MLD group interface statistics information.

Parameters *service-name* — Displays information associated with the specified service name.

ip-int-name — Displays information associated with the specified IP interface name.

host

Syntax **host** [*ipv6-address*]

Context show>router>mld>statistics

Description This command displays MLD host statistics information.

Parameters *ipv6-address* — Only displays the information associated with the specified IPv6 address.

status

Syntax **status**

Context show>router>mld

Description This command displays MLD status information.

If MLD is not enabled, the following message appears:

```
A:NYC# show router mld status
MINOR: CLI MLD is not configured.
A:NYC#
```

Output MLD Status Output

The following table provides MLD status field descriptions.

Table 14 **MLD Status Fields**

Label	Description
Admin State	Displays the administrative status of MLD.
Oper State	Displays the current operating state of this MLD protocol instance on this router.
Query Interval	The frequency at which MLD query packets are transmitted.
Last Listener Query Interval	The maximum response time inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages.
Query Response Interval	The maximum query response time advertised in MLDv2 queries.
Robust Count	Displays the number of times the router will retry a query.

Sample Output

```
*A:ALA-BA# show router mld status
===============================================================================
MLD Status
===============================================================================
Admin State                         : Up
Oper State                          : Up
Query Interval                      : 125
Last Listener Query Interval        : 1
Query Response Interval             : 10
Robust Count                        : 2
===============================================================================
*A:ALA-BA#
```

4.4.2.2 Clear Commands

mld

Syntax **mld**

Context clear>router

Description This command enables the context to clear and reset MLD entities.

database

Syntax
database [**group** *ipv6-address* [**source** *ipv6-address*]]
database interface {*ip-int-name* **|** *ipv6-address*]} [**group** *ipv6-address* [**source** *ipv6-address*]]
database ipsec-interface *ip-int-name* [**group** *ipv6-address* [**source** *ipv6-address*]]
database host *ipv6-address* [**group** *ipv6-address* [**source** *ipv6-address*]]
database host all [**group** *ipv6-address* [**source** *ipv6-address*]]
database group-interface *interface-name* [**fwd-service** *service-id*] [**group** *grp-ipv6-address* [**source** *ipv6-address*]]
database group-interface all

Context clear>router>mld

Description This command clears MLD database parameters.

Parameters
host *ipv6-address* — Clears the MLD database on the specified host.

host all — Clears the MLD database on all hosts.

interface *ip-int-name* — Clears database information for the specified MLD interface name.

interface *ipv6-address* — Clears database information for the specified MLD interface IPv6 address.

ipsec-interface *ip-int-name* — Clears database information for the specified dynamic name for the MLD-enabled child_SA.

group *ipv6-address* — Clears database information for the specified MLD group IPv6 address.

source *ipv6-address* — Clears database information for the specified MLD source IPv6 address.

statistics

Syntax
statistics group-interface [**fwd-service** *service-id*] *ip-int-name*
statistics group-interface all
statistics host *ipv6-address*
statistics host all
statistics [*ip-int-name* | *ipv6-address*]
statistics ipsec-interface *ip-int-name*

Context clear>router>mld

Description This command clears MLD statistics parameters.

Parameters
fwd-service *service-id* — [1to 2148007980] | <svc-name:64 char max>

group-interface *interface-name* — Clears the MLD statistics on the specified group interface.

group-interface all — Clears the MLD statistics on all group interfaces.

host all — Clears the MLD statistics on all hosts.

host *ipv6-address* — Clears the MLD statistics on the specified host.

ip-int-name — Clears statistics for the specified MLD interface name.

ipv6-address — Clears statistics for the specified MLD IPv6 address.

ipsec-interface *ip-int-name* — Clears statistics information for the specified dynamic name for the MLD-enabled child_SA.

version

Syntax
version group-interface [**fwd-service** *service-id*] *ip-int-name*
version group-interface all
version host *ipv6-address*
version host all
version [*ip-int-name* | *ipv6-address*]

Context clear>router>mld

Description This command clears MLD version parameters.

Parameters **group-interface** *interface-name* — Clears the MLD version on the specified group interface.

group-interface all — Clears the MLD version on all group interfaces.

fwd-service *service-id* — [1to 2148007980] | <svc-name:64 char max>

host *ipv6-address* — Clears the MLD version on the specified host.

host all — Clears the MLD version on all hosts.

ip-int-name — Clears version information for the specified MLD interface name.

ipv6-address — Clears version information for the specified MLD IPv6 address.

5 PIM

5.1 PIM Overview

PIM-SM leverages the unicast routing protocols that are used to create the unicast routing table, OSPF, IS-IS, BGP, and static routes. Because PIM uses this unicast routing information to perform the multicast forwarding function it is effectively IP protocol independent. Unlike DVMRP, PIM does not send multicast routing tables updates to its neighbors.

PIM-SM uses the unicast routing table to perform the Reverse Path Forwarding (RPF) check function instead of building up a completely independent multicast routing table.

PIM-SM only forwards data to network segments with active receivers that have explicitly requested the multicast group. PIM-SM in the ASM model initially uses a shared tree to distribute information about active sources. Depending on the configuration options, the traffic can remain on the shared tree or switch over to an optimized source distribution tree. As multicast traffic starts to flow down the shared tree, routers along the path determine if there is a better path to the source. If a more direct path exists, then the router closest to the receiver sends a join message toward the source and then reroutes the traffic along this path.

As stated above, PIM-SM relies on an underlying topology-gathering protocol to populate a routing table with routes. This routing table is called the Multicast Routing Information Base (MRIB). The routes in this table can be taken directly from the unicast routing table, or it can be different and provided by a separate routing protocol such as MBGP. Regardless of how it is created, the primary role of the MRIB in the PIM-SM protocol is to provide the next hop router along a multicast-capable path to each destination subnet. The MRIB is used to determine the next hop neighbor to whom any PIM join/prune message is sent. Data flows along the reverse path of the join messages. Thus, in contrast to the unicast RIB that specifies the next hop that a data packet would take to get to some subnet, the MRIB gives reverse-path information, and indicates the path that a multicast data packet would take from its origin subnet to the router that has the MRIB.

Note: For proper functioning of the PIM protocol, multicast data packets need to be received by the CPM CPU. Therefore CPM Filters and Management Access Filters must be configured to allow forwarding of multicast data packets.

5.1.1 PIM-SM Functions

PIM-SM functions in three phases:

5.1.1.1 Phase One

In this phase, a multicast receiver expresses its interest in receiving traffic destined for a multicast group. Typically it does this using IGMP or MLD, but other mechanisms might also serve this purpose. One of the receiver's local routers is elected as the DR for that subnet. When the expression of interest is received, the DR sends a PIM join message towards the RP for that multicast group. This join message is known as a (*,G) join because it joins group G for all sources to that group. The (*,G) join travels hop-by-hop towards the RP for the group, and in each router it passes through the multicast tree state for group G is instantiated. Eventually the (*,G) join either reaches the RP or reaches a router that already has (*,G) join state for that group. When many receivers join the group, their join messages converge on the RP and form a distribution tree for group G that is rooted at the RP. This is known as the RP tree and is also known as the shared tree because it is shared by all sources sending to that group. Join messages are resent periodically as long as the receiver remains in the group. When all receivers on a leaf-network leave the group, the DR will send a PIM (*,G) prune message towards the RP for that multicast group. However if the prune message is not sent for any reason, the state will eventually time out.

A multicast data sender starts sending data destined for a multicast group. The sender's local router (the DR) takes those data packets, unicast-encapsulates them, and sends them directly to the RP. The RP receives these encapsulated data packets, removes the encapsulation, and forwards them onto the shared tree. The packets then follow the (*,G) multicast tree state in the routers on the RP tree, being replicated wherever the RP tree branches, and eventually reaching all the receivers for that multicast group. The process of encapsulating data packets to the RP is called registering, and the encapsulation packets are known as PIM register packets.

At the end of phase one, multicast traffic is flowing encapsulated to the RP, and then natively over the RP tree to the multicast receivers.

5.1.1.2 Phase Two

In this phase, register-encapsulation of data packets is performed. However, register-encapsulation of data packets is unsuitable for the following reasons:

- Encapsulation and de-encapsulation can be resource intensive operations for a router to perform depending on whether or not the router has appropriate hardware for the tasks.
- Traveling to the RP and then back down the shared tree can cause the packets to travel a relatively long distance to reach receivers that are close to the sender. For some applications, increased latency is unwanted.

Although register-encapsulation can continue indefinitely, for these reasons, the RP will normally switch to native forwarding. To do this, when the RP receives a register-encapsulated data packet from source S on group G, it will normally initiate an (S,G) source-specific join towards S. This join message travels hop-by-hop towards S, instantiating (S,G) multicast tree state in the routers along the path. (S,G) multicast tree state is used only to forward packets for group G if those packets come from source S. Eventually the join message reaches S's subnet or a router that already has (S,G) multicast tree state, and then packets from S start to flow following the (S,G) tree state towards the RP. These data packets can also reach routers with (*,G) state along the path towards the RP - if so, they can short-cut onto the RP tree at this point.

While the RP is in the process of joining the source-specific tree for S, the data packets will continue being encapsulated to the RP. When packets from S also start to arrive natively at the RP, the RP will be receiving two copies of each of these packets. At this point, the RP starts to discard the encapsulated copy of these packets and it sends a register-stop message back to S's DR to prevent the DR unnecessarily encapsulating the packets. At the end of phase 2, traffic will be flowing natively from S along a source-specific tree to the RP and from there along the shared tree to the receivers. Where the two trees intersect, traffic can transfer from the shared RP tree to the shorter source tree.

Note: A sender can start sending before or after a receiver joins the group, and thus, phase two may occur before the shared tree to the receiver is built.

5.1.1.3 Phase Three

In this phase, the RP joins back towards the source using the shortest path tree. Although having the RP join back towards the source removes the encapsulation overhead, it does not completely optimize the forwarding paths. For many receivers the route via the RP can involve a significant detour when compared with the shortest path from the source to the receiver.

To obtain lower latencies, a router on the receiver's LAN, typically the DR, may optionally initiate a transfer from the shared tree to a source-specific shortest-path tree (SPT). To do this, it issues an (S,G) Join towards S. This instantiates state in the routers along the path to S. Eventually this join either reaches S's subnet or reaches a router that already has (S,G) state. When this happens, data packets from S start to flow following the (S,G) state until they reach the receiver.

At this point the receiver (or a router upstream of the receiver) will be receiving two copies of the data - one from the SPT and one from the RPT. When the first traffic starts to arrive from the SPT, the DR or upstream router starts to drop the packets for G from S that arrive via the RP tree. In addition, it sends an (S,G) prune message towards the RP. The prune message travels hop-by-hop instantiating state along the path towards the RP indicating that traffic from S for G should not be forwarded in this direction. The prune message is propagated until it reaches the RP or a router that still needs the traffic from S for other receivers.

By now, the receiver will be receiving traffic from S along the shortest-path tree between the receiver and S. In addition, the RP is receiving the traffic from S, but this traffic is no longer reaching the receiver along the RP tree. As far as the receiver is concerned, this is the final distribution tree.

5.1.2 Encapsulating Data Packets in the Register Tunnel

Conceptually, the register tunnel is an interface with a smaller MTU than the underlying IP interface towards the RP. IP fragmentation on packets forwarded on the register tunnel is performed based upon this smaller MTU. The encapsulating DR can perform path-MTU discovery to the RP to determine the effective MTU of the tunnel. This smaller MTU takes both the outer IP header and the PIM register header overhead into consideration.

5.1.3 PIM Bootstrap Router Mechanism

For proper operation, every PIM-SM router within a PIM domain must be able to map a particular global-scope multicast group address to the same RP. If this is not possible, then black holes can appear (this is where some receivers in the domain cannot receive some groups). A domain in this context is a contiguous set of routers that all implement PIM and are configured to operate within a common boundary.

The bootstrap router (BSR) mechanism provides a way in which viable group-to-RP mappings can be created and distributed to all the PIM-SM routers in a domain. Each candidate BSR originates bootstrap messages (BSMs). Every BSM contains a BSR priority field. Routers within the domain flood the BSMs throughout the domain. A candidate BSR that hears about a higher-priority candidate BSR suppresses its sending of further BSMs for a period of time. The single remaining candidate BSR becomes the elected BSR and its BSMs inform the other routers in the domain that it is the elected BSR.

It is adaptive, meaning that if an RP becomes unreachable, it will be detected and the mapping tables will be modified so the unreachable RP is no longer used and the new tables will be rapidly distributed throughout the domain.

5.1.4 PIM-SM Routing Policies

Multicast traffic can be restricted from certain source addresses by creating routing policies. Join messages can be filtered using import filters. PIM join policies can be used to reduce denial of service attacks and subsequent PIM state explosion in the router and to remove unwanted multicast streams at the edge of the network before it is carried across the core. Route policies are created in the **config>router>policy-options** context. Join and register route policy match criteria for PIM-SM can specify the following:

- Router interface or interfaces specified by name or IP address.
- Neighbor address (the source address in the IP header of the join and prune message).
- Multicast group address embedded in the join and prune message.
- Multicast source address embedded in the join and prune message.

Join policies can be used to filter PIM join messages so no *,G or S,G state will be created on the router.

Table 15 **Join Filter Policy Match Conditions**

Match Condition	Matches the:
Interface	RTR interface by name
Neighbor	The neighbors source address in the IP header
Group Address	Multicast Group address in the join/prune message
Source Address	Source address in the join/prune message

PIM register message are sent by the first hop designated router that has a direct connection to the source. This serves a dual purpose:

- Notifies the RP that a source has active data for the group
- Delivers the multicast stream in register encapsulation to the RP and its potential receivers.
- If no one has joined the group at the RP, the RP will ignore the registers.

In an environment where the sources to particular multicast groups are always known, it is possible to apply register filters at the RP to prevent any unwanted sources from transmitting multicast stream. You can apply these filters at the edge so that register data does not travel unnecessarily over the network towards the RP.

Table 16 **Register Filter Policy Match Conditions**

Match Condition	Matches the:
Interface	RTR interface by name
Group Address	Multicast Group address in the join/prune message
Source Address	Source address in the join/prune message

5.1.5 Reverse Path Forwarding Checks

Multicast implements a reverse path forwarding check (RPF). RPF checks the path that multicast packets take between their sources and the destinations to prevent loops. Multicast requires that an incoming interface is the outgoing interface used by unicast routing to reach the source of the multicast packet. RPF forwards a multicast packet only if it is received on an interface that is used by the router to route to the source.

If the forwarding paths are modified due to routing topology changes then any dynamic filters that may have been applied must be re-evaluated. If filters are removed then the associated alarms are also cleared.

5.1.6 Anycast RP for PIM-SM

The implementation of Anycast RP for PIM-SM environments enable fast convergence when a PIM rendezvous point (RP) router fails by allowing receivers and sources to rendezvous at the closest RP. It allows an arbitrary number of RPs per group in a single shared-tree protocol Independent Multicast-Sparse Mode (PIM-SM) domain. This is, in particular, important for triple play configurations that opt to distribute multicast traffic using PIM-SM, not SSM. In this case, RP convergence must be fast enough to avoid the loss of multicast streams which could cause loss of TV delivery to the end customer.

Anycast RP for PIM-SM environments is supported in the base routing/PIM-SM instance of the service router. This feature is supported in Layer 3-VPRN instances that are configured with PIM.

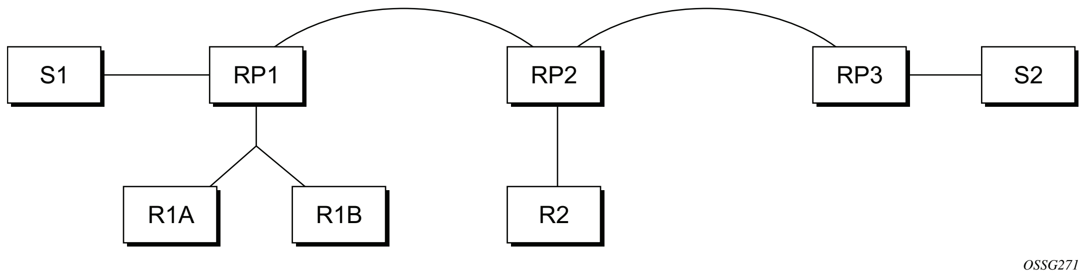
5.1.6.1 Implementation

The Anycast RP for PIM-SM implementation is defined in RFC 4610, *Anycast-RP Using Protocol Independent Multicast (PIM)*, and is similar to that described in RFC 3446, *Anycast Rendezvous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*, and extends the register mechanism in PIM so Anycast RP functionality can be retained without using Multicast Source Discovery Protocol (MSDP) (see Multicast in Virtual Private Networks).

The mechanism works as follows:

- An IP address is chosen to use as the RP address. This address is statically configured, or distributed using a dynamic protocol, to all PIM routers throughout the domain.
- A set of routers in the domain are chosen to act as RPs for this RP address. These routers are called the Anycast-RP set.
- Each router in the Anycast-RP set is configured with a loopback interface using the RP address.
- Each router in the Anycast-RP set also needs a separate IP address to be used for communication between the RPs.
- The RP address, or a prefix that covers the RP address, is injected into the unicast routing system inside of the domain.
- Each router in the Anycast-RP set is configured with the addresses of all other routers in the Anycast-RP set. This must be consistently configured in all RPs in the set.

Figure 1 Anycast RP for PIM-SM Implementation Example



Assume the scenario in Figure 1 is completely connected where R1A, R1B, and R2 are receivers for a group, and S1 and S2 send to that group. Assume RP1, RP2, and RP3 are all assigned the same IP address which is used as the Anycast-RP address (for example, the IP address is RPA).

Note: The address used for the RP address in the domain (the Anycast-RP address) must be different than the addresses used by the Anycast-RP routers to communicate with each other.

The following procedure is used when S1 starts sourcing traffic:

1. S1 sends a multicast packet.
2. The DR directly attached to S1 forms a PIM register message to send to the Anycast-RP address (RPA). The unicast routing system delivers the PIM register message to the nearest RP, in this case RP1A.
3. RP1 receives the PIM register message, de-encapsulates it, and sends the packet down the shared-tree to get the packet to receivers R1A and R1B.
4. RP1 is configured with RP2 and RP3's IP address. Because the register message did not come from one of the RPs in the anycast-RP set, RP1 assumes the packet came from a DR. If the register message is not addressed to the Anycast-RP address, an error has occurred and it should be rate-limited logged.
5. RP1 sends a copy of the register message from S1's DR to both RP2 and RP3. RP1 uses its own IP address as the source address for the PIM register message.
6. RP1 may join back to the source-tree by triggering a (S1,G) Join message toward S1; however, RP1 must create (S1,G) state.
7. RP2 receives the register message from RP1, de-encapsulates it, and also sends the packet down the shared-tree to get the packet to receiver R2.

8. RP2 sends a register-stop message back to the RP1. RP2 may wait to send the register-stop message if it decides to join the source-tree. RP2 should wait until it has received data from the source on the source-tree before sending the register-stop message. If RP2 decides to wait, the register-stop message will be sent when the next register is received. If RP2 decides not to wait, the register-stop message is sent now.
9. RP2 may join back to the source-tree by triggering a (S1,G) Join message toward S1; however, RP2 must create (S1,G) state.
10. RP3 receives the register message from RP1, de-encapsulates it, but since there are no receivers joined for the group, it can discard the packet.
11. RP3 sends a register-stop message back to the RP1.
12. RP3 creates (S1,G) state so when a receiver joins after S1 starts sending, RP3 can join quickly to the source-tree for S1.
13. RP1 processes the register-stop message from each of RP2 and RP3. RP1 may cache on a per-RP/per-(S,G) basis the receipt of register-stop message messages from the RPs in the anycast-RP set. This option is performed to increase the reliability of register message delivery to each RP. When this option is used, subsequent register messages received by RP1 are sent only to the RPs in the Anycast-RP set which have not previously sent register-stop message messages for the (S,G) entry.
14. RP1 sends a register-stop message back to the DR the next time a register message is received from the DR and (when the option in the last bullet is in use) if all RPs in the Anycast-RP set have returned register-stop messages for a particular (S,G) route.

The procedure for S2 sending follows the same steps as above, but it is RP3 which sends a copy of the register originated by S2's DR to RP1 and RP2. Therefore, this example shows how sources anywhere in the domain, associated with different RPs, can reach all receivers, also associated with different RPs, in the same domain.

5.1.7 Distributing PIM Joins over Multiple ECMP Paths

Commonly used multicast load-balancing method is per bandwidth/round robin, but the interface in an ECMP set can also be used for a particular channel to be predictable without knowing anything about the other channels using the ECMP set.

The **mc-ecmp-hashing-enabled** command enables PIM joins to be distributed over the multiple ECMP paths based on a hash of S and G. 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. Existing multicast streams using the other ECMP links stay on those links until they are pruned, unless the **rebalance** option is specified.

The default is **no mc-ecmp-hashing-enabled**, which means that the use of multiple ECMP paths (if enabled at the **config>service>vprn** context) is controlled by the existing implementation and CLI commands, that is, **mc-ecmp-balance**.

The **mc-ecmp-hashing-enabled** command and the **mc-ecmp-balance** command cannot be used together in the same context.

To achieve distribution of streams across the ECMP links, following are the hashings steps:

1. For a given S, G get all possible nHops.
2. Sort these nHops based on nhops address.
3. xor S and G addresses.
4. Hash the xor address over number of pim next hops.
5. Use the hash value obtained in step 4, and get that element, in the sorted list, we obtained in step 2 as the preferred nHop.
6. If this element is not available/is not a PIM Next hop (PIM neighbor), the next available next hop is chosen.

The following example displays PIM status indicating ECMP Hashing is disabled:

```
*B:BB# show router 100 pim status

===============================================================================
PIM Status ipv4
===============================================================================
Admin State                       : Up
Oper State                        : Up

IPv4 Admin State                  : Up
IPv4 Oper State                   : Up

BSR State                         : Accept Any

Elected BSR
    Address                       : None
    Expiry Time                   : N/A
    Priority                      : N/A
    Hash Mask Length              : 30
    Up Time                       : N/A
    RPF Intf towards E-BSR        : N/A
```

```
Candidate BSR
    Admin State                  : Down
    Oper State                   : Down
    Address                      : None
    Priority                     : 0
    Hash Mask Length             : 30

Candidate RP
    Admin State                  : Down
    Oper State                   : Down
    Address                      : 0.0.0.0
    Priority                     : 192
    Holdtime                     : 150

SSM-Default-Range                : Enabled
SSM-Group-Range
    None

MC-ECMP-Hashing                  : Disabled

Policy                           : None

RPF Table                        : rtable-u

Non-DR-Attract-Traffic           : Disabled
===============================================================================

----------------------------------------------
*B:BB>config>service>vprn>pim# no mc-ecmp-balance mc-ecmp-balance mc-ecmp-balance-
hold
*B:BB>config>service>vprn>pim# no mc-ecmp-balance
*B:BB>config>service>vprn>pim# mc-ecmp-mc-ecmp-balance mc-ecmp-balance-hold mc-ecmp-
hashing-enabled
*B:BB>config>service>vprn>pim# mc-ecmp-hashing-enabled
*B:BB>config>service>vprn>pim# info
----------------------------------------------
                apply-to all
                rp
                    static
                        address 10.3.3.3
                            group-prefix 224.0.0.0/4
                        exit
                    exit
                    bsr-candidate
                        shutdown
                    exit
                    rp-candidate
                        shutdown
                    exit
                exit
                no mc-ecmp-balance
                mc-ecmp-hashing-enabled
----------------------------------------------
*B:BB>config>service>vprn>pim#
apply-to        - Create/remove interfaces in PIM
 [no] import          - Configure import policies
 [no] interface       + Configure PIM interface
 [no] mc-ecmp-balance - Enable/
Disable multicast balancing of traffic over ECMP links
```

```
 [no] mc-ecmp-balanc* - Configure hold time for multicast balancing over ECMP links
 [no] mc-ecmp-hashin* - Enable/
Disable hash based multicast balancing of traffic over ECMP links
 [no] non-dr-attract* - Enable/disable attracting traffic when not DR
      rp              + Configure the router as static or Candidate-RP
 [no] shutdown        - Administratively enable or disable the operation of PIM
 [no] spt-switchover* -
 Configure shortest path tree (spt tree) switchover threshold for a group prefix
 [no] ssm-default-ra* - Enable the disabling of SSM Default Range
 [no] ssm-groups      + Configure the SSM group ranges
```

The following example shows distribution of PIM joins over multiple ECMP paths.

```
*A:BA# show router 100 pim group

===============================================================================
PIM Groups ipv4
===============================================================================
Group Address                          Type     Spt Bit Inc Intf       No.Oifs
   Source Address                         RP
-------------------------------------------------------------------------------
239.1.1.1                              (S,G)    spt     to_C0          1
   172.0.100.33                           10.20.1.6
239.1.1.2                              (S,G)    spt     to_C3          1
   172.0.100.33                           10.20.1.6
239.1.1.3                              (S,G)    spt     to_C2          1
   172.0.100.33                           10.20.1.6
239.1.1.4                              (S,G)    spt     to_C1          1
   172.0.100.33                           10.20.1.6
239.1.1.5                              (S,G)    spt     to_C0          1
   172.0.100.33                           10.20.1.6
239.1.1.6                              (S,G)    spt     to_C3          1
   172.0.100.33                           10.20.1.6

239.2.1.1                              (S,G)    spt     to_C0          1
   172.0.100.33                           10.20.1.6
239.2.1.2                              (S,G)    spt     to_C3          1
   172.0.100.33                           10.20.1.6
239.2.1.3                              (S,G)    spt     to_C2          1
   172.0.100.33                           10.20.1.6
239.2.1.4                              (S,G)    spt     to_C1          1
   172.0.100.33                           10.20.1.6
239.2.1.5                              (S,G)    spt     to_C0          1
   172.0.100.33                           10.20.1.6
239.2.1.6                              (S,G)    spt     to_C3          1
   172.0.100.33                           10.20.1.6

239.3.1.1                              (S,G)    spt     to_C0          1
   172.0.100.33                           10.20.1.6
239.3.1.2                              (S,G)    spt     to_C3          1
   172.0.100.33                           10.20.1.6
239.3.1.3                              (S,G)    spt     to_C2          1
   172.0.100.33                           10.20.1.6
239.3.1.4                              (S,G)    spt     to_C1          1
   172.0.100.33                           10.20.1.6
239.3.1.5                              (S,G)    spt     to_C0          1
```

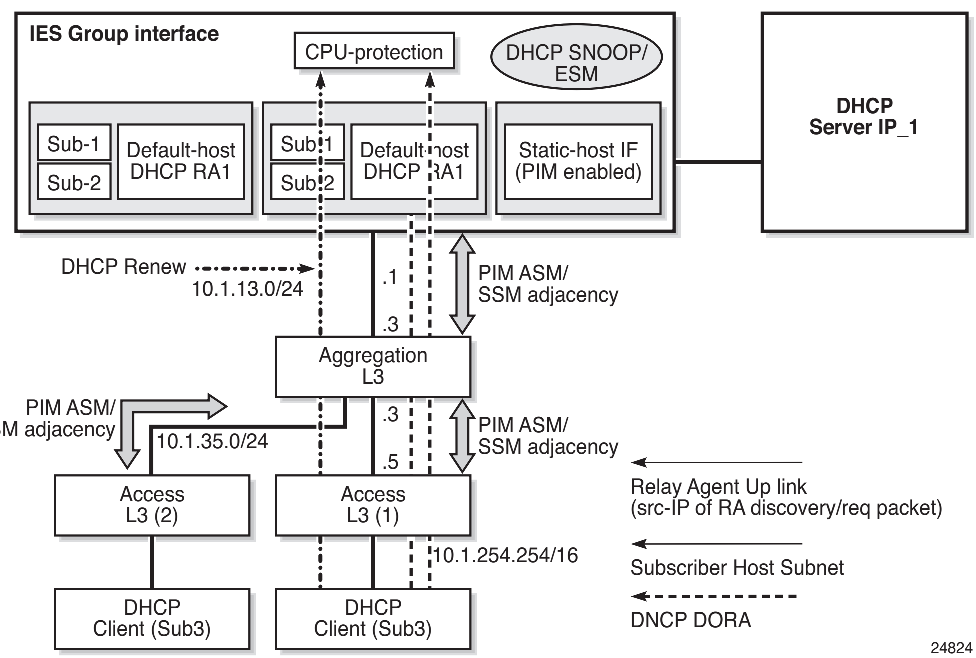
```
   172.0.100.33                                10.20.1.6
239.3.1.6                                   (S,G)     spt     to_C3          1
   172.0.100.33                                10.20.1.6

239.4.1.1                                   (S,G)     spt     to_C0          1
   172.0.100.33                                10.20.1.6
239.4.1.2                                   (S,G)     spt     to_C3          1
   172.0.100.33                                10.20.1.6
239.4.1.3                                   (S,G)     spt     to_C2          1
   172.0.100.33                                10.20.1.6
239.4.1.4                                   (S,G)     spt     to_C1          1
   172.0.100.33                                10.20.1.6
239.4.1.5                                   (S,G)     spt     to_C0          1
   172.0.100.33                                10.20.1.6
239.4.1.6                                   (S,G)     spt     to_C3          1
   172.0.100.33                                10.20.1.6
-------------------------------------------------------------------------------
Groups : 24
===============================================================================
```

5.1.8 PIM Interface on IES Subscriber Group Interfaces

PIM on a subscriber group interface allows for SAP-level replication over an ESM Group interface by establishing PIM adjacency to a downstream router. Figure 2 depicts the model:

Figure 2 **PIM Interface on IES Subscriber Group Interface**



On an IES subscriber-interface, an Ethernet SAP is configured (LAG or physical port). On the SAP, a static-host is configured for connectivity to downstream Layer 3 aggregation devices (including PIM adjacency) while multiple default-hosts can be configured for subscriber traffic. Single SAP with a single static-host per group interface is supported to establish PIM adjacency on a given subscriber group interface. Both IPv4 PIM ASM and SSM are supported.

Feature caveats:

- Only IPv4 PIM is supported with a single static host used to form a PIM interface under a group interface. Using multiple hosts or non-static hosts is not supported. Configuring IPv6-related parameters in **config**>**router**>**pim**>**interface** *group-ift* is not blocked, but takes no effect.
- **config**>**router**>**pim**>**apply-to** configuration does not apply to PIM interfaces on IES subscriber group interfaces.
- PIM on group interfaces is not supported in VPRN context.
- Extranet is not supported.
- Locally attached receivers are not supported (no IGMP/MLD and PIM mix in OIF list).
- Default anti-spoofing must be configured (IP+MAC).
- A subscriber profile with pim-policy enabled cannot combine with the following policies (**config**>**subscr-mgmt**>**sub-prof**):
  - [**no**] **host-tracking** — Apply a host tracking policy
  - [**no**] **igmp-policy** — Apply an IGMP policy
  - [**no**] **mld-policy** — Apply an MLD policy
  - [**no**] **nat-policy** — Apply a NAT policy
  - [**no**] **sub-mcac-policy** — Apply a subscriber MCAC policy (MCAC policy can be used when configured in PIM interface context)
- The feature is supported on IOM3-XP or newer line cards. When enabling the feature on older hardware, joins may be accepted and an outgoing interface may be created for the group, but traffic will not be sent out on egress because no OIF is created in forwarding.

5.1.9 Multicast-Only Fast Reroute (MoFRR)

With large scale multicast deployments, a link or nodal failure impacts multiple subscribers or a complete region or segment of receivers. This failure interrupts the receiver client experience. Besides the impact on user experience, though multicast client applications may buffer streams for short period of time, the loss of stream data may trigger unicast request for the missing stream data to the source in certain middleware implementations. Those requests can overload the network resources, if a traffic loss persists for a prolonged period.

To minimize service interruption to end-users and protect the network from sudden surge of unicast requests, SR OS implements a fast failover scheme for native IP networks. SR OS MoFRR implementation is based on RFC 7431, *Multicast-Only Fast Reroute*, and relies on:

- sending a join to a primary and a single standby upstream nodes over disjoined paths
- fast failover to a standby stream upon detection of a failure

The functionality relies on failure detection on the primary path to switch to forwarding the traffic from the standby path. The traffic failure can happen with or without physical links or nodes going down. Various mechanisms for link or node failure detections are supported; however, to achieve best performance and resilience, it is recommended to enable MoFRR on every node in the network and use hop-by-hop BFD for fast link failure or data plane failure detection on each upstream link. Without BFD, the PIM adjacency loss or route change could be used to detect traffic failure. Figure 3 and Figure 4 depict MoFRR behavior.

Figure 3 **MoFRR Steady State No Failure**

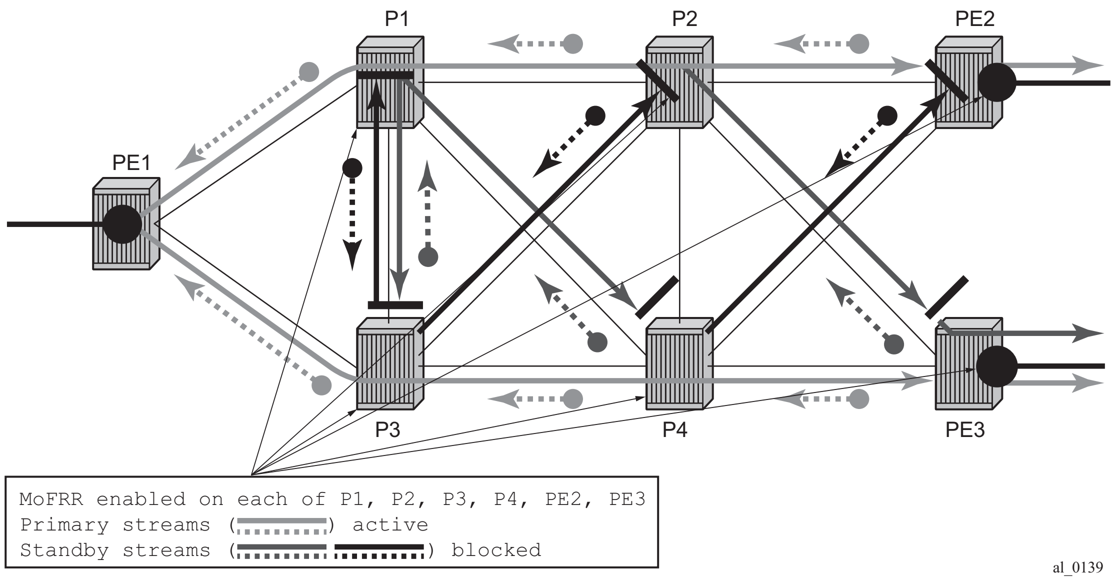
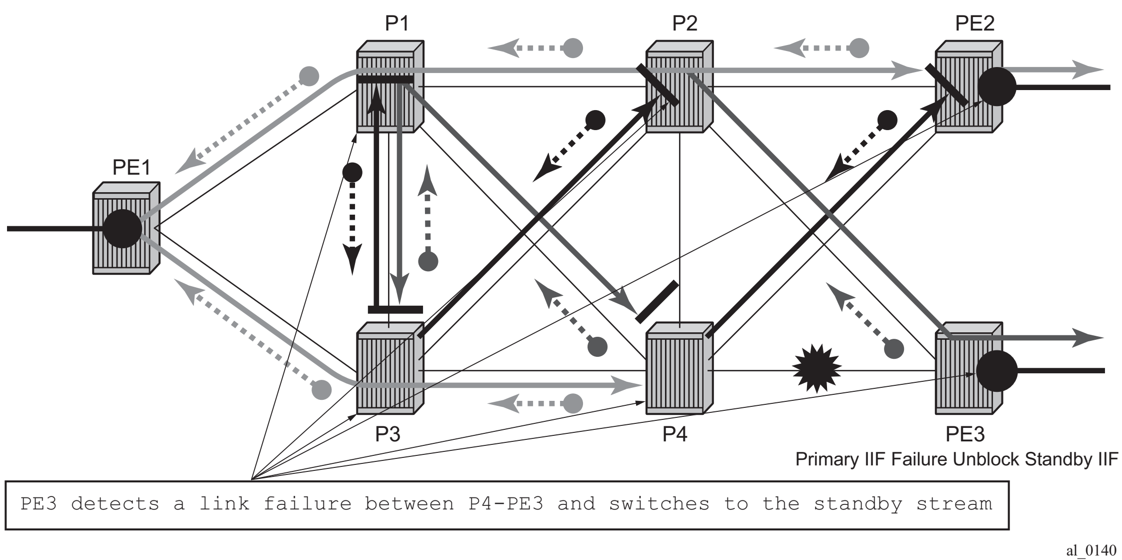


Figure 4 **MoFRR Switch to Standby Stream on a Link Failure**



MoFRR functionality supports the following:

- IPv4 or IPv6 link or node failure protection in global routing instance
- Rosen PIM-SSM with MDT SAFI
- active streams and a single standby stream over disjoint ECMP paths

- active streams and a single standby stream joins over IS-IS or OSPF Loop-Free Alternate paths
- all regular PIM interfaces supporting MoFRR for all multicast streams (tunnel interfaces are ignored)

Note: MoFRR (**config**>**router**>**pim**>**multicast-fast-failover** or **config**>**router**>**pim**>**multicast6-fast-failover**) cannot be configured when GTM auto-discovery (**config**>**router**>**pim**>**gtm**>**auto-discovery**) is enabled.

5.1.10 Automatic Discovery of Group-to-RP Mappings (Auto-RP)

Auto-RP is a proprietary group discovery and mapping mechanism for IPv4 PIM that is described in cisco-ipmulticast/pim-autorp-spec, *Auto-RP: Automatic discovery of Group-to-RP mappings for IP multicast*. The functionality is similar to the IETF standard bootstrap router (BSR) mechanism that is described in RFC 5059, *Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*, to dynamically learn about the availability of Rendezvous Points (RPs) in a network. When a router is configured as an RP-mapping agent with the **pim>rp>auto-rp-discovery** command, it listens to the CISCO-RP-ANNOUNCE (224.0.1.39) group and caches the announced mappings. The RP-mapping agent then periodically sends out RP-mapping packets to the CISCO-RP-DISCOVERY (224.0.1.40) group. PIM dense-mode (PIM-DM) as described in RFC 3973, *Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)*, is used for the auto-RP groups to support multihoming and redundancy. The RP-mapping agent supports announcing, mapping, and discovery functions; candidate RP functionality is not supported. SR OS supports version 1 of the Auto-RP specification; the ability to deny RP-mappings by advertising negative group prefixes is not supported.

Auto-RP is supported for IPv4 in multicast VPNs and in the global routing instance. Either BSR or auto-RP for IPv4 can be configured; the two mechanisms cannot be enabled together. BSR for IPv6 and auto-RP for IPv4 can be enabled together. In a multicast VPN, auto-RP cannot be enabled together with sender-only or receiver-only multicast distribution trees (MDTs), or wildcard S-PMSI configurations that could block flooding.

5.1.11 VRRP Aware PIM

The Virtual Router Redundancy Protocol (VRRP) eliminates the single point of failure inherent in the static default-routed environment. VRRP describes a method of implementing a redundant IP interface that provides dynamic failover if the VRRP master router (MR) becomes unavailable.

VRRP provides information on the state of a router. However, PIM operates independently of VRRP group states. The PIM DR and the VRRP MR may not be the same router and IP multicast traffic may not necessarily follow the same path as elected by VRRP.

In order to leverage the redundancy capabilities of VRRP that are lacking in PIM, the VRRP Aware PIM mechanism allows PIM to monitor and react to changes in the VRRP MR. This ensures that the multicast traffic follows the unicast traffic through the same gateway as the VRRP MR, providing consistent IP multicast forwarding in a redundant network.

5.1.11.1 Configuring VRRP Aware PIM

The VRRP Aware PIM feature enables PIM to track the state of a VRRP instance and to identify whether the associated VRRP interface is the master. PIM uses an operational group parameter (**oper-group** *group-name***)** to monitor the state of VRRP. One operational group can be created for IPv4, and another for IPv6. When VRRP is the MR, the operational group is up; for all other VRRP states, the operational group is down. A VRRP instance can only be associated with one operational group, and an operational group can have one or more associated VRRP instances. This feature is supported on base router, IES, and VPRN interfaces.

If the monitored interface is the VRRP MR, PIM becomes the DR by setting its priority to the configured **oper-group-active-priority** value. In order for the router to become the DR, the proper priorities must be configured so that the **oper-group-active-priority** is the highest priority on the IP interface.

If a PIM router is the DR and then receives an indication from VRRP that the interface is no longer the VRRP MR, PIM relinquishes the DR role by setting its priority back to the default or configured priority value.

If the configured VRRP instance or **oper-group** is not configured, PIM operates as normal with the default or configured priority value, and does not set its priority to **oper-group-active-priority**. A change in the operational group status is independent of the address family; IPv4 and IPv6 priorities are configured independently of each other. Two operational groups are supported per PIM interface, one for IPv4 and one for IPv6.

5.1.11.2 Configuration Recommendations

When configuring VRRP Aware PIM, consider the following recommendations.

- VRRP could be configured to use BFD to speed up failure detection in addition to the functionality provided by VRRP Aware PIM.
- To optimize failover, the **config**>**router**>**pim**>n**on-dr-attract-traffic** command can be enabled on the primary and secondary routers to make them a hot-standby redundant pair. This configuration ignores the DR state and attracts traffic to populate the router's PIM database. This setting should not be used if multicast traffic must only follow the VRRP MR.
- The **config**>**service**>**oper-group**>**hold-time**>**group**>**up** time on the primary router and **config**>**service**>**oper-group**>**hold-time**>**group**>**down** time on the secondary router should both be set to the time needed to repopulate the PIM database; for example, 10 seconds. This allows the primary router to populate its PIM database again before becoming the DR if a failure occurs from the primary to secondary router, and recover from the secondary back to the primary router.
- The **config**>**service**>**oper-group**>**hold-time**>**group**>**up** time should be set to 0 on the secondary router so that it assumes the DR role immediately if the primary router fails. The up hold time is set to 4 seconds by default, which delays the DR change unnecessarily.
- The sticky DR setting should be disabled if it is configured with the **config**>**router**>**pim**>**if**>**sticky-dr** command. Sticky DR enables the secondary router to continue to act as the DR after the primary router comes back up. Sticky DR is incompatible with the VRRP Aware PIM mechanism that tracks the VRRP MR.

The following is a basic configuration example for VRRP Aware PIM.

```
service
    oper-group “VAwP1” create
    exit
vprn 1 customer 1 create
    interface to-LAN
        vrrp 1 create
            oper-group “VAwP1”
```

```
        exit
    pim
        interface to-LAN
            monitor-oper-group “VAwP1” family ipv4 add 90
            monitor-oper-group “VAwP1” family ipv6 add 90
        exit
        interface to-LAN2
            monitor-oper-group “VAwP1” family ipv4 add 90
            monitor-oper-group “VAwP2” family ipv6 set 90
        exit
    exit
exit
```

5.1.11.2.1 Primary Router Example

```
*B:Dut-C>config>service# info
----------------------------------------------
        oper-group "vrrp1_1" create
            hold-time
                group up 10
            exit
        exit
        oper-group "vrrp1_1_ipv6" create
            hold-time
                group up 10
            exit
        exit
        customer 1 create
            description "Default customer"
        exit
        vprn 1 customer 1 create
            interface "toRemoteSite_1001" create
                address 10.1.1.5/24
                bfd 500 receive 500 multiplier 3
                vrrp 1
                    backup 10.1.1.100
                    priority 200
                    ping-reply
                    message-interval 5
                    oper-group "vrrp1_1"
                    bfd-enable 1 interface "toRemoteSite_1001" dst-ip 10.1.1.4
                exit
                ipv6
                    address 2001:db8:1:1:1:5/112
                    link-local-address ff00:db8:1:1:1:5 preferred
                    bfd 500 receive 500 multiplier 3
                    vrrp 1
                        backup ff00:db8:1:1:1:100
                        priority 200
                        ping-reply
                        message-interval 5
                        oper-group "vrrp1_1_ipv6"
                        bfd-enable 1 interface "toRemoteSite_1001"
dst-ip 2001:db8:1:1:1:4
                    exit
                exit
            exit
```

```
interface "toDC" create
    address 10.1.30.5/24
    bfd 500 receive 500 multiplier 3
    vrrp 255
        backup 10.1.30.100
        priority 200
        policy 1
        ping-reply
        message-interval 5
        bfd-enable 1 interface "toDC" dst-ip 10.1.30.4
    exit
    ipv6
        address 2001::db8:1:30:5/112
        link-local-address ff00:db8:30:1:30:5 preferred
        bfd 500 receive 500 multiplier 3
        vrrp 255
            backup ff00:db8:30:1:30:100
            priority 200
            policy 1001
            ping-reply
            message-interval 5
            bfd-enable 1 interface "toDC" dst-ip 2001::db8:1:30:4
        exit
    exit
    sap 2/1/2:1 create
    exit
exit
router-advertisement
    interface "toRemoteSite_1001"
        use-virtual-mac
        no shutdown
    exit
    interface "toDC"
        use-virtual-mac
        no shutdown
    exit
exit
igmp
    interface "toDC"
        no shutdown
    exit
    no shutdown
exit
mld
    interface "toDC"
        no shutdown
    exit
    no shutdown
exit
pim
    no ipv6-multicast-disable
    interface "toRemoteSite_1001"
        monitor-oper-group "vrrp1_1" family ipv4 set 5
        monitor-oper-group "vrrp1_1_ipv6" family ipv6 set 5
    exit
    interface "toDC"
        monitor-oper-group "vrrp1_1" family ipv4 set 5
        monitor-oper-group "vrrp1_1_ipv6" family ipv6 set 5
    exit
```

```
                    rp
                        static
                            address 10.1.10.245
                                group-prefix 224.0.0.0/4
                            exit
                        exit
                        bsr-candidate
                            shutdown
                        exit
                        rp-candidate
                            shutdown
                        exit
                        ipv6
                            static
                                address 2001:db8:1:10:245
                                    group-prefix ff00:db8::/8
                                exit
                            exit
                        exit
                    exit
                    non-dr-attract-traffic
                    no shutdown
                exit
                no shutdown
            exit
```

5.1.11.2.2 Secondary Router Example

```
*B:Dut-E>config>service# info
----------------------------------------------
        oper-group "vrrp1_1" create
            hold-time
                group down 10
                group up 0
            exit
        exit
        oper-group "vrrp1_1_ipv6" create
            hold-time
                group down 10
                group up 0
            exit
        exit
        customer 1 create
            description "Default customer"
        exit
        vprn 1 customer 1 create
            snmp
                community "XldhYQtqb7c" hash2 rw version both
            exit
            route-distinguisher 10.1.10.244:1
            interface "system" create
                address 10.1.10.244/32
                ipv6
                    address 2001:db8:1:10:244/128
                exit
                loopback
            exit
```

```
                    interface "toRemoteSite_1001" create
                        address 10.1.1.4/24
                        ip-mtu 1454
                        bfd 500 receive 500 multiplier 3
                        vrrp 1
                            backup 10.1.1.100
                            ping-reply
                            standby-forwarding
                            message-interval 5
                            oper-group "vrrp1_1"
                            bfd-enable 1 interface "toRemoteSite_1001" dst-ip 10.1.1.5
                        exit
                        ipv6
                            address 2001:db8:1:1:4/112
                            link-local-address ff00:db8:1:1:1:4 preferred
                            bfd 500 receive 500 multiplier 3
                            vrrp 1
                                backup ff00:db8:1:1:1:100
                                ping-reply
                                standby-forwarding
                                message-interval 5
                                oper-group "vrrp1_1_ipv6"
                                bfd-enable 1 interface "toRemoteSite_1001"
dst-ip 2001:db8:1:1:5
                            exit
                        exit
                    exit
                    interface "toDC" create
                        address 10.1.30.4/24
                        bfd 500 receive 500 multiplier 3
                        vrrp 255
                            backup 10.1.30.100
                            ping-reply
                            standby-forwarding
                            message-interval 5
                            bfd-enable 1 interface "toDC" dst-ip 10.1.30.5
                        exit
                        ipv6
                            address 2001:db8:1:30:4/112
                            link-local-address ff00:db8:30:1:30:4 preferred
                            bfd 500 receive 500 multiplier 3
                            vrrp 255
                                backup ff00:db8:30:1:30:100
                                ping-reply
                                standby-forwarding
                                message-interval 5
                                bfd-enable 1 interface "toDC" dst-ip 2001::db8:1:30:5
                            exit
                        exit
                        sap 1/1/5:1 create
                        exit
                    exit
                    static-route-entry 10.1.10.245/32
                        next-hop 10.1.30.5
                            no shutdown
                        exit
                    exit
                    static-route-entry 2001:db8:1:10:245/128
                        next-hop 2001:db8:1:30:5
```

```
        no shutdown
    exit
exit
router-advertisement
    interface "toRemoteSite_1001"
        use-virtual-mac
        no shutdown
    exit
    interface "toDC"
        use-virtual-mac
        no shutdown
    exit
exit
igmp
    interface "toDC"
        no shutdown
    exit
    no shutdown
exit
mld
    interface "toDC"
        no shutdown
    exit
    no shutdown
exit
pim
    no ipv6-multicast-disable
    interface "toRemoteSite_1001"
        monitor-oper-group "vrrp1_1" family ipv4 set 255
        monitor-oper-group "vrrp1_1_ipv6" family ipv6 set 255
    exit
    interface "toDC"
        monitor-oper-group "vrrp1_1" family ipv4 set 255
        monitor-oper-group "vrrp1_1_ipv6" family ipv6 set 255
    exit
    rp
        static
            address 10.1.10.245
                group-prefix 224.0.0.0/4
            exit
        exit
        bsr-candidate
            shutdown
        exit
        rp-candidate
            shutdown
        exit
        ipv6
            static
                address 2001:db8:1:10:245
                    group-prefix ff00:db8:/8
                exit
            exit
        exit
    exit
    non-dr-attract-traffic
    no shutdown
exit
no shutdown
```

```
exit
```

5.2 IPv6 PIM models

IPv6 multicast enables multicast applications over native IPv6 networks. There are two service models: Any Source Multicast (ASM) and Source Specific Multicast (SSM) which includes PIM-SSM and MLD (see MLD Overview). SSM does not require source discovery and only supports single source for a specific multicast stream. As a result, SSM is easier to operate in a large scale deployment that uses the one-to-many service model.

5.2.1 PIM-SSM

The IPv6 address family for SSM model is supported. This includes the ability to choose which RTM table to use (unicast RTM, multicast RTM, or both). OSPF3, IS-IS and static-route have extensions to support submission of routes into the IPv6 multicast RTM.

5.2.2 PIM ASM

IPv6 PIM ASM is supported. All PIM ASM related functions such as bootstrap router, RP, and so on, support both IPv4 and IPv6 address-families. IPv6 specific parameters are configured under **config>router>pim>rp>ipv6**.

5.2.3 Embedded RP

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).

5.3 Configuring PIM with CLI

This section provides information to configure PIM using the command line interface.

5.3.1 PIM Configuration Overview

PIM is not enabled by default. When PIM is enabled, data is forwarded to network segments with active receivers that have explicitly requested the multicast group. When enabled, at least one interface must be specified in the PIM context as PIM is an interface function. Creating an interface enables PIM.

5.3.2 Basic PIM Configuration

Perform the following basic PIM configuration tasks:

- Enable PIM (required)
- Add interfaces so the protocol establishes adjacencies with the neighboring routers (required)
- Configure a way to calculate group-to-RP mapping (required) by either:
  - Static group-to-RP mapping
  - Enable Candidate RP/Bootstrap mechanism on some routers.
- Enable unicast routing protocols to learn routes towards the RP/source for reverse path forwarding (required)
- Add SSM ranges (optional)
- Enable Candidate BSR (optional)
- Enable Candidate RP (optional)
- Change hello interval (optional)
- Configure route policies (bootstrap-export, bootstrap-import, import join and register)

5.3.3 Configuring PIM Parameters

5.3.3.1 Enabling PIM

When configuring PIM, make sure to enable PIM on all interfaces for the routing instance, otherwise multicast routing errors can occur.

Use the following CLI syntax to enable PIM.

