FSOS

IPv6 Multicast Configuration Guide

Contents

Figures

1 Configuring IPv6 Multicast-Routing

1.1 Overview

Multicast protocols allow a group or channel to be accessed over different networks by multiple stations (clients) for the receipt and transmit of multicast data.

Distribution of stock quotes, video transmissions such as news services and remote classrooms, and video conferencing are all examples of applications that use multicast routing.

- Mulitcast Listener Discovery (MLD) is used among hosts on a LAN and the routers (and multilayer switches) on that LAN to track the multicast groups of which hosts are members.
- Protocol-Independent Multicast (PIM) protocol is used among routers and multilayer switches to track which multicast packets to forward to each other and to their directly connected LANs. PIM has two modes: Sparse-mode and Dense-mode. Currently, we only support Sparse-mode

1.2 Configuration

The Max allowed IPv6 Multicast Route number can be configured. By default, 2048 IPv6 multicast routes are supported.

Switch# configure terminal	Enter Configuration mode
Switch(config)# ipv6 enable	Enable ipv6
Switch(config)# ipv6 multicast route-limit 1000	Configuring max allowed ipv6 muticast route

1.3 Validation

Switch# show ipv6 mroute 2001:1::1234

```
IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface

2001:1::1234, ff0e::1234:5678
uptime 00:00:31, stat expires 00:03:08
Owner PIM-SMv6, Flags: TF
  Incoming interface: eth-0-1
  Outgoing interface list:
    Register
    eth-0-2

2001:1::1234, ff0e::6666:6666
uptime 00:00:00, stat expires 00:03:30
Owner PIM-SMv6, Flags: TF
  Incoming interface: eth-0-1
  Outgoing interface list:
    Register
```

2 Configuring MLD

2.1 Overview

To participate in IPv6 multicasting, multicast hosts, routers, and multilayer switches must have the MLD operating. This protocol defines the query and host roles:

- A query is a network device that sends query messages to discover which network devices are members of a given multicast group.
- A host is a receiver that sends report messages (in response to query messages) to inform a querier of a host membership.

A set of queries and hosts that receive IPv6 multicast data streams from the same source is called an IPv6 multicast group. Queries and hosts use MLD messages to join and leave IPv6 multicast groups.

Any host, regardless of whether it is a member of a group, can send to a group. However, only the members of a group receive the message. Membership in a multicast group is dynamic; hosts can join and leave at any time. There is no restriction on the location or number of members in a multicast group.

A host can be a member of more than one multicast group at a time. How active a multicast group is and what members it has can vary from group to group and from time to time. A multicast group can be active for a long time, or it can be very short-lived. Membership in a group can constantly change. A group that has members can have no activity.

MLD packets are sent using these IPv6 multicast group addresses:

- MLD general queries are destined to the address ff02::1 (all systems on a subnet).
- MLD group-specific queries are destined to the group IPv6 address for which the switch is querying.

- MLD group membership reports are destined to the group IPv6 address for which the switch is reporting.
- MLD Version 1 (MLDv1) leave messages are destined to the address ff02::2 (all-multicast-routers on a subnet). In some old host IPv6 stacks, leave messages might be destined to the group IPv6 address rather than to the all-routers address.

2.2 References

The MLD module is based on the following RFC

- RFC 2710
- RFC 3810

2.3 Configuration

There is no explicit command to enable MLD, which is always combined with PIMv6-SM. When PIMv6-SM is enabled on an interface, MLD will be enabled automatically on this interface, vice versa. But notice, before MLD can work, IPv6 Multicast-routing must be enabled globally firstly. We support build MLD group record by learning MLD packets or configuring static MLD group by administer.

Enable MLD

Switch# configure terminal	Enter Configuration mode
Switch(config)# ipv6 enable	Enable ipv6
Switch(config)# ipv6 multicast-routing	Enable IPv6 Multicast routing globally
Switch(config)# interface eth-0-1	Enter interface eth-0-1
Switch(config-if)# no switchport	Change eth-0-1 as routed port
Switch(config-if)# ipv6 address 2001::1/64	Set the interface IPv6 address
Switch(config-if)# ipv6 pim sparse-mode	Enable ipv6 pim sparse mode & enable mld

Configuring MLD Interface Parameters

Switch# configure terminal	Enter Configuration mode
Switch(config)# interface eth-0-1	Enter interface eth-0-1
Switch(config-if)# ipv6 mld version 2	Set mld version
Switch(config-if)# ipv6 mld query-interval 120	Set mld query interval
Switch(config-if)# ipv6 mld query-max-response-time 12	Set mld query max response time
Switch(config-if)# ipv6 mld robustness-variable 3	Set mld robustness value
Switch(config-if)# ipv6 mld last-member-query-count 3	Set mld last member query count
Switch(config-if)# ipv6 mld last-member-query-interval 2000	Set mld last member query interval

Limit Max MLD Group Number

The limit can be configured globally or per interface.