CLI Syntax: `config>router# pim`

The following example displays the detailed output when PIM is enabled.

```
A:LAX>>config>router# info detail
...
#------------------------------------------
echo "PIM Configuration"
#------------------------------------------
        pim
            no import join-policy
            no import register-policy
            apply-to none
            rp
                no bootstrap-import
                no bootstrap-export
                static
                exit
                bsr-candidate
                    shutdown
                    priority 0
                    hash-mask-len 30
                    no address
                exit
                rp-candidate
                    shutdown
                    no address
                    holdtime 150
                    priority 192
                exit
            exit
            no shutdown
        exit
#------------------------------------------
...
A:LAX>>config>system#
```

5.3.3.2 Configuring PIM Interface Parameters

The following example displays the command usage to configure PIM interface parameters:

Example:

```
A:LAX>config>router# pim
A:LAX>config>router>pim# interface "system"
A:LAX>config>router>pim>if# exit
A:LAX>config>router>pim# interface "lax-vls"
A:LAX>config>router>pim>if# exit
A:LAX>config>router>pim# interface "lax-sjc"
A:LAX>config>router>pim>if# exit
A:LAX>config>router>pim# interface "p1-ix"
A:LAX>config>router>pim>if# exit
A:LAX>config>router>pim# rp
A:LAX>config>router>pim>rp# static
A:LAX>config>router>pim>rp>static# address
 239.22.187.237
A:LAX>config>router>..>address# group-prefix
 239.24.24.24/32
A:LAX>config>router>pim>rp>static>address# exit
A:LAX>config>router>pim>rp>static# exit
A:LAX>config>router>pim>rp# exit
A:LAX>config>router>pim#
```

The following example displays the PIM configuration:

```
A:LAX>config>router>pim# info
----------------------------------------------
            interface "system"
            exit
            interface "lax-vls"
            exit
            interface "lax-sjc"
            exit
            interface "p1-ix"
            exit
            rp
                static
                    address 239.22.187.237
                        group-prefix 239.24.24.24/32
                    exit
                    address 10.10.10.10
                    exit
                exit
                bsr-candidate
                    shutdown
                exit
                rp-candidate
                    shutdown
                exit
            exit
----------------------------------------------
```

```
A:LAX>config>router>pim#
```

Example:

```
A:SJC>config>router# pim
A:SJC>config>router>pim# interface "system"
A:SJC>config>router>pim>if# exit
A:SJC>config>router>pim# interface "sjc-lax"
A:SJC>config>router>pim>if# exit
A:SJC>config>router>pim# interface "sjc-nyc"
A:SJC>config>router>pim>if# exit
A:SJC>config>router>pim# interface "sjc-sfo"
A:SJC>config>router>pim>if# exit
A:SJC>config>router>pim# rp
A:SJC>config>router>pim>rp# static
A:SJC>config>router>pim>rp>static# address
 239.22.187.237
A:SJC>config>router>pim>rp>static>address# group-prefix
 239.24.24.24/32
A:SJC>config>router>pim>rp>static>address# exit
A:SJC>config>router>pim>rp>static# exit
A:SJC>config>router>pim>rp# exit
A:SJC>config>router>pim#
```

```
A:SJC>config>router>pim# info
----------------------------------------------
            interface "system"
            exit
            interface "sjc-lax"
            exit
            interface "sjc-nyc"
            exit
            interface "sjc-sfo"
            exit
            rp
                static
                    address 239.22.187.237
                        group-prefix 239.24.24.24/32
                    exit
                exit
                bsr-candidate
                    shutdown
                exit
                rp-candidate
                    shutdown
                exit
            exit
----------------------------------------------
A:SJC>config>router>pim#
```

Example:

```
A:MV>config>router# pim
A:MV>config>router>pim# interface "system"
A:MV>config>router>pim>if# exit
A:MV>config>router>pim# interface "mv-sfo"
A:MV>config>router>pim>if# exit
```

```
A:MV>config>router>pim# interface "mv-v1c"
A:MV>config>router>pim>if# exit
A:MV>config>router>pim# interface "p3-ix"
A:MV>config>router>pim>if# exit
A:MV>config>router>pim# rp
A:MV>config>router>pim>rp# static
A:MV>config>router>pim>rp>static# address 239.22.187.237
A:MV>config>router>pim>rp>static>address# group-prefix
 239.24.24.24/32
A:MV>config>router>pim>rp>static>address# exit
A:MV>config>router>pim>rp>static#
A:MV>config>router>pim>rp# exit
A:MV>config>router>pim#
```

```
A:MV>config>router>pim# info
----------------------------------------------
            interface "system"
            exit
            interface "mv-sfo"
            exit
            interface "mv-vlc"
            exit
            interface "p3-ix"
            exit
            rp
                static
                    address 239.22.187.237
                        group-prefix 239.24.24.24/32
                    exit
                exit
                bsr-candidate
                    address 2.22.187.236
                    no shutdown
                exit
                rp-candidate
                    address 2.22.187.236
                    no shutdown
                exit
            exit
----------------------------------------------
A:MV>config>router>pim#
```

Example:

```
A:SFO>config>router# pim
A:SFO>config>router>pim# interface "system"
A:SFO>config>router>pim>if# exit
A:SFO>config>router>pim# interface "sfo-sfc"
A:SFO>config>router>pim>if# exit
A:SFO>config>router>pim# interface "sfo-was"
A:SFO>config>router>pim>if# exit
A:SFO>config>router>pim# interface "sfo-mv"
A:SFO>config>router>pim>if# exit
A:SFO>config>router>pim# rp
A:SFO>config>router>pim>rp# static
```

```
A:SFO>config>router>pim>rp>static# address
 239.22.187.237
A:SFO>config>router>pim>rp>static>address# group-prefix
 239.24.24.24/32
A:SFO>config>router>pim>rp>static>address# exit
A:SFO>config>router>pim>rp>static# exit
A:SFO>config>router>pim>rp # exit
A:SFO>config>router>pim#
```

```
A:SFO>config>router>pim# info
----------------------------------------------
            interface "system"
            exit
            interface "sfo-sjc"
            exit
            interface "sfo-was"
            exit
            interface "sfo-mv"
            exit
            rp
                static
                    address 239.22.187.237
                        group-prefix 239.24.24.24/32
                    exit
                exit
                bsr-candidate
                    address 239.22.187.239
                    no shutdown
                exit
                rp-candidate
                    address 239.22.187.239
                    no shutdown
                exit
            exit
----------------------------------------------
A:SFO>config>router>pim#
```

Example:

```
A:WAS>config>router# pim
A:WAS>config>router>pim# interface "system"
A:WAS>config>router>pim>if# exit
A:WAS>config>router>pim# interface "was-sfo"
A:WAS>config>router>pim>if# exit
A:WAS>config>router>pim# interface "was-vlc"
A:WAS>config>router>pim>if# exit
A:WAS>config>router>pim# interface "p4-ix"
A:WAS>config>router>pim>if# exit
A:WAS>config>router>pim# rp
A:WAS>config>router>pim>rp# static
A:WAS>config>router>pim>rp>static# address
 239.22.187.237
A:WAS>config>router>pim>rp>static>address# group-prefix
 239.24.24.24/32
A:WAS>config>router>pim>rp>static>address# exit
```

```
A:WAS>config>router>pim>rp>static# exit
A:WAS>config>router>pim>rp# bsr-candidate
A:WAS>config>router>pim>rp>bsr-cand# address
 239.22.187.240
A:WAS>config>router>pim>rp>bsr-cand# no shutdown
A:WAS>config>router>pim>rp>bsr-cand# exit
A:WAS>config>router>pim>rp# exit
A:WAS>config>router>pim#
```

```
A:WAS>config>router>pim# info
----------------------------------------------
            interface "system"
            exit
            interface "was-sfo"
            exit
            interface "was-vlc"
            exit
            interface "p4-ix"
            exit
            rp
                static
                    address 239.22.187.237
                        group-prefix 239.24.24.24/32
                    exit
                exit
                bsr-candidate
                    address 239.22.187.240
                    no shutdown
                exit
                rp-candidate
                    address 239.22.187.240
                    no shutdown
                exit
            exit
----------------------------------------------
A:WAS>config>router>pim#
```

5.3.3.3 Configuring PIM Join/Register Policies

Join policies are used in Protocol Independent Multicast (PIM) configurations to prevent the transportation of multicast traffic across a network and the dropping of packets at a scope at the edge of the network. PIM Join filters reduce the potential for denial of service (DoS) attacks and PIM state explosion—large numbers of Joins forwarded to each router on the RPT, resulting in memory consumption. Refer to the Importing PIM Join/Register Policies section of the Multicast Routing Guide for more information.

*,G or S,G is the information used to forward unicast or multicast packets.

- **group-address** matches the group address policy in join/prune messages group-address “group-address-policy”

- **source-address** matches the source address in join/prune messages
  source-address 192.168.0.1
- **interface** matches any join message received on the specified interface
  interface port 1/1/1
- **neighbor** matches any join message received from the specified neighbor
  neighbor 1.1.1.1

The following configuration example will not allow join messages for group 229.50.50.208/32 and source 192.168.0.1 but allows other join messages.

Configuring policy-statement

```
A:ALA-B>config>router# policy-options
A:ALA-B>config>router>policy-options# begin
A:ALA-B>config>router>policy-options# policy-statement foo
A:ALA-B>config>router>policy-options>policy-statement$ entry 10
A:ALA-B>config>router>policy-options>policy-statement>entry$ from
A:ALA-B>config>router>policy-options>policy-statement>entry>from$ group-address
“group-address-policy”
A:ALA-B>config>router>policy-options>policy-statement>entry>from$ source-address
192.168.0.1
A:ALA-B>config>router>policy-options>policy-statement>entry>from$ exit
A:ALA-B>config>router>policy-options>policy-statement>entry# action reject
A:ALA-B>config>router>policy-options>policy-statement>entry#
```

5.3.3.4 Importing PIM Join/Register Policies

The import command provides a mechanism to control the (*,G) and (S,G) state that gets created on a router. Import policies are defined in the **config>router>policy-options** context.

Note: In the import policy, if an action is not specified in the entry then the default-action takes precedence. If no entry matches then the default-action also takes precedence. If no default-action is specified, then the default default-action is executed.

Use the following commands to configure PIM parameters:

CLI Syntax:
```
config>router# pim
      import {join-policy | register-policy} [policy-name
        [.. policy-name]
```

The following example displays the command usage to apply the policy statement which does not allow join messages for group 229.50.50.208/32 and source 192.168.0.0/16 but allows join messages for 192.168.0.0/16, 229.50.50.208 (refer to the “Configuring Route Policy Components” section of the *7450 ESS, 7750 SR, 7950 XRS, and VSR Unicast Routing Protocols Guide*).

Example:

```
config>router# pim
config>router>pim# import join-policy "foo"
config>router>pim# no shutdown
```

The following example displays the PIM configuration:

```
A:LAX>config>router>pim# info
----------------------------------------------
            import join-policy "foo"
            interface "system"
            exit
            interface "lax-vls"
            exit
            interface "lax-sjc"
            exit
            interface "p1-ix"
            exit
            rp
                static
                    address 239.22.187.237
                        group-prefix 239.24.24.24/3
                    exit
                    address 10.10.10.10
                    exit
                exit
                bsr-candidate
                    shutdown
                exit
                rp-candidate
                    shutdown
                exit
            exit
----------------------------------------------
A:LAX>config>router>pim#
```

5.3.3.5 Configuring Bootstrap Message Import and Export Policies

Bootstrap import and export policies are used to control the flow of bootstrap messages to and from the RP.

The following configuration example specifies that no BSR messages received or sent out of interface port 1/1/1.

```
A:ALA-B>config>router>policy-options# policy-statement pim-import
```

```
:A:ALA-B>config>router>policy-options>policy-statement$ entry 10
:A:ALA-B>config>router>policy-options>policy-statement>entry$ from
:A:ALA-B>config>router>policy-options>policy-statement>entry>from$ interface
port 1/1/1
:A:ALA-B>config>router>policy-options>policy-statement>entry>from$ exit
:A:ALA-B>config>router>policy-options>policy-statement>entry# action reject
:A:ALA-B>config>router>policy-options>policy-statement>entry# exit
:A:ALA-B>config>router>policy-options>policy-statement# exit

:A:ALA-B>config>router>policy-options# policy-statement pim-export
:A:ALA-B>config>router>policy-options>policy-statement$ entry 10
:A:ALA-B>config>router>policy-options>policy-statement>entry$ to
:A:ALA-B>config>router>policy-options>policy-statement>entry>to$interface port 1/1/1
:A:ALA-B>config>router>policy-options>policy-statement>entry# action reject
:A:ALA-B>config>router>policy-options>policy-statement>entry# exit
:A:ALA-B>config>router>policy-options>policy-statement# exit

:A:ALA-B>configure router pim rp bootstrap-import pim-import
:A:ALA-B>configure router pim rp bootstrap-export pim-export
```

5.3.4 Disabling PIM

Use the following CLI syntax to disable PIM.

CLI Syntax:

```
config>router#
      pim
            shutdown
```

The following example displays the command usage to disable multicast:

Example:

```
config>router# pim
config>router>pim# shutdown
config>router>pim# exit
```

The following example displays the configuration output:

```
A:LAX>config>router# info
----------------------------------------------
...
#------------------------------------------
echo "PIM Configuration"
#------------------------------------------
        pim
            shutdown
            import join-policy "foo"
            interface "system"
            exit
            interface "lax-sjc"
            exit
            interface "lax-vls"
            exit
            interface "p1-ix"
```

```
            exit
            rp
                static
                    address 239.22.187.237
                        group-prefix 239.24.24.24/32
                    exit
                    address 10.10.10.10
                    exit
                exit
                bsr-candidate
                    shutdown
                exit
                rp-candidate
                    shutdown
                exit
            exit
        exit
#------------------------------------------
....
------------------------------------------
A:LAX>config>router#
```

5.4 PIM Configuration Command Reference

5.4.1 Command Hierarchies

- Configuration Commands

5.4.1.1 Configuration Commands

config
- **— router**
  - **—** [**no**] **pim**
    - **— apply-to** {**ies** | **non-ies** | **all** | **none**}
    - **—** [**no**] **enable-mdt-spt**
    - **— gtm**
      - **— auto-discovery** [**default**]
      - **— no auto-discovery**
    - **— import** {**join-policy** | **register-policy**} *policy-name* [.. *policy-name*]
    - **— no import** {**join-policy** | **register-policy**}
    - **—** [**no**] **interface** *ip-int-name*
      - **— assert-period** *assert-period*
      - **— no assert-period**
      - **—** [**no**] **bfd-enable** [**ipv4** | **ipv6**]
      - **—** [**no**] **bsm-check-rtr-alert**
      - **— hello-interval** *hello-interval*
      - **— no hello-interval**
      - **— hello-multiplier** *deci-units*
      - **— no hello-multiplier**
      - **—** [**no**] **improved-assert**
      - **—** [**no**] **instant-prune-echo**
      - **—** [**no**] **ipv4-multicast-disable**
      - **—** [**no**] **ipv6-multicast-disable**
      - **— max-groups** *value*
      - **— no max-groups**
      - **— monitor-oper-group** *group-name* **family** {**ipv4** | **ipv6**} {**add** | **set** | **subtract**} *value*
      - **— no monitor-oper-group** [**family** {**ipv4** | **ipv6**}]
      - **— multicast-senders** {**auto** | **always** | **never**}
      - **— no multicast-senders**
      - **—** [**no**] **p2mp-ldp-tree-join** [**ipv4**] [**ipv6**]
      - **— priority** *dr-priority*
      - **— no priority**
      - **—** [**no**] **shutdown**
      - **— sticky-dr** [**priority** *dr-priority*]
      - **— no sticky-dr**
      - **— three-way-hello** [**compatibility-mode**]
      - **— no three-way-hello**

— [**no**] **tracking-support**
— [**no**] **ipv4-multicast-disable**
— **ipv6-multicast-disable**
— [**no**] **lag-usage-optimization**
— [**no**] **mc-ecmp-balance**
— **mc-ecmp-balance-hold** *minutes*
— **no mc-ecmp-balance-hold**
— [**no**] **mc-ecmp-hashing-enabled** [**rebalance**]
— [**no**] **multicast-fast-failover**
— [**no**] **multicast6-fast-failover**
— [**no**] **non-dr-attract-traffic**
— **rp**
— [**no**] **anycast** *rp-ip-address*
— [**no**] **rp-set-peer** *ip-address*
— [**no**] **auto-rp-discovery**
— **bootstrap-export** *policy-name* [.. *policy-name*]
— **no bootstrap-export**
— **bootstrap-import** *policy-name* [.. *policy-name*]
— **no bootstrap-import**
— **bsr-candidate**
— **address** *ipv4-address*
— **no address**
— **hash-mask-len** *hash-mask-length*
— **no hash-mask-len**
— **priority** *bootstrap-priority*
— **no priority**
— [**no**] **shutdown**
— **ipv6**
— [**no**] **anycast** *rp-ip-address*
— [**no**] **rp-set-peer** *ip-address*
— **bsr-candidate**
— **address** *ipv6-address*
— **no address**
— **hash-mask-len** *hash-mask-length*
— **no hash-mask-len**
— **priority** *bootstrap-priority*
— **no priority**
— [**no**] **shutdown**
— [**no**] **embedded-rp**
— [**no**] **group-range** *ipv6-address/prefix-length*
— [**no**] **shutdown**
— **rp-candidate**
— **address** *ip-address*
— **no address**
— [**no**] **group-range** {*grp-ip-addressImask* | *grp-ip-address netmask*}
— **holdtime** *holdtime*
— **no holdtime**
— **priority** *priority*
— **no priority**
— [**no**] **shutdown**
— **static**
— [**no**] **address** *ipv6-address*
— [**no**] **group-prefix** *grp-ipv6-addressIprefix-length*

— [**no**] **override**
— **rp-candidate**
— **address** *ip-address*
— **no address**
— [**no**] **group-range** {*grp-ip-address/mask* | *grp-ip-address netmask*}
— **holdtime** *holdtime*
— **no holdtime**
— **priority** *priority*
— **no priority**
— [**no**] **shutdown**
— **static**
— [**no**] **address** *ip-address*
— [**no**] **group-prefix** {*grp-ip-address/mask* | *grp-ip-address netmask*}
— [**no**] **override**
— **rpf-table** {**rtable-m** | **r table-u** | **both**}
— **no rpf-table**
— **rpf6-table** {**rtable6-m** | **rtable6-u** | **both**}
— **no rpf6-table**
— **rpfv core**
— **rpfv mvpn**
— **rpfv core mvpn**
— **no rpfv** [**core**] [**mvpn**]
— [**no**] **shutdown**
— **spt-switchover-threshold** {*grp-ipv4-prefix/ipv4-prefix-length* | *grp-ipv4-prefix netmask* | *grp-ipv6-prefix/ipv6-prefix-length*} *spt-threshold*
— **no spt-switchover-threshold** {*grp-ipv4-prefix/ipv4-prefix-length* | *grp-ipv4-prefix netmask* | *grp-ipv6-prefix/ipv6-prefix-length*}
— [**no**] **ssm-groups**
— [**no**] **group-range** {*ip-prefix/mask* | *ip-prefix netmask*}
— [**no**] **tunnel-interface rsvp-p2mp** *lsp-name* [**sender** *ip-address*]

5.4.2 Command Descriptions

5.4.2.1 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 no pim

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 apply-to none

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.

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 re-initiate setup.

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

Default no enable-mdt-spt

gtm

Syntax **gtm**

Context config>router>pim

Description This command enables the context to configure GTM parameters.

auto-discovery

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

Context config>router>pim>gtm

Description This command enables or disables multicast auto-discovery via BGP for GTM.

The **no** form of the command disables auto-discovery.

Default no auto-discovery

Parameters **default** — Enables the default auto-discovery mode.

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

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

register-policy — 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 — Specifies the route policy name up to 32 characters in length. Route policies are configured in the **config>router>policy-options** context.

interface

Syntax [**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* — Specifies 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, and so on.), the entire string must be enclosed within double quotes.

Values 1 to 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.

assert-period

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

Context config>router>pim>interface

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 to 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)

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 resets the configuration to the default value.

Default hello-interval 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 to 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.

Default hello-multiplier 35

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

(**hello-interval** * **hello-multiplier**) / 10

This allows the PIMv2 default **hello-multiplier** of 3.5 and the default timeout of 105 seconds to be supported.

Values 20 to 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 RFC 4601, *Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (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 improved-assert

instant-prune-echo

Syntax [**no**] **instant-prune-echo**

Context config>router>pim>interface

Description This command enables PIM to send an instant prune echo when the router starts the prune pending timer for a group on the interface. All downstream routers will see the prune message immediately, and can send a join override if they are interested in receiving the group. Configuring instant-prune-echo is recommended on broadcast interfaces with more than one PIM neighbor to optimize multicast convergence.

The **no** form of the command disables instant Prune Echo on the PIM interface.

Default no instant-prune-echo

ipv4-multicast-disable

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

Context config>router>pim
config>router>pim>interface

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

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

ipv6-multicast-disable

Syntax **ipv6-multicast-disable**

Context config>router>pim
config>router>pim>interface

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

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

Default ipv6-multicast-disable

max-groups

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

Context config>router>pim>interface

Description This command specifies the maximum number of groups for which PIM can have local receiver information based on received PIM 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.

The **no** form of the command sets no limit to the number of groups.

Default no max-groups

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

Values 1 to 16000

monitor-oper-group

Syntax **monitor-oper-group** *group-name* **family** {**ipv4** | **ipv6**} {**add** | **set** | **subtract**} *value*
no monitor-oper-group [**family** {**ipv4** | **ipv6**}]

Context config>router>pim>if

Description This command configures PIM to monitor the state of an operational group to provide a redundancy mechanism. PIM monitors the operational group and changes its DR priority to the specified value when the status of the operational group is up. This enables the router to become the PIM DR only when the operational group is up. If the operational group status changes to down, PIM changes its DR priority to the default or the value configured with **priority** under **config**>**router**>**pim**>**if**. The **oper-group** *group-name* must already be configured under the **config**>**service** context before its name is referenced in this command. Two operational groups are supported per PIM interface.

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

Parameters *group-name* — Specifies the operational group identifier up to 32 characters in length.

family — Specifies the address family.

ipv4 — Specifies the IPv4 designated router priority.

ipv6 — Specifies the IPv6 designated router priority.

add — Specifies that the value is to be added to the existing priority to become the designated router.

subtract — Specifies that the value is to be subtracted from the existing priority to become the designated router.

set — Specifies the priority to become the designated router.

value — Specifies the priority modifier expressed as a decimal integer.

Values 1 to 4294967295

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 multicast-senders 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; however, 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).

Default no p2mp-ldp-tree-join

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).

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 priority 1

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

Values 1 to 4294967295

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 designated 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 no sticky-dr

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 to 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 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

lag-usage-optimization

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

Context config>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 forwarding complexes that own at least one link in the LAG.

Note: Changes made for multicast hashing cause Layer 4 multicast traffic to not be hashed. This is independent of if **lag-usage-optimization** is enabled or disabled.

Using this command and the **mc-ecmp-hashing-enabled** command on mixed port speed LAGs is not recommended, because some groups may be forwarded incorrectly.

Default no lag-usage-optimization

mc-ecmp-balance

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

Context config>router>pim

Description This command enables multicast balancing of traffic over ECMP links based on the number of (S, G) distributed over each link. When enabled, each new multicast stream that needs to be forwarded over an ECMP link is compared to the count of (S, G) already using each link, so that the link with the fewest (S, G) is chosen.

This command cannot be used together with the **mc-ecmp-hashing-enabled** command.

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

mc-ecmp-balance-hold

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

Context config>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** [**rebalance**]

Context config>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 address). When a link in the ECMP set is removed, the multicast flows that were using that link are redistributed 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 flows 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 cannot be used together with the **mc-ecmp-balance** command. Using this command and the **lag-usage-optimization** command on mixed port speed LAGs is not recommended, because some groups may be forwarded incorrectly.

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

Default no mc-ecmp-hashing-enabled

Parameters **rebalance** — Specifies to rebalance flows to newly added links immediately, instead of waiting until they are pruned.

multicast-fast-failover

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

Context config>router>pim

Description This command configures the option to enable Multicast-Only Fast Reroute (MoFRR) functionality for IPv4 PIM-SSM interfaces in the global routing table instance.

The **no** version of this command disables MoFRR for IPv4 PIM-SSM interfaces.

Default no multicast-fast-failover

multicast6-fast-failover

Syntax [**no**] **multicast6-fast-failover**

Context config>router>pim

Description This command configures the option to enable Multicast-Only Fast Reroute (MoFRR) functionality for IPv6 PIM-SSM interfaces in the global routing table instance.

The **no** version of this command disables MoFRR for IPv6 PIM-SSM interfaces.

Default no multicast6-fast-failover

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 designated 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-traffic can be used in the PIM context to have the router ignore the DR state and attract traffic when not DR. 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

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.

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.

Either **bsr-candidate** for IPv4 or **auto-rp-discovery** can be configured; the two mechanisms cannot be enabled together. **bsr-candidate** for IPv6 and **auto-rp-discovery** for IPv4 can be enabled together.

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

Default no auto-rp-discovery

bootstrap-export

Syntax **bootstrap-export** *policy-name* [*policy-name*]
no bootstrap-export

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 five 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*]
no bootstrap-import

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.

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.

Either **bsr-candidate** for IPv4 or **auto-rp-discovery** can be configured; the two mechanisms cannot be enabled together. **bsr-candidate** for IPv6 and **auto-rp-discovery** for IPv4 can be enabled together.

Default bsr-candidate shutdown

address

Syntax **address** *ip-address*

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

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

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.

Default hash-mask-len 30 — for config>router>pim>rp>bsr-candidate

hash-mask-len 126 — for config>router>pim>rp>ipv6>bsr-candidate

Parameters *hash-mask-length* — Specifies the hash mask length.

Values 0 to 32 (v4)
0 to 128 (v6)

priority

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

Context config>router>pim>rp>bsr-candidate
config>router>pim>rp>ipv6>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 priority 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 to 255

ipv6

Syntax **ipv6**

Context config>router>pim>rp

Description This command enables the context to configure IPv6 parameters.

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 candidate 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.

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 priority 192

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

Values 0 to 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 to FFFF]H
- d: [0 to 255]D

prefix-length: 16 to 128

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 rp-candidate shutdown

address

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

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

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* — Specifies the *ip-address.*

Values 1.0.0.0 – 223.255.255.255

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* — Specifies the multicast group IP address expressed in dotted decimal notation.

Values 224.0.0.0 to 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 decimal notation (255.255.0.0).

Values 4 to 32

netmask — Specifies the subnet mask in dotted decimal notation.

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

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*
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* — Specifies 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

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* — Specifies the IP prefix in dotted decimal notation for the range used by the ABR to advertise that summarizes the area into another area ipv6-prefix.

Values ipv4-prefix:

- a.b.c.d

ipv4-prefix-le: 0 to 32

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 to FFFF]H
- d: [0 to 255]D

ipv6-prefix-le: 0 to 128

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

netmask — Specifies the subnet mask in dotted decimal notation.

Values 0.0.0.0 to 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 to 255

group-prefix

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

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-ipv6-address* — Specifies the multicast group IPv6 address expressed in dotted decimal notation.

Values grp-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 — Specifies the prefix length of the IPv6 address

Values 8 to 128

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 dynamically-learned Rendezvous Points (RPs).

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

Default no override

rpf-table

Syntax **rpf-table** {**rtable-m** | **rtable-u** | **both**}
no rpf-table

Context config>router>pim

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 or rendezvous point. However, the operator can specify one of the following:

- use the unicast route table only
- use the multicast route table only
- use both the route tables

Default rpf-table rtable-u

Parameters

rtable6-m — Specifies that only the multicast route table will be used by the multicast protocol (PIM) for IPv4 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 IPv4 RPF checks. This route table will contain routes submitted by all the unicast routing protocols.

both — Specifies to 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. Rtable-m is checked before rtable6-u.

rpf6-table

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

Context config>router>pim

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:

- use unicast route table only
- use multicast route table only or
- use both the route tables

Default rpf6-table rtable6-u

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 that only 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 — Specifies that the multicast route table will be used first by the multicast protocol (PIM) for IPv6 RPF checks, and then the unicast route table will be used if the multicast route table lookup fails.

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.

If **rpfv** is configured, MLDP inter-AS resolution cannot be used. These two features are mutually exclusive.

Default no rpfv

Parameters

mvpn — Enables MVPN RPF vector processing for Inter-AS Option B/C MVPN based on RFC 5496 and RFC 6513. 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 SR OS 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 SR OS 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.

shutdown

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

Context 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>interface>mcac>mc-constraints

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 and 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

spt-switchover-threshold

Syntax **spt-switchover-threshold** {*grp-ipv4-prefix*/*ipv4-prefix-length* | *grp-ipv4-prefix netmask* | *grp-ipv6-prefix*/*ipv6-prefix-length*} *spt-threshold*

no spt-switchover-threshold {*grp-ipv4-prefix*/*ipv4-prefix-length* | *grp-ipv4-prefix netmask* | *grp-ipv6-prefix*/*ipv6-prefix-length*}

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-ipv4-prefix* — Specifies the group IPv4 multicast address in dotted decimal notation

Values a.b.c.d

ipv4-prefix-length — Specifies the length of the IPv4 prefix

Values 4 to 32

netmask — Specifies the netmask associated with the IPv4 prefix, expressed in dotted decimal notation. Network bits must be 1, and host bits must be 0.

Values a.b.c.d

grp-ipv6-prefix — Specifies the group IPv6 multicast address in hexadecimal notation

Values xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (eight 16-bit pieces)
x:x:x:x:x:x:d.d.d.d
xx — 0 to FF (hex)

ipv6-prefix-length — Specifies the length of the IPv6 prefix

Values 8 to 128

spt-threshold — Specifies the configured threshold in kilobits per second (kb/s) for a group prefix. A switchover is attempted only if the traffic rate on the shared tree for the group exceeds this configured threshold. When the **infinity** keyword is specified, no switchover will occur at any time, regardless of the traffic level is detected.

Values 1 to 4294967294 | infinity

ssm-groups

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

Context config>router>pim

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

tunnel-interface

Syntax [**no**] **tunnel-interface rsvp-p2mp** *lsp-name* **sender** *ip-address*

Context config>router>pim

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.

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

ip-address — :Specifies the sender IP address: a.b.c.d.

5.5 Show, Clear, and Debug Command Reference

5.5.1 Command Hierarchies

- Show Commands
- Clear Commands
- Debug Commands

5.5.1.1 Show Commands

show
— **router**
— **pim**
— **anycast** [**detail**]
— **crp** [*ip-address*]
— **s-pmsi** [*data-mt-interface-name*] [**detail**]
— **group** [*grp-ip-address*] [**source** *ip-address*] [**type** {**starstarrp** | **starg** | **sg**}] [**detail**] [**family**]
— **interface** [*ip-int-name* | *mt-int-name* | *ip-address*] [**group** [*grp-ip-address*] **source** *ip-address*] [**type** {**starstarrp** | **starg** | **sg**}] [**detail**] [**family**]
— **neighbor** [*ip-address* | *ip-int-name* [**address** *ip-address*]] [**detail**] [**family**]
— **rp** [*ip-address*]
— **rp-hash** *grp-ip-address*
— **statistics** [*ip-int-name* | *mt-int-name* | *ip-address*] [**family**]
— **status** [**detail**] [**family**]
— **tunnel-interface** [*ip-int-name* | *mt-int-name* | *int-ip-address*] [**group** [*grp-ip-address*] **source** *ip-address*] [**type** {**starstarrp** | **starg** | **sg**}] [**detail**] [*family*]

5.5.1.2 Clear Commands

clear
— **router**
— **pim**
— **database** [**interface** *ip-int-name* | *ip-address* | *mt-int-name*] [**group** *grp-ip-address* [**source ip-address**]] [**family**]]
— **neighbor** [**interface** *ip-int-name* | *ip-address*] [**family**]
— **s-pmsi** [*mdSrcAddr*] [*mdGrpAddr*] [*vprnSrcAddr vprnGrpAddr*]
— **statistics** [{[**interface** *ip-int-name* | *ip-address* | *mt-int-name*]} {[**group** *grp-ip-address* [**source** *ip-address*]]}][*family*]]

5.5.1.3 Debug Commands

debug
- **router**
  - **pim**
    - [**no**] **adjacency**
    - **all** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
    - **no all**
    - **assert** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
    - **no assert**
    - **auto-rp** [**detail**]
    - **no auto-rp**
    - **bgp** [**source** *ip-address*] [**group** *group-ip-address*] [**peer** *peer-ip-address*]
    - **no bgp**
    - **bsr** [**detail**]
    - **no bsr**
    - **data** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
    - **no data**
    - **db** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
    - **no db**
    - **dynmldp** [**detail**]
    - **no dynmldp**
    - **extranet** [**detail**]
    - **no extranet**
    - **grafts** [**source** *ip-address*] [**group** *grp-ip-address*] [**detail**]
    - **no grafts**
    - **interface** [*ip-int-name* | *mt-int-name*| *ip-address*] [**detail**]
    - **no interface**
    - **jp** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
    - **no jp**
    - [**no**] **mofrr**
    - **mrib** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
    - **no mrib**
    - **msg** [**detail**]
    - **no msg**
    - **mvpn-rtcache** [**group** *grp-ip-address*] [**peer** *ip-address*]
    - **no mvpn-rtcache**
    - **packet** [**hello** | **register** | **register-stop** | **jp** | **bsr** | **assert** | **crp** | **mdt-tlv** | **auto-rp-announcement** | **auto-rp-mapping** | **graft** | **graft-ack**] [*ip-int-name* | *mt-int-name* | *int-ip-address* | *mpls-if-name*] [**family** {**ipv4** | **ipv6**}] [**send** | **receive**]
    - **no packet**
    - **red** [**detail**]
    - **no red**
    - **register** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
    - **no register**
    - **rpfv** [**detail**]
    - **no rpfv**
    - **rtm** [**detail**]
    - **no rtm**
    - **s-pmsi** [{*vpnSrcAddr* [*vpnGrpAddr*]} [*mdSrcAddr*]] [**detail**]
    - **no s-pmsi**
    - **tunnel-interface** [**ldp-p2mp** *p2mp-id*] [**sender** *ip-address*] [**detail**]

— **no tunnel-interface** [**ldp-p2mp** *p2mp-id*] [**sender** *ip-address*]
— **tunnel-interface** [**rsvp-p2mp** *lsp-name*] [**sender** *ip-address*] [**detail**]
— **no tunnel-interface** [**rsvp-p2mp** *lsp-name*] [**sender** *ip-address*]

5.5.2 Command Descriptions

5.5.2.1 Show Commands

The command outputs in the following section are examples only; actual displays may differ depending on supported functionality and user configuration.

anycast

Syntax **anycast** [**detail**]

Context show>router>pim

Description This command displays PIM anycast rp-set information.

Parameters **detail** — Displays detailed information.

Output The following output displays an example of a PIM anycast configuration.

Sample Output

```
A:dut-d# show router pim anycast
===================================================
PIM Anycast RP Entries
===================================================
Anycast RP               Anycast RP Peer
---------------------------------------------------
100.100.100.1            10.102.1.1
                         10.103.1.1
                         10.104.1.1
---------------------------------------------------
PIM Anycast RP Entries : 3
===================================================
```

The following table provides PIM anycast field descriptions

Table 17 **PIM Anycast Fields**

Label	Description
Anycast Address	Displays the candidate anycast address.

Table 17 **PIM Anycast Fields (Continued)**

Label	Description
Anycast RP Peer	Displays the candidate anycast RP peer address.

crp

Syntax **crp** [*ip-address*]

Context show>router>pim

Description Display PIM candidate RP (CRP) information received at the elected Bootstrap router (BSR).

Parameters *ip-address* — The candidate RP IP address.

Output The following output is an example of a PIM CRP configuration.

Sample Output

```
A:WAS# show router pim crp
============================================================================
PIM Candidate RPs
============================================================================
RP Address      Group Address      Priority    Holdtime  Expiry Time
----------------------------------------------------------------------------
239.22.187.236    224.0.0.0/4        192         150       0d 00:02:19
239.22.187.239    224.0.0.0/4        192         150       0d 00:02:19
239.22.187.240    224.0.0.0/4        192         150       0d 00:02:09
----------------------------------------------------------------------------
Candidate RPs : 3
============================================================================
A:WAS#

A:WAS# show router pim crp 239.22.187.236
============================================================================
PIM Candidate RPs
============================================================================
RP Address      Group Address      Priority    Holdtime  Expiry Time
----------------------------------------------------------------------------
239.22.187.236    224.0.0.0/4        192         150       0d 00:01:43
----------------------------------------------------------------------------
Candidate RPs : 1
============================================================================
A:WAS#
```

The following table provides PIM CRP field descriptions.

Table 18 **PIM CRP Fields**

Label	**Description**
RP Address	Displays the Candidate RP address.
Group Address	Displays the range of multicast group addresses for which the CRP is the Candidate RP.
Priority	Displays the Candidate RP's priority for becoming a rendezvous point (RP). This value is used to elect RP for a group range. A value of 0 is considered as the highest priority.
Holdtime	Displays the hold time of the candidate RP. It is used by the Bootstrap router to time out the RP entries if it does not listen to another CRP advertisement within the holdtime period.
Expiry	The minimum time remaining before the CRP will be declared down. If the local router is not the BSR, this value is 0.
Candidate RPs	Displays the number of CRP entries.

s-pmsi

Syntax **s-pmsi** [*mdSrcAddr* [*mdGrpAddr*]] [**detail**]

Context show>router>pim

Description Displays the list of selective provider multicast service interfaces that are currently active.

Parameters *mdSrcAddr* — Specifies the source address of the multicast sender.

mdGrpAddr — Specifies the group address of the multicast sender.

detail — Displays detailed output.

Output The following output is an example of a PIM data MDT configuration

Sample Output PIM Selective Provider Tunnel

```
*B:node-6# show router 100 pim s-pmsi
===============================================================================
PIM Selective provider tunnels
===============================================================================
MD Src Address        MD Grp Address        MT Index      Num VPN SGs
-------------------------------------------------------------------------------
239.200.200.7         239.0.89.72           24603         1
239.200.200.7         239.0.89.73           24604         1
239.200.200.7         239.0.89.74           24605         1
239.200.200.7         239.0.89.75           24606         1
239.200.200.7         239.0.89.76           24607         1
239.200.200.7         239.0.89.77           24608         1
239.200.200.7         239.0.89.78           24609         1
```

```
239.200.200.7        239.0.89.79          24610         1
239.200.200.7        239.0.89.80          24611         1
239.200.200.7        239.0.89.81          24612         1
239.200.200.7        239.0.89.82          24613         1
239.200.200.7        239.0.89.83          24614         1
239.200.200.7        239.0.89.84          24615         1
239.200.200.7        239.0.89.85          24616         1
239.200.200.7        239.0.89.86          24617         1
239.200.200.7        239.0.89.87          24618         1
...
===============================================================================
*B:node-6#
```

Sample Output PIM Selective Provider Tunnel Detail

```
*B:node-6# show router 100 pim s-pmsi detail
===============================================================================
PIM Selective provider tunnels
===============================================================================
Md Source Address  : 239.200.200.7      Md Group Address   : 239.0.89.72
Number of VPN SGs  : 1                  Uptime             : 0d 00:00:18
MT IfIndex         : 24603              Egress Fwding Rate : 163.2 kbps

VPN Group Address  : 239.1.0.0          VPN Source Address : 10.2.102.1
State              : RX Joined
Expiry Timer       : 0d 00:02:41
===============================================================================
PIM Selective provider tunnels
===============================================================================
Md Source Address  : 239.200.200.7      Md Group Address   : 239.0.89.73
Number of VPN SGs  : 1                  Uptime             : 0d 00:00:18
MT IfIndex         : 24604              Egress Fwding Rate : 163.2 kbps

VPN Group Address  : 239.1.0.1          VPN Source Address : 10.2.102.1
State              : RX Joined
Expiry Timer       : 0d 00:02:41
===============================================================================
PIM Selective provider tunnels
===============================================================================
Md Source Address  : 239.200.200.7      Md Group Address   : 239.0.89.74
Number of VPN SGs  : 1                  Uptime             : 0d 00:00:20
MT IfIndex         : 24605              Egress Fwding Rate : 165.7 kbps

VPN Group Address  : 239.1.0.2          VPN Source Address : 10.2.102.1
State              : RX Joined
Expiry Timer       : 0d 00:02:39
===============================================================================
PIM Selective provider tunnels
===============================================================================
Md Source Address  : 239.200.200.7      Md Group Address   : 239.0.89.75
Number of VPN SGs  : 1                  Uptime             : 0d 00:00:20
MT IfIndex         : 24606              Egress Fwding Rate : 165.7 kbps

VPN Group Address  : 239.1.0.3          VPN Source Address : 10.2.102.1
State              : RX Joined
Expiry Timer       : 0d 00:02:39
===============================================================================
```

```
*B:node-6#
```

Sample Output for Rosen MVPN S-PMSI Tunnel

```
B:Dut-E# show router 100 pim s-pmsi
===============================================================================
PIM Selective provider tunnels
===============================================================================
MD Src Address      MT Index          Num VPN SGs  MD RP for ASM   State
   MD Grp Address      Multistream ID
-------------------------------------------------------------------------------
10.20.1.5           5798467           1            N/A             TX Joined
   233.0.0.5           5
10.20.1.5           5798468           1            N/A             TX Joined
   233.0.0.6           6
10.20.1.5           5798469           1            N/A             TX Joined
   233.0.0.7           7
10.20.1.5           5798470           1021         N/A             TX Joined
   233.0.0.8           8
===============================================================================
PIM Selective provider tunnels Interfaces : 4
```

Sample Output RX Tracking for RSVP S-PMSI Tunnel

```
*A:Dut-C# show router 1 pim s-pmsi
===============================================================================
PIM RSVP Spmsi tunnels
===============================================================================
P2mp ID   Tunnel ID   Ext Tunnel Adrs       SPMSI Index   Num VPN   State
                                                          SGs
-------------------------------------------------------------------------------
0         0           10.20.1.4             1030144       1         RX Tracking
0         0           10.20.1.4             1030144       1         RX Tracking
===============================================================================
PIM RSVP Spmsi Interfaces : 2
===============================================================================
*A:Dut-C# show router 21 pim s-pmsi

====================================================================
PIM LDP Spmsi tunnels
====================================================================
Lsp ID    Root Addr             SPMSI Index   Num VPN   State
                                              SGs
--------------------------------------------------------------------
0         10.20.1.4             1030144       1         RX Tracking
0         10.20.1.4             1030144       1         RX Tracking
====================================================================
PIM LDP Spmsi Interfaces : 2
====================================================================
*A:Dut-C#
```

Sample Output RX Tracking for RSVP S-PMSI Tunnel Detail

```
*A:Dut-C# show router 1 pim s-pmsi detail
===============================================================================
PIM RSVP Spmsi tunnels
```

```
===============================================================================
P2MP ID            : 0                    Tunnel ID          : 0
Ext Tunnnel Addrs  : 10.20.1.4            Spmsi IfIndex      : 1030144
Number of VPN SGs  : 1                    Uptime             : 0d 00:02:48

VPN Group Address  : 239.100.0.0
VPN Source Address : 10.1.101.2
State              : RX Tracking        Mdt Threshold      : 0

===============================================================================
PIM RSVP Spmsi tunnels
===============================================================================
P2MP ID            : 0                    Tunnel ID          : 0
Ext Tunnnel Addrs  : 10.20.1.4            Spmsi IfIndex      : 1030144
Number of VPN SGs  : 1                    Uptime             : 0d 00:02:47

VPN Group Address  : ff0e:db8:225:100::
VPN Source Address : 2001:db8:1:101::2
State              : RX Tracking        Mdt Threshold      : 0
===============================================================================
PIM RSVP Spmsi Interfaces : 2
===============================================================================
*A:Dut-C#

*A:Dut-C# show router 21 pim s-pmsi detail
===============================================================================
PIM LDP Spmsi tunnels
===============================================================================
LSP ID             : 0
Root Addr          : 10.20.1.4            Spmsi IfIndex      : 1030144
Number of VPN SGs  : 1                    Uptime             : 0d 00:03:35

VPN Group Address  : 239.100.0.0
VPN Source Address : 10.1.101.2
State              : RX Tracking        Mdt Threshold      : 0

===============================================================================
PIM LDP Spmsi tunnels
===============================================================================
LSP ID             : 0
Root Addr          : 10.20.1.4            Spmsi IfIndex      : 1030144
Number of VPN SGs  : 1                    Uptime             : 0d 00:03:34

VPN Group Address  : ff0e:db8:225:100::
VPN Source Address : 2001:db8:1:101::2
State              : RX Tracking        Mdt Threshold      : 0
===============================================================================
PIM LDP Spmsi Interfaces : 2
===============================================================================
*A:Dut-C#
```

Sample Output TX Tracking for RSVP S-PMSI Tunnel Detail

```
*A:Dut-C# show router 1 pim s-pmsi detail
===============================================================================
PIM RSVP Spmsi tunnels
===============================================================================
P2MP ID            : 1                    Tunnel ID          : 61442
```

```
Ext Tunnnel Addrs  : 10.20.1.4          Spmsi IfIndex      : 74230
Number of VPN SGs  : 1                  Uptime             : 0d 00:05:11

VPN Group Address  : 239.100.0.0
VPN Source Address : 10.1.101.2
State              : TX Join Pending    Mdt Threshold      : 1
Join Timer         : N/A                Holddown Timer     : 0d 00:00:47
Receiver Count     : 4

===============================================================================
PIM RSVP Spmsi tunnels
===============================================================================
P2MP ID            : 1                  Tunnel ID          : 61443
Ext Tunnnel Addrs  : 10.20.1.4          Spmsi IfIndex      : 74231
Number of VPN SGs  : 1                  Uptime             : 0d 00:05:10

VPN Group Address  : ff0e:225:100::
VPN Source Address : 2001:db8:1:101::2
State              : TX Join Pending    Mdt Threshold      : 1
Join Timer         : N/A                Holddown Timer     : 0d 00:00:50
Receiver Count     : 4
===============================================================================
PIM RSVP Spmsi Interfaces : 2
===============================================================================
*A:Dut-C#

*A:Dut-D# show router 21 pim s-pmsi detail
===============================================================================
PIM LDP Spmsi tunnels
===============================================================================
LSP ID             : 8194
Root Addr          : 10.20.1.4          Spmsi IfIndex      : 74228
Number of VPN SGs  : 1                  Uptime             : 0d 00:05:56

VPN Group Address  : 239.100.0.0
VPN Source Address : 10.1.101.2
State              : TX Join Pending    Mdt Threshold      : 1
Join Timer         : N/A                Holddown Timer     : 0d 00:00:02
Receiver Count     : 4

===============================================================================
PIM LDP Spmsi tunnels
===============================================================================
LSP ID             : 8195
Root Addr          : 10.20.1.4          Spmsi IfIndex      : 74229
Number of VPN SGs  : 1                  Uptime             : 0d 00:05:55

VPN Group Address  : ff0e:db8:225:100::
VPN Source Address : 2001:db8:1:101::2
State              : TX Join Pending    Mdt Threshold      : 1
Join Timer         : N/A                Holddown Timer     : 0d 00:00:05
Receiver Count     : 4
===============================================================================
PIM LDP Spmsi Interfaces : 2
===============================================================================
*A:Dut-D#
```

Table 19 provides PIM data MDT descriptions.

Table 19 **PIM Data MDT**

Label	**Description**
MD Grp Address	Displays the IP multicast group address for which this entry contains information.
MD Src Address	Displays the source address of the multicast sender. It will be 0 if the type is configured as **starg**. It will be the address of the Rendezvous Point (RP) if the type is configured as **starRP**.
MT Index	Displays the index number.
Num VP SGs	Displays the VPN number.

group

Syntax **group** *grp-ip-address* [**source** *ip-address* [**type** {**starstarrp** | **starg** | **sg**}] [**detail**] [*family*]

Context show>router>pim

Description This command displays PIM source group database information.

Parameters *grp-ip-address* — Specifies the IP multicast group address for which this entry contains information.

source *ip-address* — Specifies the source address for which this entry contains information.

type starstarrp — Specifies that only (*, *, rp) entries be displayed.

type starg — Specifies that only (*,G) entries be displayed.

type sg — specifies that only (S,G) entries be displayed.

detail — Displays detailed group information.

family — Displays either IPv4 or IPv6 information.

Output PIM Group Output

The following table provides PIM Group field descriptions.

Table 20 **PIM Group Fields**

Label	**Description**
Group Address	Displays the IP multicast group address for which this entry contains information.

Table 20 **PIM Group Fields (Continued)**

Label	Description
Source Address	Displays the source address of the multicast sender. It will be 0 if the type is configured as starg. It will be the address of the Rendezvous Point (RP) if the type is configured as starRP.
RP Address	Displays the RP address.
Type	Specifies the type of entry, (*,*, rp)/(*,G) or (S,G).
Spt Bit	Specifies whether to forward on (*,*, rp)/(*,G) or on (S,G) state. It is updated when the (S,G) data comes on the RPF interface towards the source.
Incoming Intf	Displays the interface on which the traffic comes in. It can be the RPF interface to the RP (if starg) or the source (if sg).
Num Oifs	Displays the number of interfaces in the inherited outgoing interface list. An inherited list inherits the state from other types.
Flags	Displays the different lists that this interface belongs to.
Keepalive Timer Exp	The keepalive timer is applicable only for (S,G) entries. The (S,G) keepalive timer is updated by data being forwarded using this (S,G) Forwarding state. It is used to keep (S,G) state alive in the absence of explicit (S,G) joins.
MRIB Next Hop	Displays the next hop address towards the RP.
MRIB Src Flags	Displays the MRIB information about the source. If the entry is of type starg or starstarrp, it will contain information about the RP for the group.
Up Time	Displays the time since this source group entry was created.
Resolved By	Displays the route table used for RPF check.
Up JP State	Displays the upstream join prune state for this entry on the interface. PIM join prune messages are sent by the downstream routers towards the RPF neighbor.
Up JP Expiry	Displays the minimum amount of time remaining before this entry will be aged out.
Up JP Rpt	Displays the join prune Rpt state for this entry on the interface. PIM join/prune messages are sent by the downstream routers towards the RPF neighbor. (S,G, rpt) state is a result of receiving (S,G, rpt) JP message from the downstream router on the RP tree.

Table 20 **PIM Group Fields (Continued)**

Label	Description
Up JP Rpt Override	Displays the value used to delay triggered Join (S,G, rpt) messages to prevent implosions of triggered messages. If this has a non-zero value, it means that the router was in 'notPruned' state and it saw a prune (S,G, rpt) message being sent to RPF (S,G, rpt). If the router sees a join (S,G, rpt) override message being sent by some other router on the LAN while the timer is still non-zero, it simply cancels the override timer. If it does not see a join (S,G, rpt) message, then on expiry of the override timer, it sends its own join (S,G, rpt) message to RPF (S,G, rpt). A similar scenario exists when RPF (S,G, rpt) changes to become equal to RPF (*,G).
Register State	Specifies the register state. The register state is kept at the source DR. When the host starts sending multicast packets and if there are no entries programmed for that group, the source DR sends a register packet to the RP (g). Register state transition happen based on the register stop timer and the response received from the RP.
Register Stop Exp	Displays the time remaining before the register state might transition to a different state.
Register from Anycast RP	Displays if the register packet for that group has been received from one of the RP from the anycast-RP set.
RPF Neighbor	Displays the address of the RPF neighbor.
Outgoing Intf List	Displays a list of interfaces on which data is forwarded.
Curr Fwding Rate	Displays the current forwarding rate of the multicast data for this group and source. This forwarding rate is calculated before ingress QoS policing or shaping is applied.
Forwarded Packets	Displays the number of multicast packets that were forwarded to the interfaces in the outgoing interface list. This packet count is before ingress QoS policing or shaping is applied.
Discarded Packets	Displays the number of multicast packets that matched this source group entry but were discarded. For (S,G) entries, if the traffic is getting forwarded on the SPT, the packets arriving from the RPT will be discarded.
Forwarded Octets	Displays the number of octets forwarded.
RPF Mismatches	Displays the number of multicast packets that matched this source group entry but they did not arrive on the interface.

Table 20 PIM Group Fields (Continued)

Label	Description
Spt threshold	Displays the value of the SPT threshold configured for that group. 0 kb/s means that the switch to the SP tree will happen immediately.

Sample Output

```
A:Dut-A# show router pim group
===============================================================================
PIM Group ipv4
===============================================================================
Group Address                Type              Spt Bit Inc Intf         no.Oifs
 Source Address                RP                        Inc Intf(S)
-------------------------------------------------------------------------------
239.1.1.1                    (S,G)                     ip-10.10.2.1      1
   10.1.1.2                      10.20.1.4                 ip-10.10.1*
===============================================================================
A:Dut-A#

*A:Dut-C# show router 100 pim group ipv6
===============================================================================
Legend:  A = Active   S = Standby
===============================================================================
PIM Groups ipv6
===============================================================================
Group Address                Type               Spt Bit  Inc Intf       No.Oifs
   Source Address               RP                  State    Inc Intf(S)
-------------------------------------------------------------------------------
ff04:db8:224:100:0:0            (*,G)                        vprn_itf_C_11* 2
   *                             2001:db8:110:100:1*
ff04:db8:224:100:0:0            (S,G)               spt      mpls-if-74457* 3
   2001:db8:100:114:1:2            2001:db8:110:100:1*
ff04:db8:224:100:0:1            (*,G)                        vprn_itf_C_11* 2
   *                            2001:db8:110:100:1*
ff04:db8:224:100:0:1            (S,G)               spt      mpls-if-74457* 3
   2001:db8:100:114:1:2            2001:db8:110:100:1*
ff04:db8:224:100:0:2            (*,G)                        vprn_itf_C_11* 2
   *                            2001:db8:110:100:1*
ff04:db8:224:100:0:2            (S,G)               spt      mpls-if-74457* 3
   2001:db8:100:114:1:2            2001:db8:110:100:1*
ff04:db8:224:100:0:3            (*,G)                        vprn_itf_C_11* 2
   *                            2001:db8:110:100:1*
ff04:db8:224:100:0:3            (S,G)               spt      mpls-if-74457* 3
    2001:db8:100:114:1:2            2001:db8:110:100:1*
ff04:db8:224:100:0:4            (*,G)                        vprn_itf_C_11* 2
   *                            2001:db8:110:100:1*
ff04:db8:224:100:0:4            (S,G)               spt      mpls-if-74457* 3
    2001:db8:100:114:1:2            2001:db8:110:100:1*
-------------------------------------------------------------------------------
Groups : 10
===============================================================================
* indicates that the corresponding row element may have been truncated.
*A:Dut-C#
```

```
A:NYC>show>router>pim# group 239.255.255.250
===============================================================================
PIM Groups
===============================================================================
Group Address   Source Address  RP Address      Type     Spt Incoming      Num
                                                         Bit Intf          Oifs
-------------------------------------------------------------------------------
239.255.255.250 *               10.22.187.240   <*,G>      nyc-sjc        1
-------------------------------------------------------------------------------
Groups : 1
===============================================================================
A:NYC>show>router>pim#

A:NYC>show>router>pim# group 239.255.255.250 detail
===============================================================================
PIM Source Group
===============================================================================
Group Address      : 239.255.255.250 Source Address     : 10.1.1.2
RP Address         : 10.100.100.1      Type               : (S,G)
Flags              : spt, rpt-prn-des   Keepalive Timer Exp: 0d 00:03:07
MRIB Next Hop      : 10.1.1.2           MRIB Src Flags     : direct
Up Time            : 0d 00:00:50        Resolved By        : rtable-u

Up JP State        : Joined             Up JP Expiry       : 0d 00:00:00
Up JP Rpt          : Pruned             Up JP Rpt Override : 0d 00:00:00

Register State     : Pruned             Register Stop Exp  : 0d 00:00:47
Reg From Anycast RP: No

RPF Neighbor       : 10.1.1.2
Incoming Intf      : SOURCE-3
Outgoing Intf List : To-Dut-A

Curr Fwding Rate   : 482.9 kbps
Forwarded Packets  : 1262               Discarded Packets  : 0
Forwarded Octets   : 1269572            RPF Mismatches     : 0
Spt threshold      : 0 kbps
===============================================================================
A:NYC>show>router>pim#

B:Dut-C# show router pim group 239.0.0.1 type sg detail
===============================================================================
PIM Source Group ipv4
===============================================================================
Group Address      : 239.0.0.1
Source Address     : 10.11.0.1
RP Address         : 10.20.1.3
Flags              : rpt-prn-des        Type               : (S,G)
MRIB Next Hop      : 10.11.0.1
MRIB Src Flags     : direct             Keepalive Timer    : Not Running
Up Time            : 0d 00:04:17        Resolved By        : rtable-u

Up JP State        : Joined             Up JP Expiry       : 0d 00:00:00
Up JP Rpt          : Pruned             Up JP Rpt Override : 0d 00:00:00

Register State     : No Info
Reg From Anycast RP: No

Rpf Neighbor       : 10.11.0.1
```

```
Incoming Intf      : svc_itf
Outgoing Host List : 239.112.1.1

Curr Fwding Rate   : 0.0 kbps
Forwarded Packets  : 0                  Discarded Packets  : 0
Forwarded Octets   : 0                  RPF Mismatches     : 0
Spt threshold      : 0 kbps             ECMP opt threshold : 7
Admin bandwidth    : 1 kbps             Preference         : 0

===============================================================================
PIM Source Group ipv4
===============================================================================
Group Address      : 239.0.0.1
Source Address     : 10.11.0.2
RP Address         : 10.20.1.3
Flags              :                    Type               : (S,G)
MRIB Next Hop      : 10.11.0.2
MRIB Src Flags     : direct             Keepalive Timer    : Not Running
Up Time            : 0d 00:04:18        Resolved By        : rtable-u

Up JP State        : Joined             Up JP Expiry       : 0d 00:00:00
Up JP Rpt          : Not Pruned         Up JP Rpt Override : 0d 00:00:00

Register State     : No Info
Reg From Anycast RP: No

Rpf Neighbor       : 10.11.0.2
Incoming Intf      : svc_itf
Outgoing Host List : 10.112.1.1, 10.112.1.2

Curr Fwding Rate   : 0.0 kbps
Forwarded Packets  : 0                  Discarded Packets  : 0
Forwarded Octets   : 0                  RPF Mismatches     : 0
Spt threshold      : 0 kbps             ECMP opt threshold : 7
Admin bandwidth    : 1 kbps             Preference         : 0
-------------------------------------------------------------------------------
Groups : 2
===============================================================================
*B:Dut-C#

A:Dut-A# show router pim group detail
===============================================================================
PIM Source Group ipv4
===============================================================================
Group Address      : 239.1.1.1
Source Address     : 10.1.1.21
RP Address         : 10.20.1.4
Advt Router        : 10.20.1.3
Flags              :                    Type               : (S,G)
MRIB Next Hop      : 10.10.2.3
MRIB Src Flags     : remote             Standby Src Flags  : remote
keepalive Timer    : Not Running
Up Time            : 0d 00:01:22        Resolved By        : rtable-u

Up JP State        : Joined             Up JP Expiry       : 0d 00:00:00
Up JP Rpt          : Pruned             Up JP Rpt Override : 0d 00:00:00
Up Stdby JP State  : Joined             Up Stdby JP Expiry : 0d 00:00:12

Register State     : No Info
```

```
Reg From Anycast RP: No

Rpf Neighbor       : 10.10.2.3          Stdby Rpf Neighbor : 10.10.1.2
Incoming Intf      : ip-10.10.2.1       Stdby Intf         : ip-10.10.1.1
Outgoing Host List : ix

Curr Fwding Rate   : 0.0 kbps
Forwarded Packets  : 0                  Discarded Packets  : 0
Forwarded Octets   : 0                  RPF Mismatches     : 0
Spt threshold      : 0 kbps             ECMP opt threshold : 7
Admin bandwidth    : 1 kbps
===============================================================================
PIM Source Group ipv4
```

interface

Syntax **interface** [*ip-int-name* | *mt-int-name* | *ip-address*] [**group** *grp-ip-address* | **source** *ip-address* [**type** {**starstarrp** | **starg** | **sg**}] [**detail**] [**family**]

Context show>router>pim

Description This command displays PIM interface information and the (S,G)/(*,G)/(*, *, rp) state of the interface.

Parameters *ip-int-name* — Only displays the interface information associated with the specified IP interface name.

mt-int-name — Specifies the Multicast Tunnel (MT) interface for a VPRN.

Values <*vprn-id*>-mt-<*grp-ip-address*>

ip-address — Only displays the interface information associated with the specified IP address.

group *grp-ip-address* — Specifies the IP multicast group address for which this entry contains information.

source *ip-address* — Specifies the source address for which this entry contains information.

If the type is starg, the value of this object will be zero.

If the type is starstarrp, the value of this object will be address of the RP.

type — Specifies the type of this entry.

Values **starstarrp**, **starg**, **sg**

detail — Displays detailed interface information.

family — Displays IPv4 or IPv6 information for the interface.

Output The following output is an example of a PIM interface configuration.

Sample Output

```
ALA-1# show router pim interface
```

```
===============================================================================
PIM Interfaces
===============================================================================
Interface                       Admin  Oper   DR              DR        Hello
                                State  State                  Priority  Intvl
-------------------------------------------------------------------------------
system                          Up     Up     N/A             1         30
ip-10.1.7.1                     Up     Up     10.1.7.7        5         30
ip-10.1.2.1                     Up     Up     10.1.2.2        5         30
ip-10.111.1.1                   Up     Up     10.111.1.1     5         30
-------------------------------------------------------------------------------
Interfaces : 4
===============================================================================
ALA-1#

ALA-1# show router pim interface ip-10.1.2.1 detail
===============================================================================
PIM Interface ip-10.1.2.1
===============================================================================
Interface                       Admin  Oper   DR              DR        Hello
                                State  State                  Priority  Intvl
-------------------------------------------------------------------------------
ip-10.1.2.1                     Up     Up     10.1.2.2        5         30
-------------------------------------------------------------------------------
PIM Group Source
-------------------------------------------------------------------------------
Group Address      : 239.101.0.5        Src Address        : 10.111.1.2
Interface          : ip-10.1.2.1        Type               : <S,G>
RP Address         : 239.200.200.4

Join Prune State   : Join               Expires            : 0d 00:03:00
Prune Pend Expires : N/A

Assert State       : No Info
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
ALA-1#

ALA-1# show router pim interface group
===============================================================================
PIM Interface ip-10.1.7.1
===============================================================================
Interface                       Admin  Oper   DR              DR        Hello
                                State  State                  Priority  Intvl
-------------------------------------------------------------------------------
ip-10.1.7.1                     Up     Up     10.1.7.7        5         30
-------------------------------------------------------------------------------
Group Address    Source Address   RP Address       Type     JP        Assert
-------------------------------------------------------------------------------
239.101.0.0      10.111.1.2      239.200.200.4    <S,G>    Join      No Info
239.101.0.1      10.111.1.2      239.200.200.4    <S,G>    Join      No Info
239.101.0.2      10.111.1.2      239.200.200.4    <S,G>    Join      No Info
239.101.0.3      10.111.1.2      239.200.200.4    <S,G>    Join      No Info
239.101.0.4      10.111.1.2      239.200.200.4    <S,G>    Join      No Info
239.101.0.6      10.111.1.2      239.200.200.4    <S,G>    Join      No Info
239.101.0.7      10.111.1.2      239.200.200.4    <S,G>    Join      No Info
239.101.0.8      10.111.1.2      239.200.200.4    <S,G>    Join      No Info
239.101.0.9      10.111.1.2      239.200.200.4    <S,G>    Join      No Info
```

```
===============================================================================
PIM Interface ip-10.1.2.1
===============================================================================
Interface                       Admin  Oper   DR              DR        Hello
                                State  State                  Priority  Intvl
-------------------------------------------------------------------------------
ip-10.1.2.1                     Up     Up     10.1.2.2        5         30
-------------------------------------------------------------------------------
Group Address    Source Address   RP Address       Type     JP        Assert
-------------------------------------------------------------------------------
239.101.0.5      10.111.1.2      239.200.200.4    <S,G>    Join      No Info
===============================================================================
PIM Interface ip-10.111.1.1
===============================================================================
Interface                       Admin  Oper   DR              DR        Hello
                                State  State                  Priority  Intvl
-------------------------------------------------------------------------------
ip-10.111.1.1                  Up     Up     10.111.1.1     5         30
-------------------------------------------------------------------------------
Group Address    Source Address   RP Address       Type     JP        Assert
-------------------------------------------------------------------------------
239.102.0.0      *                239.200.200.4    <*,G>    Join      No Info
239.102.0.1      *                239.200.200.4    <*,G>    Join      No Info
239.102.0.2      *                239.200.200.4    <*,G>    Join      No Info
239.102.0.3      *                239.200.200.4    <*,G>    Join      No Info
239.102.0.4      *                239.200.200.4    <*,G>    Join      No Info
239.102.0.5      *                239.200.200.4    <*,G>    Join      No Info
239.102.0.6      *                239.200.200.4    <*,G>    Join      No Info
239.102.0.7      *                239.200.200.4    <*,G>    Join      No Info
239.102.0.8      *                239.200.200.4    <*,G>    Join      No Info
239.102.0.9      *                239.200.200.4    <*,G>    Join      No Info
-------------------------------------------------------------------------------
Interfaces : 3
===============================================================================
ALA-1#

ALA-1# show router pim interface group 239.102.0.0 detail
===============================================================================
PIM Interface ip-10.111.1.1
===============================================================================
Interface                       Admin  Oper   DR              DR        Hello
                                State  State                  Priority  Intvl
-------------------------------------------------------------------------------
ip-10.111.1.1                  Up     Up     10.111.1.1     5         30
-------------------------------------------------------------------------------
PIM Group Source
-------------------------------------------------------------------------------
Group Address      : 239.102.0.0        Src Address        : *
Interface          : ip-10.111.1.1     Type               : <*,G>
RP Address         : 239.200.200.4

Join Prune State   : Join               Expires            : 0d 00:02:05
Prune Pend Expires : N/A

Assert State       : No Info
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
ALA-1#
```

```
ALA-1# show router pim interface type starg
===============================================================================
PIM Interface ip-10.111.1.1
===============================================================================
Interface                     Admin  Oper   DR              DR        Hello
                              State  State                  Priority  Intvl
-------------------------------------------------------------------------------
ip-10.111.1.1                Up     Up     10.111.1.1     5         30
-------------------------------------------------------------------------------
Group Address    Source Address   RP Address       Type     JP        Assert
-------------------------------------------------------------------------------
239.102.0.0      *                239.200.200.4    <*,G>    Join      No Info
239.102.0.1      *                239.200.200.4    <*,G>    Join      No Info
239.102.0.2      *                239.200.200.4    <*,G>    Join      No Info
239.102.0.3      *                239.200.200.4    <*,G>    Join      No Info
239.102.0.4      *                239.200.200.4    <*,G>    Join      No Info
239.102.0.5      *                239.200.200.4    <*,G>    Join      No Info
239.102.0.6      *                239.200.200.4    <*,G>    Join      No Info
239.102.0.7      *                239.200.200.4    <*,G>    Join      No Info
239.102.0.8      *                239.200.200.4    <*,G>    Join      No Info
239.102.0.9      *                239.200.200.4    <*,G>    Join      No Info
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
ALA-1#

A:SetupCLI# show router pim interface detail
===============================================================================
PIM Interface ipv4 toRemoteSite_1001
===============================================================================
Admin Status       : Up                Oper Status        : Up
IPv4 Admin Status  : Up                IPv4 Oper Status   : Up
DR                 : 10.1.1.5
Oper DR Priority   : 5
OperGroup          : vrrp1_1           OprGrp Active oper : set
Cfg OprGrp Priority: 255
BSM RA Check       : Disabled          Cfg DR Priority    : 1
Hello Interval     : 30                Time for next hello: 0d 00:00:03
Multicast Senders  : auto              Hello Multiplier   : 35
J/P Tracking Admin : Disabled          J/P Tracking Oper  : Disabled
Auto-created       : No                Improved Assert    : Enabled
Sticky-DR          : Disabled          Sticky-DR Priority : N/A
Max Groups Allowed : 0                 Max Groups Till Now: 0
Num Groups         : 0                 Bfd enabled        : No
Three-way Hello    : 0                 Assert-Period      : No
Instant Prune Echo : Disabled          P2MP LDP Tree Join : Disabled
MCAC Policy Name   : 0                 MCAC Const Adm St  : Enable
MCAC Max Unconst BW:no limit           MCAC Max Mand BW   : no limit
MCAC In use Mand BW: 0                 MCAC Avail Mand BW : unlimited
MCAC In use Opnl BW: 0                 MCAC Avail Opnl BW : unlimited
Use LAG port weight: no
MCAC If-Policy Name:
-------------------------------------------------------------------------------
Interfaces : 1 Tunnel-Interfaces : 0
===============================================================================
```

The following table provides PIM interface field descriptions.

Table 21 PIM Interface Fields

Label	Description
Admin State	Displays the administrative state for PIM protocol on this interface.
Oper State	Displays the current operational state of PIM protocol on this interface.
DR	Displays the designated router on this PIM interface.
DR Priority	Displays the priority value sent in PIM Hello messages and that is used by routers to elect the designated router (DR).
Hello Intvl	Indicates the frequency at which PIM Hello messages are transmitted on this interface.
OperGroup	Displays the OperGroup name associated with the PIM interface.
OprGrp Active oper	Displays the OperGroup operation (add, set, subtract) to the DR priority.
Cfg OprGrp Priority	Displays the configured OperGroup DR priority.

neighbor

Syntax **neighbor** [*ip-address* | *ip-int-name* [**address** *ip-address*]] [**detail**] [*family*]

Context show>router>pim

Description This command displays PIM neighbor information.

This can be important if an interface has more than one adjacency. For example, a LAN-interface configuration with three routers connected and all are running PIM on their LAN interfaces. These routers then have two adjacencies on their LAN interface, each with different neighbors. If the **address** *ip-address* parameter is not defined in this example, then the **show** command output would display two adjacencies.

Parameters **neighbor** *ip-int-name* — Only displays the interface information associated with the specified IP interface name.

neighbor *ip-address* — Only displays the interface information associated with the specified IP address.

address *ip-address* — The ip-address of the neighbor, on the other side of the interface.

detail — Displays detailed neighbor information.

family — Displays either IPv4 or IPv6 information for the specified neighbor.

Output The following output is an example of a PIM neighbor configuration.

Sample Output

```
ALA-1# show router pim neighbor
===============================================================================
PIM Neighbors
===============================================================================
Interface          Nbr DR     Nbr Address     Up Time       Expiry Time   Hold
                   Priority                                               Time
-------------------------------------------------------------------------------
ip-10.1.7.1        5          10.1.7.7        0d 00:10:39   0d 00:01:36   105
ip-10.1.2.1        5          10.1.2.2        0d 00:10:39   0d 00:01:35   105
ip-10.111.1.1      3          10.111.1.2      0d 00:09:31   0d 00:01:15   105
-------------------------------------------------------------------------------
Neighbors : 3
===============================================================================
ALA-1#

*A:Dut-C# show router 100 pim neighbor ipv6
===============================================================================
PIM Neighbor ipv6
===============================================================================
Interface               Nbr DR Prty     Up Time       Expiry Time     Hold Time
   Nbr Address
-------------------------------------------------------------------------------
vprn_itf_C_1100         1               0d 00:02:54   0d 00:01:43     105
   ff00:db8:4403:1ff:fe01:2
mpls-if-74456(W)        1               0d 00:02:10   never           65535
   ff00:db8:a14:104
mpls-if-74457(W)        1               0d 00:02:10   never           65535
   ff00:db8:a14:105
mpls-virt-if-1030145    1               0d 00:02:44   never           65535
   ff00:db8:a14:102
-------------------------------------------------------------------------------
Neighbors : 4
===============================================================================

ALA-1# show  router pim neighbor detail
===============================================================================
PIM Neighbor
===============================================================================
Interface          : ip-10.1.7.1
Neighbor Addr      : 10.1.7.7           DR Priority         : 5
Tracking Support   : No                 LAN Delay(ms)       : 500
Gen Id             : 26470              Override Intvl(ms)  : 2500
Up Time            : 0d 00:10:41        Expiry Time         : 0d 00:01:34
Hold Time(sec)     : 105
===============================================================================
PIM Neighbor
===============================================================================
Interface          : ip-10.1.2.1
Neighbor Addr      : 10.1.2.2           DR Priority         : 5
Tracking Support   : No                 LAN Delay(ms)       : 500
Gen Id             : 37928              Override Intvl(ms)  : 2500
Up Time            : 0d 00:10:42        Expiry Time         : 0d 00:01:33
Hold Time(sec)     : 105
===============================================================================
PIM Neighbor
===============================================================================
Interface          : ip-10.111.1.1
```

```
Neighbor Addr       : 10.111.1.2       DR Priority        : 3
Tracking Support    : No                LAN Delay(ms)       : 500
Gen Id              : 742098371         Override Intvl(ms)  : 2500
Up Time             : 0d 00:09:33       Expiry Time         : 0d 00:01:43
Hold Time(sec)      : 105
-------------------------------------------------------------------------------
Neighbors : 3
===============================================================================
ALA-1#
```

Table 22 provides PIM neighbor field descriptions.

Table 22 **PIM Neighbor Fields**

Label	Description
Interface	Displays the neighbor’s interface name. (W) indicates wildcard tunnels.
Nbr DR Priority	Displays the value of the neighbor's DR priority which is received in the hello message.
Nbr Address	Displays the neighbor’s address.
Up Time	Displays the time since this PIM neighbor (last) became a neighbor of the local router.
Expiry Time	Displays the minimum time remaining before this PIM neighbor will be aged out. 0—Means that this neighbor will never be aged out. This happens when the PIM neighbor sends a Hello message with holdtime set to `0xffff'.
Hold Time	Displays the value of the hold time present in the hello message.
DR Priority	Displays the value of the neighbor's DR priority which is received in the hello message.
Tracking Support	Displays whether the T bit in the LAN prune delay option was present in the hello message. This indicates the neighbor's capability to disable join message suppression.
LAN Delay	Displays the value of the LAN delay field present in the hello message received from the neighbor.
Gen Id	Displays a randomly generated 32-bit value that is regenerated each time PIM forwarding is started or restarted on the interface, including when the router itself restarts. When a hello message with a new GenID is received from a neighbor, any old hello information about that neighbor is discarded and superseded by the information from the new hello message.

Table 22 PIM Neighbor Fields (Continued)

Label	Description
Override Intvl (ms)	Displays the value of the override interval present in the Hello message.

rp

Syntax **rp** *ip-address*

Context show>router>pim

Description This command displays the rendezvous point (RP) set information built by the router.

Parameters *ip-address* — Specifies the IP address of the RP.

Output The following output is an example of a PIM RP configuration.

Sample Output

```
A:ALA-1# show router pim rp
==================================================================
PIM RP Set
==================================================================
Group Address      RP Address      Type        Priority  Holdtime
------------------------------------------------------------------
224.0.0.0/4        239.200.200.4   Dynamic     192       150
                   10.1.7.1        Static      1         N/A
------------------------------------------------------------------
Group Prefixes : 1
==================================================================
A:ALA-1#

A:ALA-1# show router pim rp 10.1.7.1
==================================================================
PIM RP Set
==================================================================
Group Address      RP Address      Type        Priority  Holdtime
------------------------------------------------------------------
224.0.0.0/4        10.1.7.1        Static      1         N/A
------------------------------------------------------------------
Group Prefixes : 1
==================================================================
A:ALA-1#
```

The following table provides PIM RP field descriptions.

Table 23 **PIM RP Fields**

Label	Description
Group Address	Displays the multicast group address of the entry.
RP Address	Displays the address of the Rendezvous Point (RP).
Type	Specifies whether the entry was learned through the Bootstrap mechanism or if it was statically configured.
Priority	Displays the priority for the specified group address. The higher the value, the higher the priority.
Holdtime	Displays the value of the hold time present in the BSM message.

rp-hash

Syntax **rp-hash** *grp-ip-address*

Context show>router>pim

Description This command hashes the RP for the specified group from the RP set.

Parameters *grp-ip-address* — Displays specific multicast group addresses.

Output The following output is an example of a PIM RP-Hash configuration.

Sample Output

```
A:ALA-1# show router pim rp-hash 239.101.0.0
==============================================
PIM Group-To-RP mapping
==============================================
Group Address      RP Address      Type
----------------------------------------------
239.101.0.0        239.200.200.4   Bootstrap
==============================================
A:ALA-1#

A:ALA-1# show router pim rp-hash 239.101.0.6
==============================================
PIM Group-To-RP mapping
==============================================
Group Address      RP Address      Type
----------------------------------------------
239.101.0.6        239.200.200.4   Bootstrap
==============================================
A:ALA-1#
```

The following table provides RP-Hash output field descriptions.

Table 24 **RP-Hash Fields**

Label	Description
Group Address	Displays the multicast group address of the entry.
RP Address	Displays the address of the Rendezvous Point (RP).
Type	Specifies whether the entry was learned through the Bootstrap mechanism or if it was statically configured.

statistics

Syntax **statistics** [*ip-int-name* | *mt-int-name* | *ip-address*] [*family*]

Context show>router>pim

Description This command displays statistics for a particular PIM instance.

Parameters *ip-int-name* — Only displays the interface information associated with the specified IP interface name.

ip-address — Only displays the interface information associated with the specified IP address.

family — Displays either IPv4 or IPv6 information.

Output PIM Statistics Output

Sample output

```
A:ALA-1# show router pim statistics
==================================================================
PIM Statistics ipv4
==================================================================
Message Type        Received       Transmitted    Rx Errors
------------------------------------------------------------------
Hello               18009          12834          0
Join Prune          9135           1129           10
Core RPFV JP        0              0              0
MVPN RPFV JP        0              0              0
Asserts             0              0              0
Register            0              0              0
Null Register       0              0              0
Register Stop       0              0              0
BSM                 0              0              0
Candidate RP Adv    0              0              0
Auto-RP Announce    2049           0              0
Auto-RP Mapping     2066           0              0
PIM DM Grafts       0              0              0
PIM DM Graft Acks   0              0              0
Total Packets       31231          13963
------------------------------------------------------------------
Intra-AS AD         0              0              0
```

```
Inter-AS AD         0              0              0
Mdt-Safi            1323           10             0
S-PMSI AD           0              0              0
Leaf AD             0              0              0
Source-Active AD    0              0              0
Shared Tree Join    0              0              0
Source Tree Join    0              0              0
Total BGP Packets   1323           10
-------------------------------------------------------------------------------
General Statistics
-------------------------------------------------------------------------------
Rx Invalid Register              : 0
Rx Neighbor Unknown              : 10
Rx Bad Checksum Discard          : 0
Rx Bad Encoding                  : 0
Rx Bad Version Discard           : 0
Rx CRP No Router Alert           : 0
Rx BSM Router Alert Drops        : 0
Rx BSM Wrong If Drops            : 0
Rx Invalid Join Prune            : 0
Rx Invalid Auto-RP PDU           : 0
RPF Mismatch Auto-RP Mapping PDU  : 65
RPF Mismatch Auto-RP Announce PDU : 80
Rx Unknown PDU Type              : 0
Join Policy Drops                : 0
Register Policy Drops            : 0
Bootstrap Import Policy Drops    : 0
Bootstrap Export Policy Drops    : 0
Mcac Policy Drops                : 0
Fwd Candidate RP Adv             : 0
Fwd Candidate RP Adv Drops       : 0
S-pmsi Join TLV PDUs txd.        : 0
S-pmsi Join TLV PDUs rcd.        : 0
S-pmsi Join TLV PDUs txd. Drops  : 0
S-pmsi Join TLV PDUs rcd. Drops  : 0
S-pmsi Maximum-P2mp-Spmsi Hits   : 0
P2mp Pmsi Create Failures        : 0
P2mp Pmsi Request Failures       : 0
PDU Drops on Non-PIM/Down Intf   : 0
Active Tx S-pmsis                : 0
Active Tx MS-pmsis               : 0
Active Rx S-pmsis                : 0
Active Rx Pseudo S-pmsis         : 0
Total Tx S-pmsis                 : 0
Total Rx S-pmsis                 : 0
-------------------------------------------------------------------------------
Source Group Statistics
-------------------------------------------------------------------------------
(S,G)                            : 2
(*,G)                            : 2
(*,*,RP)                         : 0
================================================================
```

Table 25 PIM Statistics Output Fields

Label	Description
PIM Statistics	The section listing the PIM statistics for a particular interface.
Message Type	Displays the type of message. Hello — Displays the number of PIM hello messages received or transmitted. Join Prune — Displays the number of PIM join prune messages received or transmitted. Asserts — Displays the number of PIM assert messages received or transmitted. Register — Displays the number of register messages received or transmitted. Null Register — Displays the number of PIM null register messages received or transmitted. Register Stop — Displays the number of PIM register stop messages received or transmitted. BSM — Displays the number of PIM Bootstrap messages (BSM) received or transmitted. Candidate RP Adv — Displays the number of candidate RP advertisements. Auto-RP Announce — Displays the number of auto-RP announce (224.0.1.39) messages received or transmitted. Auto-RP Mapping — Displays the number of auto-RP mapping (224.0.1.40) messages received or transmitted.
Message Type	PIM DM Grafts — Displays the number of PIM graft messages received or transmitted. PIM DM Graft Acks — Displays the number of PIM graft acknowledgment messages received or transmitted. Total Packets — Displays the total number of packets transmitted and received.
Received	Displays the number of messages received.
Transmitted	Displays the number of multicast data packets transmitted.
Rx Errors	Displays the total number of receive errors.
General Interface Statistics	The section listing the general PIM interface statistics.
Register TTL Drop	Displays the number of multicast data packets which could not be encapsulated in Register messages because the time to live (TTL) was zero.

Table 25 PIM Statistics Output Fields (Continued)

Label	Description
Tx Register MTU Drop	Displays the number of Bootstrap messages received on this interface but were dropped.
Rx Invalid Register	Displays the number of invalid PIM register messages received.
Rx Neighbor Unknown	Displays the number of PIM messages (other than hello messages) which were received and were rejected because the adjacency with the neighbor router was not already established.
Rx Bad Checksum Discard	Displays the number of PIM messages received, and which were discarded because of bad checksum.
Rx Bad Encoding	Displays the number of PIM messages with bad encodings received.
Rx Bad Version Discard	Displays the number of PIM messages with bad versions received.
Rx CRP No Router Alert	Displays the number of candidate-rp advertisements (C-RP-Adv) received, and which had no router alert option set.
Rx Invalid Join Prune	Displays the number of invalid PIM join prune messages received.
Rx Unknown PDU Type	Displays the number of packets received with an unsupported PIM type.
Join Policy Drops	Displays the number of times the join policy match resulted in dropping PIM join-prune message or one of the source group contained in the message.
Register Policy Drops	Displays the number of times the register policy match resulted in dropping PIM register message.
Bootstrap Import Policy Drops	Displays the number of Bootstrap messages received that were dropped because of Bootstrap import policy.
Bootstrap Export Policy Drops	Displays the number of Bootstrap messages that were not transmitted because of Bootstrap export policy.
Source Group Statistics	The section listing the source group statistics.
(S,G)	Displays the number of entries in which the type is (S,G).
(*,G)	Displays the number of entries in which the type is (*,G).
(*,*,RP)	Displays the number of entries in which the type is (*, *, rp).

The following table provides PIM statistics output field descriptions.

status

Syntax **status** [**detail**] [*family*]

Context show>router>pim

Description This command displays PIM status. The Oper Status reflects the combined operational status of IPv4/IPv6 PIM protocol status. If both are down, then Oper Status will be reflected as down. If IPv4 or IPv6 reflects up, the Oper Status will reflect up.

If PIM is not enabled, the following message appears:

```
A:NYC# show router pim status
MINOR: CLI PIM is not configured.
A:NYC#
```

Parameters **detail** — Displays detailed status information.

family — Displays either IPv4 or IPv6 information.

Output The following output displays an example of a PIM status configuration.

Sample Output

```
A:dut-d# show router pim status
===============================================================================
PIM Status ipv4
===============================================================================
Admin State                       : Up
Oper State                        : Up
IPv4 Admin State                  : Up
IPv4 Oper State                   : Up
BSR State                         : Accept Any
Elected BSR
    Address                       : None
    Expiry Time                   : N/A
    Priority                      : N/A
    Hash Mask Length              : 30
    Up Time                       : N/A
    RPF Intf towards E-BSR        : N/A
Candidate BSR
    Admin State                   : Down
    Oper State                    : Down
    Address                       : None
    Priority                      : 0
    Hash Mask Length              : 30
Candidate RP
    Admin State                   : Down
    Oper State                    : Down
    Address                       : 0.0.0.0
    Priority                      : 192
    Holdtime                      : 150
Auto-RP                           : Disabled
Multicast-Fast-Failover           : Disabled
SSM-Default-Range                 : Enabled
SSM-Assert-Comp-Mode              : Disabled
```

```
SSM-Group-Range
    None
MC-ECMP-Hashing                  : Disabled
MC-ECMP-Hashing-Rebalance        : Disabled
Enable-MDT-SPT                   : Disabled
Policy                           : None
RPF Table                        : rtable-u
Non-DR-Attract-Traffic           : Disabled
Rpf-Vector                       : None
ESM                              : Disabled
===============================================================================
A:dut-d#
```

The following table provides PIM status output field descriptions.

Table 26 **PIM Status Output Fields**

Label	Description
Admin State	Displays the administrative status of PIM.
Oper State	Displays the current operating state of this PIM protocol instance.
BSR State	Displays the state of the router with respect to the Bootstrap mechanism.
Address	Displays the address of the elected Bootstrap router.
Expiry Time	Displays the time remaining before the router sends the next Bootstrap message.
Priority	Displays the priority of the elected Bootstrap router. The higher the value, the higher the priority.
Hash Mask Length	Displays the hash mask length of the Bootstrap router.
Up Time	Displays the time since the current E-BSR became the Bootstrap router.
RPF Intf towards	Displays the RPF interface towards the elected BSR. The value is zero if there is no elected BSR in the network.
Address	Displays the address of the candidate BSR OS.
Expiry Time	Displays the time remaining before the router sends the next Bootstrap message.
Auto-RP	Displays if auto-RP functionality is enabled or disabled.
Priority	Displays the priority of the Bootstrap router. The higher the value, the higher the priority.
Hash Mask Length	Displays the hash mask length of the candidate Bootstrap router.
Up Time	Displays the time since becoming the Bootstrap router.

Table 26 PIM Status Output Fields (Continued)

Label	Description
Admin State	Displays the administrative status of CRP.
Oper State	Displays the current operating state of the C-RP mechanism.
Address	Displays the local RP address.
Priority	Displays the CRP's priority for becoming a rendezvous point (RP). A 0 value is the highest priority.
Holdtime	Displays the hold time of the candidate RP. It is used by the Bootstrap router to timeout the RP entries if it does not listen to another CRP advertisement within the holdtime period.
Policy	Displays the PIM policies for a particular PIM instance.
Default Group	Displays the default core group address.
RPF Table	Displays the route table used for RPF check.
MC-ECMP-Hashing	Displays if hash-based multicast balancing of traffic over ECMP links is enabled or disabled.

tunnel-interface

Syntax **tunnel-interface** [*ip-int-name* **|** *mt-int-name* **|** *int-ip-address*] [**group** [*grp-ip-address*] **source** *ip-address*] [**type** {**starstarrp | starg | sg**}] [**detail**] [*family*]

Context show>router>pim

Description This command displays PIM tunnel interface information.

Parameters *ip-int-name* — Specifies the IP interface name. A string up to 32 characters.

mt-int-name — Specifies the Multicast Tunnel (MT) interface for a VPRN.

Values *vprn-id*-mt-*grp-ip-address*

int-ip-address — Specifies the interface IPv4 or IPv6 address.

grp-ip-address — Specifies the IP multicast group address, or 0.

ip-address — Specifies the source or RP IPv4 or IPv6 address.

type — Specifies the type of entry.

Values **starstarrp | starg | sg**

detail — Displays detailed interface information.

family — Specifies the IPv4 or IPv6 address family.

Output The following output is an example of PIM tunnel interface information.

Sample Output

```
*A:Dut-C# show router pim tunnel-interface
===================================================================================
PIM Interfaces ipv4
================================================================================
Interface                        Originator Address   Adm  Opr  Transport Type
--------------------------------------------------------------------------------
mpls-if-73728                    N/A                  Up   Up   Tx-IPMSI
mpls-if-73729                    N/A                  Up   Up   Tx-IPMSI
mpls-if-73730                    N/A                  Up   Up   Tx-IPMSI
mpls-if-73731                    N/A                  Up   Up   Tx-IPMSI
mpls-if-73732                    N/A                  Up   Up   Tx-IPMSI
--------------------------------------------------------------------------------
Interfaces : 5
================================================================================
```

mvpn-list

Syntax **mvpn-list** [**type** *type*] [**auto-discovery** *auto-discovery*] [**signalling** *signalling*] [**group** *group*]

Context show>router

Description This command displays the list of multicast VPNs.

Parameters *type* — Specifies the MVPN type.

Values pim, rsvp, ldp

auto-discovery — Specifies the auto-discovery mode.

Values none, default, mdt-s

signalling — Specifies the signalling type.

Values bgp, pim

group — Specifies the group address.

Output The following output is an example of router MVPN list information.

Sample Output

```
*A:Dut-D# show router mvpn-list

Legend: Sig = Signal  Pim-a = pim-asm  Pim-s = pim-ssm  A-D = Auto-Discovery
SR = Sender-Receiver  SO = Sender-Only  RO = Receiver-Only
================================================================================
MVPN List
================================================================================
VprnID    A-D      iPmsi/sPmsi GroupAddr/Lsp-Template          IPv4(S,G)/(*,G)
           Sig      Mdt-Type                                    IPv6(S,G)/(*,G)
--------------------------------------------------------------------------------
100       None     Pim-a/None  239.100.201.101                 0/0
           Pim      N/A                                         0/0
```

```
-------------------------------------------------------------------------------
Total Mvpns : 1
===============================================================================
===============================================================================
Total                              PIM           RSVP          MLDP
-------------------------------------------------------------------------------
I-PMSI tunnels                     1             0             0
TX S-PMSI tunnels                  0             0             0
RX S-PMSI tunnels                  0             0             0
RX PSEUDO S-PMSI tunnels   0              0              0
-------------------------------------------------------------------------------
Total IPv4 (S,G)/(*,G) : 0/0
Total IPv6 (S,G)/(*,G) : 0/0
===============================================================================
*A:Dut-D#
```

5.5.2.2 Clear Commands

database

Syntax **database** [**interface** *ip-int-name* | *mt-int-name* | *int-ip-address*] [**group** *grp-ip-address* [**source** *ip-address*]] [*family*]

Context clear>router>pim

Description This command clears IGMP or PIM database statistics on a specified interface or IP address.

Parameters *ip-int-name* — Clears the IGMP or PIM database on the specified interface.

mt-int-name — Clears the default core group address of the Multicast Distribution Tree (MDT) for the VPRN instance. The Multicast Tunnel (MT) interface for a VPRN is created when this object is set to a valid group address.

Syntax: *vprn-id*-mt-*grp-ip-addres*s

int-ip-address — Clears the IGMP or PIM database on the specified IP address.

group-ip-address — Clears the multicast group address (ipv4/ipv6) or zero in the specified address group.

ip-address — Clears the IGMP or PIM database from the specified source IP address.

family — Clears either IPv4 or IPv6 information.

mpls-if-name — Clears the MPLS interface name.

Syntax: mpls-if-*index*

s-pmsi

Syntax **s-pmsi** [*mdSrcAddr*] [*mdGrpAddr*] [*vprnSrcAddr vprnGrpAddr*]

Context clear>router>pim

Description This command clears PIM selective provider multicast service interface cache.

Parameters *mdSrcAddr* — Clears the specified source address used for Multicast Distribution Tree (MDT).

mdGrpAddr — Clears the specified group address used for Multicast Distribution Tree (MDT).

vprnSrcAddr — Clears the specified source address of the multicast sender.

vprnGrpAddr — Clears the specified multicast group address.

statistics

Syntax **statistics** [{[**interface** *ip-int-name* | *ip-address* | *mt-int-name*]} {[**group** *grp-ip-address* [**source** *ip-address*]]}] [*family*]]

Context clear>router>pim

Description This command clears PIM statistics on a specified interface or IP address.

Note: An interface and group or source cannot be specified at the same time.

Parameters *ip-int-name* — Clears PIM statistics on the specified interface.

ip-address — Clears PIM statistics on the specified IP address.

mt-int-name — Clears the default core group address of the Multicast Distribution Tree (MDT) for the VPRN instance. The Multicast Tunnel (MT) interface for a VPRN is created when this object is set to a valid group address.

syntax: *vprn-id*-mt-*grp-ip-address*

grp-ip-address — When only the group address is specified and no source is specified, (*,G) statistics are cleared. When the group address is specified along with the source address, then the (S,G) statistics are reset to zero.

ip-address — When the source address is specified along with the group address, then the (S,G) statistics are reset to zero.

family — Clears either IPv4 or IPv6 information.

neighbor

Syntax **neighbor** [*ip-int-name* | *ip-address*] [*family*]

Context clear>router>pim

Description This command clears PIM neighbor data on a specified interface or IP address.

Parameters *ip-int-name* — Clears PIM neighbor on the specified interface.

ip-address — Clears PIM neighbor on the specified IP address.

family — Clears either IPv4 or IPv6 information.

5.5.2.3 Debug Commands

adjacency

Syntax [**no**] **adjacency**

Context debug>router>pim

Description This command enables/disables debugging for PIM adjacencies.

all

Syntax **all** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
no all

Context debug>router>pim

Description This command enables/disables debugging for all the PIM modules.

Parameters *grp-ip-address* — Debugs information associated with all PIM modules.

Values IPv4 or IPv6 address

ip-address — Debugs information associated with all PIM modules.

Values IPv4 or IPv6 address

detail — Debugs detailed information on all PIM modules.

assert

Syntax **assert** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
no assert

Context debug>router>pim

Description This command enables/disables debugging for PIM assert mechanism.

Parameters *grp-ip-address* — Debugs information associated with the PIM assert mechanism.

Values multicast group address (ipv4/ipv6)

ip-address — Debugs information associated with the PIM assert mechanism.

Values source address (ipv4/ipv6)

detail — Debugs detailed information on the PIM assert mechanism.

auto-rp

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

Context debug>router>pim

Description This command enables/disables debugging for PIM auto-RP.

Parameters **detail** — Debugs detailed information on the PIM auto-RP mechanism.

bgp

Syntax **bgp** [**source** *ip-address*] [**group** *group-ip-address*] [**peer** *peer-ip-address*]
no bgp

Context debug>router>pim

Description This command enables/disables debugging for PIM/BGP specific interoperation.

Parameters *ip-address* — Debugs BGP information associated with the specified source.

Values source address (ipv4/ipv6)

group-ip-address — Debugs BGP information associated with the specified group.

Values group address (ipv4/ipv6)

peer-ip-address — Debugs BGP information associated with the specified peer.

Values peer address (ipv4/ipv6)

bsr

Syntax **bsr** [**detail**]
no bsr

Context debug>router>pim

Description This command enables/disables debugging for the PIM bootstrap mechanism.

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

Parameters **detail** — Debugs detailed information on the PIM bootstrap mechanism.

data

Syntax **data** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
no data

Context debug>router>pim

Description This command enables/disables debugging for PIM data exception.

Parameters *grp-ip-address* — Debugs information associated with the specified data exception.

Values multicast group address (ipv4/ipv6)

ip-address — Debugs information associated with the specified data exception.

Values source address (ipv4/ipv6)

detail — Debugs detailed IP data exception information.

db

Syntax **db** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
no db

Context debug>router>pim

Description This command enables/disables debugging for PIM database.

Parameters *grp-ip-address* — Debugs information associated with the specified database.

Values multicast group address (ipv4/ipv6) or zero

ip-address — Debugs information associated with the specified database.

Values source address (ipv4/ipv6)

detail — Debugs detailed IP database information.

dynmldp

Syntax **dynmldp** [**detail**]
no dynmldp

Context debug>router>pim

Description This command enables/disables debugging for dynamic MLDP.

Parameters **detail** — Debugs detailed dynamic MLDP information.

extranet

Syntax **extranet** [**detail**]
no extranet

Context debug>router>pim

Description This command enables/disables debugging for extranet PIM.

Parameters **detail** — Debugs detailed extranet PIM information.

grafts

Syntax **grafts** [**source** *ip-address*] [**group** *grp-ip-address*] [**detail**]
no grafts

Context debug>router>pim

Description This command enables/disables debugging for PIM grafts.

Parameters *ip-address* — Debugs graft information associated with the specified source.

Values source address (ipv4/ipv6)

grp-ip-address — Debugs graft information associated with the specified group.

Values multicast group address (ipv4/ipv6)

detail — Debugs detailed graft information.

interface

Syntax **interface** [*ip-int-name* | *mt-int-name* | *ip-address*] [**detail**]
no interface

Context debug>router>pim

Description This command enables/disables debugging for PIM interface information.

Parameters *ip-int-name* — Debugs the information associated with the specified IP interface name.

Values IPv4 or IPv6 interface address

mt-int-address — Debugs the information associated with the specified VPRN ID and group address.

ip-address — Debugs the information associated with the specified IP address.

detail — Debugs detailed IP interface information.

jp

Syntax **jp** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
no jp

Context debug>router>pim

Description This command enables/disables debugging for PIM join and prune mechanisms.

Parameters *grp-ip-address* — Debugs information associated with the specified Join-Prune mechanism.

Values multicast group address (ipv4/ipv6) or zero

ip-address — Debugs information associated with the specified Join-Prune mechanism.

Values source address (ipv4/ipv6)

detail — Debugs detailed Join-Prune mechanism information.

mofrr

Syntax [**no**] **mofrr**

Context debug>router>pim

Description This command enables/disables debugging for PIM multicast fast failover.

mrib

Syntax **mrib** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
no mrib

Context debug>router>pim

Description This command enables/disables debugging for PIM MRIB.

Parameters *grp-ip-address* — Debugs information associated with the specified PIM MRIB.

Values multicast group address (ipv4/ipv6)

ip-address — Debugs information associated with the specified PIM MRIB.

Values source address (ipv4/ipv6)

detail — Debugs detailed MRIB information.

msg

Syntax **msg** [**detail**]
no msg

Context debug>router>pim

Description This command enables/disables debugging for PIM messaging.

Parameters **detail** — Debugs detailed messaging information.

mvpn-rtcache

Syntax **mvpn-rtcache** [**group** *grp-ip-address*] [**peer** *ip-address*]
no mvpn-rtcache

Context debug>router>pim

Description This command enables/disables debugging for the PIM MVPN route cache.

Parameters *grp-ip-address* — Debugs information associated with the specified group.

Values multicast group address (ipv4/ipv6) or zero

peer-ip-address — Debugs information associated with the specified peer.

Values peer address (ipv4/ipv6)

packet

Syntax **packet** [**hello | register | register-stop | jp | bsr | assert | crp | mdt-tlv | auto-rp-announcement | auto-rp-mapping | graft | graft-ack**] [*ip-int-name* | *mt-int-name* | *int-ip-address* | *mpls-if-name*] [**family** {**ipv4 | ipv6**}] [**send | receive**]
no packet

Context debug>router>pim

Description This command enables/disables debugging for PIM packets.

Parameters **hello | register | register-stop | jp | bsr | assert | crp | mdt-tlv | auto-rp-announcement | auto-rp-mapping | graft | graft-ack** — Specifies PIM packet types.

ip-int-name — Debugs the information associated with the specified IP interface name, up to 32 characters.

mt-int-name — Debugs the information associated with the specified VPRN ID and group address.

Values *vprn-id*-mt-*grp-ip-address*

int-ip-address — Debugs the information associated with the specified IP address.

ipv4 — Specifies to display IPv4 packets.

ipv6 — Specifies to display IPv6 packets.

mpls-if-name — Debugs the information associated with the specified MPLS interface.

Values mpls-if-*index*

receive — Specifies to display received packets.

send — Specifies to display sent packets.

red

Syntax **red** [**detail**]
no red

Context debug>router>pim

Description This command enables/disables debugging for PIM redundancy messages to the standby CPM.

Parameters **detail** — Displays detailed redundancy information.

register

Syntax **register** [**group** *grp-ip-address*] [**source** *ip-address*] [**detail**]
no register

Context debug>router>pim

Description This command enables/disables debugging for PIM register mechanism.

Parameters *grp-ip-address* — Debugs information associated with the specified PIM register.

Values multicast group address (ipv4/ipv6)

ip-address — Debugs information associated with the specified PIM register.

Values source address (ipv4/ipv6)

detail — Debugs detailed register information.

rpfv

Syntax **rpfv** [**detail**]
no rpfv

Context debug>router>pim

Description This command enables/disables debugging for PIM RPF vector.

Parameters **detail** — Debugs detailed RPF vector information.

rtm

Syntax **rtm** [**detail**]
no rtm

Context debug>router>pim

Description This command enables/disables debugging for PIM RTM.

Parameters **detail** — Displays detailed RTM information.

s-pmsi

Syntax **s-pmsi** [{*vpnSrcAddr* [*vpnGrpAddr*]} [*mdSrcAddr*]] [**detail**]
no s-pmsi

Context debug>router>pim

Description This command enables debugging for PIM selective provider multicast service interface.

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

Parameters *vpnSrcAddr* — Specifies the VPN source address.

vpnGrpAddr — Specifies the VPN group address

mdSrcAddr — Specifies the source address of the multicast domain.

detail — Displays detailed information for selective PMSI.

tunnel-interface

Syntax **tunnel-interface** [**rsvp-p2mp** *lsp-name*] [**sender** *ip-address*] [**detail**]
tunnel-interface [**ldp-p2mp** *p2mp-id*] [**sender** *ip-address*] [**detail**]
no tunnel-interface [**rsvp-p2mp** *lsp-name*] [**sender** *ip-address*]
no tunnel-interface [**ldp-p2mp** *p2mp-id*] [**sender** *ip-address*]

Context debug>router>pim

Description This command enables/disables debugging for PIM tunnel interfaces.

Parameters *lsp-name* — Specifies the LSP for RSVP P2MP.

ip-address — Specifies the IP address of the sender.

p2mp-id — Specifies the P2MP ID for LDP P2MP.

detail — Displays detailed information for PIM tunnel interfaces.

6 MSDP

6.1 Multicast Source Discovery Protocol

MSDP-speaking routers in a PIM-SM domain have MSDP peering relationship with MSDP peers in another domain. The peering relationship is made up of a TCP connection in which control information is exchanged. Each domain has one or more connections to this virtual topology.

When a PIM-SM RP learns about a new multicast source within its own domain from a standard PIM register mechanism, it encapsulates the first data packet in an MSDP source-active message and sends it to all MSDP peers.

The source-active message is flooded (after an RPF check) by each peer to its MSDP peers until the source-active message reaches every MSDP router in the interconnected networks. If the receiving MSDP peer is an RP, and the RP has a (*.G) entry (receiver) for the group, the RP creates state for the source and joins to the shortest path tree for the source. The encapsulated data is de-encapsulated and forwarded down the shared tree of that RP. When the packet is received by the last hop router of the receiver, the last hop router also may join the shortest path tree to the source.

The MSDP speaker periodically sends source-active messages that include all sources.

6.1.1 Anycast RP for MSDP

MSDP is a mechanism that allows rendezvous points to share information about active sources. When RPs in remote domains hear about the active sources, they can pass on that information to the local receivers and multicast data can be forwarded between the domains. MSDP allows each domain to maintain an independent RP that does not rely on other domains but enables RPs to forward traffic between domains. PIM-SM is used to forward the traffic between the multicast domains.

Using PIM-SM, multicast sources and receivers register with their local RP by the closest multicast router. The RP maintains information about the sources and receivers for any particular group. RPs in other domains do not have any knowledge about sources located in other domains.

MSDP is required to provide inter-domain multicast services using Any Source Multicast (ASM). Anycast RP for MSDP enables fast convergence when should an MSDP/PIM PR router fail by allowing receivers and sources to rendezvous at the closest RP.

6.1.2 MSDP Procedure

When an RP in a PIM-SM domain first learns of a new sender, for example, by PIM register messages, it constructs a source-active (SA) message and sends it to its MSDP peers. The SA message contains the following fields:

- Source address of the data source
- Group address the data source sends to
- IP address of the RP

Note: An RP that is not a designated router on a shared network does not originate SAs for directly-connected sources on that shared network. It only originates in response to receiving register messages from the designated router.

Each MSDP peer receives and forwards the message away from the RP address in a peer-RPF flooding fashion. The notion of peer-RPF flooding is with respect to forwarding SA messages. The Multicast RPF Routing Information Base (MRIB) is examined to determine which peer towards the originating RP of the SA message is selected. Such a peer is called an RPF peer.

If the MSDP peer receives the SA from a non-RPF peer towards the originating RP, it will drop the message. Otherwise, it forwards the message to all its MSDP peers (except the one from which it received the SA message).

When an MSDP peer which is also an RP for its own domain receives a new SA message, it determines if there are any group members within the domain interested in any group described by an (S,G) entry within the SA message. That is, the RP checks for a (*,G) entry with a non-empty outgoing interface list. This implies that some system in the domain is interested in the group. In this case, the RP triggers an (S,G) join event toward the data source as if a join/prune message was received addressed to the RP. This sets up a branch of the source-tree to this domain. Subsequent data packets arrive at the RP by this tree branch and are forwarded down the shared-tree inside the domain. If leaf routers choose to join the source-tree they have the option to do so according to existing PIM-SM conventions. If an RP in a domain receives a PIM join message for a new group G, the RP must trigger an (S,G) join event for each active (S,G) for that group in its SA cache.

This procedure is called flood-and-join because if any RP is not interested in the group, the SA message can be ignored, otherwise, they join a distribution tree.

6.1.2.1 MSDP Peering Scenarios

Draft-ietf-mboned-msdp-deploy-nn.txt, *Multicast Source Discovery Protocol (MSDP) Deployment Scenarios,* describes how protocols work together to provide intra- and inter-domain ASM service.

Inter-domain peering:

- Peering between PIM border routers (single-hop peering)
- Peering between non-border routers (multi-hop peering)
- MSDP peering without BGP
- MSDP peering between mesh groups
- MSDP peering at a multicast exchange

Intra-domain peering:

- Peering between routers configured for both MSDP and MBGP
- MSDP peer is not BGP peer (meaning, no BGP peer)

6.1.3 MSDP Peer Groups

MSDP peer groups are typically created when multiple peers have a set of common operational parameters. Group parameters not specifically configured are inherited from the global level.

6.1.4 MSDP Mesh Groups

MSDP mesh groups are used to reduce source active flooding primarily in intra-domain configurations. When a number of speakers in an MSDP domain are fully meshed they can be configured as a mesh group. The originator of the source active message forwards the message to all members of the mesh group. Because of this, forwarding the SA between non-originating members of the mesh group is not necessary.

6.1.5 MSDP Routing Policies

MSDP routing policies allow for filtering of inbound and/or outbound active source messages. Policies can be configured at different levels:

- Global level — Applies to all peers
- Group level — Applies to all peers in peer-group
- Neighbor level — Applies only to specified peer

The most specific level is used. If multiple policy names are specified, the policies are evaluated in the order they are specified. The first policy that matches is applied. If no policy is applied source active messages are passed.

Match conditions include:

- Neighbor — Matches on a neighbor address is the source address in the IP header of the source active message.
- Route filter — Matches on a multicast group address embedded in the source active message.
- Source address filter — Matches on a multicast source address embedded in the source active message.

6.1.6 Multicast in Virtual Private Networks

6.1.6.1 Draft Rosen

RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*, describes a method of providing a VPN service. A VPN provides secure connections to the network, allowing more efficient service to remote users without compromising the security of firewalls. The Rosen draft specifies the protocols and procedures which must be implemented in order for a service provider to provide a unicast VPN. The draft extends that specification by describing the protocols and procedures which a service provider must implement in order to support multicast traffic in a VPN, assuming that PIM [PIMv2] is the multicast routing protocol used within the VPN, and the SP network can provide PIM as well.

IGMP is not supported for receivers or senders directly attached to the PE.

For further information, refer to the “Virtual Private Routed Network Service” section of the *7450 ESS, 7750 SR, 7950 XRS, and VSR Layer 3 Services Guide: IES and VPRN.*

6.2 Configuring MSDP with CLI

This section provides information to configure MSDP using the command line interface.

6.2.1 Basic MSDP Configuration

Perform the following basic MSDP configuration tasks:

- Enable MSDP (required)
- Configure peer
- Configure local address

6.2.2 Configuring MSDP Parameters

Use the following commands to configure basic MSDP parameters:

CLI Syntax:
```
config>router# msdp
     peer ip-address
          active-source-limit number
          authentication-key [authentication-key | hash-
            key] [hash | hash2]
          default-peer
          export policy-name [policy-name]
          import policy-name [policy-name]
          local-address ip-address
          receive-msdp-msg-rate number interval seconds
            [threshold threshold]
          no shutdown
     no shutdown
```

Use the following CLI syntax to configure MSDP parameters.

Example:
```
config>router>msdp# peer 10.20.1.1
config>router>msdp>peer# local-address 10.20.1.6
config>router>msdp>peer# no shutdown
config>router>msdp>peer# exit
config>router>msdp# no shutdown
config>router>msdp#
```

The following example displays the MSDP configuration:

```
ALA-48>config>router>msdp# info
-------------------------------------------
         peer 10.20.1.1
             local-address 10.20.1.6
         exit
-------------------------------------------
ALA-48>config>router>msdp#
```

6.2.3 Disabling MSDP

Use the following CLI syntax to disable PIM.