Switch# configure terminal	Enter Configuration mode
Switch(config)# ipv6 mld limit 2000	Set global max mld group number
Switch(config)# interface eth-0-1	Enter interface eth-0-1
Switch(config-if)# ipv6 mld limit 1000	Set per-interface max mld group number

Configuring Static MLD Group

The static MLD Group can be configured on interface.

Switch# configure terminal	Enter Configuration mode
Switch(config)# interface eth-0-1	Enter interface eth-0-1
Switch(config-if)# ipv6 mld static-group ff0e::1234	Configure static mld group on interface eth-0-1

Configuring SSM Mapping

Switch# configure terminal	Enter Configuration mode
Switch(config)# ipv6 mld ssm-map enable	Enable ssm mapping globally
Switch(config-if)# ipv6 mld ssm-map ipv6acl 2001::2	Configure group in access list ipv6acl to map to 2001::2 when switch receives mldv1 report

Configuring Multicast Proxy Downstream And Upstream

Switch# configure terminal	Enter Configuration mode
Switch(config)# interface eth-0-1	Enter interface eth-0-1
Switch(config-if)#no switchport	Change the interface as routed port
Switch(config-if)# ipv6 pim sparse-mode	Enable PIMv6 sparse-mode
Switch(config-if)# ipv6 mld proxy-service	Set eth-0-1 as mld proxy upstream
Switch(config)# interface eth-0-2	Enter interface eth-0-2
Switch(config-if)# no switchport	Change the interface as routed port
Switch(config-if)# ipv6 pim sparse-mode	Enable PIMv6 sparse-mode
Switch(config-if)# ipv6 mld mroute-proxy eth-0-1	Set eth-0-2 as mld proxy downstream, And its upstream is interface eth-0-1

2.4 Validation

Displaying MLD Interface

Switch# show ip mld interface

```
Interface eth-0-1 (Index 1)
 MLD Active, Querier, Version 1 (default)
 Internet address is fe80::8c8e:dbff:feef:1900
 MLD interface has 0 group-record states
 MLD activity: 0 joins, 0 leaves
 MLD query interval is 125 seconds
 MLD querier timeout is 255 seconds
 MLD max query response time is 10 seconds
```

```
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
Interface eth-0-9 (Index 9)
 MLD Active, Querier, Version 1 (default)
 Internet address is fe80::8c8e:dbff:feef:1900
 MLD interface has 0 group-record states
 MLD activity: 0 joins, 0 leaves
 MLD query interval is 125 seconds
 MLD querier timeout is 255 seconds
 MLD max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
```

Displaying MLD group

Switch# show ip mld groups

```
MLD Connected Group Membership
Group Address                           Interface            Expires
ff0e::1234:5678                         eth-0-2              00:03:01
```

3 Configuring PIMv6

3.1 Overview

The Protocol Independent Multicasting-Sparse Mode for IPv6(PIMv6-SM) is a multicast routing protocol designed to operate efficiently across Wide Area Networks (WANs) with sparsely distributed groups. It helps network nodes that are geographically dispersed to conserve bandwidth, and reduces traffic by simultaneously delivering a single stream of information to multiple locations.

PIMv6-SM uses the IPv6 multicast model of receiver-initiated membership, supporting both shared and shortest-path trees, and uses soft-state mechanisms to adapt to changing network conditions. It relies on a topology-gathering protocol to populate a multicast routing table with routes.

3.2 References

The PIMv6-SM module is based on the following IETF standard:

RFC 4601

3.3 Terminology

Following is a brief description of terms and concepts used to describe the PIMv6-SM protocol:

Rendezvous Point (RP)

A Rendezvous Point (RP) router is configured as the root of the non-source-specific distribution tree for a multicast group. Join messages from receivers for a group are sent towards the RP. Data from senders is sent to the RP so that receivers can discover who the senders are, and receive traffic destined for the group.

Multicast Routing Information Base (MRIB)

The MRIB is a multicast topology table derived from the unicast routing table. In PIMv6-SM, the MRIB is used to decide where to send Join/Prune messages. It also provides routing metrics for destination addresses. These metrics are used when sending and processing Assert messages.

Reverse Path Forwarding

Reverse Path Forwarding (RPF) is a concept of an optimized form of flooding, where the router accepts a packet from SourceA through Interface IF1 only if IF1 is the interface the router would use in order to reach SourceA. It determines whether the interface is correct by consulting its unicast routing tables. The packet that arrives through interface IF1 is forwarded because the routing table lists this interface as the shortest path to the network. The router's unicast routing table determines the shortest path for the multicast packets. Because a router accepts a packet from only one neighbor, it floods the packet only once, meaning that (assuming point-to-point links) each packet is transmitted over each link once in each direction.

Tree Information Base (TIB)

The TIB is the collection of state at a PIM router storing the state of all multicast distribution trees at that router. It is created by receiving Join/Prune messages, Assert messages, and MLD information from local hosts.

Upstream

Towards the root of the tree. The root of the tree might be either the Source or the RP.

Downstream

Away from the root of the tree. The root of tree might be either the Source or the RP.