CLI Syntax:
```
config>router#
      msdp
            shutdown
```

The following example displays the command usage to disable multicast:

Example:
```
config>router#
config>router>msdp# shutdown
config>router>msdp# exit
```

The following example displays the configuration output:

```
A:LAX>config>router# info
----------------------------------------------
...
#------------------------------------------
echo "MSDP Configuration"
#--------------------------------------------------
        msdp
            shutdown
            peer 10.20.1.1
                local-address 10.20.1.6
            exit
            group "test"
                active-source-limit 50000
                receive-msdp-msg-rate 100 interval 300 threshold 5000
                export "LDP-export"
                import "LDP-import"
                local-address 10.10.10.103
                mode mesh-group
                peer 10.10.10.104
                exit
            exit
        exit
#--------------------------------------------------
```

6.3 MSDP Configuration Command Reference

6.3.1 Command Hierarchies

- Configuration Commands

6.3.1.1 Configuration Commands

config
- **router**
  - [**no**] **msdp**
    - [**no**] **active-source-limit** *number*
    - [**no**] **data-encapsulation**
    - **export** *policy-name* [*policy-name*]
    - **no export**
    - [**no**] **group** *group-name*
      - **active-source-limit** *number*
      - **no active-source-limit**
      - **export** *policy-name* [*policy-name*]
      - **no export**
      - **import** *policy-name* [*policy-name*]
      - **no import**
      - **local-address** *address*
      - **no local-address**
      - **mode** {**mesh-group** | **standard**}
      - [**no**] **peer** *peer-address*
        - **active-source-limit** *number*
        - **no active-source-limit**
        - **authentication-key** [*authentication-key* | *hash-key*] [**hash** | **hash2**]
        - **no authentication-key**
        - [**no**] **default-peer**
        - **export** *policy-name* [*policy-name*]
        - **no export**
        - **import** *policy-name* [*policy-name*]
        - **no import**
        - **local-address** *address*
        - **no local-address**
        - **receive-msdp-msg-rate** *number* **interval** *seconds* [**threshold** *number*]
        - **no receive-msdp-msg-rate**
        - [**no**] **shutdown**
      - **receive-msdp-msg-rate** *number* **interval** *seconds* [**threshold** *number*]
      - **no receive-msdp-msg-rate**
      - [**no**] **shutdown**
    - **import** *policy-name* [*policy-name*]

— **no import**
— **local-address** *address*
— **no local-address**
— [**no**] **peer** *peer-address*
    — **active-source-limit** *number*
    — **no active-source-limit**
    — **authentication-key** [*authentication-key* | *hash-key*] [**hash** | **hash2**]
    — **no authentication-key**
    — [**no**] **default-peer**
    — **export** *policy-name* [*policy-name*]
    — **no export**
    — **import** *policy-name* [*policy-name*]
    — **no import**
    — **local-address** *address*
    — **no local-address**
    — **receive-msdp-msg-rate** *number* **interval** *seconds* [**threshold** *number*]
    — **no receive-msdp-msg-rate**
    — [**no**] **shutdown**
— **receive-msdp-msg-rate** *number* **interval** *seconds* [**threshold** *number*]
— **no receive-msdp-msg-rate**
— **rpf-table** {**rtable-m** | **rtable-u** | **both**}
— **no rpf-table**
— **sa-timeout** *seconds*
— **no sa-timeout**
— [**no**] **shutdown**
— [**no**] **source** *prefix/mask*
        — **active-source-limit** *number*
        — **no active-source-limit**

6.3.2 Command Descriptions

6.3.2.1 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.

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.

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

Default no msdp

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), effectively controlling the number of active sources that can be stored on the system.

The **no** form of this command sets no limit on the number of source active records.

Default no active-source-limit

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

Values 0 to 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>group>peer

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.

After 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.

The **no** form of this command sets no limit on the number of MSDP and source active limit messages that will be accepted.

Default no receive-msdp-msg-rate

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 to 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 to 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 particularly of use during at system startup and initialization.

Values 1 to 1000000

Default 0

shutdown

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

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

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 and 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

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.

The **no** form of the command configures acceptance of all MSDP messages and disables the MD5 signature option authentication key.

Default no authentication-key

Parameters *authentication-key* — The authentication key. Allowed values are any string up to 256 characters long composed of printable, 7-bit ASCII characters. If the string contains special characters (#, $, spaces, and so on), enclose the entire string in quotation marks (“ ”).

hash-key — The hash key. The key can be any combination of ASCII characters up to 451 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** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified

hash2 — Specifies the key is entered in a more complex encrypted form that involves more variables than the key value alone, meaning that the **hash2** encrypted variable cannot be copied and pasted. If the **hash** or **hash2** parameter is not used, the key is assumed to be in an unencrypted, clear text form. For security, all keys are stored in encrypted form in the configuration file with the **hash** or **hash2** parameter specified.

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*]
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).

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.

The **no** form of the command applies no export policies and all SA entries are announced.

Default no export

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

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.

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.

import

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

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.

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 group's policy.

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

The **no** form of the command applies no import policies and all source active messages are allowed.

Default no import

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

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. 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.

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 sessions 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 sessions will be terminated.

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

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

The **no** form 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.

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.

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.

Default mode standard

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.

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.

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, if valid, 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 will be removed. Whenever a new peering session is created or a peering session is lost, an event message should be generated.

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.

rpf-table

Syntax **rpf-table** {**rtable-m** | **rtable-u** | **both**}
no rpf-table

Context 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 one of the following options:

- use the unicast route table only
- use the multicast route table only
- use both the route tables

Default rpf-table rtable-u

Parameters **rtable6-m** — Specifies that only the multicast route table will be used by the multicast protocol (PIM) for IPv4 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 IPv4 RPF checks. This route table will contain routes submitted by all the unicast routing protocols.

both — Will always look up 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. Rtable-m is checked before rtable6-u.

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, 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 than 90) could be useful to prevent instabilities 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 to 600

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.

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.

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.

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 to 32 (mask length), 0.0.0.0 to 255.255.255.255 (dotted decimal)

6.4 Show, Clear, and Debug Command Reference

6.4.1 Command Hierarchies

- Show Commands
- Clear Commands
- Debug Commands

6.4.1.1 Show Commands

show
- — **router**
  - — **msdp**
    - — **group** [*group-name*] [**detail**]
    - — **peer** [*ip-address*] [**group** *group-name*] [**detail**]
    - — **source** [*ip-address/mask*] [**type** {**configured** | **dynamic** | **both**}] [**detail**]
    - — **source-active** [{**group** *ip-address* | **local** | **originator** *ip-address* | **peer** *ip-address* | **source** *ip-address* | **group** *ip-address* **source** *ip-address*}] [**detail**]
    - — **source-active-rejected** [**peer-group** *name*] [**group** *ip-address*] [**source** *ip-address*] [**originator** *ip-address*] [**peer** *ip-address*]
    - — **statistics** [**peer** *ip-address*]
    - — **status**

6.4.1.2 Clear Commands

clear
- — **router**
  - — **msdp**
    - — **cache** [**peer** *ip-address*] [**group** *ip-address*] [**source** *ip-address*] [**originrp** *ip-address*]
    - — **statistics** [**peer** *ip-address*]

6.4.1.3 Debug Commands

debug
- — **router**
  - — [**no**] **msdp**
    - — **packet** [*pkt-type*] [**peer** *ip-address*]

— **no packet**
— **pim** [*grp-address*]
— **no pim**
— **rtm** [*rp-address*]
— **no rtm**
— **sa-db** [**group** *grpAddr*] [source *srcAddr*] [**rp** *rpAddr*]
— **no sa-db**

6.4.2 Command Descriptions

6.4.2.1 Show Commands

The command outputs in the following section are examples only; actual displays may differ depending on supported functionality and user configuration.

group

Syntax **group** [*group-name*] [**detail**]

Context show>router>msdp

Description This command displays information about MSDP groups.

Parameters *group-name* — Displays information about the specified group name. If no group-name is specified, information about all group names display.

detail — Displays detailed MSDP group information.

Output MSDP Group Output

The following table provides MSDP group field descriptions.

Table 27 **MSDP Group Fields**

Label	Description
Group Name	Displays the MSDP group name.
Mode	Displays the groups of peers in a full mesh topology to limit excessive flooding of source-active messages to neighboring peers.
Act Srcs	Displays the configured maximum number of active source messages that will be accepted by MSDP.
Local Address	Displays the local end of a MSDP session.

Table 27 MSDP Group Fields (Continued)

Label	Description
Admin State	Displays the administrative state.
Receive Msg Rate	Displays rate that the messages are read from the TCP session.
Receive Msg Time	Displays the time of MSDP messages that are read from the TCP session within the configured number of seconds.
Receive Msg Thd	Displays the configured threshold number of MSDP messages can be processed before the MSDP message rate limiting function.
SA Limit	Displays the source-active limit.

Sample Output

```
*A:ALA-48>show>router>msdp# group
===============================================================================
MSDP Groups
===============================================================================
Group Name                       Mode       Act Srcs  Local Address
-------------------------------------------------------------------------------
main                             Mesh-group None None
loop1                            Mesh-group None None
loop2                            Mesh-group None None
loop3                            Mesh-group None None
loop4                            Mesh-group None None
loop5                            Mesh-group None None
-------------------------------------------------------------------------------
Groups : 6
=======================
*A:ALA-48>show>router>msdp#


*A:ALA-48>show>router>msdp# group test
===============================================================================
MSDP Groups
===============================================================================
Group Name                       Mode       Act Srcs  Local Address
-------------------------------------------------------------------------------
test                             Mesh-group 50000     10.10.10.103
-------------------------------------------------------------------------------
Groups : 1
===============================================================================
*A:ALA-48>show>router>msdp#


*A:ALA-48>show>router>msdp# group test detail
===============================================================================
MSDP Groups
===============================================================================
Group Name          : test
-------------------------------------------------------------------------------
Local Address       : 10.10.10.103
```

```
Admin State        : Up                Receive Msg Rate    : None
Receive Msg Time   : None              Receive Msg Thd     : None
Mode               : Mesh-group        SA Limit            : 50000
Export Policy      : None Specified / Inherited
Import Policy      : None Specified / Inherited

-------------------------------------------------------------------------------
Groups : 1
===============================================================================
*A:ALA-48>show>router>msdp#
```

peer

Syntax **peer** [*ip-address*] [**group** *group-name*] [**detail**]

Context show>router>msdp

Description This command displays information about an MSDP peer.

Parameters *ip-address* — Displays information about the specified IP address. If no IP address specified, information about all MSDP IP addresses display.

group group-name — Displays information about the specified group name. If no *group-name* is specified, information about all MSDP peers display.

detail — Displays detailed MSDP peer information.

Output MSDP Peer Output

The following table provides MSDP field descriptions.

Table 28 **MSDP Fields**

Label	Description
Peer	Displays the IP address of the peer.
Local Address	Displays the local IP address.
State	Displays the current state of the peer.
Last State Change	Displays the date and time of the peer’s last state change.
SA Learn	The number of SAs learned through a peer.

Sample Output

```
A:ALA-48# show router msdp peer
===============================================================================
MSDP Peers
===============================================================================
Peer             Local Address    State       Last State Change     SA Learnt
-------------------------------------------------------------------------------
```

```
10.20.1.1        10.20.1.6        Established 08/30/2002 03:22:131008
-------------------------------------------------------------------------------
Peers : 1
===============================================================================
A:ALA-48#


A:ALA-48# show router msdp peer detail
===============================================================================
MSDP Peers
-------------------------------------------------------------------------------
Peer Address       : 10.20.1.1
-------------------------------------------------------------------------------
Group Name         : None
Local Address      : 10.20.1.6
Last State Change  : 08/30/2002 03:22:13 Last Act Src Limit : N/A
Peer Admin State   : Up                 Default Peer       : No
Peer Connect Retry : 0                  State              : Established
SA accepted        : 1008               SA received        : 709
State timer expires: 18                 Peer time out      : 62
Active Source Limit: None               Receive Msg Rate   : 0
Receive Msg Time   : 0                  Receive Msg Thd    : 0
Auth Status        : Disabled           Auth Key           : None
Export Policy      : None Specified / Inherited
Import Policy      : None Specified / Inherited
-------------------------------------------------------------------------------
Peers : 1
===============================================================================
A:ALA-48#
```

source

Syntax **source** [*ip-address/mask*] [**type** {**configured** | **dynamic** | **both**}] [**detail**]

Context show>router>msdp

Description This command displays the discovery method for this multicast source.

Parameters **configured** — Displays user-created sources.

dynamic — Displays dynamically created sources.

both — Displays both user-configured and dynamically created sources.

detail — Displays detailed MSDP source information.

Output MSDP Source Output

The following table provides MSDP source field descriptions.

Table 29 **MSDP Source Fields**

Label	Description
Source	Displays the IP address of the peer.

Table 29 **MSDP Source Fields (Continued)**

Label	Description
Type	Displays the type of peer.
SA limit	Displays the local IP address.
State	Displays the current state of the peer.
Num excd	Indicates the number of times the global active source limit has been exceeded.
Last exceeded	Displays the date and time of the peer’s last state change.

source-active

Syntax **source-active** [{**group** *ip-address* **|** **local** **|** **originator** *ip-address* **|** **peer** *ip-address* **|** **source** *ip-address* **|** **group** *ip-address* **source** *ip-address*}] [**detail**]

Context show>router>msdp

Description This command displays source active messages accepted by MSDP.

Parameters **group** *ip-address* — Displays information about the specified group IP address.

local — Displays information about local source-active messages.

originator *ip-address* — Displays information about the specified originator IP address.

peer *ip-address* — Displays information about the specified peer IP address.

source *ip-address* — Displays information about the specified source IP address.

group *ip-address* — Displays information about the specified group IP address.

detail — Displays detailed MSDP source-active information.

Output MSDP Source-Active Output

The following table provides MSDP source-active field descriptions.

Table 30 **MSDP Source-Active Fields**

Label	Description
Grp Address	Displays the IP address of the group.

Table 30 MSDP Source-Active Fields (Continued)

Label	Description
Src Address	Displays the IP address of the source.
Origin RP	Displays the origination rendezvous point (RP) address.
Peer Address	Displays the address of the peer.
State Timer	The time-out value. If the value reaches zero, the SA is removed.

Sample Output

```
A:ALA-48# show router msdp source-active
===============================================================================
MSDP Source Active Info
===============================================================================
Grp Address      Src Address      Origin RP        Peer Address State Timer
-------------------------------------------------------------------------------
239.100.0.0      10.112.1.2      10.20.1.1        10.20.1.1 69
239.100.0.1      10.112.1.2      10.20.1.1        10.20.1.1 69
239.100.0.2      10.112.1.2      10.20.1.1        10.20.1.1 69
239.100.0.3      10.112.1.2      10.20.1.1        10.20.1.1 69
239.100.0.4      10.112.1.2      10.20.1.1        10.20.1.1 69
239.100.0.5      10.112.1.2      10.20.1.1        10.20.1.1 69
239.100.0.6      10.112.1.2      10.20.1.1        10.20.1.1 69
239.100.0.7      10.112.1.2      10.20.1.1        10.20.1.1 69
239.100.0.8      10.112.1.2      10.20.1.1        10.20.1.1 69
239.100.0.9      10.112.1.2      10.20.1.1        10.20.1.1 69
-------------------------------------------------------------------------------
MSDP Source Active : 10
===============================================================================
A:ALA-48#


A:ALA-48# show router msdp source-active detail
===============================================================================
MSDP Source Active
===============================================================================
Group Address      : 239.100.0.0       Source Address     : 10.112.1.2
Origin RP          : 10.20.1.1         Peer Address       : 10.20.1.1
State Timer        : 64                Up Time            : 3d 01:44:25
Group Address      : 239.100.0.1       Source Address     : 10.112.1.2
Origin RP          : 10.20.1.1         Peer Address       : 10.20.1.1
State Timer        : 64                Up Time            : 48d 18:22:29
Group Address      : 239.100.0.2       Source Address     : 10.112.1.2
Origin RP          : 10.20.1.1         Peer Address       : 10.20.1.1
State Timer        : 64                Up Time            : 48d 18:22:29
Group Address      : 239.100.0.3       Source Address     : 10.112.1.2
Origin RP          : 10.20.1.1         Peer Address       : 10.20.1.1
State Timer        : 64                Up Time            : 48d 18:22:29
Group Address      : 239.100.0.4       Source Address     : 10.112.1.2
Origin RP          : 10.20.1.1         Peer Address       : 10.20.1.1
State Timer        : 64                Up Time            : 48d 18:22:29
Group Address      : 239.100.0.5       Source Address     : 10.112.1.2
Origin RP          : 10.20.1.1         Peer Address       : 10.20.1.1
```

```
Origin RP          : 10.20.1.1          Peer Address       : 10.20.1.1
State Timer        : 64                 Up Time            : 48d 18:22:29
Group Address      : 239.100.0.7        Source Address     : 10.112.1.2
Origin RP          : 10.20.1.1          Peer Address       : 10.20.1.1
State Timer        : 64                 Up Time            : 48d 18:22:29
Group Address      : 239.100.0.8        Source Address     : 10.112.1.2
Origin RP          : 10.20.1.1          Peer Address       : 10.20.1.1
State Timer        : 64                 Up Time            : 48d 18:22:29
Group Address      : 239.100.0.9        Source Address     : 10.112.1.2
Origin RP          : 10.20.1.1          Peer Address       : 10.20.1.1
State Timer        : 64                 Up Time            : 48d 18:22:29
-------------------------------------------------------------------------------
MSDP Source Active : 10
===============================================================================
A:ALA-48#
```

source-active-rejected

Syntax **source-active-rejected** [**peer-group** *name*] [**group** *ip-address*] [**source** *ip-address*] [**originator** *ip-address*] [**peer** *ip-address*]

Context show>router>msdp

Description This command displays source-active messages rejected by MSDP.

Parameters **peer-group** *name* — Displays information about rejected source-active messages for the specified peer group.

group *ip-address* — Displays information about the specified group IP address.

source *ip-address* — Displays information about the source address of the source active entry that is rejected.

originator *ip-address* — Displays information about the specified originator IP address.

peer *ip-address* — Displays information about the peer from which this rejected source active entry was last received.

Output MSDP Source-Active Output

The following table provides MSDP source-active field descriptions.

Table 31 **MSDP Source-Active Fields**

Label	Description
Grp Address	Displays the IP address of the group.
Src Address	Displays the IP address of the source.
Origin RP	Displays the origination rendezvous point (RP) address.
Peer Address	Displays the address of the peer.

Table 31 MSDP Source-Active Fields (Continued)

Label	Description
Reject Reason	Displays the reason why this source active entry is rejected.

Sample Output

```
*A:ALA-48# show router msdp source-active-rejected
===============================================================================
MSDP Source Active Rejected Info
===============================================================================
Grp Address     Src Address     Origin RP       Peer Address    Reject Reason
-------------------------------------------------------------------------------
239.100.0.1     10.0.0.1        10.20.0.1       239.0.0.1       Import Policy
239.100.0.2     10.0.0.2        10.20.0.2       239.0.0.2       Export Policy
239.100.0.3     10.0.0.3        10.20.0.3       239.0.0.3       RPF Failure
239.100.0.4     10.0.0.4        10.20.0.4       239.0.0.4       Limit Exceeded
239.100.0.5     10.0.0.5        10.20.0.5       239.0.0.5       Limit Exceeded
239.100.0.6     10.0.0.6        10.20.0.6       239.0.0.6       Limit Exceeded
239.100.0.7     10.0.0.7        10.20.0.7       239.0.0.7       Limit Exceeded
-------------------------------------------------------------------------------
SA Rejected Entries : 7
===============================================================================
*A:ALA-48#
```

statistics

Syntax **statistics** [**peer** *ip-address*]

Context show>router>msdp

Description This command displays statistics information related to a MSDP peer.

Parameters *ip-address* — Displays information about the specified peer IP address

Output MSDP Statistics Output

The following table provides MSDP statistics field descriptions.

Table 32 MSDP Statistics Fields

Label	Description
Last State Change	Displays the date and time the peer state changed.
RPF Failures	Displays the number of reverse path forwarding (RPF) failures.
SA Msgs Sent	Displays the number of source-active messages sent.
SA req. Msgs Sent	Displays the number of source-active request messages sent.

Table 32 MSDP Statistics Fields (Continued)

Label	Description
SA res. Msgs Sent	Displays the number of source-active response messages sent.
KeepAlive Msgs Sent	Displays the number of keepalive messages sent.
Unknown Msgs Sent	Displays the number of unknown messages received.
Last message Peer	Displays the time the last message was received from the peer.
Remote Closes	Displays the number of times the remote peer close.
SA Msgs Recvd	Displays the number of source-active messages received.
SA req. Msgs Recvd	Displays the number of source-active request messages received.
SA res. Msgs Recvd	Displays the number of source-active response messages received.
KeepAlive Msgs Recd	Displays the number of keepalive messages received.
Error Msgs Recvd	Displays the number of unknown messages received.

Sample Output

```
A:ALA-48# show router msdp statistics
===============================================================================
MSDP Statistics
===============================================================================
Glo ActSrc Lim Excd: 0
-------------------------------------------------------------------------------
Peer Address       : 10.20.1.1
-------------------------------------------------------------------------------
Last State Change  : 0d 11:33:16        Last message Peer  : 0d 00:00:17
RPF Failures       : 0                  Remote Closes      : 0
SA Msgs Sent       : 0                  SA Msgs Recvd      : 709
SA req. Msgs Sent  : 0                  SA req. Msgs Recvd : 0
SA res. Msgs Sent  : 0                  SA res. Msgs Recvd : 0
KeepAlive Msgs Sent: 694                KeepAlive Msgs Recd: 694
Unknown Msgs Sent  : 0                  Error Msgs Recvd   : 0
-------------------------------------------------------------------------------
Peers : 1
===============================================================================
A:ALA-48#
```

status

Syntax **status**

Context show>router>msdp

Description This command displays MSDP status information.

Output MSDP Status Output

The following table provides MSDP status field descriptions.

Table 33 **MSDP Status Fields**

Label	Description
Admin State	Displays the administrative state.
Local Address	Displays the local IP address.
Active Src Limit	Displays the active source limit.
Act Src Lim Excd	Displays the active source limit which has been exceeded.
Num. Peers	Displays the number of peers.
Num. Peers Estab	Displays the number of peers established.
Num. Source Active	Displays the number of active sources.
Policies	The policy to export source active state from the source active list into MSDP.
Data Encapsulation	The rendezvous point (RP) using MSDP to encapsulate multicast data received in MSDP register messages inside forwarded MSDP source-active messages - enabled or disabled.
Rate	The receive message rate.
Time	The receive message time.
Threshold	The number of MSDP messages that can be processed before the MSDP message rate limiting function is activated.
RPF Table	The name of the reverse path forwarding table.
Last msdp Enabled	The time the last MSDP was triggered.

Sample Output

```
A:ALA-48# show router msdp status
===============================================================================
MSDP Status
===============================================================================
Admin State                        : Up
Local Address                      : None
Global Statistics
Active Src Limit                   : None
Act Src Lim Excd                   : 0
```

```
Num. Peers                        : 1
Num. Peers Estab                  : 1
Num. Source Active                : 10
Policies                          : None
Data Encapsulation                : Enabled
Receive Msg Rate
Rate                              : 0
Time                              : 0
Threshold                         : 0
Last Msdp Enabled                 : 08/30/2002 03:21:43
===============================================================================
A:ALA-48#
```

6.4.2.2 Clear Commands

msdp

Syntax **msdp**

Context clear>router

Description This command enables the context to clear and reset Multicast Source Discovery protocol (MSDP) entities and statistics.

cache

Syntax **cache** [**peer** *ip-address*] [**group** *ip-address*] [**source** *ip-address*] [**originrp** *ip-address*]

Context clear>router>msdp

Description This command clears the MSDP cache.

Parameters **peer** *ip-address* — Clears the cache of the IP address of the peer to which Multicast Source Discovery protocol (MSDP) source-active (SA) requests for groups matching this entry's group range were sent.

group *ip-address* — Clears the group IP address of the SA entry.

source *ip-address* — Clears the source IP address of the SA entry.

originrp *ip-address* — Clears the origin rendezvous point (RP) address type of the SA entry.

statistics

Syntax **statistics** [**peer** *ip-address*]

Context clear>router>msdp

Description This command clears IP address statistics of the peer to which Multicast Source Discovery Protocol (MSDP) source-active (SA) requests for groups matching this entry's group range were sent.

Parameters *ip-address* — Clears the statistics of the specified IP address.

6.4.2.3 Debug Commands

msdp

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

Context debug>router

Description This command enables debugging for Multicast Source Discovery Protocol (MSDP).

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

packet

Syntax **packet** [*pkt-type*] [**peer** *ip-address*]

Context debug>router>msdp

Description This command enables debugging for Multicast Source Discovery Protocol (MSDP) packets.

The **no** form of the command disables MSDP packet debugging.

Parameters *pkt-type* — Debugs information associated with the specified packet type.

Values keep-alive, source-active, sa-request, sa-response

ip-address — Debugs information associated with the specified peer IP address.

pim

Syntax **pim** [*grp-address*]
no pim

Context debug>router>msdp

Description This command enables debugging for Multicast Source Discovery Protocol (MSDP) PIM.

The **no** form of the command disables MSDP PIM debugging.

Parameters *grp-address* — Debugs the IP multicast group address for which this entry contains information.

rtm

Syntax **rtm** [*rp-address*]
no rtm

Context debug>router>msdp

Description This command enables debugging for Multicast Source Discovery Protocol (MSDP) route table manager (RTM).

The **no** form of the command disables MSDP RTM debugging.

Parameters *rp-address* — Debugs the IP multicast address for which this entry contains information.

sa-db

Syntax **sa-db** [**group** *grpAddr*] [**source** *srcAddr*] [**rp** *rpAddr*]
no sadb

Context debug>router>msdp

Description This command enables debugging for Multicast Source Discovery Protocol (MSDP) source-active requests.

The **no** form of the command disables the MSDP source-active database debugging.

Parameters *grpAddr* — Debugs the IP address of the group.

srcAddr — Debugs the source IP address.

rpAddr — Debugs the specified rendezvous point RP address.

7 MLDP

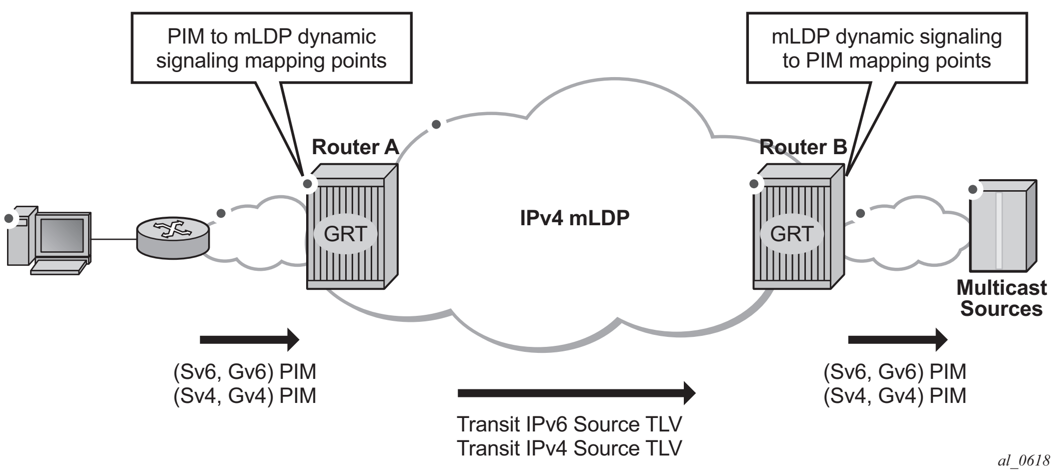
7.1 Dynamic Multicast Signaling over P2MP in GRT Instance

This feature provides a flexible multicast signaling solution to connect native IP multicast source and receivers running PIM multicast protocol via an intermediate MPLS (P2MP LDP LSP) network. The feature allows each native IP multicast flow to be connected via an intermediate P2MP LSP by dynamically mapping each PIM multicast flow to a P2MP LDP LSP.

The feature uses procedures defined in RFC 6826: *Multipoint LDP In-Band Signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*. On the leaf node of a P2MP LSP, PIM signaling is dynamically mapped to P2MP LDP tree setup. On the root node of P2MP LSP, P2MP LDP signaling is handed back to PIM. Due to dynamic mapping of multicast IP flow to P2MP LSP, provisioning and maintenance overhead is eliminated as multicast distribution services are added and removed from the network. Per (S,G) IP multicast state is also removed from the network where P2MP LSPs are used to transport multicast flows.

Figure 5 illustrates dynamic MLDP signaling for IP multicast in GRT.

Figure 5 **Dynamic MLDP Signaling for IP Multicast in GRT**



As illustrated in Figure 5, P2MP LDP LSP signaling is initiated from the router that receives PIM JOIN from a downstream router (Router A). To enable dynamic multicast signaling, p2mp-ldp-tree-join must be configured on PIM outgoing interface of Router A. This enables handover of multicast tree signaling from PIM to P2MP LDP LSP. Being a leaf node of P2MP LDP LSP, Router A selects the upstream-hop as the root node of P2MP LDP FEC based on routing table lookup. If an ECMP path is available for a given route, then the number of trees are equally balanced towards multiple root nodes. The PIM Joins are carried in Transit IPv4 (IPv4 PIM-SSM) or IPv6 (IPv6 PIM-SSM) MLDP TLVs. On the root node of P2MP LDP LSP (Router B), multicast tree signaling is handed back to PIM and propagated upstream as native-IP PIM JOIN.

The feature is supported with IPv4 and IPv6 PIM-SSM and IPv4 MLDP. Directly connected IGMP/MLD receivers are also supported with PIM enabled on outgoing interfaces and SSM mapping configured if required.

If multiple criteria exist to setup a multicast flow, the following priority is given as follows:

1. Multicast (statically provisioned) over P2MP LSP (RSVP-TE or LDP)
2. Dynamic multicast signaling over P2MP LDP
3. PIM native-IP multicast

The following are feature caveats:

- A single instance of P2MP LDP LSP is supported between the root and leaf nodes per multicast flow; there is no stitching of dynamic trees.
- Extranet functionality is not supported.
- The router LSA link ID or the advertising router ID must be a routable IPv4 address (including IPv6 into IPv4 MLDP use cases).
- IPv6 PIM with dynamic IPv4 MLDP signaling is not supported with e-BGP or i-BGP with IPv6 next-hop.
- Inter-AS and IGP inter-area scenarios where the originating router is altered at the ASBR and ABR respectively, (hence PIM has no way to create the LDP LSP towards the source), are not supported.

7.2 Inter-AS Non-segmented MLDP

This feature allows multicast services to use segmented protocols and span them over multiple autonomous systems (ASs), as done in unicast services. As IP VPN or GRT services span multiple IGP areas or multiple ASs, either for a network designed to deal with scale or as result of commercial acquisitions, operators may require Inter-AS VPN (unicast) connectivity. For example, an Inter-AS VPN can break the IGP, MPLS and BGP protocols into access segments and core segments, allowing higher scaling of protocols by segmenting them into their own islands. SR OS also allows for similar provision of multicast services and for spanning these services over multiple IGP areas or multiple ASs.

For multicast VPN (MVPN), SR OS previously supported Inter-AS option A/B/C for Rosen MVPN; however, when MPLS was used, only option A was supported for Next Generation Multicast VPN (NG-MVPN) or d-MLDP signaling. MLDP now supports non-segmented MLDP trees for inter-AS solutions, applicable for multicast services in the GRT (Global Routing Table) where they need to ride over MLDP point-to-multipoint tunnels as well as NG-MVPN services.

Refer to the “ECMP Support” subsection of the “Inter-AS Non-segmented MLDP” section in the *7450 ESS, 7750 SR, 7950 XRS, and VSR MPLS Guide* for more information.

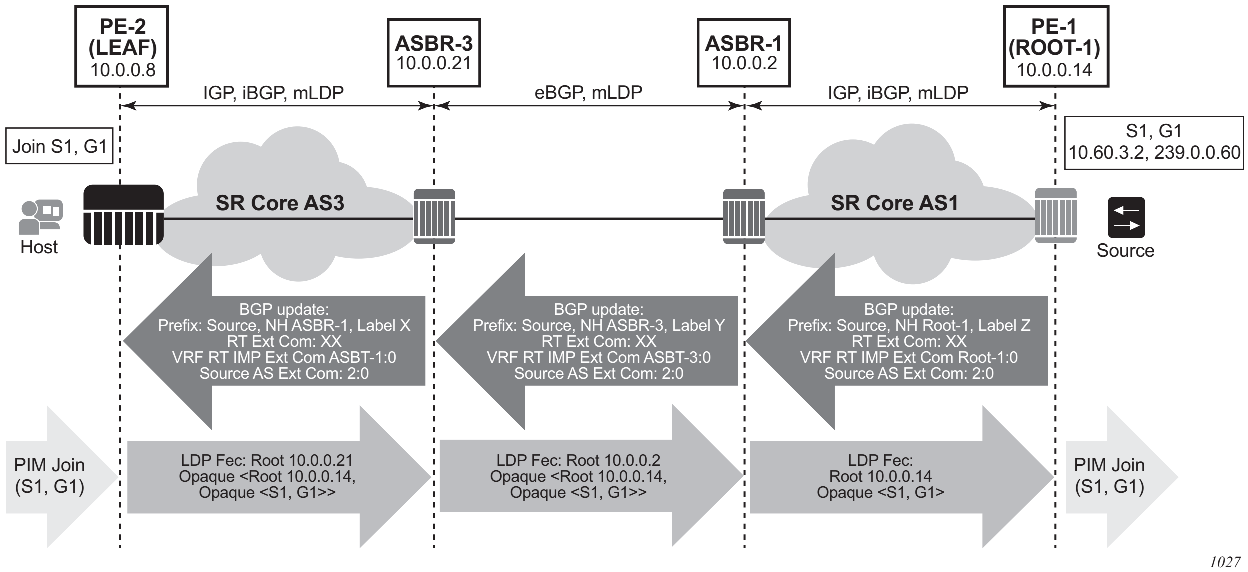
Refer to the “Dynamic mLDP and Static mLDP Co-existing on Same Node” section in the *7450 ESS, 7750 SR, 7950 XRS, and VSR MPLS Guide* for more information.

7.2.1 d-MLDP Inter-AS Trees in GRT

Figure 6 shows the processing required for d-mLDP with non-segmented mLDP Inter-AS trees in GRT (routers in AS3, including ASBR 1, have no route to ROOT-1 in IGP and must use BGP unicast routes to resolve route to ROOT-1 and to multicast source).

PE-1 (ROOT-1) is the root node of the MLDP tree, and PE-2 (LEAF) is the leaf node.

Figure 6 **In-band Signaling with Non-segmented Inter-AS MLDP Trees in GRT**



7.2.1.1 Routing

BGP unicast routes must advertise to the VRF Route Import Ext Community, identifying the root PE, for the feature to operate properly. Failure to do so will result in PIM Inter-AS joins being dropped.

The community is an address-based community where the global administrator field is the address of the root PE and local administrator field is set to 0 (GRT). No new configuration is required; however, an operator must enable inter-AS VPN and configure export policy to ensure the community is added to the BGP routes as required. The BGP unicast route is propagated across the AS, as shown in Figure 6 (the same processing, not shown, applies to a BGP route specifying address used to build mLDP tree rooted at ROOT-1). The following configuration example shows an export policy configuration.

Example:

```
policy-options
     begin
     community "A" members "target:1.1.1.1:0"
     community "B" members "ext:010b:0a1401060000"
          policy-statement "fromlocal"
               entry 10
                    from
                         protocol direct
                    exit
                    to
```

```
                                        protocol bgp
                                    exit
                                    action accept
                                        community add "A" "B"
                                    exit
                                exit
                                default-action reject
                        exit
                        policy-statement "accept_all"
                            default-action accept
                            exit
                        exit
                        commit
                    exit
                    bgp
                    …
                        enable-inter-as-vpn
                        …
                        export "fromlocal" "accept_all"
                        …
                         no shutdown
                    exit
```

Static routes must be configured on inter-ASBR LDP-enabled links because the BGP peer uses a host address from the local subnet of the links (for GRT and VPN option C), or the BGP peer uses a system IP address that is not in the base routing table (for VPN option B).

- For system-IP to system-IP, static-routes are required for bringing up the EBGP/LDP session.
- If the link IP is used for creation of EBGP and ILD, then static-routes are not required; however, static-route (host-route) is mandatory on ASBR2 for the resolution of MLDP FEC, as the link LSR ID is not resolved by LDP using a /24 route; it needs a /32 route.

7.2.1.2 Join Processing

To traverse an inter-AS domain, recursive FECs are required (refer to the “Inter-AS Non-segmented MLDP” section in the *7450 ESS, 7750 SR, 7950 XRS, and VSR MPLS Guide* for more information).

The operator must enable dynamic signaling on interfaces where Inter-AS joins are expected to be received using the existing configuration (**p2mp-ldp-tree-join** [**ipv4**] [**ipv6**]). Once enabled, the following describes the required processing of a PIM join, as shown in Figure 6.

When the leaf receives a PIM join for group (S1, G1) and, through configuration, knows dynamic signaling is required, the leaf fails to resolve the source S1 via IGP and attempts to resolve route via BGP. The leaf learns that source is reachable via Next-Hop ASBR3 and the route was advertised by PE1 (Root-1) (from VRF Import Ext Community). PE2 (leaf) sources a Recursive mLDP FEC with a root node of ASBR3, and an opaque value containing the MLDP in-band signaling information identifying the (S1, G1) group and the Root-1 (the root of the inter-AS non-segmented MLDP tree), as shown below:

LEAF FEC {Root = ASBR3, Opaque Value = {Root: ROOT-1, Opaque Value (S1, G1)}}

The FEC is forwarded using IGP to ASBR3.

When the Recursive MLDP FEC arrives at ASBR3, it notes that it is the identified root node in the local AS, and that the opaque value is a Recursive Opaque Value. Because ASBR3 fails to resolve the Recursive FEC’s root (Root-1) in IGP, ASBR3 attempts to resolves the root via BGP. Similarly to processing on LEAF, this yields a Next-Hop of ASBR1. ASBR3 creates a new mLDP FEC element with a root node of ASBR1, and the Opaque value as per received opaque value, as shown below:

ASBR3 FEC {Root = ASBR1, Opaque Value = {Root: Root-1, Opaque Value: (S1, G1)}}

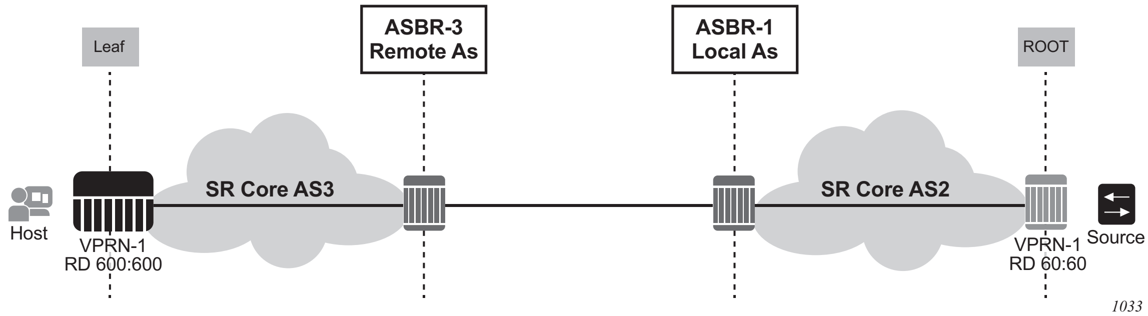
ASBR 3 forwards the FEC using IGP or eBGP.

When the MLDP FEC arrives at ASBR1, it notes that it is the identified root node, and that the opaque value is a Recursive Opaque value. Because ASBR1 can resolve the Recursive FEC’s root (Root-1) via IGP, no further recursive processing is required. ASBR 1 forwards mLDP FEC containing in-band signaling using IGP towards ROOT-1.

7.2.2 ASBR Support of PE Functionality

Figure 7 displays remote and local ASBRs.

Figure 7 **Remote and Local ASBRs**



While ASBRs can also act as PE nodes, SR OS does not support all PE functionalities in the ASBR node. Table 34 lists supported PE features on ASBRs.

Table 34 **PE Features on ASBRs**

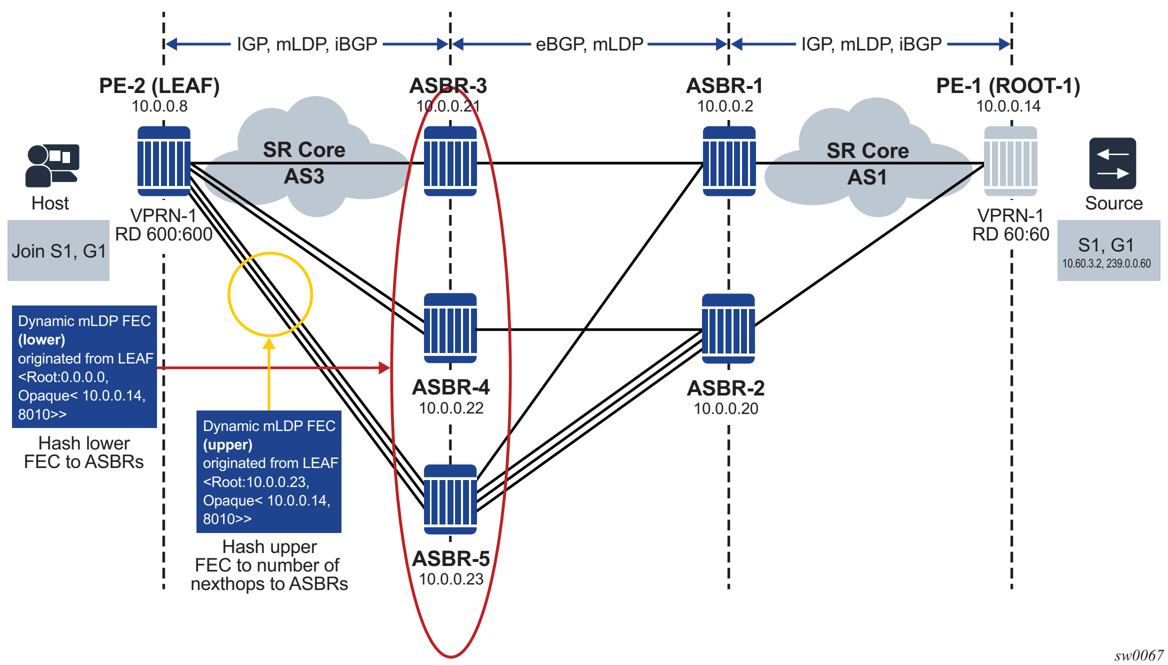
	ASBR Node	
Inter-AS Multicast Context	**Leaf or Bud**	**Root or Source**
GRT	✓	X
VPN	✓	✓

7.3 Hashing for Inter-AS

At each leaf or ASBR, there are two FECs: a lower FEC and an upper FEC. The lower FEC is used for hashing to multiple ASBRs and the upper FEC is used to choose the next-hop that connects the leaf node to the ASBR. Hashing is performed based on the opaque value of the FEC. Refer to the “Supported Recursive Opaque Values” section in the *7450 ESS, 7750 SR, 7950 XRS, and VSR MPLS Guide* for more information.

In Figure 8, the leaf generates a lower FEC <0.0.0.0, opaque <10.0.0.14, 8010>>. The lower FEC’s opaque <10.0.0.14, 8010> and number of ASBRs (three) will be used to decide which ASBR will be used based on hashing. After hashing produces ASBR-5 as the result, the upper FEC of <10.0.0.23, opaque <10.0.0.14, 8010>> is created. This upper FEC is used to resolve the ASBR-5 next-hop between the three interfaces that connect the leaf node to ASBR-5.

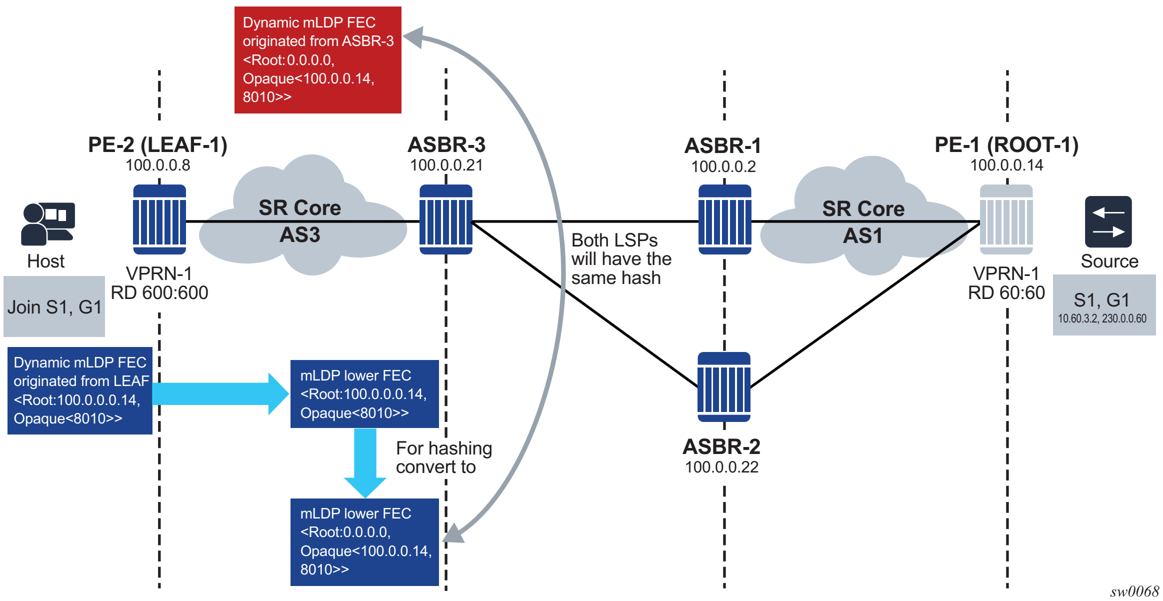
Figure 8 **Hashing for Inter-AS**



7.4 Hashing at the ASBR

Figure 9 illustrates hashing at the ASBR.

Figure 9 **Hashing at the ASBR**



In Figure 9, the leaf node will have ROOT-1 in the RTM for optimized Option C; therefore, the leaf will not generate a recursive type 7 opaque, and will only generate a type 1 opaque. When the FEC arrives at ASBR-3, it will have a basic type 1 FEC of <ROOT: 10.0.0.14, opaque <8010>>.

If the ASBR also has a host that will generate a mLDP LSP towards the root, this FEC will look up <ROOT: 0.0.0.0, opaque <10.0.0.14, 8010>>.

Hashing is performed based on the opaque value of the FEC. See “Supported Recursive Opaque Values” in the *7450 ESS, 7750 SR, 7950 XRS, and VSR MPLS Guide* for more information.

The opaque of the leaf node is not the same as the opaque of the ASBR bud node. In this scenario, the two LSPs will generate a different ASBR as the next-hop, inefficiently duplicating multicast traffic.

In order to prevent this problem, SR OS converts the lower FEC of opaque type 1 that arrives from the leaf node into a recursive type 7 FEC, so that the bud FEC generated by the ASBR and the FEC arriving from the leaf node will result in the same upper ASBR.

8 Multicast Extensions to BGP

8.1 Multicast Extensions to BGP

This section describes the implementation of extensions to MBGP to support multicast. Rather than assuming that all unicast routes are multicast-capable, some routed environments, in some cases, some ISPs do not support or have limited support for multicast throughout their AS.

BGP is capable of supporting two sets of routing information, one set for unicast routing and the other for multicast routing. The unicast and multicast routing sets either partially or fully overlay one another. To achieve this, BGP has added support for IPv4 and mcast-IPv4 address families. Routing policies can be imported or exported.

The multicast routing information can subsequently be used by the Protocol Independent Multicast (PIM) protocol to perform its Reverse Path Forwarding (RPF) lookups for multicast-capable sources. Thus, multicast traffic can only be routed across a multicast topology and not a unicast topology.

8.1.1 MBGP Multicast Topology Support

8.1.1.1 Recursive Lookup for BGP Next Hops

The next hop for multicast RPF routes learned by MBGP is not always the address of a directly-connected neighbor. For unicast routing, a router resolves the directly-connected next-hop by repeating the IGP routes. For multicast RPF routes, there are different ways to find the real next-hops.

- Scanning to see if a route encompasses the BGP next hop. If one exists, this route is used. If not, the tables are scanned for the best matching route.
- Check to see if the recursed next hop is taken from the protocol routing table with the lowest administrative distance (protocol preference). This means that the operating system algorithm must perform multiple lookups in the order of the lowest admin distance. Unlike recursion on the unicast routing table, the longest prefix match rule does not take effect; protocol preference is considered prior to prefix length. For example, the route 10.0.0.0/14 learned via MBGP will be selected over the route 10.0.0.0/16 learned via BGP.

9 MCAC

9.1 MCAC Overview

Multicast Connection Admission Control (MCAC) allows a router to limit bandwidth used by multicast channels, either on a router, on access links, or by an ESM subscriber, by controlling the number of channels that are accepted. When a pre-configured limit is reached, the router prevents receivers from joining any new channels not currently established. By rejecting new channel establishment during an overload condition, the degradation of the quality of the existing multicast service offering is avoided. However, as result, running the MCAC function might cause some channels to be temporarily unavailable to receivers under overload.

Operators can configure one or more MCAC bundle policies (**configure**>**router**>**mcac**>**policy**) to specify multicast channel admission rules and then reference a required MCAC bundle policy on multicast-enabled IPv4 and IPv6 interfaces or group-interfaces. In addition, operators can configure per-interface MCAC behavior.

MCAC is supported on ESM subscriber interfaces as well as multicast interfaces in base router instance, VPLS, and in MVPNs. MCAC is supported for IGMP, IGMP-snooping, MLD, and PIM.

The amount of bandwidth multicast channels can consume is limited by operator-configured unconstrained and mandatory bandwidth values. Those values can be configured on a per-MCAC bundle policy, per subscriber, per interface, and per MCAC interface policy. The bandwidth limits configured for a subscriber or interface limit multicast bandwidth for that particular subscriber or that interface only. The bandwidth limits configured for an MCAC interface policy limit multicast bandwidth across a set of interfaces that share the same interface policy. If bandwidth limits are defined on multiple levels, all level limits must be satisfied for a channel to be admitted. See MCAC Algorithm for more information.

Feature caveats:

- MCAC is not applicable to PIM snooping and MLD snooping

9.1.1 MCAC Bundle Policy Overview

MCAC bundle policy (shortened here to “MCAC policy” or “policy”) is used to define MCAC rules to be applied on an MCAC interface when receivers are trying to join multicast channels. Within each policy, an operator can define:

- Multicast channel:
  - A channel can be defined using multicast group address only or both source and group addresses. Ranges can be used to group multiple multicast channels into a single MCAC channel. When ranges are used, each multicast channel within range will use the same channel BW (bandwidth), class, and priority configuration.
  - Channel BW: a bandwidth value to be used for a channel in MCAC.
  - Channel type (mandatory or optional): mandatory channels have BW pre-reserved on interfaces as soon as they are defined in MCAC policy, while optional channels consume BW on-demand; only when there are active receivers for that channel and the remaining BW allows for channels to be admitted.
  - Channel class: high and low classes are supported. For LAG interfaces, the class parameter allows further prioritizing of the mandatory or optional channels. This brings the number of priority levels to four during reshuffles of the joined channels when LAG ports are changing state.

Note: Multicast channels not specified in an MCAC policy applicable on a given interface are not subject to MCAC. Treatment of such channels is configurable as either accept or discard.

- Multicast channel bundle:
  - Multicast bundle defines multicast channels as described above. A channel can only be part of one bundle.
  - Maximum bundle BW – the maximum bandwidth the channels forming a given bundle can consume on an interface.
  - MCAC constraints – set of rules governing available BW for multicast channels over LAG as LAG ports are changing state.

9.1.2 MCAC Algorithm

It is important to point out that the MCAC algorithm is based on configured BW values. The configured channel BW based on MCAC policy is CAC-ed against pre-configured maximum bundle BW and pre-configured subscriber, interface, or MCAC interface-policy multicast BW limits. A channel must pass all levels of CAC before it is accepted. The statements outline the CAC algorithm for a multicast channel defined in MCAC policy:

A join for a particular multicast channel is allowed under the following conditions.

- Mandatory channels—A sufficient bandwidth exists on the interface according to the policy settings for the interface (Interface-level MCAC and MCAC-interface-policy-level MCAC) and BW setting for a channel (Bundle-level MCAC). There is always sufficient BW available on the bundle level because mandatory channels get pre-reserved bandwidth.
- Optional channels—A sufficient BW exists on both interface (Interface-level MCAC and MCAC-interface-policy-level MCAC) and bundle level (Bundle-Level MCAC) based on channel configured BW and currently available BW on both interface and bundle.

When a policy is evaluated over a set of existing channels (applicable for MCAC on LAG when the number of ports in the LAG changes and applicable to subscribers when the submac policy is enabled on a subscriber), the channels are evaluated and admitted/dropped based on the following priority order: mandatory-high, mandatory-low, optional-high, optional-low.

This method does not guarantee that all bundles are fully allocated. However, this method does ensure that all mandatory-high channels are allocated before any mandatory-low channels are allocated.

When a new MCAC bundle policy is applied, the algorithm is forced to admit all currently joined channels to prevent any drops. This can result in an oversubscription until some of the joined channels disconnect. The same behavior applies when adding a new MCAC interface policy: all the joined channels will be admitted, without dropping anything.

9.1.2.1 Interface-level MCAC details

Interface-level MCAC constraints are applied to the interface on which the join was received. Mandatory and optional channels are allowed under the following conditions.

- Mandatory channels—The bandwidth for the already-accepted mandatory channels plus the bandwidth of this channel cannot be greater than the configured mandatory bandwidth on this interface.
- Optional channels—The bandwidth for the already-accepted optional channels plus the bandwidth of this channel cannot be greater than the configured amount of unconstrained bandwidth less the configured amount of mandatory bandwidth on this interface.

9.1.2.1.1 MCAC-interface-policy-level MCAC details

MCAC interface policies are defined system wide and used on MCAC interfaces via assignment of the policy to one or more interfaces to, for example, limit multicast BW across a group of interfaces/ports, across a line card or across a system. If an MCAC interface policy is assigned to an interface with Interface-level constraints configured, then both Interface-level MCAC as described above and MCAC-interface-policy-level MCAC must be satisfied for a channel to be admitted.

Mandatory and optional channels are allowed under the following conditions.

- Mandatory channels—The bandwidth for the already-accepted mandatory channels on this and any other interface using this MCAC interface policy plus the bandwidth of this channel cannot be greater than the configured mandatory bandwidth for this MCAC interface policy.
- Optional channels—The bandwidth for the already-accepted optional channels on this and any other interface using this MCAC interface policy plus the bandwidth of this channel cannot be greater than the configured amount of unconstrained bandwidth less the configured amount of mandatory bandwidth for this MCAC interface policy.

Thus, when MCAC interface policy is used, admitting a channel on one interface affects all interfaces sharing the same MCAC interface policy.

9.1.2.2 Bundle-level MCAC details

Bundle-level CAC is applied to the bundle to which the channel that triggered the MCAC algorithm belongs.

Mandatory and optional channels are allowed under the following conditions.

- Mandatory channels—Always.

- Optional channels—The allocated bundle bandwidth cannot exceed the configured bandwidth. The allocated bandwidth equals the bandwidth of all the mandatory channels belonging to that bundle plus the bandwidth of the optional channels already accepted plus the bandwidth of this optional channel.

9.1.3 MCAC on Link Aggregation Group Interfaces

When MCAC enabled interfaces reside on a LAG, SR OS allows operators to change MCAC behavior when the number of active ports in a LAG changes. Both MCAC policy bundle and MCAC interface allows operators to define multiple MCAC levels per LAG based on the number of active ports in the LAG. For each level, operators can configure corresponding BW limits.

When MCAC LAG constraints are enabled, the level to use is selected automatically based on the configuration and a currently active number of LAG ports. In a case of the available bandwidth reduction (for example, a LAG link failure causes change to a level with smaller BW configured), MCAC attempts first to fit all mandatory channels (in an arbitrary order). If there is no sufficient capacity to carry all mandatory channels in the degraded mode, some channels are dropped and all optional channels are dropped. If after evaluation of mandatory channels, there remains available bandwidth, then all optional channels are re-evaluated (in an arbitrary order). Channel re-evaluation employs the above-described MCAC algorithm applied at the interface and bundle levels that use the constraints for the degraded mode of operation.

9.2 Configuring MCAC with CLI

This section provides information to configure MCAC using the command line interface.

9.2.1 Basic MCAC Configuration

Perform the following basic MCAC configuration tasks:

- configure policy name
- configure bundle parameters
- specify default action

The following example displays the enabled IGMP and PIM configurations:

```
A:LAX>config>router>igmp# info
----------------------------------------------
        interface "lax-vls"
        exit
        interface "p1-ix"
        exit
----------------------------------------------
A:LAX>config>router>igmp# info detail
----------------------------------------------
        interface "lax-vls"
            no import
            version 3
            no shutdown
        exit
        interface "p1-ix"
            no import
            version 3
            no shutdown
        exit
        query-interval 125
        query-last-member-interval 1
        query-response-interval 10
        robust-count 2
        no shutdown
----------------------------------------------
A:LAX>config>router>igmp# exit
A:LAX>config>router# pim
A:LAX>config>router>pim# info
----------------------------------------------
            interface "system"
            exit
            interface "lax-vls"
            exit
            interface "lax-sjc"
            exit
```

```
            interface "p1-ix"
            exit
            rp
                static
                    address 10.22.187.237
                        group-prefix 239.24.24.24/32
                    exit
                exit
                bsr-candidate
                    shutdown
                exit
                rp-candidate
                    shutdown
                exit
            exit
----------------------------------------------
A:LAX>config>router>pim# info detail
----------------------------------------------
            no import join-policy
            no import register-policy
            interface "system"
                priority 1
                hello-interval 30
                multicast-senders auto
                no tracking-support
                bsm-check-rtr-alert
                no shutdown
            exit
            interface "lax-vls"
                priority 1
                hello-interval 30
                multicast-senders auto
                no tracking-support
                bsm-check-rtr-alert
                no shutdown
            exit
            interface "lax-sjc"
                priority 1
                hello-interval 30
                multicast-senders auto
                no tracking-support
                bsm-check-rtr-alert
                no shutdown
            exit
            interface "p1-ix"
                priority 1
                hello-interval 30
                multicast-senders auto
                no tracking-support
                bsm-check-rtr-alert
                no shutdown
            exit
            apply-to none
            rp
                no bootstrap-import
                no bootstrap-export
                static
                    address 10.22.187.237
                        no override
```

```
                group-prefix 239.24.24.24/32
            exit
        exit
        bsr-candidate
            shutdown
            priority 0
            hash-mask-len 30
            no address
        exit
        rp-candidate
            shutdown
            no address
            holdtime 150
            priority 192
        exit
    exit
    no shutdown
----------------------------------------------
A:LAX>config>router>pim#
```

9.2.2 Configuring MCAC Parameters

The MCAC policies can be added to a SAP, spoke-SDP, mesh-SDP, an IGMP interface, and a PIM interface.

The following example displays the command usage to create MCAC policies.

Example:

```
config>router# mcac
config>router>mcac# policy "btv_fr"
config>router>mcac>policy# description "foreign TV
 offering"
config>router>mcac>policy# bundle "FOR" create
config>router>mcac>policy>bundle# bandwidth 30000
config>router>mcac>policy>bundle# channel 239.0.3.1
 239.0.3.1 bw 4000
config>router>mcac>policy>bundle# channel 239.0.3.2
 239.0.3.2 bw 4000
config>router>mcac>policy>bundle# channel 239.0.4.1
 239.0.4.1 bw 3500 class high type mandatory
config>router>mcac>policy>bundle# channel 239.0.4.2
 239.0.4.2 bw 3500 class high
config>router>mcac>policy>bundle# channel 239.0.4.3
 239.0.4.3 bw 2800 type mandatory
config>router>mcac>policy>bundle# channel 239.0.4.4
 239.0.4.4 bw 2800
config>router>mcac>policy>bundle# mc-constraints
config>router>mcac>policy>bundle>mc-constraints# level 1
 bw 20000
```

```
config>router>mcac>policy>bundle>mc-constraints# level 2
 bw 20000
config>router>mcac>policy>bundle>mc-constraints# level 3
 bw 20000
config>router>mcac>policy>bundle>mc-constraints# level 4
 bw 20000
config>router>mcac>policy>bundle>mc-constraints# level 5
 bw 20000
config>router>mcac>policy>bundle>mc-constraints# level 6
 bw 20000
config>router>mcac>policy>bundle>mc-constraints# lag-
 port-down 1 number-down 1 level 1
config>router>mcac>policy>bundle>mc-constraints# lag-
 port-down 1 number-down 2 level 3
config>router>mcac>policy>bundle>mc-constraints# lag-
 port-down 1 number-down 3 level 5
config>router>mcac>policy>bundle>mc-constraints# lag-
 port-down 2 number-down 1 level 1
config>router>mcac>policy>bundle>mc-constraints# lag-
 port-down 2 number-down 2 level 3
config>router>mcac>policy>bundle>mc-constraints# lag-
 port-down 2 number-down 3 level 5
config>router>mcac>policy>bundle>mc-constraints# exit
config>router>mcac>policy>bundle# no shutdown
config>router>mcac>policy>bundle# exit
config>router>mcac>policy# exit
config>router>mcac# policy "btv_vl"
config>router>mcac>policy# description "eastern TV
 offering"
config>router>mcac>policy# bundle "VRT" create
config>router>mcac>policy>bundle# bandwidth 120000
config>router>mcac>policy>bundle# channel 239.1.2.0
 239.1.2.4 bw 4000 class high type mandatory
config>router>mcac>policy>bundle# channel 239.1.2.5
 239.1.2.5 bw 20000 type mandatory
config>router>mcac>policy>bundle# channel 239.1.2.10
 239.1.2.10 bw 8000 type mandatory
config>router>mcac>policy>bundle# channel 239.2.2.0
 239.2.2.4 bw 4000
config>router>mcac>policy>bundle# channel 239.2.2.5
 239.2.2.5 bw 10000 class high
config>router>mcac>policy>bundle# channel 239.2.2.6
 239.2.2.6 bw 10000 class high
config>router>mcac>policy>bundle# channel 239.2.2.7
 239.2.2.7 bw 10000
config>router>mcac>policy>bundle# channel 239.2.2.8
 239.2.2.8 bw 10000
config>router>mcac>policy>bundle# mc-constraints
```

```
config>router>mcac>policy>bundle>mc-constraints# level 1
 bw 60000
config>router>mcac>policy>bundle>mc-constraints# level 2
 bw 50000
config>router>mcac>policy>bundle>mc-constraints# level 3
 bw 40000
config>router>mcac>policy>bundle>mc-constraints# level 4
 bw 30000
config>router>mcac>policy>bundle>mc-constraints# level 5
 bw 20000
config>router>mcac>policy>bundle>mc-constraints# level 6
 bw 10000
config>router>mcac>policy>bundle>mc-constraints# lag-
 port-down 1 number-down 1 level 1
config>router>mcac>policy>bundle>mc-constraints# lag-
 port-down 1 number-down 2 level 3
config>router>mcac>policy>bundle>mc-constraints# lag-
 port-down 1 number-down 3 level 5
config>router>mcac>policy>bundle>mc-constraints# lag-
 port-down 2 number-down 1 level 1
config>router>mcac>policy>bundle>mc-constraints# lag-
 port-down 2 number-down 2 level 3
config>router>mcac>policy>bundle>mc-constraints# lag-
 port-down 2 number-down 3 level 5
config>router>mcac>policy>bundle>mc-constraints# exit
config>router>mcac>policy>bundle# no shutdown
config>router>mcac>policy>bundle# exit
config>router>mcac>policy# exit
```

The following example displays the configuration:

```
*A:ALA-48>config>router>mcac# info
----------------------------------------------
        policy "btv_fr"
            description "foreign TV offering"
            bundle "FOR" create
                bandwidth 30000
                channel 239.0.3.1 239.0.3.1 bw 4000
                channel 239.0.3.2 239.0.3.2 bw 4000
                channel 239.0.4.1 239.0.4.1 bw 3500 class high type mandatory
                channel 239.0.4.2 239.0.4.2 bw 3500 class high
                channel 239.0.4.3 239.0.4.3 bw 2800  type mandatory
                channel 239.0.4.4 239.0.4.4 bw 2800
                mc-constraints
                    level 1 bw 20000
                    level 2 bw 20000
                    level 3 bw 20000
                    level 4 bw 20000
                    level 5 bw 20000
                    level 6 bw 20000
                    lag-port-down 1 number-down 1 level 1
                    lag-port-down 1 number-down 2 level 3
                    lag-port-down 1 number-down 3 level 5
```

```
                lag-port-down 2 number-down 1 level 1
                lag-port-down 2 number-down 2 level 3
                lag-port-down 2 number-down 3 level 5
            exit
            no shutdown
        exit
    exit
    policy "btv_vl"
        description "eastern TV offering"
        bundle "VRT" create
            bandwidth 120000
            channel 239.1.2.0 239.1.2.4 bw 4000 class high type mandatory
            channel 239.1.2.5 239.1.2.5 bw 20000  type mandatory
            channel 239.1.2.10 239.1.2.10 bw 8000  type mandatory
            channel 239.2.2.0 239.2.2.4 bw 4000
            channel 239.2.2.5 239.2.2.5 bw 10000 class high
            channel 239.2.2.6 239.2.2.6 bw 10000 class high
            channel 239.2.2.7 239.2.2.7 bw 10000
            channel 239.2.2.8 239.2.2.8 bw 10000
            mc-constraints
                level 1 bw 60000
                level 2 bw 50000
                level 3 bw 40000
                level 4 bw 30000
                level 5 bw 20000
                level 6 bw 10000
                lag-port-down 1 number-down 1 level 1
                lag-port-down 1 number-down 2 level 3
                lag-port-down 1 number-down 3 level 5
                lag-port-down 2 number-down 1 level 1
                lag-port-down 2 number-down 2 level 3
                lag-port-down 2 number-down 3 level 5
            exit
            no shutdown
        exit
    exit
----------------------------------------------
*A:ALA-48>config>router>mcac#
```

9.3 MCAC Configuration Command Reference

9.3.1 Command Hierarchies

- MCAC Configuration Commands
- MCAC Policy Commands

9.3.1.1 MCAC Configuration Commands

config
— **router**
— [**no**] **igmp**
— [**no**] **group-interface** *ip-int-name*
— **mcac**
— **if-policy** *mcac-if-policy-name*
— **no if-policy**
— **mc-constraints**
— [**no**] **shutdown**
— **policy** *policy-name*
— **no policy**
— **unconstrained-bw** *bandwidth* **mandatory-bw** *mandatory-bw*
— **no unconstrained-bw**
— [**no**] **interface** *ip-int-name*
— **mcac**
— **if-policy** *mcac-if-policy-name*
— **no if-policy**
— **mc-constraints**
— **level** *level-id* **bw** *bandwidth*
— **no level** *level-id*
— **number-down** *number-lag-port-down* **level** *level-id*
— **no number-down** *number-lag-port-down*
— [**no**] **shutdown**
— [**no**] **use-lag-port-weight**
— **policy** *mcac-policy-name*
— **no policy**
— **unconstrained-bw** *bandwidth* **mandatory-bw** *mandatory-bw*
— **no unconstrained-bw**

config
— [**no**] **router**
— [**no**] **mld**
— [**no**] **group-interface** *ip-int-name*
— **mcac**
— **if-policy** *mcac-if-policy-name*
— **no if-policy**
— **mc-constraints**

```
                        — [no] shutdown
                        — [no] use-lag-port-weight
                    — policy policy-name
                    — no policy
                    — unconstrained-bw bandwidth mandatory-bw mandatory-bw
                    — no unconstrained-bw
            — interface ip-int-name
                — mcac
                    — if-policy mcac-if-policy-name
                    — no if-policy
                    — mc-constraints
                        — level level-id bw bandwidth
                        — no level level-id
                        — number-down number-lag-port-down level level-id
                        — no number-down number-lag-port-down
                        — [no] shutdown
                        — [no] use-lag-port-weight
                    — policy policy-name
                    — no policy
                    — unconstrained-bw bandwidth mandatory-bw mandatory-bw
                    — no unconstrained-bw
```

```
config
    — router
        — [no] pim
            — [no] interface ip-int-name
                — mcac
                    — if-policy mcac-if-policy-name
                    — no if-policy
                    — mc-constraints
                        — level level bw bandwidth
                        — no level level
                        — number-down number-lag-port-down level level-id
                        — no number-down number-lag-port-down
                        — [no] shutdown
                        — [no] use-lag-port-weight
                    — policy policy-name
                    — no policy
                    — unconstrained-bw bandwidth mandatory-bw mandatory-bw
                    — no unconstrained-bw
```

9.3.1.2 MCAC Policy Commands

```
config
    — [no] router
        — mcac
            — [no] if-policy if-policy-name
                — description description-string
                — no description
                — [no] shutdown
                — unconstrained-bw bandwidth mandatory-bw mandatory-bw
```

— no **unconstrained-bw**
— [**no**] **policy** *policy-name*
— [**no**] **bundle** *bundle-name*
— **bandwidth** *bandwidth*
— no **bandwidth**
— **channel** *start-address end-address* **bw** *bandwidth* [**class** *class*] [**type** *type*] [**source** *prefix/prefix-length*]
— no **channel** *start-address end-address* [**source** *prefix/prefix-length*]
— **description** *description-string*
— no **description**
— **mc-constraints**
— **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*
— **level** *level* **bw** *bandwidth*
— no **level** *level*
— [**no**] **use-lag-port-weight**
— [**no**] **shutdown**
— **default-action** {**accept** | **discard**}
— **description** *description-string*
— no **description**

9.3.2 Command Descriptions

9.3.2.1 MCAC Configuration Commands

shutdown

Syntax [no] **shutdown**

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

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 and 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

mcac

Syntax **mcac**

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

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

Default none

if-policy

Syntax **ip-policy** *if-policy-name*
no if-policy

Context config>router>igmp>grp-if>mcac
config>router>igmp>if>mcac
config>router>mld>grp-if>mcac
config>router>mld>if>mcac
config>router>pim>if>mcac

Description This command assigns an existing MCAC interface policy to the interface.

The **no** form removes the MCAC interface policy association.

Default no if-policy

Parameters *if-policy-name* — Specifies an existing MCAC interface policy

mc-constraints

Syntax **mc-constraints**

Context config>router>mcac>policy>bundle
config>router>igmp>grp-if>mcac
config>router>igmp>interface>mcac
config>router>mld>grp-if>mcac
config>router>mld>interface>mcac

config>router>pim>interface>mcac

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 config>router>igmp>grp-if>mcac
config>router>igmp>interface>mcac
config>router>mcac
config>router>mld>group-interface
config>router>mld>interface
config>router>pim>interface

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

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

If 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.**

unconstrained-bw

Syntax **unconstrained-bw** *bandwidth* **mandatory-bw** *mandatory-bw*

no unconstrained-bw

Context
config>router>igmp>grp-if>mcac
config>router>igmp>interface>mcac
config>router>mcac>if-policy
config>router>mld>grp-if>mcac
config>router>mld>interface>mcac
config>router>pim>interface>mcac

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 kb/s for the MCAC policy.

Values 0 to 2147483647

mandatory-bw *mandatory-bw* — Specifies the mandatory bandwidth in kb/s for the MCAC policy.

Values 0 to 2147483647

if-policy

Syntax
[**no**] **if-policy** *if-policy-name*

Context
config>router>mcac

Description
This command creates an MCAC interface policy and enables the context to configure parameters for the policy.

The **no** form deletes the MCAC interface policy.

Default
No policy is created by default.

Parameters *if-policy-name* — Specifies the name of the MCAC interface policy.

Values Any string, up to 32 characters long.

level

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

Context config>router>igmp>interface>mcac>mc-constraints
config>router>mcac>policy>bundle>mc-constraints
config>router>mld>interface>mcac>mc-constraints
config>router>pim>interface>mcac>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 kb/s 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 to 8

bw *bandwidth* — Specifies the bandwidth, in kb/s, for the level.

Values 1 to 2147483647 kb/s

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

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

Default none

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

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

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

Values 1 to 8

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

The port number is used when determining available BW per level when LAG ports go down/ come up.

bundle

Syntax [**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, and so on), 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** *class*] [**type** *type*] [**source** *prefix/prefix-length*]
no channel *start-address end-address* [**source** *prefix/prefix-length*]

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. There is always sufficient BW available on the bundle level because 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* — Specifies the beginning multicast IP address 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

end-address — Specifies the ending multicast IP address 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

prefix/prefix-length — 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 to 32] for IPv4 [0 to 128] for IPv6

bandwidth — Specifies the bandwidth required by this channel in kb/s. 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 to 10000000 kb/s

class — Provides deeper classification of channels used in the algorithm when LAG ports change state.

Values high, low

Default low

type — 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.

Values mandatory | optional

Default optional

description

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

Context config>router>mcac>if-policy
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, and so on), the entire string must be enclosed within double quotes.

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* — Specifies the 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-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 to 64 (for 64-link LAG)
1 to 32 (for other LAGs)

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

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 default-action discard

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.

9.4 Show, Clear, and Debug Command Reference

9.4.1 Command Hierarchies

- Show Commands
- Clear Commands

9.4.1.1 Show Commands

show
- **— router**
  - **— mld**
    - **— group** [*grp-ipv6-address*] [**hosts** | **interfaces** | **saps**]
    - **— group summary** [**hosts** | **interfaces** | **saps**]
    - **— group-interface** [**fwd-service** *service-id*] [*ip-int-name*] [**detail**] [**group**] [*grp-ipv6-address*]
    - **— hosts** [**detail**] [**fwd-service** *service-id*] [**grp-interface** *ip-int-name*]
    - **— hosts** [**host** *ipv6-address*] [**group** *grp-ipv6-address*] [**detail**]
    - **— hosts summary**
    - **— interface** [*ip-int-name* | *ip-address*] [**group**] [*grp-ipv6-address*] [**detail**]
    - **— ssm-translate** *interface-name*
    - **— static** [*ip-int-name* | *ipv6-address*]
    - **— statistics** [*ip-int-name* | *ipv6-address*]
    - **— statistics group-interface** [**fwd-service** *service-id*] [*ip-int-name*]
    - **— statistics host** [*ipv6-address*]
    - **— status**

9.4.1.2 Clear Commands

clear
- **— router**
  - **— mld**
    - **— database** [**group** *grp-ipv6-address* [**source** *src-ip-address*]]
    - **— database interface** {*ip-int-name* | *ipv6-address*} [**group** *grp-ipv6-address* [**source** *src-ipv6-address*]]
    - **— database host** *ipv6-address* [**group** *grp-ipv6-address* [**source** *src-ipv6-address*]]
    - **— database host all** [**group** *grp-ipv6-address* [**source** *src-ipv6-address*]]
    - **— database group-interface** *interface-name* [**fwd-service** *service-id*] [**group** *grp-ipv6-address* [**source** *src-ipv6-address*]]
    - **— database group-interface all**
    - **— statistics group-interface** [**fwd-service** *service-id*] *ip-int-name*
    - **— statistics group-interface all**

— **statistics host** *ipv6-address*
— **statistics host all**
— **statistics** [**interface** *ip-int-name* | *ipv6-address*]
— **version group-interface** [**fwd-service** *service-id*] *ip-int-name*
— **version group-interface all**
— **version host** *ipv6-address*
— **version host all**
— **version** [**interface** *ip-int-name* | *ip-address*]

9.4.2 Command Descriptions

9.4.2.1 Show Commands

The command outputs in the following section are examples only; actual displays may differ depending on supported functionality and user configuration.

mld

Syntax **mld**

Context show>router

Description This command enables the context to show MLD entities.

group

Syntax **group** [*grp-ipv6-address*] [**hosts** | **interfaces** | **saps**]
group summary [**hosts** | **interfaces** | **saps**]

Context show>router>mld

Description This command displays the multicast group and (S,G) addresses. If no *grp-ipv6-address* parameters are specified, then all MLD group, (*,G) and (S,G) addresses are displayed.

Parameters *grp-ipv6-address* — Displays specific multicast group addresses.

hosts — Displays hosts for the multicast group address.

interfaces — Displays interfaces for the multicast group address.

saps — Displays SAPs for the multicast group address.

Output MLD Group Output

The following table describes the output fields for MLD group information.

Table 35 MLD Group Information Output Fields

Label	Description
MLD Groups	Displays the IP multicast sources corresponding to the IPv6 multicast groups.
Fwd List	Displays the list of interfaces in the forward list.
Blk List	Displays the list of interfaces in the blocked list.

Sample Output

```
*A:Dut-A# show router mld group
===============================================================================
MLD Interface Groups
===============================================================================
(*,ff04:db8:224:100:0:0)                                     UpTime: 0d
00:10:09
     Fwd List  : intf_to_ixia
(*,ff04:db8:224:100:0:1)                                     UpTime: 0d
00:10:09
     Fwd List  : intf_to_ixia
(*,ff04:db8:224:100:0:2)                                     UpTime: 0d
00:10:09
     Fwd List  : intf_to_ixia
(*,ff04:db8:224:100:0:3)                                     UpTime: 0d
00:10:09
     Fwd List  : intf_to_ixia
(*,ff04:db8:224:100:0:4)                                     UpTime: 0d
00:10:09
     Fwd List  : intf_to_ixia
-------------------------------------------------------------------------------
Entries : 5
===============================================================================
MLD Host Groups
===============================================================================
No Matching Entries
===============================================================================
MLD SAP Groups
===============================================================================
No Matching Entries
===============================================================================
*A:Dut-A#

*A:Dut-A# show router mld group summary
===============================================================================
MLD Interface Groups Summary                              Nbr Fwd    Nbr Blk
===============================================================================
(*,ff04:db8:224:100:0:0) 1          0
(*,ff04:db8:224:100:0:1) 1          0
(*,ff04:db8:224:100:0:2) 1          0
(*,ff04:db8:224:100:0:3) 1          0
(*,ff04:db8:224:100:0:4) 1          0
-------------------------------------------------------------------------------
Entries : 5
```

```
===============================================================================
MLD Host Groups Summary                                    Nbr Fwd    Nbr Blk
===============================================================================
No Matching Entries
===============================================================================
MLD SAP Groups Summary                                     Nbr Fwd    Nbr Blk
===============================================================================
No Matching Entries
===============================================================================
*A:Dut-A#

*A:Dut-A# show router mld group ff04:db8:224:100:0:0
===============================================================================
MLD Interface Groups
===============================================================================
(*,ff04:db8:224:100:0:0)                                      UpTime: 0d
00:10:24
     Fwd List  : intf_to_ixia
-------------------------------------------------------------------------------
Entries : 1
===============================================================================
MLD Host Groups
===============================================================================
No Matching Entries
===============================================================================
MLD SAP Groups
===============================================================================
No Matching Entries
===============================================================================
*A:Dut-A#
```

group-interface

Syntax **group-interface** [**fwd-service** *service-id*] [*ip-int-name*] [**detail**] [**group**] [*grp-ipv6-address*]

Context show>router>mld

Description This command displays MLD group-interface information.

Parameters *service-id* — Displays information about the specified service ID.

Values 1 to 2148007980, svc-name:64 char max

ip-int-name — Displays information about the specified IP interface name up to 32 characters.

detail — Displays detailed information.

group — Displays information about the group IPv6 address.

grp-ipv6-address — Displays IPv6 address information.

hosts

Syntax **hosts** [**detail**] [**fwd-service** *service-id*] [**grp-interface** *ip-int-name*]
hosts [**host** *ipv6-address*] [**group** *grp-ipv6-address*] [**detail**]
hosts summary

Context show>router>mld

Description This command shows MLD hosts information.

Parameters *grp-ipv6-address* — Specifies the group IPv6 address.

service-id — [1 to 2148007980]| <svc-name: 64 characters maximum>

ip-int-name — IP interface name. A string up to 32 characters.

ipv6-address — IPv6 address.

Output

Sample Output

```
A:Dut-C# show router mld hosts
===============================================================================
MLD Hosts
===============================================================================
Host                                             Subscriber
   Oper-State Oper-Ver Fwd-Svc Num-Groups Group-Interface
-------------------------------------------------------------------------------
192:168:9::1                                     oli_1
   Up         2        1       0                  grp-1-2-1
192:168:9::2                                     oli_1
   Up         2        1       0                  grp-1-2-1
-------------------------------------------------------------------------------
Hosts : 2
===============================================================================
A:Dut-C#

A:Dut-C# show router mld hosts detail
================================================================================
MLD Host 192:168:9::1
================================================================================
Oper Status      : Up         MacAddress     : 00:00:11:00:00:01
Oper Version     : 2          Subscriber     : oli_1
NumGrps          : 0          GrpItf         : grp-1-2-1
MaxGrps Till Now : 0          MLD Policy     : oli1
PPPoE SessionId  : N/A        Next Query Time: 0d 00:00:06
FwdSvcId         : 1          MaxSrcs Allowed: No Limit
MaxGrps Allowed  : No Limit   MaxGrpSrcs All*: No Limit
Qry Interval     : 125        Qry Last Lstnr*: 1
Qry Resp Interval: 10         Router Alert C*: Enabled
Bonding Conn Idx : 0          Bonding Id     : None
================================================================================
MLD Host 192:168:9::2
================================================================================
Oper Status      : Up         MacAddress     : 00:00:11:00:00:02
Oper Version     : 2          Subscriber     : oli_1
```

```
NumGrps          : 0          GrpItf         : grp-1-2-1
MaxGrps Till Now : 0          MLD Policy     : oli1
PPPoE SessionId  : N/A        Next Query Time: 0d 00:00:06
FwdSvcId         : 1          MaxSrcs Allowed: No Limit
MaxGrps Allowed  : No Limit   MaxGrpSrcs All*: No Limit
Qry Interval     : 125        Qry Last Lstnr*: 1
Qry Resp Interval: 10         Router Alert C*: Enabled
Bonding Conn Idx : 0          Bonding Id     : None
-------------------------------------------------------------------------------
Hosts : 2
===============================================================================
* indicates that the corresponding row element may have been truncated.
A:Dut-C#
```

interface

Syntax **interface** [*ip-int-name* **|** *ipv6-address*] [**group**] [*grp-ipv6-address*] [**detail**]

Context show>router>mld

Description This command displays MLD interface information.

Parameters *ip-int-name* — Only displays the information associated with the specified IPv6 interface name.

ipv6-address — Only displays the information associated with the specified IPv6 address.

group *grp-ipv6-address* — Only displays IPv6 multicast group address for which this entry contains information.

detail — Displays detailed IPv6 interface information along with the source group information learned on that interface.

Output MLD Interface Output

The following table provides MLD field descriptions.

Table 36 **MLD Fields**

Label	Description
Interface	Displays the interfaces that participate in the MLD protocol.
Adm Admin Status	Displays the administrative state for the MLD protocol on this interface.
Oper Oper Status	Displays the current operational state of MLD protocol on the interface.
Querier	Displays the address of the MLD querier on the IP subnet to which the interface is attached.

Table 36 MLD Fields (Continued)

Label	Description
Querier Up Time	Displays the time since the querier was last elected as querier.
Querier Expiry Timer	Displays the time remaining before the querier ages out. If the querier is the local interface address, the value will be zero.
Cfg/Opr Version Admin/Oper version	Cfg The configured version of MLD running on this interface. For MLD to function correctly, all routers on a LAN must be configured to run the same version of MLD on that LAN. Opr The operational version of MLD running on this interface.
Num Groups	The number of multicast groups which have been learned by the router on the interface.
Policy	Displays the policy that is to be applied on the interface.
Group Address	Displays the IP multicast group address for which this entry contains information.

Sample Output

```
*A:Dut-A# show router mld interface
===============================================================================
MLD Interfaces
===============================================================================
Interface              Adm  Oper Cfg/Opr         Num Policy
    Querier                        Version         Groups
-------------------------------------------------------------------------------
intf_to_ixia           Up   Up   2/2             5 none
    ff00:db8:4403:1ff:fe01:3
-------------------------------------------------------------------------------
Interfaces : 1
===============================================================================
*A:Dut-A#
```

ssm-translate

Syntax **ssm-translate**
ssm-translate interface *interface-name*

Context show>router>mld

Description This command displays MLD SSM translate configuration information.

Parameters *interface-name* — IP interface name. A string up to 32 characters.

Output MLD Interface Output

The following table provides MLD field descriptions.

Table 37 **MLD Fields**

Label	Description
Start Address End Address	Displays the address ranges of the multicast groups for which this router can be an RP.
Source Address	Displays the unicast address that sends data on an interface.
Interface	Displays the interface name.
SSM Translate Entries	Displays the total number of SSM translate entries.

Sample Output

```
*A:ALA-BA# show router mld static
===============================================================================
MLD SSM Translate Entries
===============================================================================
Start Address      : ff0e:db8:9
End Address        : ff0e:db8:c
   Source Address  : 2001:db8::1

Start Address      : ff04:db8:2
End Address        : ff04:db8:10
   Source Address  : 2001:db8:3:4:5:6:7:8
       Interface   : lax-vls

Start Address      : ff0e:db8:9
End Address        : ff0e:db8:c
   Source Address  : 2001:db8::1
       Interface   : lax-vls
-------------------------------------------------------------------------------
SSM Translate Entries : 3
===============================================================================
*A:ALA-BA#
```

static

Syntax **static** [*ip-int-name* | *ipv6-address*]

Context show>router>mld

Description This command displays static MLD, (*,G) and (S,G) information.

Parameters *ip-int-name* — Only displays the information associated with the specified IP interface name.

ipv6-address — Only displays the information associated with the specified IPv6 address.

Output Static MLD Output

The following table provides static MLD field descriptions.

Table 38 **MLD Static Fields**

Label	Description
Source	Displays entries which represents a source address from which receivers are interested/not interested in receiving multicast traffic.
Group	Displays the IPv6 multicast group address for which this entry contains information.
Interface	Displays the interface name.

Sample Output

```
*A:ALA-BA# show router mld static
================================================================================
Rtr Base MLD Static Group Sources
================================================================================
Source                                      Interface
  Group Start                               [Group Step]
  [Group End]                               [Group Count]
--------------------------------------------------------------------------------
2001:db8:2016:10ff::4                       lax-vls
  ff05:db8:1
*                                           lax-vls
  ff06:db8:1
*                                           lax-vls
  ff01:db8:1                                   ::4:0
  ff01:db8:100:0                               64
3::1                                        lax-vls
  ff05:db8:1                                   ::1
  ff05:db8:20                                  32
*                                           lax-vls
  ff05:db8:2:1                                 ::1
  ff05:db8:2:3ff                               1023
3::1                                        lax-vls
  ff05:db8:3:0                                 ::64
  ff05:db8:4:0                                 656
3::2                                        lax-vls
  ff05:db8:3:0                                 ::64
  ff05:db8:4:0                                 656
4::1                                        flax-vlsoo
  ff05:db8:3:0                                 ::64
  ff05:db8:4:0                                 656
5::1                                        lax-vls
  ff05:db8:3:0                                 ::64
  ff05:db8:4:0                                 656
--------------------------------------------------------------------------------
Static (*,G)/(S,G) Entries : 9
================================================================================
*A:ALA-BA#
```

statistics

Syntax **statistics** [*ip-int-name* | *ipv6-address*]
statistics group-interface [**fwd-service** *service-id*] [*ip-int-name*]
statistics host [*ipv6-address*]

Context show>router>mld

Description This command displays MLD statistics information.

Parameters *ip-int-name* — Only displays the information associated with the specified IP interface name.

ipv6-address — Only displays the information associated with the specified IPv6 address.

Output MLD Statistics Output

The following table provides statistical MLD field descriptions.

Table 39 **MLD Statistics Fields**

Label	Description
MLD Interface Statistics	Lists the MLD statistics for a particular interface.
Message Type	Queries — The number of MLD general queries transmitted or received on this interface. Report — The total number of MLD V1 or V2 reports transmitted or received on this interface. Dones — The total number of MLD dones transmitted on this interface.
Received	Displays the total number of MLD packets received on this interface.
Transmitted	Displays the total number of MLD packets transmitted from this interface.
General Interface Statistics	Lists the general MLD statistics.
Bad Length	Displays the total number of MLD packets with bad length received on this interface.
Bad Checksum	Displays the total number of MLD packets with bad checksum received on this interface.
Unknown Type	Displays the total number of MLD packets with unknown type received on this interface.

Table 39 MLD Statistics Fields (Continued)

Label	Description
Bad Receive If	Displays the total number of MLD packets incorrectly received on this interface.
Rx Non Local	Displays the total number of MLD packets received from a non-local sender.
Rx Wrong Version	Displays the total number of MLD packets with wrong versions received on this interface.
Policy Drops	Displays the total number of MLD packets dropped by import policies on this interface.
No Router Alert	Displays the total number of MLD packets received on this interface which did not have the router alert flag set.
Rx Bad Encodings	Displays the total number of MLD packets with bad encodings received on this interface.
Rx Pkt Drops	Displays the total number of MLD receive packet drops on this interface.
Local Scope Pkts	Displays the total number of MLD packets with local scope received on this interface.
Resvd Scope Pkts	Displays the total number of MLD packets with reserved scope received on this interface.
MCAC Policy Drops	Displays the total number of MLD packets dropped by MCAC policies on this interface.

Sample Output

```
*A:ALA-BA# show router mld statistics
==================================================
MLD Interface Statistics
==================================================
Message Type        Received       Transmitted
--------------------------------------------------
Queries             0              9
Report V1           0              0
Report V2           0              0
Dones               0              0
-------------------------------------------------------------------------------
General Interface Statistics
-------------------------------------------------------------------------------
Bad Length         : 0
Bad Checksum       : 0
Unknown Type       : 0
Bad Receive If     : 0
Rx Non Local       : 0
Rx Wrong Version   : 0
```

```
Policy Drops      : 0
No Router Alert   : 0
Rx Bad Encodings  : 0
Rx Pkt Drops      : 0
Local Scope Pkts  : 0
Resvd Scope Pkts  : 0
MCAC Policy Drops : 0
-------------------------------------------------------------------------------
Source Group Statistics
-------------------------------------------------------------------------------
(S,G)             : 0
(*,G)             : 5
==================================================
*A:Dut-A#
```

status

Syntax **status**

Context show>router>mld

Description This command displays MLD status information.

If MLD is not enabled, the following message appears:

```
A:NYC# show router mld status
MINOR: CLI MLD is not configured.
A:NYC#
```

Output MLD Status Output

The following table provides MLD status field descriptions.

Table 40 **MLD Status Fields**

Label	Description
Admin State	Displays the administrative status of MLD.
Oper State	Displays the current operating state of this MLD protocol instance on this router.
Query Interval	The frequency at which MLD query packets are transmitted.
Last Listener Query Interval	The maximum response time inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages.
Query Response Interval	The maximum query response time advertised in MLDv2 queries.
Robust Count	Displays the number of times the router will retry a query.

Sample Output

```
*A:ALA-BA# show router mld status
===============================================================================
MLD Status
===============================================================================
Admin State                         : Up
Oper State                          : Up
Query Interval                      : 125
Last Listener Query Interval        : 1
Query Response Interval             : 10
Robust Count                        : 2
===============================================================================
*A:ALA-BA#
```

9.4.2.2 Clear Commands

mld

Syntax **mld**

Context clear>router

Description This command enables the context to clear and reset MLD entities.

database

Syntax
database [**group** *ipv6-address* [**source** *ipv6-address*]]
database [**interface** *ip-int-name* **|** *ipv6-address*] [**group** *ipv6-address* [**source** *ipv6-address*]]
database host *ipv6-address* [**group** *ipv6-address* [**source** *ipv6-address*]]
database host all [**group** *ipv6-address* [**source** *ipv6-address*]]
database group-interface *interface-name* [**fwd-service** *service-id*] [**group** *grp-ipv6-address* [**source** *ipv6-address*]]
database group-interface all

Context clear>router>mld

Description This command clears MLD database parameters.

Parameters

host *ipv6-address* — Clears the MLD database on the specified host.

host all — Clears the MLD database on all hosts.

interface *ip-int-name* — Clears database information for the specified MLD interface name.

interface *ipv6-address* — Clears database information for the specified MLD interface IPv6 address.

group *ipv6-address* — Clears database information for the specified MLD group IPv6 address.

source *ipv6-address* — Clears database information for the specified MLD source IPv6 address.

statistics

Syntax
statistics group-interface [**fwd-service** *service-id*] *ip-int-name*
statistics group-interface all
statistics host *ipv6-address*
statistics host all
statistics [*ip-int-name* **|** *ipv6-address*]

Context clear>router>mld

Description This command clears MLD statistics parameters.

Parameters
fwd-service *service-id* — [1to 2148007980] | <svc-name:64 char max>

group-interface *interface-name* — Clears the MLD statistics on the specified group interface.

group-interface all — Clears the MLD statistics on all group interfaces.

host all — Clears the MLD statistics on all hosts.

host *ipv6-address* — Clears the MLD statistics on the specified host.

ip-int-name — Clears statistics for the specified MLD interface name.

ipv6-address — Clears statistics for the specified MLD IPv6 address.

version

Syntax
version group-interface [**fwd-service** *service-id*] *ip-int-name*
version group-interface all
version host *ipv6-address*
version host all
version [*ip-int-name* **|** *ipv6-address*]

Context clear>router>mld

Description This command clears MLD version parameters.

Parameters
group-interface *interface-name* — Clears the MLD version on the specified group interface.

group-interface all — Clears the MLD version on all group interfaces.

fwd-service *service-id* — [1to 2148007980] | <svc-name:64 char max>

host *ipv6-address* — Clears the MLD version on the specified host.

host all — Clears the MLD version on all hosts.

ip-int-name — Clears version information for the specified MLD interface name.

ipv6-address — Clears version information for the specified MLD IPv6 address.

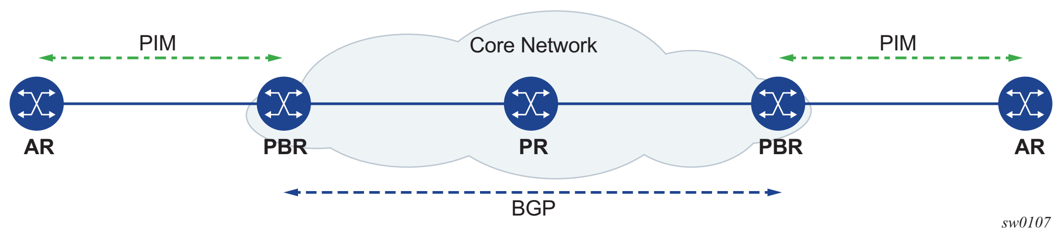
10 GTM

10.1 GTM Overview

GTM with BGP Multicast VPN (BGP-MVPN), as specified in RFC 7716, allows a Service Provider (SP) to use the same multicast architecture that was originally developed for VPNs to distribute multicast routing information that is not specific to VPNs. Instead of storing the routing information in VRFs, multicast routing information is maintained in a global table for the router.

The architecture can be logically divided into a core network and non-core (attachment) networks. The multicast routing protocol used in the core network may not be the same as the protocol used in the attachment networks. As there is a protocol boundary between the core and attachment networks, the term Protocol Boundary Router (PBR) refers to the core routers that are at the boundary. A PBR is not necessarily an edge router in the PE sense; however, a PBR in the SP network marks the border of any tunnels that are used to transport multicast traffic across the core network. Routers that are attached to the PBRs but that are not part of the core network are referred to as Attachment Routers (ARs).

Figure 10 **GTM Network Topology Example**



Multicast data traffic from an AR is tunneled through the core network from an ingress PBR to one or more egress PBRs, using multicast routing information stored in the PBR’s global table. The global table learns the PBR’s multicast routing information from the ARs attached to the PBR, and distributes the information among the PBRs using BGP. PBRs use the same BGP-MVPN procedures used by PE routers to route multicast VPN traffic, with some adaptations to the procedures to use the global table instead of a VRF.

By using the BGP procedures designed for MVPN to support GTM, a single control plane is available to govern the use of both VPN and non-VPN multicast. The features and characteristics of MVPN carry over automatically to GTM, including, but not limited to:

- scaling
- aggregation
- transport over RSVP tunnels in the SP network
- support for non-segmented intra-autonomous systems (ASs) tunnels
- support for PIM-SSM outside of the core
- support for both IPv4 and IPv6 multicast flows over an IPv4 SP infrastructure
- support for unsolicited flooded data (including support for BSR as an RP-to-group mapping protocol

10.1.1 Using BGP-MVPN Procedures in GTM

10.1.1.1 Route Distinguishers and Route Targets

The BGP routes used in the MVPN procedures have a Subsequent Address Family Identifier (SAFI) value of 5, or MCAST-VPN. The Network Layer Reachability Information (NLRI) format for MCAST-VPN routes consists of a Route Type (RT) field and depending on the RT, a Route Distinguisher (RD) Extended Community (EC) field.

Note: The ECs are automatically configured for GTM and are not visible in the configuration.

To distinguish MCAST-VPN routes originated for VPNs from MCAST-VPN routes in support of GTM, the RD field, if defined within that route's NLRI, must be set to zero (that is, 64 bits of zero). An RD of all zeros associates that route with GTM, as no VRF can have an RD of zero.

MVPN procedures use two types of RTs, one of which is carried only in the routes of C-multicast shared tree joins, C-multicast source tree joins, and leaf auto-discovery routes (A-D routes). This RT type identifies the PE router that has been selected by the route's originator as the Upstream PE or as the Upstream Multicast Hop (UMH) for a particular multicast flow or set of multicast flows. This RT must be an IPv4- or IPv6-address-specific EC, where the Global Administrator field identifies the Upstream PE or the UMH. If the Global Administrator field identifies the Upstream PE, the Local Administrator field identifies a particular VRF in that PE.

To support GTM, this type of RT is used in the same situations as in the MVPN specifications, with the modification that the Local Administrator field of this RT type must always be set to zero. This implicitly identifies the global table rather than identifying a VRF. This type of RT is referred to as an upstream-node-identifying RT.

10.1.1.2 UMH-Eligible Routes

For MVPN, routes of SAFI 128 or 129 are UMH-eligible routes. For GTM, routes of SAFI 1, SAFI 4, or SAFI 2 are UMH-eligible routes. Imported routes of SAFI 2 in the global table are UMH-eligible routes; otherwise, routes of SAFI 1 or SAFI 4 are considered UMH-eligible routes. For UMH determination, SAFI 1 and SAFI 4 routes containing the same IP prefix in their respective NLRI fields are considered by the BGP best-path selection process to be comparable.

UMH-eligible routes that have a SAFI of 1, 2, or 4 carry both the VRF Route Import EC and the Source AS EC. These ECs are automatically configured for GTM.

10.1.1.3 BGP Route Types Supported

Table 41 **BGP Route Types**

BGP Route Type	Name	Description	Supported for GTM
1	Intra-AS I-PMSI AD route	Originated by all PBR routers. Used for advertising and learning intra-AS MVPN membership information.	Yes, always originated by SR OS
2	Inter-AS I-PMSI A-D route	Originated by ASBR routers. Used for advertising and learning inter-AS MVPN membership information.	No (no Inter-AS support)
3	S-PMSI A-D route	Originated by sender PBRs. Used for initiating a selective P-tunnel for a particular (C-S, C-G).	Yes
4	Leaf A-D route	Originated by receiver PBRs in response to receiving a Type 3 route. Used by sender PBR to discover the leaves of a selective P-tunnel.	Yes

Table 41 **BGP Route Types (Continued)**

BGP Route Type	Name	Description	Supported for GTM
5	Source Active A-D route	Originated by the PBR that discovers an active VPN multicast source. Used by PBRs to learn the identity of active VPN multicast sources.	Yes
6	Shared Tree Join route	Originated by receiver PBRs. Originated when a PE receives a shared tree C-join (C-*, C-G) through its PE-CE interface.	Yes
7	Source Tree Join route	Originated by receiver PBRs. Originated when a PBR receives a source tree C-join (C-S, C-G) or originated by the PBR that already has a Type 6 route and receives a Type 5 route.	Yes, for non-segmented trees.

10.2 Configuring GTM

10.2.1 Configuration Recommendations

When configuring GTM, the following recommendations should be considered.

- In a dual-homing configuration, ECMP to the upstream multicast hop (UMH) routers must be configured for the BGP routes to be used. If the UMH routers are unreachable via ECMP, it may cause duplicate traffic in the core. This behavior is consistent with RFC 7716, section 2.3.4., which states that the single forwarder selection (SFS) procedure cannot be applied to GTM.
- For IPv6 GTM, the IPv4 address must be configured as the IPv6 system address, as in the following example.

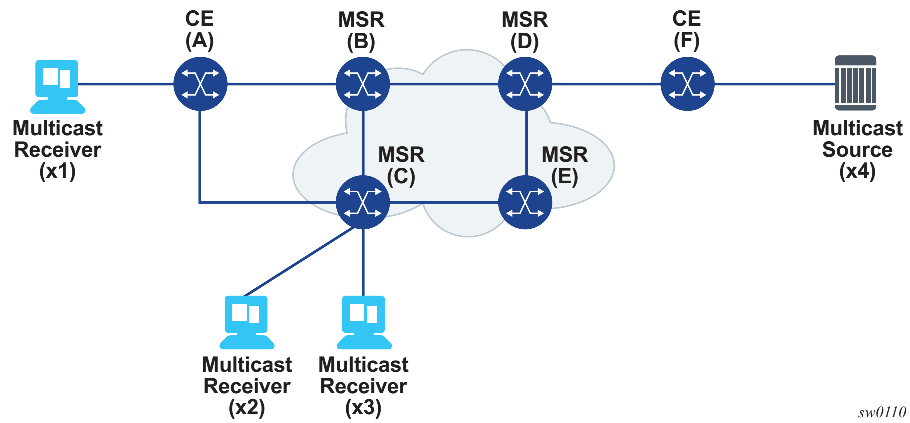
```
*A:Dut-F>config>router#
        interface "system"
            address 10.20.1.4/32
            ipv6
                address ff0e::db8:104/128
            exit
            no shutdown
        exit
```

Note: GTM auto-discovery (**config**>**router**>**pim**>**gtm**>**auto-discovery**) cannot be configured when MoFRR (**multicast-fast-failover** or **multicast6-fast-failover**) is enabled.

10.2.2 Configuring GTM with CLI

Consider the following example configuration:

Figure 11 **Example Configuration**



where

- routers A and F are CE routers
- routers B, C, D, and E are MSR routers in the core network
- the multicast source is at x4
- the multicast receivers are at x1, x2, and x3

Perform the following steps to configure GTM:

Step 1. Configure PIM parameters for GTM.

The following output displays the PIM configuration.

```
*B:Dut-D>config>router>pim# info
----------------------------------------------
             interface "intf_to_B"
                 shutdown
             exit
             interface "intf_to_E"
                 shutdown
             exit
             apply-to all
             rp
                 static
                     address 10.100.1.1
                         group-prefix 224.0.0.0/4
                     exit
                 exit
                 bsr-candidate
                     shutdown
                 exit
                 rp-candidate
                     shutdown
                 exit
             exit
             gtm
```

```
                auto-discovery default
            exit
            no mc-ecmp-balance
            no shutdown
----------------------------------------------
*B:Dut-D>config>router>pim#
```

Step 2. Configure the GTM parameters.

The following output displays the GTM configuration.

```
*B:Dut-D>config>router>gtm# info
----------------------------------------------
            mvpn
            provider-tunnel
                inclusive
                    rsvp
                        lsp-template "IpmsiTmpl"
                        no shutdown
                    exit
                exit
                selective
                    rsvp
                        lsp-template "SpmsiTmpl"
                        no shutdown
                    exit
                    maximum-p2mp-spmsi 4000
                    data-threshold 224.0.0.0/4 1
                exit
            exit
----------------------------------------------
*B:Dut-D>config>router>gtm#
```

Step 3. Configure a route policy for BGP.

The following output displays the route policy configuration.

```
*B:Dut-D>config>router>policy-options# info
----------------------------------------------
            prefix-list "sourceList"
                prefix 10.10.0.0/16 longer
                prefix 10.100.0.0/16 longer
                prefix 10.114.0.0/16 longer
                prefix 2001:db8:10:10:0:0/96 longer
                prefix 2001:db8:100:0:0/96 longer
                prefix 2001:db8:114:0:0/96 longer
            exit
            policy-statement "acceptAll"
                default-action accept
                exit
            exit
            policy-statement "acceptAllBgp"
                entry 10
                    from
                        protocol rip
                    exit
                    action accept
                    exit
                exit
```

```
                    entry 11
                        from
                            protocol ripng
                        exit
                        action accept
                        exit
                    exit
                    default-action drop
                    exit
                exit
                policy-statement "acceptAllPref8"
                    default-action accept
                        preference 8
                    exit
                exit
----------------------------------------------
*B:Dut-D>config>router>policy-options#
```

Step 4. Configure BGP parameters for GTM.

The following output displays the BGP configuration on router D.

```
*B:Dut-D#configure router bgp
*B:Dut-D>config>router>bgp# info
----------------------------------------------
                connect-retry 1
                multipath 16
                export "acceptAllBgp"
                router-id 10.20.1.4
                rapid-withdrawal
                rapid-update mvpn-ipv4 mdt-safi mvpn-ipv6
                mvpn-vrf-import-subtype-new
                best-path-selection
                    ignore-nh-metric
                exit
                group "none"
                    family ipv4 ipv6 mvpn-ipv4 mvpn-ipv6 label-ipv4 label-ipv6
                    next-hop-self
                    local-address 10.20.1.4
                    neighbor 10.20.1.2
                        peer-as 200
                    exit
                    neighbor 10.20.1.3
                        med-out 100
                        peer-as 200
                    exit
                    neighbor 10.20.1.5
                        med-out 100
                        peer-as 200
                    exit
                exit
                no shutdown
----------------------------------------------
```

The following output displays the MVPN context on router D.

```
*B:Dut-D# show router mvpn
===============================================================================
```

```
MVPN Base configuration data
===============================================================================
signaling          : Bgp                  auto-discovery     : Default
UMH Selection      : Highest-Ip           SA withdrawn       : Disabled
intersite-shared   : Enabled              Persist SA         : Disabled
vrf-import         : N/A
vrf-export         : N/A
vrf-target         : unicast
C-Mcast Import RT  : target:10.20.1.4:0
ipmsi              : rsvp IpmsiTmpl
i-pmsi P2MP AdmSt  : Up
i-pmsi Tunnel Name : IpmsiTmpl-gtm-73881
enable-bfd-root    : false                enable-bfd-leaf    : false
Mdt-type           : sender-receiver
BSR signalling     : none
Wildcard s-pmsi    : Disabled
Multistream-SPMSI  : Disabled
spmsi              : rsvp SpmsiTmpl
s-pmsi P2MP AdmSt  : Up
max-p2mp-spmsi     : 4000
data-delay-interval: 3 seconds
enable-asm-mdt     : N/A
data-threshold     : 224.0.0.0/4 --> 1 kbps
===============================================================================
```

The following output displays the PIM source group database information on router D.

```
*B:Dut-D#show router pim group
===============================================================================
Legend:  A = Active   S = Standby
===============================================================================
PIM Groups ipv4
===============================================================================
Group Address               Type               Spt Bit  Inc Intf
No.Oifs
    Source Address              RP                  State    Inc Intf(S)
-------------------------------------------------------------------------------
239.100.0.0                 (S,G)              spt vprn_itf_D_2b* 1
    10.114.1.2                 10.100.1.1
239.100.0.1                 (S,G)              spt vprn_itf_D_2b* 1
    10.114.1.2                 10.100.1.1
239.100.0.2                 (S,G)              spt vprn_itf_D_2b* 1
    10.114.1.2                 10.100.1.1
239.100.0.3                 (S,G)              spt vprn_itf_D_2b* 1
    10.114.1.2                 10.100.1.1
-------------------------------------------------------------------------------
Groups : 4
===============================================================================
* indicates that the corresponding row element may have been truncated.
*B:Dut-D#show router pim group detail
===============================================================================
PIM Source Group ipv4
===============================================================================
Group Address      : 239.100.0.0
Source Address     : 10.114.1.2
RP Address         : 10.100.1.1
Advt Router        :
```

```
Flags              : spt                Type               : (S,G)
Mode               : sparse
MRIB Next Hop      : 10.100.1.1
MRIB Src Flags     : remote
Keepalive Timer Exp: 0d 00:02:53
Up Time            : 0d 00:09:50        Resolved By        : rtable-u
Up JP State        : Joined             Up JP Expiry       : 0d 00:00:23
Up JP Rpt          : Not Joined StarG   Up JP Rpt Override : 0d 00:00:00
Register State     : No Info
Reg From Anycast RP: No
Rpf Neighbor       : 10.100.1.1
Incoming Intf      : vprn_itf_D_2base
Outgoing Intf List : mpls-if-73881 (mpls-if-73885)
Curr Fwding Rate   : 1.3 kbps
Forwarded Packets  : 132                Discarded Packets  : 0
Forwarded Octets   : 6072               RPF Mismatches     : 0
Spt threshold      : 0 kbps             ECMP opt threshold : 7
Admin bandwidth    : 1 kbps
===============================================================================
PIM Source Group ipv4
===============================================================================
Group Address      : 239.100.0.1
Source Address     : 10.114.1.2
RP Address         : 10.100.1.1
Advt Router        :
Flags              : spt                Type               : (S,G)
Mode               : sparse
MRIB Next Hop      : 10.100.1.1
MRIB Src Flags     : remote
Keepalive Timer Exp: 0d 00:02:53
Up Time            : 0d 00:09:50        Resolved By        : rtable-u
Up JP State        : Joined             Up JP Expiry       : 0d 00:00:23
Up JP Rpt          : Not Joined StarG   Up JP Rpt Override : 0d 00:00:00
Register State     : No Info
Reg From Anycast RP: No
Rpf Neighbor       : 10.100.1.1
Incoming Intf      : vprn_itf_D_2base
Outgoing Intf List : mpls-if-73881 (mpls-if-73886)
Curr Fwding Rate   : 1.3 kbps
Forwarded Packets  : 141                Discarded Packets  : 0
Forwarded Octets   : 6486               RPF Mismatches     : 0
Spt threshold      : 0 kbps             ECMP opt threshold : 7
Admin bandwidth    : 1 kbps
===============================================================================
PIM Source Group ipv4
===============================================================================
Group Address      : 239.100.0.2
Source Address     : 10.114.1.2
RP Address         : 10.100.1.1
Advt Router        :
Flags              : spt                Type               : (S,G)
Mode               : sparse
MRIB Next Hop      : 10.100.1.1
MRIB Src Flags     : remote
Keepalive Timer Exp: 0d 00:02:52
Up Time            : 0d 00:09:51        Resolved By        : rtable-u
Up JP State        : Joined             Up JP Expiry       : 0d 00:00:22
Up JP Rpt          : Not Joined StarG   Up JP Rpt Override : 0d 00:00:00
Register State     : No Info
```

```
Reg From Anycast RP: No
Rpf Neighbor       : 10.100.1.1
Incoming Intf      : vprn_itf_D_2base
Outgoing Intf List : mpls-if-73881 (mpls-if-73887)
Curr Fwding Rate   : 1.3 kbps
Forwarded Packets  : 140                Discarded Packets  : 0
Forwarded Octets   : 6440               RPF Mismatches     : 0
Spt threshold      : 0 kbps             ECMP opt threshold : 7
Admin bandwidth    : 1 kbps
===============================================================================
PIM Source Group ipv4
===============================================================================
Group Address      : 239.100.0.3
Source Address     : 10.114.1.2
RP Address         : 10.100.1.1
Advt Router        :
Flags              : spt                Type               : (S,G)
Mode               : sparse
MRIB Next Hop      : 10.100.1.1
MRIB Src Flags     : remote
Keepalive Timer Exp: 0d 00:02:52
Up Time            : 0d 00:09:51        Resolved By        : rtable-u
Up JP State        : Joined             Up JP Expiry       : 0d 00:00:22
Up JP Rpt          : Not Joined StarG   Up JP Rpt Override : 0d 00:00:00
Register State     : No Info
Reg From Anycast RP: No
Rpf Neighbor       : 10.100.1.1
Incoming Intf      : vprn_itf_D_2base
Outgoing Intf List : mpls-if-73881 (mpls-if-73888)
Curr Fwding Rate   : 1.3 kbps
Forwarded Packets  : 140                Discarded Packets  : 0
Forwarded Octets   : 6440               RPF Mismatches     : 0
Spt threshold      : 0 kbps             ECMP opt threshold : 7
Admin bandwidth    : 1 kbps
-------------------------------------------------------------------------------
Groups : 4
===============================================================================
```

The following output displays the PMSI information on router D.

```
*B:Dut-D# show router pim s-pmsi
===============================================================================
PIM RSVP Spmsi tunnels
===============================================================================
P2mp  Tunnel ID   Ext Tunnel Adrs       SPMSI Index   Num State   Multistre
ID                                                    VPN SGs         am-ID
-------------------------------------------------------------------------------
1     61444       10.20.1.4             73885         1 Up      0
1     61445       10.20.1.4             73886         1 Up      0
1     61446       10.20.1.4             73887         1 Up      0
1     61447       10.20.1.4             73888         1 Up      0
===============================================================================
PIM RSVP Spmsi Interfaces : 4
===============================================================================
*B:Dut-D# show router pim s-pmsi detail
===============================================================================
PIM RSVP Spmsi tunnels
===============================================================================
```

```
P2MP ID            : 1                 Tunnel ID          : 61444
Ext Tunnnel Addrs  : 10.20.1.4         Spmsi IfIndex      : 73885
Number of VPN SGs  : 1                 Up Time            : 0d 00:00:09
VPN Group Address  : 239.100.0.0
VPN Source Address : 10.114.1.2
Up Time            : 0d 00:00:09       Multistream-Id     : N/A
State              : TX Joined         Mdt Threshold      : 1
Join Timer         : N/A               Holddown Timer     : 0d 00:00:50
===============================================================================
PIM RSVP Spmsi tunnels
===============================================================================
P2MP ID            : 1                 Tunnel ID          : 61445
Ext Tunnnel Addrs  : 10.20.1.4         Spmsi IfIndex      : 73886
Number of VPN SGs  : 1                 Up Time            : 0d 00:00:09
VPN Group Address  : 239.100.0.1
VPN Source Address : 100.114.1.2
Up Time            : 0d 00:00:09       Multistream-Id     : N/A
State              : TX Joined         Mdt Threshold      : 1
Join Timer         : N/A               Holddown Timer     : 0d 00:00:50
===============================================================================
PIM RSVP Spmsi tunnels
===============================================================================
P2MP ID            : 1                 Tunnel ID          : 61446
Ext Tunnnel Addrs  : 10.20.1.4         Spmsi IfIndex      : 73887
Number of VPN SGs  : 1                 Up Time            : 0d 00:00:09
VPN Group Address  : 239.100.0.2
VPN Source Address : 10.114.1.2
Up Time            : 0d 00:00:09       Multistream-Id     : N/A
State              : TX Joined         Mdt Threshold      : 1
Join Timer         : N/A               Holddown Timer     : 0d 00:00:50
===============================================================================
PIM RSVP Spmsi tunnels
===============================================================================
P2MP ID            : 1                 Tunnel ID          : 61447
Ext Tunnnel Addrs  : 10.20.1.4         Spmsi IfIndex      : 73888
Number of VPN SGs  : 1                 Up Time            : 0d 00:00:10
VPN Group Address  : 239.100.0.3
VPN Source Address : 10.114.1.2
Up Time            : 0d 00:00:10       Multistream-Id     : N/A
State              : TX Joined         Mdt Threshold      : 1
Join Timer         : N/A               Holddown Timer     : 0d 00:00:49
===============================================================================
PIM RSVP Spmsi Interfaces : 4
===============================================================================


*B:Dut-D#  show router pim tunnel-interface
===============================================================================
PIM Interfaces ipv4
===============================================================================
Interface                        Originator Address   Adm  Opr Transport
Type
-------------------------------------------------------------------------------
mpls-if-73881                    10.20.1.4            Up   Up Tx-IPMSI
mpls-if-73882                    10.20.1.3            Up   Up Rx-IPMSI
mpls-if-73883                    10.20.1.2            Up   Up Rx-IPMSI
mpls-if-73884                    10.20.1.5            Up   Up Rx-IPMSI
mpls-if-73885                    10.20.1.4            Up   Up Tx-SPMSI
mpls-if-73886                    10.20.1.4            Up   Up Tx-SPMSI
mpls-if-73887                    10.20.1.4            Up   Up Tx-SPMSI
```

```
mpls-if-73888                    10.20.1.4             Up   Up Tx-SPMSI
-------------------------------------------------------------------------------
Interfaces : 8
===============================================================================
```

10.3 GTM Configuration Command Reference

10.3.1 Command Hierarchies

- Configuration Commands

10.3.1.1 Configuration Commands

config
- **router**
  - **gtm**
    - [**no**] **mvpn**
    - **provider-tunnel**
      - **inclusive**
        - [**no**] **rsvp**
          - **lsp-template** *lsp-template*
          - **no lsp-template**
          - [**no**] **shutdown**
      - **selective**
        - **data-delay-interval** *value*
        - **no data-delay-interval**
        - **data-threshold** {*c-grp-ip-addr/mask* | *c-grp-ip-addr netmask*} *s-pmsi-threshold* [**pe-threshold-add** *pe-threshold-add*] [**pe-threshold-delete** *pe-threshold-delete*]
        - **data-threshold** *c-grp-ipv6-addr/prefix-length s-pmsi-threshold* [**pe-threshold-add** *pe-threshold-add*] [**pe-threshold-delete** *pe-threshold-delete*]
        - **no data-threshold** {*c-grp-ip-addr/mask* | *c-grp-ip-addr netmask*}
        - **no data-threshold** {*c-grp-ip-addr/prefix-length*}
        - **maximum-p2mp-spmsi** *range*
        - **no maximum-p2mp-spmsi**
        - [**no**] **rsvp**
          - **lsp-template** *lsp-template*
          - **no lsp-template**
          - [**no**] **shutdown**
  - **pim**
    - **gtm**
      - **auto-discovery** [**default**]
      - **no auto-discovery**

10.3.2 Command Descriptions

10.3.2.1 GTM Commands

gtm

Syntax **gtm**

Context config>router

Description This command enters the context to configure GTM parameters.

mvpn

Syntax [**no**] **mvpn**

Context config>router>gtm

Description This command enables and disables the context to configure MVPN-related parameters.

provider-tunnel

Syntax **provider-tunnel**

Context config>router>gtm

Description This command enables context to configure tunnel parameters for the GTM.

inclusive

Syntax **inclusive**

Context config>router>gtm>provider-tunnel

Description This command enables the context for specifying inclusive provider tunnels parameters.

rsvp

Syntax [**no**] **rsvp**

Context config>router>gtm>provider-tunnel>inclusive config>router>gtm>provider-tunnel>selective

Description This command enables the use of P2MP RSVP as the inclusive or selective provider tunnel.

The **no** form of the command removes the RSVP context including all the statements in the context.

Default no rsvp

lsp-template

Syntax **lsp-template** *lsp-template*
no lsp-template

Context Context config>router>gtm>provider-tunnel>inclusive>rsvp
Context config>router>gtm>provider-tunnel>selective>rsvp

Description This command specifies the use of automatically created P2MP LSP as the provider tunnel. The P2MP LSP will be signaled using the parameters specified in the template, such as bandwidth constraints.

Default no lsp-template

Parameters *lsp-template* — Specifies the name of the LSP template, up to 32 characters.

shutdown

Syntax **shutdown**
no shutdown

Context config>router>gtm>provider-tunnel>inclusive>rsvp
config>router>gtm>provider-tunnel>selective>rsvp

Description This command administratively disables an entity. When disabled, an entity does not change, reset, or remove any configuration settings or statistics.

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.

Services are created in the administratively down (**shutdown**) state. When a **no shutdown** command is entered, the service becomes administratively up and then tries to enter the operationally up state.

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

Default no shutdown

selective

Syntax **selective**

Context config>router>gtm>provider-tunnel

Description This command enables the context for specifying selective provider tunnel parameters.

data-delay-interval

Syntax **data-delay-interval** *value*
no data-delay-interval

Context config>router>>gtm>provider-tunnel>selective

Description This command specifies the interval, in seconds, before a PBR connected to the source switches traffic from the inclusive provider tunnel to the selective provider tunnel.

This command is not applicable to multi-stream S-PMSIs.

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

Default data-delay-interval 3

Parameters *value* — Specifies the data delay interval, in seconds.

Values 3 to 180

Default 3

data-threshold

Syntax **data-threshold** {*c-grp-ip-addr/mask* | *c-grp-ip-addr netmask*} *s-pmsi-threshold* [**pe-threshold-add** *pe-threshold-add*] [**pe-threshold-delete** *pe-threshold-delete*]
data-threshold *c-grp-ipv6-addr/prefix-length s-pmsi-threshold* [**pe-threshold-add** *pe-threshold-add*] [**pe-threshold-delete** *pe-threshold-delete*]
no data-threshold {*c-grp-ip-addr/mask* | *c-grp-ip-addr netmask*}
no data-threshold *c-grp-ipv6-addr/prefix-length*

Context config>router>gtm>provider-tunnel>selective

Description This command specifies the data rate threshold that triggers the switch from the inclusive provider tunnel to the selective provider tunnel for (C-S, C-G) within the group range. Optionally, PBR thresholds for creating or deleting NG-MVPN S-PMSI may also be specified. Omitting the PBR thresholds preserves currently set values (or defaults if never set). Multiple statements (one per a unique group) are allowed in the configuration.

This command is not applicable to multi-stream S-PMSIs.

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

Default no data-threshold

Parameters *c-grp-ip-addr/mask* | *c-grp-ip-addr netmask* — Specifies an IPv4 multicast group address and netmask length or network mask.

c-grp-ipv6-addr/prefix-length — Specifies an IPv6 multicast group address and prefix length.

s-pmsi-threshold — Specifies the rate, in kb/s. If the rate for a (C-S, C-G)) within the specified group range exceeds the threshold, traffic for the (C-S, C-G) will be switched to the selective provider tunnel.

s-pmsi-threshold-add — Specifies the number of receiver PBRs for creating S-PMSI. When the number of receiver PBRs for a given multicast group configuration is non-zero and below the threshold and BW threshold is satisfied, S-PMSI is created.

s-pmsi-threshold-delete — Specifies the number of receiver PBRs for deleting S-PMSI. When the number of receiver PBRs for a given multicast group configuration is above the threshold, S-PMSI is deleted and the multicast group is moved to I-PMSI or a wildcard S-PMSI. It is recommended that the delete threshold be significantly larger than the add threshold to avoid re-signaling of S-PMSI as the receiver PBR count fluctuates.

Values

c-grp-ip-addr	multicast group address a.b.c.d
mask	4 to 32
netmask	a.b.c.d (network bits all 1 and host bits all 0)
s-pmsi-threshold	1 to 4294967294 (threshold in kb/s)
c-grp-ipv6-addr	multicast 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 to FFFF]H d [0 to 255]D prefix-length [1 to 128]
pe-threshold-add	1 to 65535 Default: 65535 (delete threshold always met)
pe-threshold-delete	2 to 65535 Default: 65535:(delete threshold always met)

maximum-p2mp-spmsi

Syntax **maximum-p2mp-spmsi** *range*
no maximum-p2mp-spmsi

Context config>router>gtm>provider-tunnel>selective

Description This command specifies the maximum number of RSVP P2MP or LDP P2MP S-PMSI tunnels for the GTM. When the limit is reached, no more RSVP P2MP S-PMSI or LDP P2MP S-P MSI tunnels are created and traffic over the data-threshold will stay on I-PMSI.

Default maximum-p2mp-spmsi 10

Parameters *range* — Specifies the maximum number of RSVP P2MP or LDP P2MP S-PMSI tunnels for the GTM.

Values 1 to 4000

Default 10

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 no pim

gtm

Syntax **gtm**

Context config>router>pim

Description This command enables the context to configure GTM parameters.

auto-discovery

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

Context config>router>pim>gtm

Description This command enables or disables multicast auto-discovery via BGP for GTM.

The **no** form of the command disables auto-discovery.

Default no auto-discovery

Parameters **default** — Enables the default auto-discovery mode.

10.4 Show, Clear, and Debug Command Reference

10.4.1 Command Hierarchies

- Show Commands

10.4.1.1 Show Commands

show
— **router**
— **gtm**

10.4.2 Command Descriptions

10.4.2.1 Show Commands

gtm

Syntax **gtm**

Context show>router

Description This command multicast GTM related information.

Output GTM Output

Sample Output

```
*A:Dut-A# show router gtm

===============================================================================
GTM (MVPN Base) configuration data
===============================================================================
signaling           : Bgp                    auto-discovery      : Default
UMH Selection       : Highest-Ip             SA withdrawn        : Disabled
intersite-shared    : Enabled                Persist SA          : Disabled
vrf-import          : N/A
vrf-export          : N/A
vrf-target          : unicast
C-Mcast Import RT   : target:10.20.1.2:0
```

```
ipmsi              : rsvp IpmsiTmpl
i-pmsi P2MP AdmSt  : Up
i-pmsi Tunnel Name : IpmsiTmpl-gtm-73780
enable-bfd-root    : false                enable-bfd-leaf    : false
Mdt-type           : sender-receiver

BSR signalling     : none
Wildcard s-pmsi    : Disabled
Multistream-SPMSI  : Disabled
s-pmsi             : none
data-delay-interval: 3 seconds
enable-asm-mdt     : N/A
===============================================================================
```

11 BIER

11.1 BIER Overview

Bit Indexed Explicit Replication (BIER) architecture allows optimal forwarding of multicast packets without requiring a legacy multicast protocol to build multicast trees or for intermediate routers to maintain any per-multicast flow state. This provides a simplified control plane since BIER information is distributed using underlay IGP.

The following terms are used in BIER:

- Bit Forwarding Router (BFR) — A BFR is a router supporting BIER with a unique BFR prefix and optionally, a BIER ID assigned by the operator. A BFR establishes BFR adjacencies (IGP or SDN-programmed), computes the BIER routing table, and forwards or replicates BIER packets.
- BIER domain and sub-domain — A BIER domain is a connected set of BFRs, each with a unique BFR ID. A BIER domain can be divided into sub-domains for scalability without a linear increase in size of the BIER header. For example, in IS-IS, a BIER sub-domain is IS-IS multi topology, where ipv4-unicast is a single sub-domain and ipv4-multicast is another sub-domain.

  Sub-domains provide minimum traffic engineering and separation of services.
- Bit Forwarding Ingress Router (BFIR) — A BFIR is the first PE in a BIER domain entered by a multicast packet. The BFIR adds a BIER header and forwards the packet using the BIER routing table.
- Bit Forwarding Egress Router (BFER) — A BFER is the last PE that processes a BIER packet in a BIER domain. The BFER removes the BIER header before forwarding the packet. This is the only PE that requires a BIER ID as it is a PE with receiver connectivity.
- Transit Bit Forwarding Router (transit BFR): A transit BFT is a router in the BFR domain that is not a BFIR or a BFER that forwards the packet using the best path.

SR OS does not support multicast MPLS packets over an IGP shortcut. This includes BIER MPLS encapsulation. IGP shortcuts can be configured on SR OS for unicast and installed in the RIB or FIB, but BIER will not be resolved over the IGP shortcut. If an IGP shortcut is used for unicast resolution, an IPv4-multicast MT can be used to create a separate MT for BIER without the IGP shortcut.

11.1.1 BIER Hardware

BIER is only supported on FP4 network interfaces. BIER is not supported FP3 or earlier cards, or on access interfaces.

If a chassis has a mix of FP3 and FP4 network ports, BIER is signaled on all FP3 and FP4 interfaces which are part of the IS-IS. From a control plain perspective, BIER TLVs will be advertised using IS-IS on FP3 and FP4 interfaces. The BIER forwarding table will not be downloaded to FP3 cards. As such, there will be no BIER packet forwarding or processing on these cards. If IGP chooses FP3 L3 interfaces, there will be BIER forwarding issues. An event log is generated if an FP3 is part of the BIER sub-domain.

11.1.2 BIER ECMP

BIER supports ECMP/LAG. SR OS only uses the smallest IP address in the ECMP/ LAG group to resolve the BFRs.

After an ECMP switch, IGP must download the BIER forwarding table to the new interface or card so BIER ECMP does not have a sub-millisecond recovery. The recovery time is inline with IGP convergence time.

11.1.3 BIER Redundancy and Resiliency

SR OS does not support LFA/TI-LFA for BIER. When there is a failure on the primary next-hop, even if there is a protection next-hop (LFA/TI-LFA), BIER does not switch to the protection next-hop. After the failure, BIER waits for IGP to converge and a new next-hop to be available, which means that traffic interruption is equal to the IGP convergence time. LFA is still configurable when BIER is enabled and can be used for other IP and MPLS functionality.

11.1.4 BIER Layers

A multicast BIER network can be divided into three layers:

- routing underlay (IGP)
  - establishes BIER adjacencies based on BIER configuration
  - populates BIER routing table (best path reachability)

   - provides routing-underlay-based redundancy and convergence, ECMP
- BIER layer (BIER routing table, BIER header)
   - advertises and configures the BFR prefix and BIER ID (bitmask bit) for BIER routers
   - imposes a new BIER header (bitmask: "OR" for receiver PEs based on their BIER IDs as dictated by multicast flow overlay)
   - forwards multicast traffic using the BIER header and BIER routing table
   - prevents loops and duplication by using bitmask manipulation and removing the bits for PEs that are not reachable using the L3 interface next hop
- multicast flow overlay (MVPN, BGP)
   - uses MP-BGP to distribute and discover the endpoints (RFC-6513 and RFC-6514)

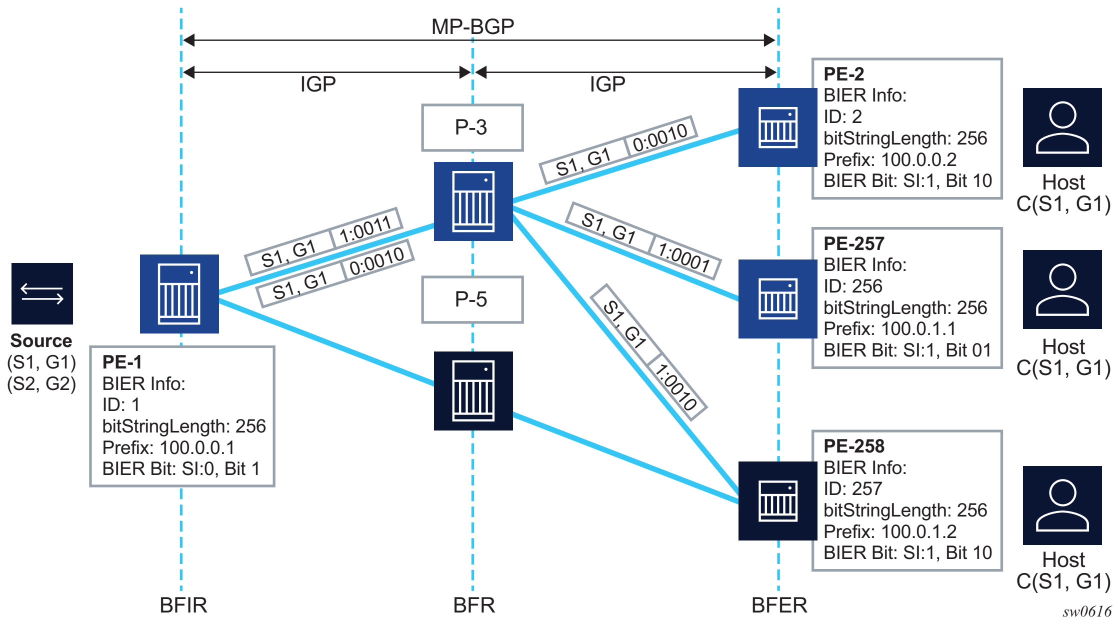
11.1.5 Implementation

Figure 12 shows multicast with BIER deployed. IGP is used as the routing underlay, and MP-BGP for NG-MVPN is used as the multicast flow overlay. The BFIR is the source PE-1, BFERs 2, 256, and 257 are receiver PEs, and the remaining routers are BFRs. All routers have their BIER prefix assigned and, additionally, the BFERs have BIER BFR-IDs assigned.

A BFR prefix is a unicast routable IP address (either IPv4 or IPv6) that is either a system loopback or a loopback interface. BFR prefixes are unique within a BIER domain.

A BFR ID is a unique number assigned to BFERs and BFIRs that is used to build the BIER bitmask used to forward packets. BIER IDs should be allocated as a continuous set of IDs starting at 1 to ensure a minimum number of sets are required to achieve multicast BIER connectivity. Sets allow scaling of BIER beyond the bitmask length supported; however, sets require a separate copy of the multicast packet to be forwarded on the same link which may result in unwanted replication.

Figure 12 **BIER High-level IGP and Overlay**



11.1.5.1 BIER Sub-domains

Each BIER domain can be divided into sub-domains. A BIER domain supports sub-domains numbered from 0 to 255. Each BIER domain must contain at least one sub-domain, and sub-domain 0 is the default. If a BIER domain contains more than one sub-domain, each BFR in the domain must be provisioned with the set of sub-domains to which it belongs.

A BIER domain is an IGP area, and sub-domains are the different topologies within that area. In IS-IS and OSPF each topology must also have its own sub-domain ID. For example, in IS-IS a sub-domain is an IS-IS multi-topology. SR OS supports two sub-domains in IS-IS: IPv4-multicast and IPv4-unicast MTs. A sub-domain creates the least traffic engineering in a BIER domain. A user can use separate L3 interfaces into IPv4-unicast MT and a set of disjointed interfaces into the IPv4-multicast MT. This creates separation and traffic engineering for different multicast streams.

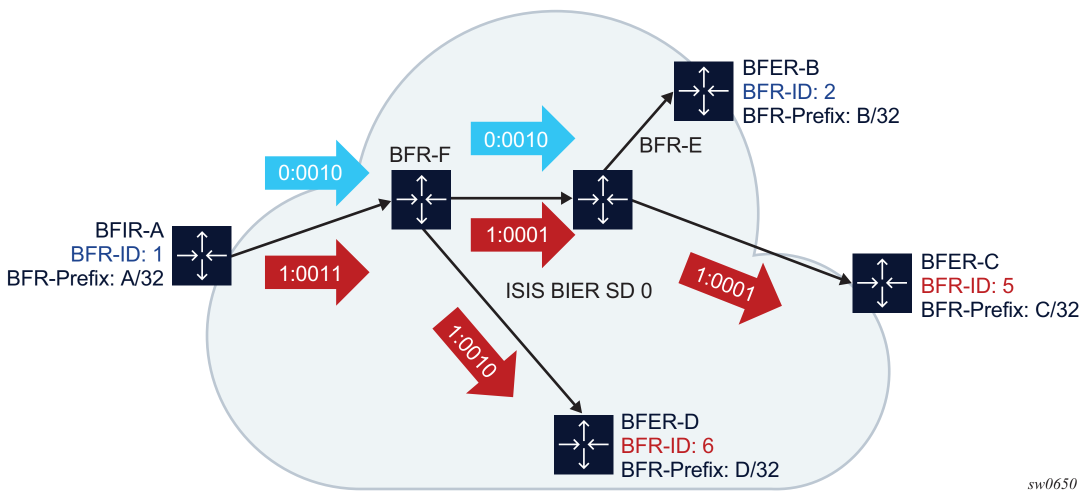
For each sub-domain to which a given BFR belongs, if the BFR is capable of acting as a BFIR or a BFER, it must be provisioned with a BFR ID that is unique within the sub-domain. If a given BFR belongs to more than one sub-domain, it may have a different BFR ID for each sub-domain but this is not required.

11.1.5.2 BIER Set IDs

To increase scalability of BIT String Length (BSL), routers can be grouped into BIER sets.

The BSL dictates how many BFRs can be represented in a BIER set. Each BIER set can contain as many routers as the length of BSL, and it is represented by a BIER Set ID (SI). The Set Id is part of the packet and represented as <SI:Bit Position>. Figure 13 shows an example set with a BSL of 4.

Figure 13 **BIER Set**



The BFR ID is programmed into <SI, Bit Position> based on the network BSL.

SI = (BFR-ID – 1)/BSL

BP = ((BFR-ID – 1) mod BSL)+1

For example: BSL 4 and BFR-ID 6 = <SI=1, BP=2>.

BIER works well in an IP TV deployment where the network is in a spine and leaf deployment. SR OS supports 16 set IDs in this type of deployment where there is no packet duplication at the spine.

- The SHO can be connected to as many as 16 VHOs.
- Each tree can have 256 LEAFs without packet duplication.
- Each leaf can have as many hosts on it as the number of supported IGMP/MLD hosts

11.1.5.3 BIER Encapsulation

SR OS supports BIER MPLS encapsulation.

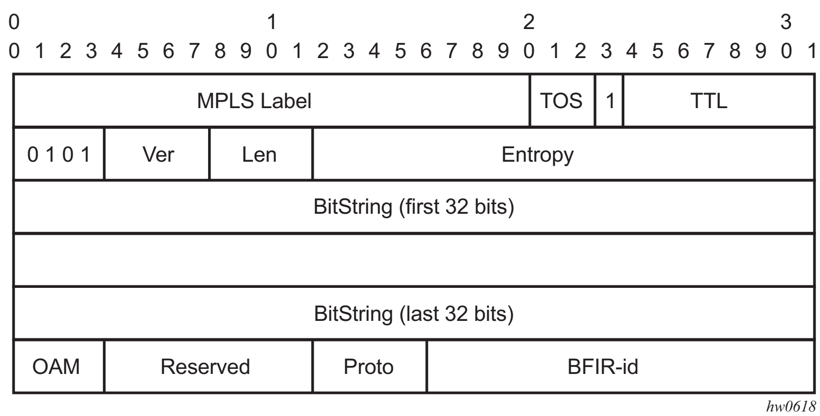
11.1.5.3.1 BIER MPLS Encapsulation

The BIER MPLS labels are downstream-assigned MPLS labels that are unique only to the BFR that advertises them. BIER MPLS labels can be advertised using IGP (IS-IS) extension sub-TLVs or BGP extension sub-TLVs.

Penultimate Hop Popping (PHP) is not supported by BIER-MPLS labels as the labels are used to identify the BIER forwarding table that packets need to be looked up in.

Figure 14 shows the BIER MPLS encapsulation label.

Figure 14 **BIER MPLS Encapsulation**



A BIER MPLS label is bound to the forwarding element class. A BIER label is assigned per BIER <SD, <BSL, SI>>. The SR OS supports only a BSL of 256.

Labels are chosen from the first available label in the label pool, and are only allocated locally when IGP advertises the BIER sub-TLVs.

When a packet arrives on a BFR the BIER forwarding table is identified using the MPLS label. BIER forwarding is then completed using the BIER header.

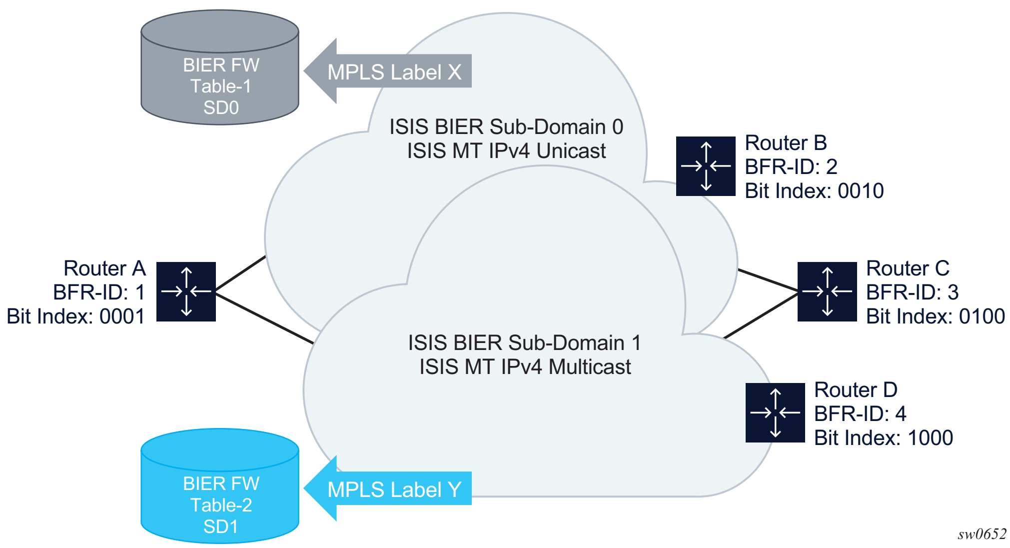
11.1.5.4 BIER Forwarding Tables

A BIER forwarding table is built based on the combination of:

- Set ID (SI)
- BIER String Length (BSL)
- Sub Domain (SD)

and saved in the format <SD, BSL, SI>. Figure 15 shows an example of how forwarding tables are built.

Figure 15 **BIER Forwarding Tables**



For example, if there are 2 SDs and there are 256 PEs in each SD, there will be two forwarding tables, one for each SD. One for <SD=0, BSL=256, SI=0> and the other for <SD=1, BSL=256, SI=0>.

Similarly, if there are 512 PEs in an SD and the BSL is 256, there will be two forwarding tables, one for <SD=0, BSL=256, SI=0> and the other for <SD=0, BSL=256, SI=1>

An MPLS label is assigned locally for each BIER routing table, and advertised.

11.1.5.5 BIER IS-IS Sub-TLVs

BFRs establish BIER adjacencies through IS-IS and exchange their BFR prefixes and BIER IDs as well as transport-related information. IS-IS can be used to exchange the information. Figure 16 shows the IS-IS extensions for BIER and Figure 17 shows a BIER MPLS sub-sub-TLV.

Figure 16 **BIER IGP Sub-TLV**

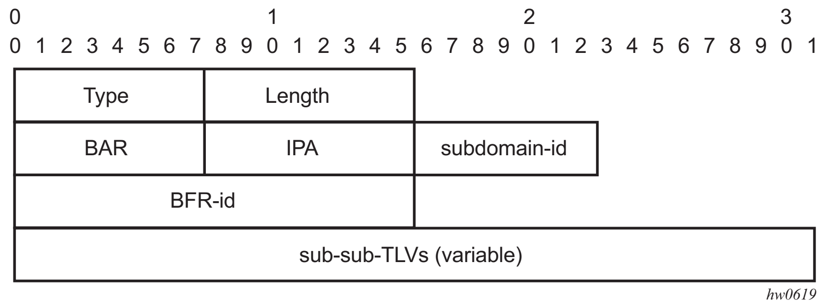
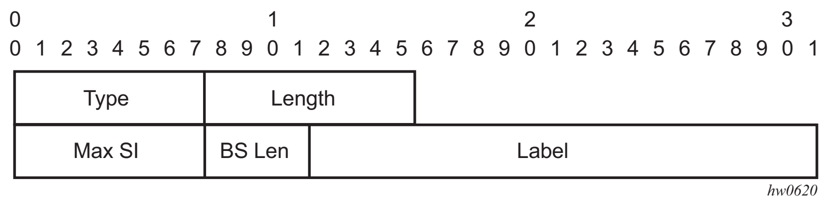


Figure 17 **BIER MPLS Sub-Sub-TLV**



In IS-IS, a new BIER sub-TLV is advertised as part of extended prefix opaque LSA carrying the BFR IP address (loopback) and supported BIER bitmask length for this BFR (multiple TLVs are used to convey support for multiple bitmask lengths). In addition, when MPLS encapsulation is used, a BIER MPLS encapsulation sub-TLV is included that contains the label range used for BIER. The label ranges advertised within the area are unique to a BFR and are used to identify the BIER forwarding context.

Based on the information exchanged, IGP creates a BIER routing table (unicast SPF) to reach each BFER that can be used to route BIER packets. The routing table specifies the shortest unicast path to reach each BFER through (BFERs bitmask, next-hop BFR)-tuples.

BIER sub-TLVs having the wrong length or illegal encoding are ignored and no error is raised. All other sub-TLV or sub-sub-TLV validation is done by the BIER module.

11.1.5.6 IS-IS BIER Support

IS-IS supports multiple levels and BIER is supported under each level using the following rules.

- If the ABR is not a BFIR or BFER, the BIER sub-TLV must be leaked between different levels (areas) at the ABR. A BIER template without a BFR ID must be on both levels.
- The ABR can support BFIR and BFER functionality. ABR does not support BIER header stitching.
- A single area can have level 1 and level 2. In this case, the same template can be programmed on both levels.

11.1.5.7 IS-IS Multi-topologies

IS-IS supports multi-topologies (MT), such as ipv4-unicast, ipv4-multicast, ipv6-unicast, and ipv6-multicast. SR OS supports ipv4-unicast and ipv4-multicast MTs for BIER.

A sub-domain is supported within only one topology. The mapping is indicated by the pair <MT,SD>.

For example, the following combination of <MT, SD>, where MT 0 is IPv4 Unicast and MT 3 is IPv4 multicast, are valid:

<MT=0, SD=0>

<MT=0, SD =1>

<MT=0, SD =2>

However, this combination, where MT 0 is IPv4 Unicast and MT 3 is IPv4 multicast, is invalid because an SD belongs to more than one MT:

<MT=0, SD=0>

<MT=3, SD=0>

IPv4-multicast imports routes into the multicast RTM and ipv4-unicast imports routes into the unicast RTM.

A BIER forwarding table (BIFT) is identified using a label. A BIER label is assigned per (<MT,SD>, SI, BSL) and as such, different MTs point to different BIFTs.

The MT can be used to engineer multicast and BIER routes separately from unicast routes.

11.1.5.8 BIER Intra-AS Solution

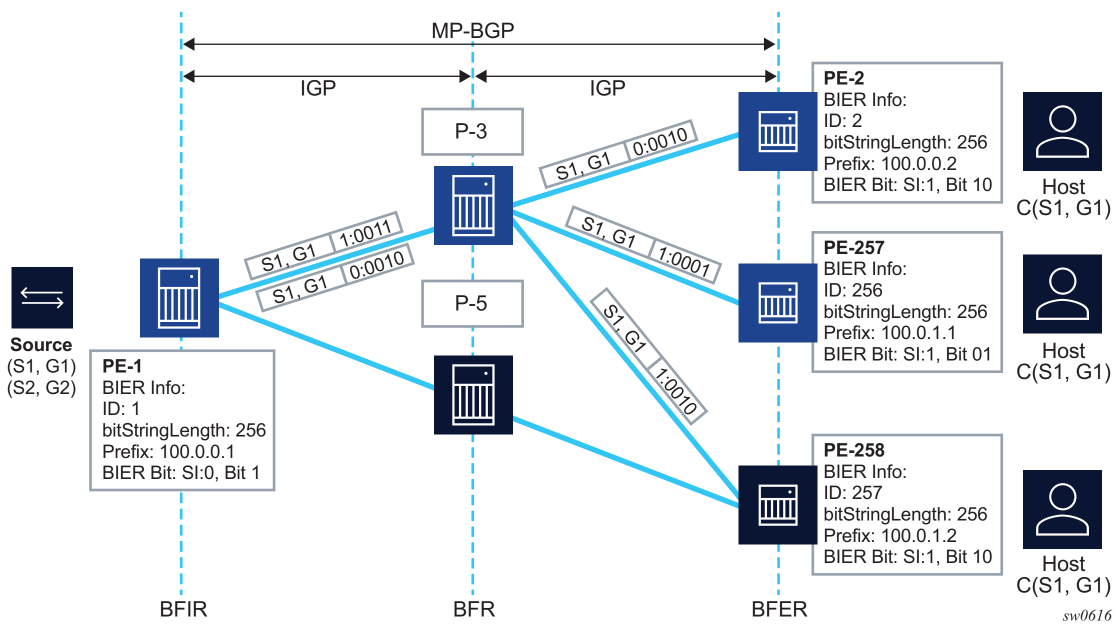
For intra-AS solutions, ensure that the ABR loopback interface used as the BIER prefix is included in both Level 1 and Level 2, otherwise the BIER prefix is not resolved at the level into which the route was leaked.

Nokia recommends having the loopback interface used as the BIER prefix in Level1/Level2 for intra-AS solutions, which is the default configuration for SR OS.

11.1.5.9 BIER Forwarding

Figure 18 shows that IGP builds the BIFT using IGP. Each node also builds its LTN table based on IGP-advertised MPLS labels.

Figure 18 **BIER Forwarding**



The BFIR PE (root) has the full BIFT and the corresponding MPLS LTN table.

MP-BGP (multicast overlay) signals each PE interested in a specific customer (S,G) from LEAF PEs to the root PE.

Each PE belongs to a BIER sub-domain based on the IGP multi-topology configuration. For example, PE257 and PE256 are part of the IPv4 unicast topology, while PE2 and PE256 are part of the IPv4 multicast topology.

When the root PE wants to forward a multicast stream, for example a stream for C(S3,G3), it looks up the appropriate PEs in the BIFT. The appropriate SI:BitPosition is assigned a logical “OR” operation to build a single BitString. In this example, BFER-B is assigned 0:0010, BFER-C is assigned 0:0100 and BFER-D is assigned 0:1000, so the "OR" of the two PEs BIFT results in 0:1110 SI:BitString.

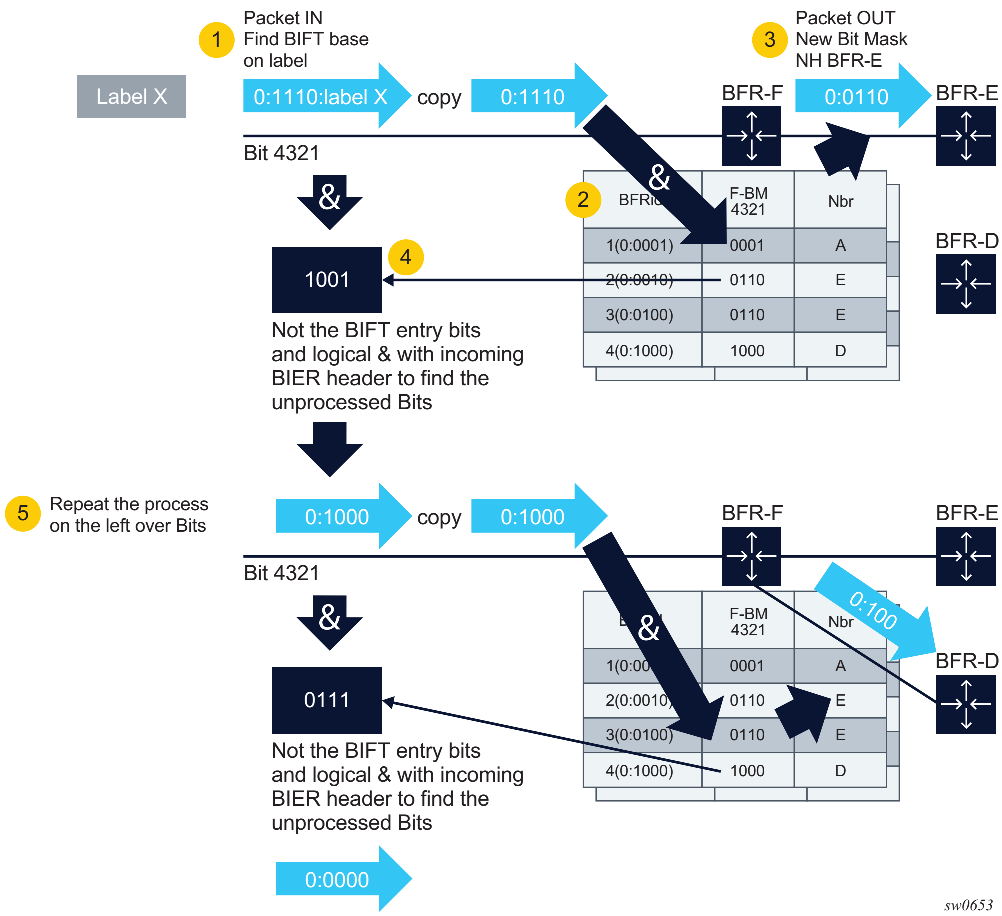
The MPLS label (1001) for (SD0,SI0,BSL256) is appended to the BIER BitString and forwarded to BFR-F.

The BFR-F, which has label 1001 as its local label, pops the label and maps the label to the SD0, SI0, BSL256 BIER forwarding table. It then looks up the BIFT for BFER-B, C, and D, and assigns the new SI:BitString of 0:0110 for BFER-B and BFER-C and forwards the packet to BFR-E. In addition, it builds the 0:1000 bit string for BFER-D and forwards the packet to BFER-D. It then looks up the appropriate label for the BFR-E and BFER-D and appends the corresponding label before forwarding the BIER packet.

11.1.5.9.1 BIER FIB Packet Handling

Figure 19 shows how BIER packets are handled in the FIB.

Figure 19 **BIER FIB Packet Handling**



1. When a BIER packet arrives, the PE checks the label and finds the BIFT for that label and then pops the label.
2. For the incoming BIER header, it walks the bit index and finds the first entry in the BIFT for that bit position.
3. Using a logical “AND”, the BIER header is combined with the BIFT bit-mask and forwarded to the neighbor. If there are multiple neighbors, the BIFT is programmed with a single entry, the neighbor with the smallest IP address.
4. Using a logical “NOT” on the BIFT bit-mask entry, the PE finds out which bits remain to be processed.
5. Repeat the process until all the BIER header’s bits are processed.

11.1.5.10 BIER MVPN

BIER MVPN uses MP-BGP as an overlay to signal MVPN. It uses RFC 6514 the same way P2MP RSVP-TE.

BIER MVPN introduces a new tunnel type of BIER (0x0B).

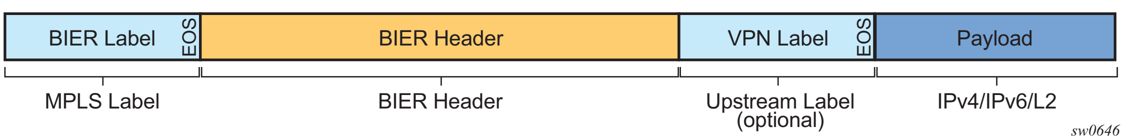
BIER PMSI will replace PIM, mLDP, and RSVP-TE P2MP in the core. There is no PMSI per (C-S, C-G), PMSI is used to reach all PE nodes interested in the C-Flow.

The VC label represents the VRF. Within the VRF, the payload IP header (C-S,C-G) will find the OIF based on PIM, IGP, and MLD states.

When a root PE (BFIR) receives a multicast packet and determines that the packet needs to be forwarded to the appropriate BFERs, the source PE encapsulates the multicast packet in a BIER header as described in BIER Encapsulation. The root PE adds the appropriate VC label advertised by MP-BGP and PTA and forwards it to the BIER domain.

Figure 20 shows the BIER MVPN packet format.

Figure 20 **BIER MVPN Packet Format**



The original packet has a VC label identifying the VRF added first, then the packet (MPLS payload) is forwarded using BIER PMSI by adding a BIER header identifying the BFERs and BIER label learned using IGP from the next-hop router, as described in BIER Forwarding. Finally, when the packet arrives on the BFER, the BIER label is stripped, the BIFT is used to identify whether the packet needs to be handled by a corresponding VRF (since the bit in the header corresponds to the BFER BFR-ID). The BFER strips the BIER header, uses the VC label to identify the VRF instance, strips the VC label, and forwards the packet according to the legacy multicast protocols configured on the SAPs of the MVPN (for example, PIM, IGMP, and MLD OIFs).

SR OS supports BIER as I-PMSI and S-PMSI. By default, all (C-S, C-G) are forwarded using I-PMSI. If a throughput threshold is configured in MVPN and that threshold is surpassed by a (C-S, C-G), then the traffic for that stream is switched from I-PMSI to S-PMSI. BIER uses standard NG-MVPN signaling for S-PMSI and uses leaf AD routes from the leaf PEs to set up S-PMSI to the corresponding leaf that is interested in a specific (C-S, C-G).

The BIER MVPN configuration is as follows.

```
 *A:Dut-A>config>service>vprn>mvpn# info
            ---------------------------------------------
                auto-discovery default
                c-mcast-signaling bgp
                umh-selection hash-based
                provider-tunnel
                    inclusive
                        bier
                            sub-domain 0
                            no shutdown
                        exit
                    exit
                    selective
                        bier
                            sub-domain 0
                            no shutdown
                        exit
                        data-threshold 224.0.0.0/4 1
                    exit
                exit
                vrf-target unicast
                exit
---------------------------------------------
*A:Dut-A>config>service>vprn>mvpn#
```

11.1.5.10.1 BIER MVPN IPv4 and IPv6

BIER MVPN only generates a single VC label and PMSI for IPv4 or IPv6 traffic belonging to the same VRF.

The BIER header protocol is set to "mpls packet with upstream-assigned label". This label is the VC label identifying the VRF that the packet belongs to. After finding the VRF and removing the VC label, a second lookup on the IP header identifies the packet address family (IPv4 or IPv6). Based on the destination IP, which is the multicast group address, the packet is forwarded out the appropriate MVPN OIF SAPs.

11.1.5.10.2 BIER MVPN Sub-domain

An MVPN belongs to a single sub-domain (SD). An SD is assigned to the PMSI of the MVPN, and forces the MVPN to resolve the BGP nexthop within that SD. Both I-PMSI and S-PMSI must be configured with the same SD.

Different MVPNs can belong to different SDs. For example, mvpn-1 can belong to SD 0 which is an IPv4 unicast MT and mvpn-2 can belong to SD 1 which is an IPv4 multicast MT. This allows different MVPNs to be traffic engineered between different SDs or IS-IS MTs as needed.

11.1.5.10.3 BIER Templates

A BIER template can be created under the **configure>router** context and provides a centralized BIER configuration where the operator can configure all the BIER parameters. The BIER template contains the sub-domain to multi-topology mapping and other BIER configurations, such as the BFR ID and BIER prefix.

Each sub-domain can contain a single IGP multi-topology (MT). Currently, SR OS only supports MT for IS-IS but not for OSPF.

A BIER template can contain many MTs and SDs. Each SD has its own BIER prefix and BFR ID and can belong to a different MT. The default MT is ipv4-unicast MT.

A sample BIER template:

```
*A:swsim100_a>config>router>bier>template# info
----------------------------------------------
        sub-domain 0
            prefix 100.0.0.100
            bfr-id 4096
        exit
        sub-domain 1
            prefix 100.0.0.101
            bfr-id 1
            mt ipv4-multicast
        exit
        no shutdown
----------------------------------------------
```

After a template is configured it can be assigned to a corresponding IGP protocol. The IGP protocol chooses the first <SD, MT> that matches its own configured MT. For example, if the IS-IS has an MT of IPv4-multicast for the example BIER template, it will use the sub-domain 1 configuration. It will build its BIER forwarding table base on SD 1 SI, BSL and use the BIER prefix configured under sub-domain 1 for its IGP sub-TLVs.

11.2 BIER Configuration Command Reference

11.2.1 Command Hierarchies

- Configuration Commands

11.2.1.1 Configuration Commands

config
- **— router**
  - **—** [**no**] **bier**
    - **—** [**no**] **shutdown**
    - **—** [**no**] **template** *template-name*
      - **—** [**no**] **shutdown**
      - **—** [**no**] **sub-domain** *sub-domain*
      - **—** [**no**] **sub-domain** **start** *sub-domain* **end** *sub-domain*
        - **—** [**no**] **bfr-id** *bfr-id*
        - **— mt** {**ipv4-unicast** | **ipv4-multicast**}
        - **— no mt**
        - **— prefix** *ip-address*
        - **— no prefix**

11.2.2 Command Descriptions

11.2.2.1 BIER Commands

bier

Syntax [**no**] **bier**

Context config>router

Description This command enters the context to configure BIER.

shutdown

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

Context config>router>bier
config>router>bier>template

Description This command shuts down BIER or a BIER template.

The **no** form of this command enables BIER or the BIER template.

template

Syntax [**no**] **template** *template-name*

Context config>router>bier

Description This command creates a BIER template to be assigned to IGP.

The **no** form of this command removes a specific template.

Parameters *template-name* — The name of the template to be created or removed, up to 32 characters.

sub-domain

Syntax [**no**] **sub-domain** *sub-domain*
[**no**] **sub-domain start** *sub-domain* **end** *sub-domain*

Context config>router>bier>template

Description This command creates a BIER sub-domain or range of sub-domains. For example, for IS-IS each sub-domain is associated with a single IS-IS topology, which may be any of the topologies supported by IS-IS.

The **no** form of this command removes a sub-domain.

Default sub-domain 0

Parameters *sub-domain* — The ID of the sub-domain to be created or removed.

Values 0 to 255

bfr-id

Syntax **bfr-id** *bfr-id*
no bfr-id

Context config>router>bier>template>sub-domain

Description This command specifies the BIER-ID for this sub-domain. BIER-IDs should be assigned sequentially as the SI and BIER bit position are driven by the IDs. The equation used to drive BIER SI and bit positions from the ID is as follows:

SI = (BFR-id -1) /BitStringLength

bit position = ((BFR-id -1) modulo BitStringLength

If the BIER-ID is sequential then the all bit positions in a bit string length will be utilized before moving on to the next SetID (SI).

BFR ID configuration is only necessary for BFIR and BFER, and not for transit BFRs

The **no** form of this command removes the BIER-ID.

Parameters *bfr-id* — The BIER-ID of the router.

Values 1 to 4096

mt

Syntax **mt** {**ipv4-unicast** | **ipv4-multicast**}
no mt

Context config>router>bier>template>sub-domain

Description This command specifies the multi-topology for this sub-domain.

The **no** form of this command removes the multi-topology from this sub-domain.

Parameters **ipv4-unicast** — Specifies that the sub-domain uses IPv4 unicast topology. IPv4 unicast imports routes into the unicast RTM.

ipv4-multicast — Specifies that the sub-domain uses IPv4 multicast topology. IPv4 multicast imports routes into the multicast RTM.

prefix

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

Context config>router>bier>template>sub-domain

Description This command specifies the prefix used for BFR. The prefix should be an IPv4 /32 address. The prefix can be a loopback interface or system IP address.

The **no** form of this command removes the prefix.

Parameters *ip-address* — Specifies the IP address to be used as the BFR prefix in dotted decimal format.

11.3 Show, Clear, and Debug Command Reference

11.3.1 Command Hierarchies

- Show Commands

11.3.1.1 Show Commands

show
— **router**
— **bier**
— **database** [**sub-domain** *sub-domain*] [**template** *template-name*]
— **forwarding** [**sub-domain** *sub-domain*] [**bsl** *bsl*] [**neighbor-prefix** *ip-address*] [**si** *si*]
— **routing** [**sub-domain** *sub-domain*] [**bsl** *bsl*] [**neighbor-prefix** *ip-address*] [**dest-prefix** *ip-address*]
— **statistics**
— **tunnel** [**type** {**rx** | **tx**}] [**prefix** *ip-address*] [**tunnel-id** *tunnel-id*]
— **tunnel** [**prefix** *ip-address*] [**tunnel-id** *tunnel-id*] **leaf**

11.3.2 Command Descriptions

11.3.2.1 Show Commands

The command outputs in the following section are examples only; actual displays may differ depending on supported functionality and user configuration.

database

Syntax **database** [**sub-domain** *sub-domain*] [**template** *template-name*]

Context show>router>bier

Description This command shows the BIER database and assigned labels for <SD, BSL, SI>.

Parameters *sub-domain* — Displays detailed information about the sub-domain.

Values 0 to 255

template-name — Displays template information.

Output The following output displays an example of a BIER database.

Sample Output

```
*A:Dut-A# show router bier database
===============================================================================
BIER Database
===============================================================================
Template                        MT             Sub-domain     BSL
BFR-ID                          Start          End            Total
BFR-Prefix
-------------------------------------------------------------------------------
temp1                           ipv4-unicast   0              256
1                               1048464        1048479        16
10.20.1.1

temp1                           ipv4-unicast   1              256
255                             1048447        1048462        16
10.20.1.1

temp1                           ipv4-unicast   2              256
2966                            1048430        1048445        16
10.20.1.1

temp1                           ipv4-unicast   3              256
1                               1048413        1048428        16
10.20.1.1

temp1                           ipv4-unicast   4              256
255                             1048396        1048411        16
10.20.1.1

===============================================================================
BIER Database entries : 5
===============================================================================
*A:Dut-A#
```

The following table provides BIER database field descriptions

Table 42 Bier Database Fields

Label	Description
Template	Displays the template name.
MT	Displays the IGP topology associated with the sub-domain.
Sub-domain	Displays the sub-domain ID.
BSL	Displays the BitStringLength used in the sub-domain.
BFR-ID	Displays the BFR ID which identifies the router in the BitString.
Start	Displays the start label allocated for this sub-domain.

Table 42 Bier Database Fields (Continued)

Label	Description
End	Displays the end label allocated for this sub-domain.
Total	Displays the total number of labels allocated for this sub-domain.
BFR-Prefix	Displays the routable IP address of a BFR, used by BIER to identify a BFR.

forwarding

Syntax **forwarding** [**sub-domain** *sub-domain*] [**bsl** *bsl*] [**neighbor-prefix** *ip-address*] [**si** *si*]

Context show>router>bier

Description Display PIM candidate RP (CRP) information received at the elected Bootstrap router (BSR).

Parameters *sub-domain* — Specifies a sub-domain.

Values 0 to 255

bsl — Specifies a bit string length.

Values 256 to 1024

ip-address — Specifies a neighbor-prefix in IP address format.

si — Specifies an SI.

Output The following output is an example of a BIER forwarding configuration.

Sample Output

```
*A:Dut-A# show router bier forwarding sub-domain 0
===============================================================================
Neighbor
  Nexthop
  Interface
  [SI]: Label
     Forwarding Bit Mask
       BFR-ID : Prefix
-------------------------------------------------------------------------------
===============================================================================
BIER Forwarding Database Sub-Domain 0 BSL 256
===============================================================================
10.20.1.2
  10.180.1.2
  ip-10.180.1.1
  [0]: 1048556
     0x0000000000000000000000000000000000000000000000000000000000000036
       2 : 10.20.1.2
       3 : 10.20.1.3
       5 : 10.20.1.5
```

```
       6 : 10.20.1.6
===============================================================================
Total (Sub-Domain 0): 1
===============================================================================
Total BIER Forwarding entries : 1
===============================================================================
*A:Dut-A#
```

The following table provides BIER forwarding field descriptions.

Table 43 **BIER Forwarding Fields**

Label	Description
Neighbor	Displays the neighbor IP address.
Nexthop	Displays the next-hop IP address.
Interface	Displays the egress interface name for the programmed tunnel.
[SI]:Label	Displays the SI and label. The BitString and the SI together determine the set of BFERs to which a given packet will be delivered. The label is the egress transport label used for the given SI/SD.
Forwarding Bit Mask	Displays the BitString forwarding mask.
BFR-ID: Prefix	Displays the BFR ID and the prefix reachable through this SD/SI/BFR-ID.

routing

Syntax **routing** [**sub-domain** *sub-domain*] [**bsl** *bsl*] [**neighbor-prefix** *ip-address*] [**dest-prefix** *ip-address*]

Context show>router>bier

Description This command shows the BIER routing table.

Parameters *sub-domain* — Specifies a sub-domain.

Values 0 to 255

bsl — Specifies a bit string length.

Values 256 to 1024

ip-address — Specifies a prefix in IP address format.

Output The following output is an example of a BIER router table.

Sample Output

```
*A:Dut-A# show router bier routing sub-domain 0
===============================================================================
Destination Prefix                          Bfr-ID          Age
  Neighbor
    Nexthop
    Interface
-------------------------------------------------------------------------------
===============================================================================
BIER Routing Database Sub-Domain 0 BSL 256
===============================================================================
10.20.1.2                                   2               0d 23:05:23
  10.20.1.2
    10.180.1.2
    ip-10.180.1.1

10.20.1.3                                   3               0d 23:05:20
  10.20.1.2
    10.180.1.2
    ip-10.180.1.1

10.20.1.4                                   0               0d 23:05:20
  10.20.1.2
    10.180.1.2
    ip-10.180.1.1

10.20.1.5                                   5               0d 23:05:16
  10.20.1.2
    10.180.1.2
    ip-10.180.1.1

10.20.1.6                                   6               0d 23:05:16
  10.20.1.2
    10.180.1.2
    ip-10.180.1.1

===============================================================================
Total (Sub-Domain 0): 5
===============================================================================
Total BIER Routing entries : 5
===============================================================================
*A:Dut-A#
```

The following table provides BIER routing field descriptions.

Table 44 **BIER Routing Fields**

Label	Description
Destination Prefix	Displays the destination prefix.
BFR-ID	Displays the BFR ID.
Age	Displays how long the tunnel has been up.
Neighbor	Displays the neighbor IP address.
Nexthop	Displays the next-hop IP address.

Table 44 **BIER Routing Fields (Continued)**

Label	Description
Interface	Displays the egress interface name for the programmed tunnel.

statistics

Syntax **statistics**

Context show>router>bier

Description This command displays BIER statistics.

tunnel

Syntax **tunnel** [**type** {**rx** | **tx**}] [**prefix** *ip-address*] [**tunnel-id** *tunnel-id*]
tunnel [**prefix** *ip-address*] [**tunnel-id** *tunnel-id*] **leaf**

Context show>router>bier

Description This command shows the BIER tunnel table used for MVPN.

Parameters *ip-address* — Specifies a prefix in IP address format.

tunnel-id — Specifies a tunnel identifier.

Values 0 to 4294967295

Output The following output is an example of a BIER tunnel table.

Sample Output

```
*A:Dut-A# show router bier tunnel prefix 10.20.1.3
===============================================================================
BIER Tunnels
===============================================================================
Tunnel-id           Type                Oper                No. Of Leaves
BFR Prefx           Bfr-ID              Mpls Label          Sub-domain
-------------------------------------------------------------------------------
73941               rx                  In service          0
10.20.1.3           767                 1048475             4
73942               rx                  In service          0
10.20.1.3           767                 1048473             1
73943               rx                  In service          0
10.20.1.3           767                 1048573             1
73944               rx                  In service          0
10.20.1.3           3                   1048474             0
73945               rx                  In service          0
10.20.1.3           3                   1048471             3
73946               rx                  In service          0
10.20.1.3           767                 1048470             4
```

```
73947           rx              In service      0
10.20.1.3       3               1048574         0
73948           rx              In service      0
10.20.1.3       1593            1048472         2
73949           rx              In service      0
10.20.1.3       3               1048477         3
73950           rx              In service      0
10.20.1.3       1593            1048480         2
73951           rx              In service      0
10.20.1.3       767             1048476         4

73952           rx              In service      0
10.20.1.3       3               1048478         3
73955           rx              In service      0
10.20.1.3       1593            1048481         2
73956           rx              In service      0
10.20.1.3       767             1048485         1
73957           rx              In service      0
10.20.1.3       3               1048490         0
===============================================================================
BIER Tunnel entries : 15
===============================================================================
```

The following table provides BIER tunnel table descriptions.

Table 45 **BIER Tunnel Fields**

Label	Description
Tunnel-id	Displays the tunnel ID allocated for this tunnel.
Type	Displays the tunnel type, indicated if it is a terminating tunnel or an originating one.
Oper	Displays the operational status of the tunnel.
No. of Leaves	Displays the number of leaves associated with the tunnel if the tunnel type is tx or BFIR, this field represent the number of leafs associated with it. If the tunnel type is rx or BFER, this field is zero.
BFR Prefix	Displays the BFR prefix associated with the root of the tunnel.
Bfr-ID	BFR ID associated with the root of the tunnel.
Mpls Label	If the tunnel type is tx or BFIR, this field represents the egress VPRN label allocated. If the tunnel type is rx or BFER, this field represents the ingress VPRN label allocated by the root.
Sub-domain	Displays the sub-domain associated with the root of the tunnel.

12 Troubleshooting Tools

12.1 Mtrace

Assessing problems in the distribution of IP multicast traffic can be difficult. The **mtrace** feature utilizes a tracing feature implemented in multicast routers that is accessed via an extension to the IGMP protocol. The **mtrace** feature is used to print the path from the source to a receiver; it does this 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 should be gathered and returned to the requester.

Data added by each hop includes:

- query arrival time
- incoming interface
- outgoing interface
- previous hop router address
- input packet count
- output packet count
- total packets for this source/group
- routing protocol
- TTL threshold
- forwarding/error code

The information enables the network administrator to determine:

- where multicast flows stop
- the flow of the multicast stream

When the trace response packet reaches the first hop router (the router that is directly connected to the source’s net), that router sends the completed response to the response destination (receiver) address specified in the trace query.

If some multicast router along the path does not implement the multicast traceroute feature or if there is some outage, then no response is returned. To solve this problem, the trace query includes a maximum hop count field to limit the number of hops traced before the response is returned. This allows a partial path to be traced.

The reports inserted by each router contain not only the address of the hop, but also the TTL required to forward and some flags to indicate routing errors, plus counts of the total number of packets on the incoming and outgoing interfaces and those forwarded for the specified group. Taking differences in these counts for two traces separated in time and comparing the output packet counts from one hop with the input packet counts of the next hop allows the calculation of packet rate and packet loss statistics for each hop to isolate congestion problems.

12.1.1 Finding the Last Hop Router

The trace query must be sent to the multicast router which is the last hop on the path from the source to the receiver. If the receiver is on the local subnet (as determined using the subnet mask), then the default method is to multicast the trace query to all-routers.mcast.net (224.0.0.2) with a TTL of 1. Otherwise, the trace query is multicast to the group address since the last hop router will be a member of that group if the receiver is. Therefore, it is necessary to specify a group that the intended receiver has joined. This multicast is sent with a default TTL of 64, which may not be sufficient for all cases.

When tracing from a multihomed host or router, the default receiver address may not be the desired interface for the path from the source. In that case, the desired interface should be specified explicitly as the receiver.

12.1.2 Directing the Response

By default, mtrace first attempts to trace the full reverse path, unless the number of hops to trace is explicitly set with the hop option. If there is no response within a 3 second timeout interval, a "*" is printed and the probing switches to hop-by-hop mode. Trace queries are issued starting with a maximum hop count of one and increasing by one until the full path is traced or no response is received. At each hop, multiple probes are sent. The first attempt is made with the unicast address of the host running mtrace as the destination for the response. Since the unicast route may be blocked, the remainder of attempts request that the response be multicast to mtrace.mcast.net (224.0.1.32) with the TTL set to 32 more than what’s needed to pass the thresholds seen so far along the path to the receiver. For the last attempts the TTL is increased by another 32.

Alternatively, the TTL may be set explicitly with the TTL option.

For each attempt, if no response is received within the timeout, a "*" is printed. After the specified number of attempts have failed, mtrace will try to query the next hop router with a DVMRP_ASK_NEIGHBORS2 request (as used by the mrinfo program) to determine the router type.

The output of mtrace is a short listing of the hops in the order they are queried, that is, in the reverse of the order from the source to the receiver. For each hop, a line is printed showing the hop number (counted negatively to indicate that this is the reverse path); the multicast routing protocol; the threshold required to forward data (to the previous hop in the listing as indicated by the up-arrow character); and the cumulative delay for the query to reach that hop (valid only if the clocks are synchronized). The response ends with a line showing the round-trip time which measures the interval from when the query is issued until the response is received, both derived from the local system clock.

Mtrace/mstat packets use special IGMP packets with IGMP type codes of 0x1E and 0x1F.

12.2 Mstat

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 the network operator because it identifies nodes with high drop and duplicate counts. Duplicate counts are shown as negative drops.

The output of **mstat** provides a limited pictorial view of the path in the forward direction with data flow indicated by arrows pointing downward and the query path indicated by arrows pointing upward. For each hop, both the entry and exit addresses of the router are shown if different, along with the initial ttl required on the packet in order to be forwarded at this hop and the propagation delay across the hop assuming that the routers at both ends have synchronized clocks. The output consists of two columns, one for the overall multicast packet rate that does not contain lost/sent packets and a column for the (S,G)-specific case. The S,G statistics do not contain lost/sent packets.

12.3 Mrinfo

The simple **mrinfo** mechanism is based on the **ask_neighbors igmp** to display the configuration information from the target multicast router. The type of information displayed includes the Multicast of the router, code version, metrics, ttl-thresholds, protocols and status. This information, for instance, can be used by network operators to verify if bi-directional adjacencies exist. After the specified multicast router responds, the configuration is displayed.

12.4 Troubleshooting Configuration Command Reference

12.4.1 Command Hierarchies

- Operational Commands

12.4.1.1 Operational Commands

<GLOBAL>

— **mrinfo** {*ip-address* | *dns-name*} [**router** *router-instance* | **service-name** *service-name*]
— **mstat source** [*ip-address* | *dns-name*] **group** {*ip-address* | *dns-name*} [**destination** *ip-address* | *dns-name*] [**hop** *hop*] [**router** *router-instance* | **service-name** *service-name*] [**wait-time** *wait-time*]
— **mstat2 source** [*ip-address* | *dns-name* | starg] **group** {*ip-address* | *dns-name*} [**destination** *ip-address* | *dns-name*] [**hop** *hop*] [**router** *router-instance* | **service-name** *vprn-service-name*] [**wait-time** *seconds*]
— **mtrace source** [*ip-address* | *dns-name*] **group** {*ip-address* | *dns-name*} [**destination** *ip-address* | *dns-name*] [**hop** *hop*] [**router** *router-instance* | **service-name** *service-name*] [**wait-time** *wait-time*]
— **mtrace2 source** [*ip-address* | *dns-name* | *starg*] **group** {*ip-address* | *dns-name*} [**destination** *ip-address* | *dns-name*] [**hop** *hop*] [**router** *router-instance* | **service-name** *service-name*] [**wait-time** *wait-time*]

12.4.2 Command Descriptions

12.4.2.1 Operational Commands

mrinfo

Syntax **mrinfo** {*ip-address* **|** *dns-name*} [**router** *router-instance* **| service-name** *service-name*]

Context <global>

Description This command is used to print relevant multicast information from the target multicast router. Information displayed includes adjacency information, protocol, metrics, thresholds, and flags from the target multicast route.

Parameters *ip-address* — Specifies the IP address of the multicast-capable target router.

Values ipv4 unicast address (a.b.c.d)

dns-name — Specifies the DNS name (if DNS name resolution is configured), up to 63 characters.

router-instance — Specifies the router name or service ID for the router instance.

Values *router-name*: Base
vprn-service-id: 1 to 2147483647

Default Base

service-name — Specifies the service name up to 64 characters in length.

Output

Table 46 **Mrinfo 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.

Output Sample

```
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]
  10.1.1.3 -> 0.0.0.0 [1/0/pim/down/disabled]
  10.1.1.4 -> 0.0.0.0 [1/0/pim/querier/leaf]
  239.200.200.3 -> 239.200.200.5 [1/0/tunnel/pim]...
```

mstat

Syntax **mstat source** [*ip-address* | *dns-name*] **group** {*ip-address* | *dns-name*} [**destination** *ip-address* | *dns-name*] [**hop** *hop*] [**router** *router-instance* | **service-name** *service-name*] [**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.

Parameters **source** *ip-address* — Specifies the ip-address of the multicast capable target router.

Values ipv4 address (a.b.c.d)

dns-name — Specifies the DNS name (if DNS name resolution is configured), up to 63 characters.

group *ip-address* — Specifies the multicast address or DNS name of the group that resolves to the multicast group address that will be used. If the group is not specified, address 224.2.0.1 (the MBone audio) is used. This will suffice if packet loss statistics for a particular multicast group are not needed.

destination *ip-address* — Specifies either the IP address or the DNS name of the unicast destination. If this parameter is omitted the IP address of the system where the command is entered will be used. The receiver parameter can also be used to specify a local interface address as the destination address for sending the trace query. The response is also returned to the address specified as the receiver.

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

Values 1 to 255

Default 32 hops (infinity for the DVMRP routing protocol)

router-instance — Specifies the router name or service ID used to identify the router instance.

Values

router-name:	Base
service-id:	1 to 2147483647

Default Base

service-name — Specifies the service name up to 64 characters in length.

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

Values 1 to 60

Output

Table 47 **Mstat 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 two nodes a line is printed, following the same layout as other routers with an implementation derived from mrouted. Consider the following:

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

Output Sample

```
  Source          Response Dest     Overall       Packet Statistics for Traffic From
10.10.16.9        10.20.1.6        Mcast Pkt       10.10.16.9 to 239.5.6.7
     |         __/  rtt   29 ms     Rate           Lost/Sent = Pct Rate
     v        /                    ---------       --------------------
10.10.16.3
10.10.2.3         ?
     |       ^      ttl   2          1pps              0/0   = --     0 pps
     v       |
10.10.2.1
10.10.1.1         ?
     |       ^      ttl   3          1pps              0/0   = --     0 pps
     v       |
10.10.1.2
10.10.4.2         ?             Reached RP/Core
     |       ^      ttl   4          1pps              0/0   = --     0 pps
     v       |
10.10.4.4
10.10.6.4         ?
     |       ^      ttl   5          1pps              0/0   = --     0 pps
     v       |
10.10.6.5
10.10.10.5        ?
     |       \__    ttl   6          1pps              0/0   = --     0 pps
     v          \
10.10.10.6       10.20.1.6
Receiver         Query Source
```

mstat2

Syntax **mstat2 source** [*ip-address* **|** *dns-name* **|** *starg*] **group** {*ip-address* **|** *dns-name*} [**destination** *ip-address* | *dns-name*] [**hop** *hop*] [**router** *router-instance* **| service-name** *vprn-service-name*] [**wait-time** *seconds*]

Context <global>

Description This command traces a multicast path from a source to a receiver and displays multicast packet rate and loss information.

Parameters **source** *ip-address* — Specifies the ip-address of the multicast capable target router.

Values ipv4-prefix:
- a.b.c.d

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 to FFFF]H
- d: [0 to 255]D

dns-name — Specifies the DNS name (if DNS name resolution is configured), up to 63 characters.

starg — Specifies a static (*,G) entry. This command can only be enabled if no existing source addresses for this source is specified.

group *ip-address* — Specifies the multicast address or DNS name of the group that resolves to the multicast group address that will be used. If the group is not specified, address 224.2.0.1 (the MBone audio) is used. This will suffice if packet loss statistics for a particular multicast group are not needed.

Values ipv4-prefix:
- a.b.c.d

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 to FFFF]H
- d: [0 to 255]D

destination *ip-address* — Specifies either the IP address or the DNS name of the unicast destination. If this parameter is omitted the IP address of the system where the command is entered will be used. The receiver parameter can also be used to specify a local interface address as the destination address for sending the trace query. The response is also returned to the address specified as the receiver.

Values ipv4-prefix:
- a.b.c.d

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 to FFFF]H
- d: [0 to 255]D

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

Values 1 to 255

Default 32

router-instance — Specifies the router name or service ID used to identify the router instance.

Values

router-name:	Base
service-id:	1 to 2147483647

Default Base

vprn-service-name — Specifies the service name up to 64 characters in length.

seconds — Specifies the number of seconds to wait for the response.

Values 1 to 60

Default 3

Output

Table 48 **Mstat2 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 two nodes a line is printed, following the same layout as other routers with an implementation derived from mrouted. Consider the following:

- The forwarding information/error code is only displayed when different from “No Error”.
- “?” means there is no reverse DNS translation.

- There is no “Overall Mcast Pkt Rate” available in the PE for the VPRN case.

Output Sample

```
*A:Dut-A# mstat2 group 239.225.6.1 source 10.0.1.66
Mtrace2 from 150.0.1.66 via group 225.6.6.1 Querying full reverse path...
Waiting to accumulate statistics...Results after 10 seconds:
 Source        Response Dest    Overall     Packet Statistics For
Traffic From
10.0.1.66      10.0.0.1         Mcast Pkt    10.10.1.66 To 239.5.6.7
      |       __/  rtt 24.0ms     Rate       Lost/Sent = Pct  Rate
      v      /                    -------     ---------------------
10.0.1.6
10.0.1.6       ?
      |     ^      ttl    2        10 pps        0/100  =  0%   10 pps
      v     |
10.0.1.4
10.10.4.4       usilhc03-hb2.ndc.lucent.com Reached RP/Core
      |     ^      ttl    3        10 pps        0/100  =  0%   10 pps
      v     |
10.10.4.2
10.0.1.2       10.1.0.110.ap.yournet.ne.jp
      |      \__   ttl    4        10 pps        0/100  =  0%   10 pps
      v         \
10.0.1.1       10.0.0.1
   Receiver      Query Source

*A:Dut-A# mstat2  group ff05::225:6:6:1 source 3ffe::150:0:1:66
Mtrace2 from source
<S> = 3ffe::150:0:1:66
via group
<G> = ff05::225:6:6:1
Querying full reverse path...
Waiting to accumulate statistics...Results after 10 seconds:
Destination <D> = 3ffe::120:0:1:1
Response Destination <RD> = 3ffe::1
   Source        Response Dest    Overall     Packet Statistics For
Traffic From
<S>             <RD>            Mcast Pkt    Source <S> To Group <G>
      |       __/  rtt 23.0ms     Rate       Lost/Sent = Pct  Rate
      v      /                    -------     ---------------------
Remote Address ::
Incoming IF 4
3ffe::6 ?
Outgoing IF 3
      |     ^      ttl    2        20 pps        0/100  =  0%   10 pps
      v     |
Remote Address fe80::a248:1ff:fe01:2
Incoming IF 2
3ffe::5 ? Reached RP/Core
Outgoing IF 3
      |     ^      ttl    3        20 pps        0/100  =  0%   10 pps
      v     |
Remote Address fe80::a246:1ff:fe01:1
Incoming IF 3
3ffe::3 ?
Outgoing IF 2
      |      \__   ttl    4        30 pps        0/100  =  0%   10 pps
```

```
      v          \
<D>              <RD>
   Receiver       Query Source
```

mtrace

Syntax **mtrace source** [*ip-address* | *dns-name*] **group** {*ip-address* | *dns-name*} [**destination** *ip-address* | *dns-name*] [**hop** *hop*] [**router** *router-instance* | **service-name** *service-name*] [**wait-time** *wait-time*]

Context <global>

Description This command traces a multicast path from a source to a receiver.

Parameters **source** *ip-address* — Specifies the ip-address of the multicast capable target router.

Values ipv4 address (a.b.c.d)

dns-name — Specifies the DNS name (if DNS name resolution is configured). 63 characters maximum.

group *ip-address* — Specifies the multicast address or DNS name of the group that resolves to the multicast group address that will be used. If the group is not specified, address 224.2.0.1 (the MBone audio) will be used. This will suffice if packet loss statistics for a particular multicast group are not needed.

destination *ip-address* — Specifies either the IP address or the DNS name of the unicast destination. If this parameter is omitted the IP address of the system where the command is entered will be used. The receiver parameter can also be used to specify a local interface address as the destination address for sending the trace query. The response will also be returned to the address specified as the receiver.

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

Values 1 to 255

Default 32 hops (infinity for the DVMRP routing protocol)

router-instance — Specifies the router name or service ID used the identify the router instance.

Values

router-name:	“Base”
service-id:	1 to 2147483647

Default Base

service-name — Specifies the service name up to 64 characters in length.

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

Values 1 to 60

Output

Table 49 **Mtrace 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.

Output Sample

```
A:Dut-F# mtrace source 10.10.16.9 group 239.5.6.7

Mtrace from 10.10.16.9 via group 239.5.6.7
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.
```

mtrace2

Syntax **mtrace2 source** [*ip-address* | *dns-name* | *starg*] **group** {*ip-address* | *dns-name*} [**destination** *ip-address* | *dns-name*] [**hop** *hop*] [**router** *router-instance* | **service-name** *service-name*] [**wait-time** *wait-time*]

Context <global>

Description This command traces a multicast path from a source to a receiver.

Parameters **source** *ip-address* — Specifies the ip-address of the multicast capable target router.

Values ipv4-prefix:
- a.b.c.d

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 to FFFF]H
- d: [0 to 255]D

dns-name — Specifies the DNS name (if DNS name resolution is configured). 63 characters maximum.

starg — Specifies a static (*,G) entry. This command can only be enabled if no existing source addresses for this source is specified.

group *ip-address* — Specifies the multicast address or DNS name of the group that resolves to the multicast group address that will be used. If the group is not specified, address 224.2.0.1 (the MBone audio) will be used. This will suffice if packet loss statistics for a particular multicast group are not needed.

Values ipv4-prefix:

- a.b.c.d

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 to FFFF]H
- d: [0 to 255]D

destination *ip-address* — Specifies either the IP address or the DNS name of the unicast destination. If this parameter is omitted the IP address of the system where the command is entered will be used. The receiver parameter can also be used to specify a local interface address as the destination address for sending the trace query. The response will also be returned to the address specified as the receiver.

Values ipv4-prefix:

- a.b.c.d

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 to FFFF]H
- d: [0 to 255]D

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

Values 1 to 255

Default 32 hops (infinity for the DVMRP routing protocol)

router-instance — Specifies the router name or service ID used the identify the router instance.

Values

router-name: “Base”
service-id: 1 to 2147483647

Default Base

service-name — Specifies the service name, up to 64 characters.

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

Values 1 to 60

Output

Table 50 **Mtrace2 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.

Output Sample

```
*A:Dut-A# mtrace2 group 239.225.6.1 source 192.0.1.66
Mtrace2 from 192.0.1.66 via group 239.225.6.1 Querying full reverse path...
   0  1.1.0.110.ap.yournet.ne.jp (110.0.1.1)
  -1  2.1.0.110.ap.yournet.ne.jp (110.0.1.2)  rtg=ospf mrtg=pimSparseMode  thresh^ 1
  No Error
  -2  usilhc03-
hb2.ndc.lucent.com(10.10.4.4)rtg=ospf mrtg=pimSparseMode thresh^ 1 Reached RP/ Core
  -3  ? (10.0.1.6)  rtg=local mrtg=pimSparseMode  thresh^ 1  No Error
  -4  ? (10.0.1.66)
Round trip time 23.3 ms; total ttl of 3 required.

*A:Dut-A# mtrace2 group ff05::225:2:6:1 source 3ffe::255:0:1:66
Mtrace2 from source
<S> = 3ffe::255:0:1:66
via group
<G> = ff05::225:6:6:1
Querying full reverse path...
   0  ? (3ffe::120:0:1:1)
  -1  ? (3ffe::3)  IIF=3 OIF=2  rtg=ospf mrtg=pimSparseMode thresh^ N/A No Error
  -2  ? (3ffe::5)  IIF=2 OIF=3  rtg=ospf mrtg=pimSparseMode thresh^ N/A Reached RP/
Core
  -3  ? (3ffe::6)  IIF=4 OIF=3  rtg=local mrtg=pimSparseMode thresh^ N/A  No Error
  -4  ? (3ffe::150:0:1:66)
```

```
Round trip time 46.5 ms; total ttl of 3 required.
```

12.5 Show Command Reference

12.5.1 Command Hierarchies

- Show Commands

12.5.1.1 Show Commands

show
  — **router**
    — **tunnel-interface** [**protocol** *protocol*] [**senderAddr** *senderAddr*] [**rootNode** *rootNode*]

show
  — **router**
    — **ldp**
      — **bindings active**
    — **mvpn**
    — **mvpn-list** [**type** *type*] [**auto-discovery** *auto-discovery*] [**signalling** *signalling*] [**group** *group*]

show
  — **router**
    — **tunnel-table** [**summary**] [{**ipv4** | **ipv6**}]
    — **tunnel-table** [**protocol** *protocol*] {**ipv4** | **ipv6**}
    — **tunnel-table** [*ip-prefix*[/*mask*]] [**alternative**] [{**ipv4** | **ipv6**}] [**detail**]
    — **tunnel-table mpls-tp**
    — **tunnel-table** [*ip-prefix*[/*mask*]] **protocol** *protocol* [**detail**]
    — **tunnel-table** [*ip-prefix*[/*mask*]] **sdp** *sdp-id*

12.5.2 Command Descriptions

12.5.2.1 Show Commands

The command outputs in the following section are examples only; actual displays may differ depending on supported functionality and user configuration.

tunnel-interface

Syntax **tunnel-interface** [**protocol** *protocol*] [**senderAddr** *senderAddr*] [**rootNode** *rootNode*]

Context show>router

Description This command displays tunnel interface information.

Parameters *protocol* — Specifies the protocol.

Values ldp, rsvp

senderAddr — Specifies the IP address of the sender.

rootNode — Specifies to show root nodes.

Values Yes, No

Output The following is an example of router tunnel interface information.

Sample Output

```
*A:Dut-C# show router tunnel-interface
===============================================================================
 P2MP-RSVP P2MP-LDP Tunnel-Interfaces
===============================================================================
LSP/LDP           Type        SenderAddr          IfIndex            RootNode
-------------------------------------------------------------------------------
1                 ldp         10.20.1.2          73728              No
2                 ldp         10.20.1.2          73729              No
3                 ldp         10.20.1.2          73730              No
4                 ldp         10.20.1.2          73731              No
5                 ldp         10.20.1.2          73732              No
-------------------------------------------------------------------------------
Interfaces : 5
===============================================================================
*A:Dut-B# show router tunnel-interface
===============================================================================
 P2MP-RSVP P2MP-LDP Tunnel-Interfaces
===============================================================================
LSP/LDP           Type        SenderAddr          IfIndex            RootNode
-------------------------------------------------------------------------------
1                 ldp         10.20.1.2          73728              Yes
2                 ldp         10.20.1.2          73729              Yes
3                 ldp         10.20.1.2          73730              Yes
4                 ldp         10.20.1.2          73731              Yes
5                 ldp         10.20.1.2          73732              Yes
-------------------------------------------------------------------------------
Interfaces : 5
===============================================================================
```

bindings

Syntax **bindings active**

Context show>router>ldp

Description This command displays LDP bindings information.

Output The following output is an example of LDP active bindings information.

Sample Output

```
*A:Dut-A# show router ldp bindings active

========================================================================
Legend: U - Label In Use,  N - Label Not In Use, W - Label Withdrawn
        WP - Label Withdraw Pending, BU - Alternate For Fast Re-Route
        (S) - Static       (M) - Multi-homed Secondary Support
        (B) - BGP Next Hop (BU) - Alternate Next-hop for Fast Re-Route
========================================================================
LDP IPv4 Prefix Bindings (Active)
========================================================================
Prefix                  Op   IngLbl    EgrLbl    EgrIntf/LspId  EgrNextHop
------------------------------------------------------------------------
10.20.1.1/32            Pop  131071      --        --             --
10.20.1.2/32            Push   --      131071    1/1/1          10.10.1.2
10.20.1.2/32            Swap 131070    131071    1/1/1          10.10.1.2
10.20.1.2/32            Push   --      262141BU  1/1/2          10.10.2.3
10.20.1.2/32            Swap 131070    262141BU  1/1/2          10.10.2.3
10.20.1.3/32            Push   --      131069BU  1/1/1          10.10.1.2
10.20.1.3/32            Swap 131069    131069BU  1/1/1          10.10.1.2
10.20.1.3/32            Push   --      262143    1/1/2          10.10.2.3
10.20.1.3/32            Swap 131069    262143    1/1/2          10.10.2.3
10.20.1.4/32            Push   --      131068    1/1/1          10.10.1.2
10.20.1.4/32            Swap 131068    131068    1/1/1          10.10.1.2
10.20.1.4/32            Push   --      262140BU  1/1/2          10.10.2.3
10.20.1.4/32            Swap 131068    262140BU  1/1/2          10.10.2.3
10.20.1.5/32            Push   --      131067BU  1/1/1          10.10.1.2
10.20.1.5/32            Swap 131067    131067BU  1/1/1          10.10.1.2
10.20.1.5/32            Push   --      262139    1/1/2          10.10.2.3
10.20.1.5/32            Swap 131067    262139    1/1/2          10.10.2.3
10.20.1.6/32            Push   --      131066    1/1/1          10.10.1.2
10.20.1.6/32            Swap 131066    131066    1/1/1          10.10.1.2
10.20.1.6/32            Push   --      262138BU  1/1/2          10.10.2.3
10.20.1.6/32            Swap 131066    262138BU  1/1/2          10.10.2.3
------------------------------------------------------------------------

-------------------------------------------------------------------------------
No. of IPv4 Prefix Active Bindings: 10
===============================================================================

===============================================================================
LDP IPv6 Prefix Bindings (Active)
===============================================================================
Prefix                                    Op              IngLbl    EgrLbl
EgrNextHop                                EgrIf/LspId
-------------------------------------------------------------------------------
No Matching Entries Found
===============================================================================

===============================================================================
LDP Generic IPv4 P2MP Bindings (Active)
```

```
===============================================================================
P2MP-Id                                        Interface
RootAddr                                       Op              IngLbl    EgrLbl
EgrNH                                          EgrIf/LspId
-------------------------------------------------------------------------------
No Matching Entries Found
===============================================================================
===============================================================================
LDP Generic IPv6 P2MP Bindings (Active)
===============================================================================
P2MP-Id                                        Interface
RootAddr                                       Op              IngLbl    EgrLbl
EgrNH                                          EgrIf/LspId
-------------------------------------------------------------------------------
No Matching Entries Found
===============================================================================
===============================================================================
LDP In-Band-SSM IPv4 P2MP Bindings (Active)
===============================================================================
Source
Group                                          Interface
RootAddr                                       Op              IngLbl    EgrLbl
EgrNH                                          EgrIf/LspId
-------------------------------------------------------------------------------
No Matching Entries Found
===============================================================================
===============================================================================
LDP In-Band-SSM IPv6 P2MP Bindings (Active)
===============================================================================
Source
Group                                          Interface
RootAddr                                       Op              IngLbl    EgrLbl
EgrNH                                          EgrIf/LspId
-------------------------------------------------------------------------------
No Matching Entries Found
===============================================================================
===============================================================================
LDP In-Band-VPN-SSM IPv4 P2MP Bindings (Active)
===============================================================================
Source
Group                                          RD              Op
RootAddr                                       Interface       IngLbl    EgrLbl
EgrNH                                          EgrIf/LspId
-------------------------------------------------------------------------------
No Matching Entries Found
===============================================================================
===============================================================================
LDP In-Band-VPN-SSM IPv6 P2MP Bindings (Active)
===============================================================================
Source
Group                                          RD              Op
RootAddr                                       Interface       IngLbl    EgrLbl
EgrNH                                          EgrIf/LspId
-------------------------------------------------------------------------------
No Matching Entries Found
===============================================================================


*A:Dut-A# show router ldp bindings
```

```
========================================================================
LDP Bindings (IPv4 LSR ID 10.1.1.1:0)
             (IPv6 LSR ID ::[0])
===============================================================================
Legend: U - Label In Use, N - Label Not In Use, W - Label Withdrawn
        S - Status Signaled Up,  D - Status Signaled Down
        E - Epipe Service, V - VPLS Service, M - Mirror Service
        A - Apipe Service, F - Fpipe Service, I - IES Service, R - VPRN service
        P - Ipipe Service, WP - Label Withdraw Pending, C - Cpipe Service
        BU - Alternate For Fast Re-Route, TLV - (Type, Length: Value)
===============================================================================
LDP IPv4 Prefix Bindings
========================================================================
Prefix            Peer            IngLbl     EgrLbl EgrIntf/    EgrNextHop
                                                   LspId
------------------------------------------------------------------------
10.20.1.1/32      10.20.1.2       131071U     --     --          --
10.20.1.1/32      10.20.1.3       131071U     --     --          --
10.20.1.2/32      10.20.1.2         --       131071 1/1/1       10.10.1.2
10.20.1.2/32      10.20.1.3       131070U    262141 1/1/2       10.10.2.3
10.20.1.3/32      10.20.1.2       131069U    131069 1/1/1       10.10.1.2
10.20.1.3/32      10.20.1.3         --       262143 1/1/2       10.10.2.3
10.20.1.4/32      10.20.1.2       131068N    131068 1/1/1       10.10.1.2
10.20.1.4/32      10.20.1.3       131068BU    262140 1/1/2      10.10.2.3
10.20.1.5/32      10.20.1.2       131067U    131067 1/1/1       10.10.1.2
10.20.1.5/32      10.20.1.3       131067N    262139 1/1/2       10.10.2.3
10.20.1.6/32      10.20.1.2       131066N    131066 1/1/1       10.10.1.2
10.20.1.6/32      10.20.1.3       131066BU   262138 1/1/2       10.10.2.3
------------------------------------------------------------------------
No. of IPv4 Prefix Bindings: 12
===============================================================================
LDP IPv6 Prefix Bindings
===============================================================================
Prefix                                      IngLbl                    EgrLbl
Peer                                        EgrIntf/LspId
EgrNextHop
-------------------------------------------------------------------------------
No Matching Entries Found
===============================================================================
LDP Generic IPv4 P2MP Bindings
===============================================================================
P2MP-Id
RootAddr                                    Interface       IngLbl    EgrLbl
EgrNH                                       EgrIf/LspId
Peer
-------------------------------------------------------------------------------
100
10.1.1.1                                     Unknw             --      131051
10.90.90.2                                  1/1/6
10.2.2.2:0

104
10.1.1.1                                     Unknw             --      131050
10.90.90.2                                  1/1/6
10.2.2.2:0

600
10.1.1.1                                     Unknw             --      131049
10.90.90.2                                  1/1/6
```

```
10.2.2.2:0

700
10.1.1.1                                    Unknw             --       131048
10.90.90.2                                 1/1/6
10.2.2.2:0

800
10.1.1.1                                    Unknw             --       131047
10.90.90.2                                 1/1/6
10.2.2.2:0

900
10.1.1.1                                    Unknw             --       131046
10.90.90.2                                 1/1/6
10.2.2.2:0

1500
10.1.1.1                                    Unknw             --       131045
10.90.90.2                                 1/1/6
10.2.2.2:0

100
10.6.6.6                                    Unknw             --       131044
10.90.90.2                                 1/1/6
10.2.2.2:0

900
10.6.6.6                                    Unknw             --       131043
10.90.90.2                                 1/1/6
10.2.2.2:0
-------------------------------------------------------------------------------
No. of Generic IPv4 P2MP Bindings: 9
===============================================================================
LDP Generic IPv6 P2MP Bindings
===============================================================================
P2MP-Id
RootAddr                                   Interface       IngLbl    EgrLbl
EgrNH                                      EgrIf/LspId
Peer
-------------------------------------------------------------------------------
No Matching Entries Found
===============================================================================
LDP In-Band-SSM IPv4 P2MP Bindings
===============================================================================
Source
Group
RootAddr                                   Interface       IngLbl    EgrLbl
EgrNH                                      EgrIf/LspId
Peer
-------------------------------------------------------------------------------
No Matching Entries Found
===============================================================================
LDP In-Band-SSM IPv6 P2MP Bindings
===============================================================================
Source
Group
RootAddr                                   Interface       IngLbl    EgrLbl
EgrNH                                      EgrIf/LspId
```

```
Peer
-------------------------------------------------------------------------------
No Matching Entries Found
===============================================================================
LDP In-Band-VPN-SSM IPv4 P2MP Bindings
===============================================================================
Source
Group                                       RD
RootAddr                                    Interface        IngLbl    EgrLbl
EgrNH                                       EgrIf/LspId
Peer
-------------------------------------------------------------------------------
10.1.1.1
239.0.0.1                                  1.1.1.1:100
10.3.3.3                                    Unknwn             --         100
10.60.60.1                                 1/1/1
10.2.2.2:100

10.1.1.1
239.0.0.1                                  1.1.1.1:100
10.3.3.3                                    Unknwn             --         100
10.60.60.1                                 1/1/1
10.2.2.2:100

10.1.1.1
239.0.0.1                                  1.1.1.1:100
10.3.3.3                                    Unknwn             --         100
10.60.60.1                                 1/1/1
10.2.2.2:100

-------------------------------------------------------------------------------
No. of In-Band-VPN-SSM IPv4 P2MP Bindings: 3
===============================================================================
LDP In-Band-VPN-SSM IPv6 P2MP Bindings
===============================================================================
Source
Group                                       RD
RootAddr                                    Interface        IngLbl    EgrLbl
EgrNH                                       EgrIf/LspId
Peer
-------------------------------------------------------------------------------
10.1.1.1
239.0.0.1                                  1.1.1.1:100
2001:db8::3000                             Unknwn             --         100
10.60.60.1                                 1/1/1
10.2.2.2:100

10.1.1.1
239.0.0.1                                  1.1.1.1:100
2001:db8::3000                             Unknwn             --         100
10.60.60.1                                 1/1/1
10.2.2.2:100

10.1.1.1
239.0.0.1                                  1.1.1.1:100
2001:db8::3000                             Unknwn             --         100
10.60.60.1                                 1/1/1
10.2.2.2:100
-------------------------------------------------------------------------------
```

```
No. of In-Band-VPN-SSM IPv6 P2MP Bindings: 3
===============================================================================
LDP Service FEC 128 Bindings
===============================================================================
Type                                          VCId       SDPId      IngLbl  LMTU
Peer                                          SvcId                 EgrLbl  RMTU
-------------------------------------------------------------------------------
?-Eth                                         100        R. Src       --    None
10.2.2.2:0                                     Ukwn                  131023D 986

?-Eth                                         500        R. Src       --    None
10.2.2.2:0                                     Ukwn                  131022D 1386

?-Eth                                         2001       R. Src       --    None
10.2.2.2:0                                     Ukwn                  131019D 986

?-Eth                                         2003       R. Src       --    None
10.2.2.2:0                                     Ukwn                  131017D 986

?-Ipipe                                       1800       R. Src       --    None
10.2.2.2:0                                     Ukwn                  131014D 1486
-------------------------------------------------------------------------------
No. of VC Labels: 5
===============================================================================
LDP Service FEC 129 Bindings
===============================================================================
SAII                                            AGII        IngLbl    LMTU
TAII                                            Type        EgrLbl    RMTU
Peer                                            SvcId       SDPId
-------------------------------------------------------------------------------
No Matching Entries Found
===============================================================================
```

mvpn

Syntax **mvpn**

Context show>router router-instance

Description This command displays Multicast VPN related information. The router instance must be specified.

Output The following output is an example of MVPN information.

Sample Output

```
*A:Dut-C# show router 1 mvpn
===============================================================================
MVPN 1 configuration data
===============================================================================
signaling          : Bgp                  auto-discovery     : Default
UMH Selection      : Highest-Ip           SA withdrawn       : Disabled
intersite-shared   : Enabled              Persist SA         : Disabled
vrf-import         : N/A
vrf-export         : N/A
```

```
vrf-target          : unicast
C-Mcast Import RT   : target:10.20.1.4:105

ipmsi               : rsvp IpmsiTemplate
i-pmsi P2MP AdmSt   : Up
i-pmsi Tunnel Name  : IpmsiTemplate-1-74216
enable-bfd-root     : false                enable-bfd-leaf     : false
Mdt-type            : sender-receiver

BSR signalling      : none
Wildcard s-pmsi     : false
spmsi               : rsvp SpmsiTemplate
s-pmsi P2MP AdmSt   : Up
max-p2mp-spmsi      : 4000
data-delay-interval: 3 seconds
enable-asm-mdt      : N/A
data-threshold      : 224.0.0.0/4 --> 1 kbps
rx-threshold        : 224.0.0.0/4 --> pe-thres-add 2 --> pe-thres-delete 4
data-threshold      : ff00:db8:/8 --> 1 kbps
rx-threshold        : ff00:db8:/8 --> pe-thres-add 2 --> pe-thres-delete 4
===============================================================================

*A:Dut-D# show router 21 mvpn
===============================================================================
MVPN 21 configuration data
===============================================================================
signaling           : Bgp                  auto-discovery      : Default
UMH Selection       : Highest-Ip           SA withdrawn        : Disabled
intersite-shared    : Enabled              Persist SA          : Disabled
vrf-import          : N/A
vrf-export          : N/A
vrf-target          : unicast
C-Mcast Import RT   : target:10.20.1.4:106

ipmsi               : ldp
i-pmsi P2MP AdmSt   : Up
i-pmsi Tunnel Name  : mpls-if-74217
Mdt-type            : sender-receiver

BSR signalling      : none
Wildcard s-pmsi     : false
spmsi               : ldp
s-pmsi P2MP AdmSt   : Up
max-p2mp-spmsi      : 4000
data-delay-interval: 3 seconds
enable-asm-mdt      : N/A
data-threshold      : 224.0.0.0/4 --> 1 kbps
rx-threshold        : 224.0.0.0/4 --> pe-thres-add 2 --> pe-thres-delete 4
data-threshold      : ff00:db8:/8 --> 1 kbps
rx-threshold        : ff00:db8:/8 --> pe-thres-add 2 --> pe-thres-delete 4
===============================================================================
*A:Dut-D#
```

mvpn-list

Syntax **mvpn-list** [**type** *type*] [**auto-discovery** *auto-discovery*] [**signalling** *signalling*] [**group** *group*]

Context show>router

Description This command displays Multicast VPN list.

Parameters *type* — Specifies the MVPN type.

Values pim, svp, ldp

auto-discovery — Specifies the auto-discovery mode.

Values none, default, mdt-s

signalling — Specifies the signaling type.

Values bgp, pim

group — Specifies the group address.

Output The following output is an example of MVPN list information.

Sample Output

```
*A:Dut-D# show router mvpn-list
Legend: Sig = Signal  Pim-a = pim-asm  Pim-s = pim-ssm  A-D = Auto-Discovery
SR = Sender-Receiver  SO = Sender-Only  RO = Receiver-Only
===============================================================================
MVPN List
===============================================================================
VprnID    A-D      iPmsi/sPmsi GroupAddr/Lsp-Template          IPv4(S,G)/(*,G)
           Sig      Mdt-Type                                    IPv6(S,G)/(*,G)
-------------------------------------------------------------------------------
100       None     Pim-a/None  239.100.201.101                 0/0
           Pim      N/A                                         0/0
-------------------------------------------------------------------------------
Total Mvpns : 1
===============================================================================
Total                              PIM            RSVP           MLDP
-------------------------------------------------------------------------------
I-PMSI tunnels                     1              0              0
TX S-PMSI tunnels                  0              0              0
RX S-PMSI tunnels                  0              0              0
RX PSEUDO S-PMSI tunnels   0              0              0
-------------------------------------------------------------------------------
Total IPv4 (S,G)/(*,G) : 0/0
Total IPv6 (S,G)/(*,G) : 0/0
===============================================================================
*A:Dut-D#
```

tunnel-table

Syntax **tunnel-table** [**summary**] [{**ipv4** | **ipv6**}]
tunnel-table [**protocol** *protocol*] {**ipv4** | **ipv6**}
tunnel-table [*ip-prefix*[/*mask*]] [**alternative**] [{**ipv4** | **ipv6**}] [**detail**]
tunnel-table mpls-tp
tunnel-table [*ip-prefix*[/*mask*]] **protocol** *protocol* [**detail**]
tunnel-table [*ip-prefix*[/*mask*]] **sdp** *sdp-id*

Context show>router

Description This command displays tunnel table information.

Parameters **summary** — displays a summary of the tunnel table information

ipv4 — displays only tunnel table information for IPv4 addresses

ipv6 — displays only tunnel table information for IPv6 addresses

protocol — specifies the protocol

Values bgp, ldp, rsvp, sdp, ospf, isis, sr-te

ip-prefix/mask — the IPv4 or IPv6 prefix and, optionally, the mask of the tunnel

alternative — displays backup route details

detail — displays detailed tunnel table information

mpls-tp — displays MPLS TP tunnel table information

sdp-id — specifies the SDP ID

Values 1 to 17407

Output The following output is an example of table tunnel information.

Sample Output

```
A:Dut-C# show router tunnel-table
===============================================================================
Tunnel Table (Router: Base)
===============================================================================
Destination       Owner     Encap TunnelId  Pref     Nexthop        Metric
-------------------------------------------------------------------------------
10.0.0.1/32       isis (0)  MPLS  524309    11       1.3.4.4        10
10.20.1.2/32      isis (0)  MPLS  524312    11       1.2.3.2        10
10.20.1.4/32      isis (0)  MPLS  524310    11       1.3.4.4        10
10.20.1.5/32      isis (0)  MPLS  524311    11       1.2.3.2        20
-------------------------------------------------------------------------------
Flags: B = BGP backup route available
       E = inactive best-
external BGP route
===============================================================================
A:Dut-C#
```

```
*A:Dut-C# show router tunnel-table
===============================================================================
IPv4 Tunnel Table (Router: Base)
===============================================================================
Destination       Owner     Encap TunnelId  Pref     Nexthop        Metric
-------------------------------------------------------------------------------
10.20.1.1/32      ospf (0)  MPLS  524395    10       1.1.3.1        1000
10.20.1.2/32      ospf (0)  MPLS  524399    10       2.2.3.2        1000
10.20.1.4/32      ospf (0)  MPLS  524398    10       1.3.5.5        2000
10.20.1.4/32      ospf (0)  MPLS  524398    10       2.2.3.2        2000
10.20.1.5/32      ospf (0)  MPLS  524397    10       1.3.5.5        1000
10.20.1.6/32      ospf (0)  MPLS  524396    10       1.3.5.5        2000
-------------------------------------------------------------------------------
Flags: B = BGP backup route available
       E = inactive best-external BGP route
===============================================================================
*A:Dut-C#


*A:Dut-C# show router tunnel-table sdp 17407
========================================================================
Tunnel Table (Router: Base)
========================================================================
Destination        Owner Encap TunnelId  Pref     Nexthop        Metric
------------------------------------------------------------------------
239.0.68.0/32      sdp   MPLS  17407     5        239.0.68.0     0
========================================================================


*A:Dut-C>config>router>mpls>lsp# show router tunnel-table detail
===============================================================================
Tunnel Table (Router: Base)
===============================================================================
Destination      : 10.0.0.2/32
NextHop          : 10.1.4.4
Tunnel Flags     : exclude-for-lfa
Age              : 00h17m58s
Owner            : rsvp                Encap            : MPLS
Tunnel ID        : 115                 Preference       : 7
Tunnel Label     : 262054              Tunnel Metric    : 9
Tunnel MTU       : 1496
LSP ID           : 26116               Bypass Label     : 0
LSP Bandwidth    : 0                   LSP Weight       : 2
-------------------------------------------------------------------------------


show router tunnel-table detail
===============================================================================
Tunnel Table (Router: Base)
===============================================================================
Destination      : 10.0.0.1/32
NextHop          : 10.3.4.4
Tunnel Flags     : has-lfa exclude-for-igpshortcuts
Age              : 20h34m58s
Owner            : isis (0)            Encap            : MPLS
Tunnel ID        : 524309              Preference       : 11
Tunnel Label     : 20001               Tunnel Metric    : 10
Tunnel MTU       : 1382
-------------------------------------------------------------------------------
```

```
Destination      : 10.20.1.2/32
NextHop          : 10.2.3.2
Tunnel Flags     : has-lfa exclude-for-igpshortcuts
Age              : 20h35m04s
Owner            : isis (0)             Encap            : MPLS
Tunnel ID        : 524312               Preference       : 11
Tunnel Label     : 21002                Tunnel Metric    : 10
Tunnel MTU       : 1382
-------------------------------------------------------------------------------
Destination      : 10.20.1.4/32
NextHop          : 10.3.4.4
Tunnel Flags     : has-lfa exclude-for-igpshortcuts
Age              : 20h34m58s
Owner            : isis (0)             Encap            : MPLS
Tunnel ID        : 524310               Preference       : 11
Tunnel Label     : 21004                Tunnel Metric    : 10
Tunnel MTU       : 1382
-------------------------------------------------------------------------------
Destination      : 10.20.1.5/32
NextHop          : 10.2.3.2
Tunnel Flags     : has-lfa exclude-for-igpshortcuts
Age              : 20h34m58s
Owner            : isis (0)             Encap            : MPLS
Tunnel ID        : 524311               Preference       : 11
Tunnel Label     : 21005                Tunnel Metric    : 20
Tunnel MTU       : 1382
-------------------------------------------------------------------------------
Number of tunnel-table entries          : 4
Number of tunnel-table entries with LFA : 4
===============================================================================
A:Dut-C#
```

13 Standards and Protocol Support

Note: The information presented is subject to change without notice.

Nokia assumes no responsibility for inaccuracies contained herein.

Access Node Control Protocol (ANCP)

draft-ietf-ancp-protocol-02, *Protocol for Access Node Control Mechanism in Broadband Networks*

RFC 5851, *Framework and Requirements for an Access Node Control Mechanism in Broadband Multi-Service Networks*

Application Assurance (AA)

3GPP Release 12 (ADC rules over Gx interfaces)

RFC 3507, *Internet Content Adaptation Protocol (ICAP)*

Asynchronous Transfer Mode (ATM)

AF-ILMI-0065.000, *Integrated Local Management Interface (ILMI) Version 4.0*

AF-PHY-0086.001, *Inverse Multiplexing for ATM (IMA) Specification Version 1.1*

AF-TM-0121.000, *Traffic Management Specification Version 4.1*

AF-TM-0150.00, *Addendum to Traffic Management v4.1 optional minimum desired cell rate indication for UBR*

GR-1113-CORE, *Asynchronous Transfer Mode (ATM) and ATM Adaptation Layer (AAL) Protocols Generic Requirements, Issue 1*

GR-1248-CORE, *Generic Requirements for Operations of ATM Network Elements (NEs), Issue 3*

ITU-T I.432.1, *B-ISDN user-network interface - Physical layer specification: General characteristics (02/99)*

ITU-T I.610, *B-ISDN operation and maintenance principles and functions (11/95)*

RFC 1626, *Default IP MTU for use over ATM AAL5*

RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*

Bidirectional Forwarding Detection (BFD)

RFC 5880, *Bidirectional Forwarding Detection (BFD)*

RFC 5881, *Bidirectional Forwarding Detection (BFD) IPv4 and IPv6 (Single Hop)*

RFC 5883, *Bidirectional Forwarding Detection (BFD) for Multihop Paths*

RFC 7130, *Bidirectional Forwarding Detection (BFD) on Link Aggregation Group (LAG) Interfaces*

Border Gateway Protocol (BGP)

draft-hares-idr-update-attrib-low-bits-fix-01, *Update Attribute Flag Low Bits Clarification*

draft-ietf-idr-add-paths-guidelines-08, *Best Practices for Advertisement of Multiple Paths in IBGP*

draft-ietf-idr-best-external-03, *Advertisement of the best external route in BGP*

draft-ietf-idr-bgp-flowspec-oid-03, *Revised Validation Procedure for BGP Flow Specifications*

draft-ietf-idr-bgp-gr-notification-01, *Notification Message support for BGP Graceful Restart*

draft-ietf-idr-bgp-optimal-route-reflection-10, *BGP Optimal Route Reflection (BGP-ORR)*

draft-ietf-idr-error-handling-03, *Revised Error Handling for BGP UPDATE Messages*

draft-ietf-idr-flowspec-interfaceset-03, *Applying BGP flowspec rules on a specific interface set*

draft-ietf-idr-flowspec-path-redirect-05, *Flowspec Indirection-id Redirect* (localised ID)

draft-ietf-idr-flowspec-redirect-ip-02, *BGP Flow-Spec Redirect to IP Action*

draft-ietf-idr-link-bandwidth-03, *BGP Link Bandwidth Extended Community*

draft-ietf-sidr-origin-validation-signaling-04, *BGP Prefix Origin Validation State Extended Community*

draft-uttaro-idr-bgp-persistence-03, *Support for Long-lived BGP Graceful Restart*

RFC 1772, *Application of the Border Gateway Protocol in the Internet*

RFC 1997, *BGP Communities Attribute*

RFC 2385, *Protection of BGP Sessions via the TCP MD5 Signature Option*

RFC 2439, *BGP Route Flap Damping*

RFC 2545, *Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing*

RFC 2858, *Multiprotocol Extensions for BGP-4*

RFC 2918, *Route Refresh Capability for BGP-4*

RFC 3107, *Carrying Label Information in BGP-4*

RFC 3392, *Capabilities Advertisement with BGP-4*

RFC 4271, *A Border Gateway Protocol 4 (BGP-4)*

RFC 4360, *BGP Extended Communities Attribute*

RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*

RFC 4456, *BGP Route Reflection: An Alternative to Full Mesh Internal BGP (IBGP)*

RFC 4486, *Subcodes for BGP Cease Notification Message*

RFC 4659, *BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN*

RFC 4684, *Constrained Route Distribution for Border Gateway Protocol/ MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs)*

RFC 4724, *Graceful Restart Mechanism for BGP* (helper mode)

RFC 4760, *Multiprotocol Extensions for BGP-4*

RFC 4798, *Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)*

RFC 4893, *BGP Support for Four-octet AS Number Space*

RFC 5004, *Avoid BGP Best Path Transitions from One External to Another*

RFC 5065, *Autonomous System Confederations for BGP*

RFC 5291, *Outbound Route Filtering Capability for BGP-4*

RFC 5396, *Textual Representation of Autonomous System (AS) Numbers* (asplain)

RFC 5549, *Advertising IPv4 Network Layer Reachability Information with an IPv6 Next Hop*

RFC 5575, *Dissemination of Flow Specification Rules*

RFC 5668, *4-Octet AS Specific BGP Extended Community*

RFC 6286, *Autonomous-System-Wide Unique BGP Identifier for BGP-4*

RFC 6810, *The Resource Public Key Infrastructure (RPKI) to Router Protocol*

RFC 6811, *Prefix Origin Validation*

RFC 6996, *Autonomous System (AS) Reservation for Private Use*

RFC 7311, *The Accumulated IGP Metric Attribute for BGP*

RFC 7607, *Codification of AS 0 Processing*

RFC 7674, *Clarification of the Flowspec Redirect Extended Community*

RFC 7752, *North-Bound Distribution of Link-State and Traffic Engineering (TE) Information Using BGP*

RFC 7854, *BGP Monitoring Protocol (BMP)*

RFC 7911, *Advertisement of Multiple Paths in BGP*

RFC 7999, *BLACKHOLE Community*

RFC 8092, *BGP Large Communities Attribute*

Circuit Emulation

RFC 4553, *Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)*

RFC 5086, *Structure-Aware Time Division Multiplexed (TDM) Circuit Emulation Service over Packet Switched Network (CESoPSN)*

RFC 5287, *Control Protocol Extensions for the Setup of Time-Division Multiplexing (TDM) Pseudowires in MPLS Networks*

Ethernet

IEEE 802.1AB, *Station and Media Access Control Connectivity Discovery*
IEEE 802.1ad, *Provider Bridges*
IEEE 802.1ag, *Connectivity Fault Management*
IEEE 802.1ah, *Provider Backbone Bridges*
IEEE 802.1ak, *Multiple Registration Protocol*
IEEE 802.1aq, *Shortest Path Bridging*
IEEE 802.1ax, *Link Aggregation*
IEEE 802.1D, *MAC Bridges*
IEEE 802.1p, *Traffic Class Expediting*
IEEE 802.1Q, *Virtual LANs*
IEEE 802.1s, *Multiple Spanning Trees*
IEEE 802.1w, *Rapid Reconfiguration of Spanning Tree*
IEEE 802.1X, *Port Based Network Access Control*
IEEE 802.3ab, *1000BASE-T*
IEEE 802.3ac, *VLAN Tag*
IEEE 802.3ad, *Link Aggregation*
IEEE 802.3ae, *10 Gb/s Ethernet*
IEEE 802.3ah, *Ethernet in the First Mile*
IEEE 802.3ba, *40 Gb/s and 100 Gb/s Ethernet*
IEEE 802.3i, *Ethernet*
IEEE 802.3u, *Fast Ethernet*
IEEE 802.3x, *Ethernet Flow Control*
IEEE 802.3z, *Gigabit Ethernet*
ITU-T G.8031/Y.1342, *Ethernet Linear Protection Switching*
ITU-T G.8032/Y.1344, *Ethernet Ring Protection Switching*
ITU-T Y.1731, *OAM functions and mechanisms for Ethernet based networks*

Ethernet VPN (EVPN)

draft-ietf-bess-evpn-ac-df-01, *AC-Influenced Designated Forwarder Election for EVPN*
draft-ietf-bess-evpn-pref-df-01, *Preference-based EVPN DF Election*
draft-ietf-bess-evpn-prefix-advertisement-11, *IP Prefix Advertisement in EVPN*

draft-ietf-bess-evpn-proxy-arp-nd-04, *Operational Aspects of Proxy-ARP/ND in EVPN Networks*

draft-ietf-bess-evpn-vpls-seamless-integ-03, *(PBB-)EVPN Seamless Integration with (PBB-)VPLS*

draft-snr-bess-pbb-evpn-isid-cmacflush-01, *PBB-EVPN ISID-based CMAC-Flush*

RFC 7432, *BGP MPLS-Based Ethernet VPN*

RFC 7623, *Provider Backbone Bridging Combined with Ethernet VPN (PBB-EVPN)*

RFC 8214, *Virtual Private Wire Service Support in Ethernet VPN*

RFC 8317, *Ethernet-Tree (E-Tree) Support in Ethernet VPN (EVPN) an Provider Backbone Bridging EVPN (PBB-EVPN)*

RFC 8365, *A Network Virtualization Overlay Solution Using Ethernet VPN (EVPN)*

Frame Relay

ANSI T1.617 Annex D, *DSS1 - Signalling Specification For Frame Relay Bearer Service*

FRF.1.2, *PVC User-to-Network Interface (UNI) Implementation Agreement*

FRF.12, *Frame Relay Fragmentation Implementation Agreement*

FRF.16.1, *Multilink Frame Relay UNI/NNI Implementation Agreement*

FRF.5, *Frame Relay/ATM PVC Network Interworking Implementation*

FRF2.2, *PVC Network-to-Network Interface (NNI) Implementation Agreement*

ITU-T Q.933 Annex A, *Additional procedures for Permanent Virtual Connection (PVC) status management*

Generalized Multiprotocol Label Switching (GMPLS)

draft-ietf-ccamp-rsvp-te-srlg-collect-04, *RSVP-TE Extensions for Collecting SRLG Information*

RFC 3471, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description*

RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions*

RFC 4204, *Link Management Protocol (LMP)*

RFC 4208, *Generalized Multiprotocol Label Switching (GMPLS) User-Network Interface (UNI): Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Support for the Overlay Model*

RFC 4872, *RSVP-TE Extensions in Support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery*

RFC 5063, *Extensions to GMPLS Resource Reservation Protocol (RSVP) Graceful Restart* (helper mode)

gRPC Remote Procedure Calls (gRPC)

gnmi.proto, *gRPC Network Management Interface (gNMI), version 0.4.0*

gRPC Network Management Interface (gNMI), *Capabilities, Get, Set, Subscribe (ONCE, SAMPLE, ON_CHANGE)*

Intermediate System to Intermediate System (IS-IS)

draft-ietf-isis-mi-02, *IS-IS Multi-Instance*

draft-kaplan-isis-ext-eth-02, *Extended Ethernet Frame Size Support*

ISO/IEC 10589:2002, Second Edition, Nov. 2002, *Intermediate system to Intermediate system intra-domain routeing information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network Service (ISO 8473)*

RFC 1195, *Use of OSI IS-IS for Routing in TCP/IP and Dual Environments*

RFC 2973, *IS-IS Mesh Groups*

RFC 3359, *Reserved Type, Length and Value (TLV) Codepoints in Intermediate System to Intermediate System*

RFC 3719, *Recommendations for Interoperable Networks using Intermediate System to Intermediate System (IS-IS)*

RFC 3787, *Recommendations for Interoperable IP Networks using Intermediate System to Intermediate System (IS-IS)*

RFC 4971, *Intermediate System to Intermediate System (IS-IS) Extensions for Advertising Router Information*

RFC 5120, *M-ISIS: Multi Topology (MT) Routing in IS-IS*

RFC 5130, *A Policy Control Mechanism in IS-IS Using Administrative Tags*

RFC 5301, *Dynamic Hostname Exchange Mechanism for IS-IS*

RFC 5302, *Domain-wide Prefix Distribution with Two-Level IS-IS*

RFC 5303, *Three-Way Handshake for IS-IS Point-to-Point Adjacencies*

RFC 5304, *IS-IS Cryptographic Authentication*

RFC 5305, *IS-IS Extensions for Traffic Engineering TE*

RFC 5306, *Restart Signaling for IS-IS* (helper mode)

RFC 5307, *IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*

RFC 5308, *Routing IPv6 with IS-IS*

RFC 5309, *Point-to-Point Operation over LAN in Link State Routing Protocols*

RFC 5310, *IS-IS Generic Cryptographic Authentication*

RFC 6213, *IS-IS BFD-Enabled TLV*

RFC 6232, *Purge Originator Identification TLV for IS-IS*

RFC 6233, *IS-IS Registry Extension for Purges*

RFC 6329, *IS-IS Extensions Supporting IEEE 802.1aq Shortest Path Bridging*

RFC 7775, *IS-IS Route Preference for Extended IP and IPv6 Reachability*

RFC 7794, *IS-IS Prefix Attributes for Extended IPv4 and IPv6 Reachability*

RFC 8202, *IS-IS Multi-Instance* (single topology)

Internet Protocol (IP) — Fast Reroute

draft-ietf-rtgwg-lfa-manageability-08, *Operational management of Loop Free Alternates*

RFC 5286, *Basic Specification for IP Fast Reroute: Loop-Free Alternates*

RFC 7431, *Multicast-Only Fast Reroute*

RFC 7490, *Remote Loop-Free Alternate (LFA) Fast Reroute (FRR)*

Internet Protocol (IP) — General

draft-grant-tacacs-02, *The TACACS+ Protocol*

RFC 768, *User Datagram Protocol*

RFC 793, *Transmission Control Protocol*

RFC 854, *Telnet Protocol Specifications*

RFC 1350, *The TFTP Protocol (revision 2)*

RFC 2347, *TFTP Option Extension*

RFC 2348, *TFTP Blocksize Option*

RFC 2349, *TFTP Timeout Interval and Transfer Size Options*

RFC 2428, *FTP Extensions for IPv6 and NATs*

RFC 2784, *Generic Routing Encapsulation (GRE)*

RFC 2890, *Key and Sequence Number Extensions to GRE*

RFC 4250, *The Secure Shell (SSH) Protocol Assigned Numbers*

RFC 4251, *The Secure Shell (SSH) Protocol Architecture*

RFC 4252, *The Secure Shell (SSH) Authentication Protocol* (publickey, password)

RFC 4253, *The Secure Shell (SSH) Transport Layer Protocol*

RFC 4254, *The Secure Shell (SSH) Connection Protocol*

RFC 4632, *Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan*

RFC 5082, *The Generalized TTL Security Mechanism (GTSM)*

RFC 5656, *Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer* (ECDSA)

RFC 5925, *The TCP Authentication Option*

RFC 5926, *Cryptographic Algorithms for the TCP Authentication Option (TCP-AO)*

RFC 6398, *IP Router Alert Considerations and Usage* (MLD)

RFC 6528, *Defending against Sequence Number Attacks*

Internet Protocol (IP) — Multicast

cisco-ipmulticast/pim-autorp-spec01, *Auto-RP: Automatic discovery of Group-to-RP mappings for IP multicast* (version 1)

draft-dolganow-bess-mvpn-expl-track-01, *Explicit Tracking with Wild Card Routes in Multicast VPN*

draft-ietf-bier-mvpn-11, *Multicast VPN Using BIER*

draft-ietf-idmr-traceroute-ipm-07, *A "traceroute" facility for IP Multicast*

draft-ietf-l2vpn-vpls-pim-snooping-07, *Protocol Independent Multicast (PIM) over Virtual Private LAN Service (VPLS)*

draft-ietf-mboned-mtrace-v2-17, *Mtrace Version 2: Traceroute Facility for IP Multicast*

RFC 1112, *Host Extensions for IP Multicasting*

RFC 2236, *Internet Group Management Protocol, Version 2*

RFC 2365, *Administratively Scoped IP Multicast*

RFC 2375, *IPv6 Multicast Address Assignments*

RFC 2710, *Multicast Listener Discovery (MLD) for IPv6*

RFC 3306, *Unicast-Prefix-based IPv6 Multicast Addresses*

RFC 3376, *Internet Group Management Protocol, Version 3*

RFC 3446, *Anycast Rendevous Point (RP) mechanism using Protocol Independent Multicast (PIM) and Multicast Source Discovery Protocol (MSDP)*

RFC 3590, *Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*

RFC 3618, *Multicast Source Discovery Protocol (MSDP)*

RFC 3810, *Multicast Listener Discovery Version 2 (MLDv2) for IPv6*

RFC 3956, *Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address*

RFC 3973, *Protocol Independent Multicast - Dense Mode (PIM-DM): Protocol Specification (Revised)* (auto-RP groups)

RFC 4541, *Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches*

RFC 4604, *Using Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Protocol Version 2 (MLDv2) for Source-Specific Multicast*

RFC 4607, *Source-Specific Multicast for IP*

RFC 4608, *Source-Specific Protocol Independent Multicast in 232/8*

RFC 4610, *Anycast-RP Using Protocol Independent Multicast (PIM)*

RFC 4611, *Multicast Source Discovery Protocol (MSDP) Deployment Scenarios*

RFC 5059, *Bootstrap Router (BSR) Mechanism for Protocol Independent Multicast (PIM)*

RFC 5186, *Internet Group Management Protocol Version 3 (IGMPv3) / Multicast Listener Discovery Version 2 (MLDv2) and Multicast Routing Protocol Interaction*

RFC 5384, *The Protocol Independent Multicast (PIM) Join Attribute Format*

RFC 5496, *The Reverse Path Forwarding (RPF) Vector TLV*

RFC 6037, *Cisco Systems' Solution for Multicast in MPLS/BGP IP VPNs*

RFC 6512, *Using Multipoint LDP When the Backbone Has No Route to the Root*

RFC 6513, *Multicast in MPLS/BGP IP VPNs*

RFC 6514, *BGP Encodings and Procedures for Multicast in MPLS/IP VPNs*

RFC 6515, *IPv4 and IPv6 Infrastructure Addresses in BGP Updates for Multicast VPNs*

RFC 6516, *IPv6 Multicast VPN (MVPN) Support Using PIM Control Plane and Selective Provider Multicast Service Interface (S-PMSI) Join Messages*

RFC 6625, *Wildcards in Multicast VPN Auto-Discover Routes*

RFC 6826, *Multipoint LDP In-Band Signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Path*

RFC 7246, *Multipoint Label Distribution Protocol In-Band Signaling in a Virtual Routing and Forwarding (VRF) Table Context*

RFC 7385, *IANA Registry for P-Multicast Service Interface (PMSI) Tunnel Type Code Points*

RFC 7716, *Global Table Multicast with BGP Multicast VPN (BGP-MVPN) Procedures*

RFC 7761, *Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised)*

RFC 8279, *Multicast Using Bit Index Explicit Replication (BIER)*

RFC 8296, *Encapsulation for Bit Index Explicit Replication (BIER) in MPLS and Non-MPLS Networks* (MPLS encapsulation)

RFC 8401, *Bit Index Explicit Replication (BIER) Support via IS-IS*

Internet Protocol (IP) — Version 4

RFC 791, *Internet Protocol*

RFC 792, *Internet Control Message Protocol*

RFC 826, *An Ethernet Address Resolution Protocol*

RFC 951, *Bootstrap Protocol (BOOTP)*

RFC 1034, *Domain Names - Concepts and Facilities*

RFC 1035, *Domain Names - Implementation and Specification*

RFC 1191, *Path MTU Discovery* (router specification)

RFC 1519, *Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy*

RFC 1534, *Interoperation between DHCP and BOOTP*

RFC 1542, *Clarifications and Extensions for the Bootstrap Protocol*

RFC 1812, *Requirements for IPv4 Routers*

RFC 1918, *Address Allocation for Private Internets*

RFC 2003, *IP Encapsulation within IP*

RFC 2131, *Dynamic Host Configuration Protocol*

RFC 2132, *DHCP Options and BOOTP Vendor Extensions*

RFC 2401, *Security Architecture for Internet Protocol*

RFC 3021, *Using 31-Bit Prefixes on IPv4 Point-to-Point Links*

RFC 3046, *DHCP Relay Agent Information Option (Option 82)*

RFC 3768, *Virtual Router Redundancy Protocol (VRRP)*

RFC 4884, *Extended ICMP to Support Multi-Part Messages* (ICMPv4 and ICMPv6 Time Exceeded)

Internet Protocol (IP) — Version 6

RFC 2464, *Transmission of IPv6 Packets over Ethernet Networks*

RFC 2529, *Transmission of IPv6 over IPv4 Domains without Explicit Tunnels*

RFC 3122, *Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification*

RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

RFC 3587, *IPv6 Global Unicast Address Format*

RFC 3596, *DNS Extensions to Support IP version 6*

RFC 3633, *IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6*

RFC 3646, *DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*

RFC 3736, *Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6*

RFC 3971, *SEcure Neighbor Discovery (SEND)*

RFC 3972, *Cryptographically Generated Addresses (CGA)*

RFC 4007, *IPv6 Scoped Address Architecture*

RFC 4193, *Unique Local IPv6 Unicast Addresses*

RFC 4291, *Internet Protocol Version 6 (IPv6) Addressing Architecture*

RFC 4443, *Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification*

RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*

RFC 4862, *IPv6 Stateless Address Autoconfiguration* (router functions)

RFC 4890, *Recommendations for Filtering ICMPv6 Messages in Firewalls*

RFC 4941, *Privacy Extensions for Stateless Address Autoconfiguration in IPv6*

RFC 5007, *DHCPv6 Leasequery*

RFC 5095, *Deprecation of Type 0 Routing Headers in IPv6*

RFC 5722, *Handling of Overlapping IPv6 Fragments*

RFC 5798, *Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6* (IPv6)

RFC 5952, *A Recommendation for IPv6 Address Text Representation*

RFC 6092, *Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service* (Internet Control and Management, Upper-Layer Transport Protocols, UDP Filters, IPsec and Internet Key Exchange (IKE), TCP Filters)

RFC 6106, *IPv6 Router Advertisement Options for DNS Configuration*

RFC 6164, *Using 127-Bit IPv6 Prefixes on Inter-Router Links*

RFC 8021, *Generation of IPv6 Atomic Fragments Considered Harmful*

RFC 8200, *Internet Protocol, Version 6 (IPv6) Specification*

RFC 8201, *Path MTU Discovery for IP version 6*

Internet Protocol Security (IPsec)

draft-ietf-ipsec-isakmp-mode-cfg-05, *The ISAKMP Configuration Method*

draft-ietf-ipsec-isakmp-xauth-06, *Extended Authentication within ISAKMP/Oakley (XAUTH)*

RFC 2401, *Security Architecture for the Internet Protocol*

RFC 2403, *The Use of HMAC-MD5-96 within ESP and AH*

RFC 2404, *The Use of HMAC-SHA-1-96 within ESP and AH*

RFC 2405, *The ESP DES-CBC Cipher Algorithm With Explicit IV*

RFC 2406, *IP Encapsulating Security Payload (ESP)*

RFC 2407, *IPsec Domain of Interpretation for ISAKMP (IPsec DoI)*

RFC 2408, *Internet Security Association and Key Management Protocol (ISAKMP)*

RFC 2409, *The Internet Key Exchange (IKE)*

RFC 2410, *The NULL Encryption Algorithm and Its Use With IPsec*

RFC 3526, *More Modular Exponential (MODP) Diffie-Hellman group for Internet Key Exchange (IKE)*

RFC 3566, *The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec*

RFC 3602, *The AES-CBC Cipher Algorithm and Its Use with IPsec*

RFC 3706, *A Traffic-Based Method of Detecting Dead Internet Key Exchange (IKE) Peers*

RFC 3947, *Negotiation of NAT-Traversal in the IKE*

RFC 3948, *UDP Encapsulation of IPsec ESP Packets*

RFC 4106, *The Use of Galois/Counter Mode (GCM) in IPsec ESP*

RFC 4210, *Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)*

RFC 4211, *Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)*

RFC 4301, *Security Architecture for the Internet Protocol*

RFC 4303, *IP Encapsulating Security Payload*

RFC 4307, *Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)*

RFC 4308, *Cryptographic Suites for IPsec*

RFC 4434, *The AES-XCBC-PRF-128 Algorithm for the Internet Key Exchange Protocol (IKE)*

RFC 4543, *The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH*

RFC 4868, *Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPSec*

RFC 4945, *The Internet IP Security PKI Profile of IKEv1/ISAKMP, IKEv2 and PKIX*

RFC 5019, *The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments*

RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*

RFC 5282, *Using Authenticated Encryption Algorithms with the Encrypted Payload of the IKEv2 Protocol*

RFC 5903, *ECP Groups for IKE and IKEv2*

RFC 5998, *An Extension for EAP-Only Authentication in IKEv2*

RFC 6379, *Suite B Cryptographic Suites for IPsec*

RFC 6380, *Suite B Profile for Internet Protocol Security (IPsec)*

RFC 6712, *Internet X.509 Public Key Infrastructure -- HTTP Transfer for the Certificate Management Protocol (CMP)*

RFC 6960, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*

RFC 7296, *Internet Key Exchange Protocol Version 2 (IKEv2)*

RFC 7321, *Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)*

RFC 7383, *Internet Key Exchange Protocol Version 2 (IKEv2) Message Fragmentation*

RFC 7427, *Signature Authentication in the Internet Key Exchange Version 2 (IKEv2)*

RFC 7468, *Textual Encodings of PKIX, PKCS, and CMS Structures*

Label Distribution Protocol (LDP)

draft-ietf-mpls-ldp-ip-pw-capability-09, *Controlling State Advertisements Of Non-negotiated LDP Applications*

draft-pdutta-mpls-ldp-adj-capability-00, *LDP Adjacency Capabilities*

draft-pdutta-mpls-ldp-v2-00, *LDP Version 2*

draft-pdutta-mpls-mldp-up-redundancy-00, *Upstream LSR Redundancy for Multi-point LDP Tunnels*

draft-pdutta-mpls-multi-ldp-instance-00, *Multiple LDP Instances*

draft-pdutta-mpls-tldp-hello-reduce-04, *Targeted LDP Hello Reduction*

RFC 3037, *LDP Applicability*

RFC 3478, *Graceful Restart Mechanism for Label Distribution Protocol* (helper mode)

RFC 5036, *LDP Specification*

RFC 5283, *LDP Extension for Inter-Area Label Switched Paths (LSPs)*

RFC 5443, *LDP IGP Synchronization*

RFC 5561, *LDP Capabilities*

RFC 5919, *Signaling LDP Label Advertisement Completion*

RFC 6388, *Label Distribution Protocol Extensions for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*

RFC 6512, *Using Multipoint LDP When the Backbone Has No Route to the Root*

RFC 6826, *Multipoint LDP in-band signaling for Point-to-Multipoint and Multipoint-to-Multipoint Label Switched Paths*

RFC 7032, *LDP Downstream-on-Demand in Seamless MPLS*

RFC 7552, *Updates to LDP for IPv6*

Layer Two Tunneling Protocol (L2TP) Network Server (LNS)

draft-mammoliti-l2tp-accessline-avp-04, *Layer 2 Tunneling Protocol (L2TP) Access Line Information Attribute Value Pair (AVP) Extensions*

RFC 2661, *Layer Two Tunneling Protocol "L2TP"*

RFC 2809, *Implementation of L2TP Compulsory Tunneling via RADIUS*

RFC 3438, *Layer Two Tunneling Protocol (L2TP) Internet Assigned Numbers: Internet Assigned Numbers Authority (IANA) Considerations Update*

RFC 3931, *Layer Two Tunneling Protocol - Version 3 (L2TPv3)*

RFC 4719, *Transport of Ethernet Frames over Layer 2 Tunneling Protocol Version 3 (L2TPv3)*

RFC 4951, *Fail Over Extensions for Layer 2 Tunneling Protocol (L2TP) "failover"*

Management

draft-ieft-snmpv3-update-mib-05, *Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)*

draft-ietf-isis-wg-mib-06, *Management Information Base for Intermediate System to Intermediate System (IS-IS)*

draft-ietf-mboned-msdp-mib-01, *Multicast Source Discovery protocol MIB*

draft-ietf-mpls-ldp-mib-07, *Definitions of Managed Objects for the Multiprotocol Label Switching, Label Distribution Protocol (LDP)*

draft-ietf-mpls-lsr-mib-06, *Multiprotocol Label Switching (MPLS) Label Switching Router (LSR) Management Information Base Using SMIv2*

draft-ietf-mpls-te-mib-04, *Multiprotocol Label Switching (MPLS) Traffic Engineering Management Information Base*

draft-ietf-ospf-mib-update-08, *OSPF Version 2 Management Information Base*

draft-ietf-vrrp-unified-mib-06, *Definitions of Managed Objects for the VRRP over IPv4 and IPv6* (IPv6)

ianaaddressfamilynumbers-mib, *IANA-ADDRESS-FAMILY-NUMBERS-MIB*

ianagmplstc-mib, *IANA-GMPLS-TC-MIB*

ianaiftype-mib, *IANAifType-MIB*

ianaiprouteprotocol-mib, *IANA-RTPROTO-MIB*

IEEE8021-CFM-MIB, *IEEE P802.1ag(TM) CFM MIB*

IEEE8021-PAE-MIB, *IEEE 802.1X MIB*

IEEE8023-LAG-MIB, *IEEE 802.3ad MIB*

LLDP-MIB, *IEEE P802.1AB(TM) LLDP MIB*

openconfig-bgp.yang version 3.0.1, *BGP Module*

openconfig-bgp-common.yang version 3.0.1, *BGP Common Module*

openconfig-bgp-common-multiprotocol.yang version 3.0.1, *BGP Common Multiprotocol Module*

openconfig-bgp-common-structure.yang version 3.0.1, *BGP Common Structure Module*

openconfig-bgp-global.yang version 3.0.1, *BGP Global Module*

openconfig-bgp-neighbor.yang version 3.0.1, *BGP Neighbor Module*

openconfig-bgp-peer-group.yang version 3.0.1, *BGP Peer Group Module*

openconfig-bgp-policy.yang version 4.0.1, *BGP Policy Module*

openconfig-if-aggregate.yang version 2.0.0, *Interfaces Aggregated Model*

openconfig-if-ethernet.yang version 2.0.0, *Interfaces Ethernet Model*

openconfig-if-ip.yang version 2.0.0, *Interfaces IP Module*

openconfig-if-ip-ext.yang version 2.0.0, *Interfaces IP Extensions Module*

openconfig-interfaces.yang version 2.0.0, *Interfaces Module* openconfig-isis.yang version 0.3.0, *IS-IS Module*

openconfig-isis-lsp.yang version 0.3.0, *IS-IS LSP Module*

openconfig-isis-routing.yang version 0.3.0, *IS-IS Routing Module*

openconfig-lacp.yang version 1.1.0, *LACP Module*

openconfig-lldp.yang version 0.1.0, *LLDP Module*

openconfig-local-routing.yang version 1.0.1, *Local Routing Module*

openconfig-network-instance.yang version 0.8.0, *Network Instance Module*

openconfig-routing-policy.yang version 3.0.0, *Routing Policy Module*

openconfig-vlan.yang version 2.0.0, *VLAN Module*

RFC 1157, *A Simple Network Management Protocol (SNMP)*

RFC 1212, *Concise MIB Definitions*

RFC 1213, *Management Information Base for Network Management of TCP/IP-based Internets: MIB-II*

RFC 1215, *A Convention for Defining Traps for use with the SNMP*

RFC 1724, *RIP Version 2 MIB Extension*

RFC 1901, *Introduction to Community-based SNMPv2*

RFC 2021, *Remote Network Monitoring Management Information Base Version 2 using SMIv2*

RFC 2115, *Management Information Base for Frame Relay DTEs Using SMIv2*

RFC 2206, *RSVP Management Information Base using SMIv2*

RFC 2213, *Integrated Services Management Information Base using SMIv2*

RFC 2494, *Definitions of Managed Objects for the DS0 and DS0 Bundle Interface Type*

RFC 2514, *Definitions of Textual Conventions and OBJECT-IDENTITIES for ATM Management*

RFC 2515, *Definitions of Managed Objects for ATM Management*

RFC 2570, *SNMP Version 3 Framework*

RFC 2571, *An Architecture for Describing SNMP Management Frameworks*

RFC 2572, *Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)*

RFC 2573, *SNMP Applications*

RFC 2574, *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*

RFC 2575, *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*

RFC 2578, *Structure of Management Information Version 2 (SMIv2)*

RFC 2579, *Textual Conventions for SMIv2*

RFC 2580, *Conformance Statements for SMIv2*

RFC 2787, *Definitions of Managed Objects for the Virtual Router Redundancy Protocol*

RFC 2819, *Remote Network Monitoring Management Information Base*

RFC 2856, *Textual Conventions for Additional High Capacity Data Types*

RFC 2863, *The Interfaces Group MIB*

RFC 2864, *The Inverted Stack Table Extension to the Interfaces Group MIB*

RFC 2933, *Internet Group Management Protocol MIB*

RFC 3014, *Notification Log MIB*

RFC 3164, *The BSD syslog Protocol*

RFC 3165, *Definitions of Managed Objects for the Delegation of Management Scripts*

RFC 3231, *Definitions of Managed Objects for Scheduling Management Operations*

RFC 3273, *Remote Network Monitoring Management Information Base for High Capacity Networks*

RFC 3416. *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*

RFC 3417, *Transport Mappings for the Simple Network Management Protocol (SNMP)* (SNMP over UDP over IPv4)

RFC 3419, *Textual Conventions for Transport Addresses*

RFC 3498, *Definitions of Managed Objects for Synchronous Optical Network (SONET) Linear Automatic Protection Switching (APS) Architectures*

RFC 3584, *Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*

RFC 3592, *Definitions of Managed Objects for the Synchronous Optical Network/ Synchronous Digital Hierarchy (SONET/SDH) Interface Type*

RFC 3593, *Textual Conventions for MIB Modules Using Performance History Based on 15 Minute Intervals*

RFC 3635, *Definitions of Managed Objects for the Ethernet-like Interface Types*

RFC 3637, *Definitions of Managed Objects for the Ethernet WAN Interface Sublayer*

RFC 3826, *The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP User-based Security Model*

RFC 3877, *Alarm Management Information Base (MIB)*

RFC 3895, *Definitions of Managed Objects for the DS1, E1, DS2, and E2 Interface Types*

RFC 3896, *Definitions of Managed Objects for the DS3/E3 Interface Type*

RFC 4001, *Textual Conventions for Internet Network Addresses*

RFC 4022, *Management Information Base for the Transmission Control Protocol (TCP)*

RFC 4113, *Management Information Base for the User Datagram Protocol (UDP)*

RFC 4220, *Traffic Engineering Link Management Information Base*

RFC 4273, *Definitions of Managed Objects for BGP-4*

RFC 4292, *IP Forwarding Table MIB*

RFC 4293, *Management Information Base for the Internet Protocol (IP)*

RFC 4379, *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*

RFC 4511, *Lightweight Directory Access Protocol (LDAP): The Protocol*

RFC 4513, *Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms* (TLS)

RFC 4631, *Link Management Protocol (LMP) Management Information Base (MIB)*

RFC 4878, *Definitions and Managed Objects for Operations, Administration, and Maintenance (OAM) Functions on Ethernet-Like Interfaces*

RFC 5101, *Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information*

RFC 5102, *Information Model for IP Flow Information Export*

RFC 5246, *The Transport Layer Security (TLS) Protocol Version 1.2* (TLS client, RSA public key)

RFC 6424, *Mechanism for Performing Label Switched Path Ping (LSP Ping) over MPLS Tunnels*

RFC 6425, *Detecting Data Plane Failures in Point-to-Multipoint Multiprotocol Label Switching (MPLS) - Extensions to LSP Ping*

RFC 6991, *Common YANG Data Types*

RFC 7420, *Path Computation Element Communication Protocol (PCEP) Management Information Base (MIB) Module*

RFC 7950, *The YANG 1.1 Data Modeling Language*

SFLOW-MIB, *sFlow MIB Version 1.3 (Draft 5)*

Multiprotocol Label Switching — Transport Profile (MPLS-TP)

RFC 5586, *MPLS Generic Associated Channel*

RFC 5921, *A Framework for MPLS in Transport Networks*

RFC 5960, *MPLS Transport Profile Data Plane Architecture*

RFC 6370, *MPLS Transport Profile (MPLS-TP) Identifiers*

RFC 6378, *MPLS Transport Profile (MPLS-TP) Linear Protection*

RFC 6426, *MPLS On-Demand Connectivity and Route Tracing*

RFC 6427, *MPLS Fault Management Operations, Administration, and Maintenance (OAM)*

RFC 6428, *Proactive Connectivity Verification, Continuity Check and Remote Defect indication for MPLS Transport Profile*

RFC 6478, *Pseudowire Status for Static Pseudowires*

RFC 7213, *MPLS Transport Profile (MPLS-TP) Next-Hop Ethernet Addressing*

Multiprotocol Label Switching (MPLS)

draft-ietf-teas-sr-rsvp-coexistence-rec-02, *Recommendations for RSVP-TE and Segment Routing LSP co-existence*

RFC 3031, *Multiprotocol Label Switching Architecture*

RFC 3032, *MPLS Label Stack Encoding*

RFC 3443, *Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks*

RFC 4023, *Encapsulating MPLS in IP or Generic Routing Encapsulation (GRE)*

RFC 4182, *Removing a Restriction on the use of MPLS Explicit NULL*

RFC 5332, *MPLS Multicast Encapsulations*

RFC 5884, *Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)*

RFC 6790, *The Use of Entropy Labels in MPLS Forwarding*

RFC 7510, *Encapsulating MPLS in UDP*

Network Address Translation (NAT)

draft-ietf-behave-address-format-10, *IPv6 Addressing of IPv4/IPv6 Translators*

draft-ietf-behave-v6v4-xlate-23, *IP/ICMP Translation Algorithm*

draft-miles-behave-l2nat-00, *Layer2-Aware NAT*

draft-nishitani-cgn-02, *Common Functions of Large Scale NAT (LSN)*

RFC 4787, *Network Address Translation (NAT) Behavioral Requirements for Unicast UDP*

RFC 5382, *NAT Behavioral Requirements for TCP*

RFC 5508, *NAT Behavioral Requirements for ICMP*

RFC 6146, *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*

RFC 6333, *Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion*

RFC 6334, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6) Option for Dual-Stack Lite*

RFC 6887, *Port Control Protocol (PCP)*

RFC 6888, *Common Requirements For Carrier-Grade NATs (CGNs)*

RFC 7915, *IP/ICMP Translation Algorithm*

Network Configuration Protocol (NETCONF)

RFC 5277, *NETCONF Event Notifications*

RFC 6022, *YANG Module for NETCONF Monitoring*

RFC 6241, *Network Configuration Protocol (NETCONF)*

RFC 6242, *Using the NETCONF Protocol over Secure Shell (SSH)*

RFC 6243, *With-defaults Capability for NETCONF*

RFC 7895, *YANG Module Library*

Open Shortest Path First (OSPF)

draft-ietf-ospf-ospfv3-lsa-extend-13, *OSPFv3 LSA Extendibility*

RFC 1586, *Guidelines for Running OSPF Over Frame Relay Networks*

RFC 1765, *OSPF Database Overflow*

RFC 2328, *OSPF Version 2*

RFC 3101, *The OSPF Not-So-Stubby Area (NSSA) Option*

RFC 3509, *Alternative Implementations of OSPF Area Border Routers*

RFC 3623, *Graceful OSPF Restart Graceful OSPF Restart* (helper mode)

RFC 3630, *Traffic Engineering (TE) Extensions to OSPF Version 2*

RFC 4203, *OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)*

RFC 4222, *Prioritized Treatment of Specific OSPF Version 2 Packets and Congestion Avoidance*

RFC 4552, *Authentication/Confidentiality for OSPFv3*

RFC 4576, *Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)*

RFC 4577, *OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)*

RFC 5185, *OSPF Multi-Area Adjacency*

RFC 5187, *OSPFv3 Graceful Restart* (helper mode)

RFC 5243, *OSPF Database Exchange Summary List Optimization*

RFC 5250, *The OSPF Opaque LSA Option*

RFC 5309, *Point-to-Point Operation over LAN in Link State Routing Protocols*

RFC 5340, *OSPF for IPv6*

RFC 5709, *OSPFv2 HMAC-SHA Cryptographic Authentication*

RFC 5838, *Support of Address Families in OSPFv3*

RFC 6987, *OSPF Stub Router Advertisement*

RFC 7684, *OSPFv2 Prefix/Link Attribute Advertisement*

RFC 7770, *Extensions to OSPF for Advertising Optional Router Capabilities*

OpenFlow

TS-007, *OpenFlow Switch Specification Version 1.3.1* (OpenFlow-hybrid switches)

Path Computation Element Protocol (PCEP)

draft-alvarez-pce-path-profiles-04, *PCE Path Profiles*
draft-ietf-pce-segment-routing-08, *PCEP Extensions for Segment Routing*
draft-ietf-pce-stateful-pce-14, *PCEP Extensions for Stateful PCE*
RFC 5440, *Path Computation Element (PCE) Communication Protocol (PCEP)*

Point-to-Point Protocol (PPP)

RFC 1332, *The PPP Internet Protocol Control Protocol (IPCP)*
RFC 1377, *The PPP OSI Network Layer Control Protocol (OSINLCP)*
RFC 1661, *The Point-to-Point Protocol (PPP)*
RFC 1662, *PPP in HDLC-like Framing*
RFC 1877, *PPP Internet Protocol Control Protocol Extensions for Name Server Addresses*
RFC 1989, *PPP Link Quality Monitoring*
RFC 1990, *The PPP Multilink Protocol (MP)*
RFC 1994, *PPP Challenge Handshake Authentication Protocol (CHAP)*
RFC 2153, *PPP Vendor Extensions*
RFC 2516, *A Method for Transmitting PPP Over Ethernet (PPPoE)*
RFC 2615, *PPP over SONET/SDH*
RFC 2686, *The Multi-Class Extension to Multi-Link PPP*
RFC 2878, *PPP Bridging Control Protocol (BCP)*
RFC 4638, *Accommodating a Maximum Transit Unit/Maximum Receive Unit (MTU/MRU) Greater Than 1492 in the Point-to-Point Protocol over Ethernet (PPPoE)*
RFC 5072, *IP Version 6 over PPP*

Policy Management and Credit Control

3GPP TS 29.212 Release 11, *Policy and Charging Control (PCC); Reference points* (Gx support as it applies to wireline environment (BNG))
RFC 3588, *Diameter Base Protocol*
RFC 4006, *Diameter Credit-Control Application*

Pseudowire

draft-ietf-l2vpn-vpws-iw-oam-04, *OAM Procedures for VPWS Interworking*

MFA Forum 12.0.0, *Multiservice Interworking - Ethernet over MPLS*

MFA Forum 13.0.0, *Fault Management for Multiservice Interworking v1.0*

MFA Forum 16.0.0, *Multiservice Interworking - IP over MPLS*

MFA Forum 9.0.0, *The Use of Virtual trunks for ATM/MPLS Control Plane Interworking*

RFC 3916, *Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)*

RFC 3985, *Pseudo Wire Emulation Edge-to-Edge (PWE3)*

RFC 4385, *Pseudo Wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN*

RFC 4446, *IANA Allocations for Pseudowire Edge to Edge Emulation (PWE3)*

RFC 4447, *Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)*

RFC 4448, *Encapsulation Methods for Transport of Ethernet over MPLS Networks*

RFC 4619, *Encapsulation Methods for Transport of Frame Relay over Multiprotocol Label Switching (MPLS) Networks*

RFC 4717, *Encapsulation Methods for Transport Asynchronous Transfer Mode (ATM) over MPLS Networks*

RFC 4816, *Pseudowire Emulation Edge-to-Edge (PWE3) Asynchronous Transfer Mode (ATM) Transparent Cell Transport Service*

RFC 5085, *Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires*

RFC 5659, *An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge*

RFC 5885, *Bidirectional Forwarding Detection (BFD) for the Pseudowire Virtual Circuit Connectivity Verification (VCCV)*

RFC 6073, *Segmented Pseudowire*

RFC 6310, *Pseudowire (PW) Operations, Administration, and Maintenance (OAM) Message Mapping*

RFC 6391, *Flow-Aware Transport of Pseudowires over an MPLS Packet Switched Network*

RFC 6575, *Address Resolution Protocol (ARP) Mediation for IP Interworking of Layer 2 VPNs*

RFC 6718, *Pseudowire Redundancy*

RFC 6829, *Label Switched Path (LSP) Ping for Pseudowire Forwarding Equivalence Classes (FECs) Advertised over IPv6*

RFC 6870, *Pseudowire Preferential Forwarding Status bit*

RFC 7023, *MPLS and Ethernet Operations, Administration, and Maintenance (OAM) Interworking*

RFC 7267, *Dynamic Placement of Multi-Segment Pseudowires*

Quality of Service (QoS)

RFC 2430, *A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE)*

RFC 2474, *Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers*

RFC 2598, *An Expedited Forwarding PHB*

RFC 3140, *Per Hop Behavior Identification Codes*

RFC 3260, *New Terminology and Clarifications for Diffserv*

Remote Authentication Dial In User Service (RADIUS)

RFC 2865, *Remote Authentication Dial In User Service (RADIUS)*

RFC 2866, *RADIUS Accounting*

RFC 2867, *RADIUS Accounting Modifications for Tunnel Protocol Support*

RFC 2868, *RADIUS Attributes for Tunnel Protocol Support*

RFC 2869, *RADIUS Extensions*

RFC 3162, *RADIUS and IPv6*

RFC 4818, *RADIUS Delegated-IPv6-Prefix Attribute*

RFC 5176, *Dynamic Authorization Extensions to RADIUS*

RFC 6911, *RADIUS attributes for IPv6 Access Networks*

RFC 6929, *Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions*

Resource Reservation Protocol — Traffic Engineering (RSVP-TE)

draft-newton-mpls-te-dynamic-overbooking-00, *A Diffserv-TE Implementation Model to dynamically change booking factors during failure events*

RFC 2702, *Requirements for Traffic Engineering over MPLS*

RFC 2747, *RSVP Cryptographic Authentication*

RFC 2961, *RSVP Refresh Overhead Reduction Extensions*

RFC 3097, *RSVP Cryptographic Authentication -- Updated Message Type Value*

RFC 3209, *RSVP-TE: Extensions to RSVP for LSP Tunnels*

RFC 3473, *Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions* (IF_ID RSVP_HOP object with unnumbered interfaces and RSVP-TE graceful restart helper procedures)

RFC 3477, *Signalling Unnumbered Links in Resource ReSerVation Protocol - Traffic Engineering (RSVP-TE)*

RFC 3564, *Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering*

RFC 3906, *Calculating Interior Gateway Protocol (IGP) Routes Over Traffic Engineering Tunnels*

RFC 4090, *Fast Reroute Extensions to RSVP-TE for LSP Tunnels*

RFC 4124, *Protocol Extensions for Support of Diffserv-aware MPLS Traffic Engineering*

RFC 4125, *Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*

RFC 4127, *Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering*

RFC 4561, *Definition of a Record Route Object (RRO) Node-Id Sub-Object*

RFC 4875, *Extensions to Resource Reservation Protocol - Traffic Engineering (RSVP-TE) for Point-to-Multipoint TE Label Switched Paths (LSPs)*

RFC 4950, *ICMP Extensions for Multiprotocol Label Switching*

RFC 5151, *Inter-Domain MPLS and GMPLS Traffic Engineering -- Resource Reservation Protocol-Traffic Engineering (RSVP-TE) Extensions*

RFC 5712, *MPLS Traffic Engineering Soft Preemption*

RFC 5817, *Graceful Shutdown in MPLS and Generalized MPLS Traffic Engineering Networks*

Routing Information Protocol (RIP)

RFC 1058, *Routing Information Protocol*

RFC 2080, *RIPng for IPv6*

RFC 2082, *RIP-2 MD5 Authentication*

RFC 2453, *RIP Version 2*

Segment Routing (SR)

draft-filsfils-spring-segment-routing-policy-05, *Segment Routing Policy for Traffic Engineering*

draft-francois-rtgwg-segment-routing-ti-lfa-04, *Topology Independent Fast Reroute using Segment Routing*

draft-gredler-idr-bgp-ls-segment-routing-ext-03, *BGP Link-State extensions for Segment Routing*

draft-ietf-idr-segment-routing-te-policy-02, *Advertising Segment Routing Policies in BGP*

draft-ietf-isis-segment-routing-extensions-04, *IS-IS Extensions for Segment Routing* draft-ietf-mpls-spring-lsp-ping-02, *Label Switched Path (LSP) Ping/Trace for Segment Routing Networks Using MPLS Dataplane*

draft-ietf-ospf-segment-routing-extensions-04, *OSPF Extensions for Segment Routing*

draft-ietf-spring-conflict-resolution-05, *Segment Routing MPLS Conflict Resolution*

draft-ietf-spring-segment-routing-ldp-interop-09, *Segment Routing interworking with LDP*

Synchronous Optical Networking (SONET)/Synchronous Digital Hierarchy (SDH)

ANSI T1.105.03, *Jitter Network Interfaces*

ANSI T1.105.06, *Physical Layer Specifications*

ANSI T1.105.09, *Network Timing and Synchronization*

ITU-T G.703, *Physical/electrical characteristics of hierarchical digital interfaces*

ITU-T G.707, *Network node interface for the synchronous digital hierarchy (SDH)*

ITU-T G.813, *Timing characteristics of SDH equipment slave clocks (SEC)*

ITU-T G.823, *The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy*

ITU-T G.824, *The control of jitter and wander within digital networks which are based on the 1544 kbit/s hierarchy*

ITU-T G.825, *The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)*

ITU-T G.841, *Types and Characteristics of SDH Networks Protection Architecture, issued in October 1998 and as augmented by Corrigendum 1, issued in July 2002*

ITU-T G.957, *Optical interfaces for equipments and systems relating to the synchronous digital hierarchy*

Time Division Multiplexing (TDM)

ANSI T1.403, *DS1 Metallic Interface Specification*

ANSI T1.404, *DS3 Metallic Interface Specification*

Timing

GR-1244-CORE, *Clocks for the Synchronized Network: Common Generic Criteria, Issue 3, May 2005*

GR-253-CORE, *SONET Transport Systems: Common Generic Criteria. Issue 3, September 2000*

IEEE 1588-2008, *IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems*

ITU-T G.781, *Synchronization layer functions, issued 09/2008*

ITU-T G.813, *Timing characteristics of SDH equipment slave clocks (SEC), issued 03/2003*

ITU-T G.8261, *Timing and synchronization aspects in packet networks, issued 04/2008*

ITU-T G.8262, *Timing characteristics of synchronous Ethernet equipment slave clock (EEC), issued 08/2007*

ITU-T G.8264, *Distribution of timing information through packet networks, issued 10/2008*

ITU-T G.8265.1, *Precision time protocol telecom profile for frequency synchronization, issued 10/2010*

ITU-T G.8275.1, *Precision time protocol telecom profile for phase/time synchronization with full timing support from the network, issued 07/2014*

RFC 5905, *Network Time Protocol Version 4: Protocol and Algorithms Specification*

Two-Way Active Measurement Protocol (TWAMP)

RFC 5357, *A Two-Way Active Measurement Protocol (TWAMP)* (server, unauthenticated mode)

RFC 5938, *Individual Session Control Feature for the Two-Way Active Measurement Protocol (TWAMP)*

RFC 6038, *Two-Way Active Measurement Protocol (TWAMP) Reflect Octets and Symmetrical Size Features*

Virtual Private LAN Service (VPLS)

RFC 4761, *Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling*

RFC 4762, *Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling*

RFC 5501, *Requirements for Multicast Support in Virtual Private LAN Services*

RFC 6074, *Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)*

RFC 7041, *Extensions to the Virtual Private LAN Service (VPLS) Provider Edge (PE) Model for Provider Backbone Bridging*

RFC 7117, *Multicast in Virtual Private LAN Service (VPLS)*

Voice and Video

DVB BlueBook A86, *Transport of MPEG-2 TS Based DVB Services over IP Based Networks*

ETSI TS 101 329-5 Annex E, *QoS Measurement for VoIP - Method for determining an Equipment Impairment Factor using Passive Monitoring*

ITU-T G.1020 Appendix I, *Performance Parameter Definitions for Quality of Speech and other Voiceband Applications Utilizing IP Networks - Mean Absolute Packet Delay Variation & Markov Models*

ITU-T G.107, *The E Model - A computational model for use in planning*

ITU-T P.564, *Conformance testing for voice over IP transmission quality assessment models*

RFC 3550 Appendix A.8, *RTP: A Transport Protocol for Real-Time Applications* (estimating the interarrival jitter)

RFC 4585, *Extended RTP Profile for Real-time Transport Control Protocol (RTCP)-Based Feedback (RTP/AVPF)*

RFC 4588, *RTP Retransmission Payload Format*

Wireless Local Area Network (WLAN) Gateway

3GPP TS 23.402, *Architecture enhancements for non-3GPP accesses* (S2a roaming based on GPRS)

Customer Document and Product Support

Customer Documentation

Customer Documentation Welcome Page

Technical Support

Product Support Portal

Documentation Feedback

Customer Documentation Feedback