Source-Based Trees

In the Source-Based Trees concept, the forwarding paths are based on the shortest unicast path to the source. If the unicast routing metric is hop counts, the branches of the multicast Source-Based Trees are minimum hop. If the metric is delay, the branches are minimum delay.

For every multicast source, there is a corresponding multicast tree that directly connects the source to all receivers. All traffic to the members of an associated group passes along the tree made for their source. Source-Based Trees have two entries with a list of outgoing interfaces--the source address and the multicast group.

Shared Trees

Shared trees or RP trees (RPT) rely on a central router called the Rendezvous Point (RP) that receives all traffic from the sources, and forwards that traffic to the receivers. All hosts might not be receivers. There is a single tree for each multicast group, regardless of the number of sources. Only the routers on the tree know about the group, and information is sent only to interested receivers. With an RP, receivers have a place to join, even if no source exists.

The shared tree is unidirectional, and information flows only from the RP to the receivers. If a host other than the RP has to send data on the tree, the data must first be tunneled to the RP, and then multicast to the members. This means that even if a receiver is also a source, it can only use the tree to receive packets from the RP, and not to send packets to the RP (unless the source is located between the RP and the receivers).

Bootstrap Router (BSR)

When a new multicast sender starts sending data packets, or a new receiver starts sending the Join message towards the RP for that multicast group, it needs to know the next-hop router towards the RP. The BSR provides group-to-RP mapping information to all the PIMv6 routers in a domain, allowing them to map to the correct RP address.

Sending out Hello Messages

PIMv6 routers periodically send Hello messages to discover neighboring PIMv6 routers. Hello messages are multicast using the address ff02::d (ALL-PIMv6-ROUTERS group). Routers do not send any acknowledgement that a Hello message was received. A hold time value determines the length of time for which the information is valid. In PIMv6-SM, a downstream receiver must join a group before traffic is forwarded on the interface.

Electing a Designated Router

In a multi-access network with multiple routers connected, one of them is selected to act as a designated router (DR) for a given period of time. The DR is responsible for sending Join/Prune messages to the RP for local members.

Determining the RP

PIMv6-SM uses a BootStrap Router (BSR) to originate Bootstrap messages, and to disseminate RP information. The messages are multicast to the group on each link. If the BSR is not apparent, the routers flood the domain with advertisements. The router with the highest priority (if priorities are same, the higher IPv6 address applies) is selected to be the RP. Routers receive and store Bootstrap messages originated by the BSR. When a DR gets a membership indication from MLD for (or a data packet from) a directly connected host, for a group for which it has no entry, the DR maps the group address to one of the candidate RPs that can service that group. The DR then sends a Join/Prune message towards that RP.

In a small domain, the RP can also be configured statically.

Joining the Shared Tree

To join a multicast group, a host sends an MLD message to its upstream router, after which the router can accept multicast traffic for that group. The router sends a Join message to its upstream PIMv6 neighbor in the direction of the RP. When a router receives a Join message from a downstream router, it checks to see if a state exists for the group in its multicast routing table. If a state already exists, the Join message has reached the shared tree, and the interface from which the message was received is entered in the Outgoing Interface list. If no state

exists, an entry is created, the interface is entered in the Outgoing Interface list, and the Join message is again sent towards the RP.

Registering with the RP

A DR can begin receiving traffic from a source without having a Source or a Group state for that source. In this case, the DR has no information on how to get multicast traffic to the RP through a tree. When the source DR receives the initial multicast packet, it encapsulates it in a Register message, and unicasts it to the RP for that group. The RP deencapsulates each Register message, and forwards the extracted data packet to downstream members on the RPT.

Once the path is established from the source to the RP, the DR begins sending traffic to the RP as standard IPv6 multicast packets, as well as encapsulated within Register messages. The RP temporarily receives packets twice.

When the RP detects the normal multicast packets, it sends a Register-Stop message to the source DR, meaning it should stop sending register packets.

Sending Register-Stop Messages

When the RP begins receiving traffic from the source, both as Register messages and as unencapsulated IPv6 packets, it sends a Register-Stop message to the DR. This notifies the DR that the traffic is now being received as standard IPv6 multicast packets on the SPT. When the DR receives this message, it stops encapsulating traffic in Register messages.

Pruning the Interface

Routers attached to receivers send Prune messages to the RP to disassociate the source from the RP. When an RP receives a Prune message, it no longer forwards traffic from the source indicated in the Prune message. If all members of a multicast group are pruned, the MLD state of the DR is deleted, and the interface is removed from the Source and Group lists of the group.

Forwarding Multicast Packets

PIMv6-SM routers forward multicast traffic onto all interfaces that lead to receivers that have explicitly joined a multicast group. Messages are sent to a group address in the local

subnetwork, and have a Time to Live (TTL) of 1. The router performs an RPF check, and forwards the packet. Traffic that arrives on the correct interface is sent onto all outgoing interfaces that lead to downstream receivers if the downstream router has sent a join to this router, or is a member of this group.

3.4 Configuring General PIMv6 Sparse-mode

3.4.1 Topology

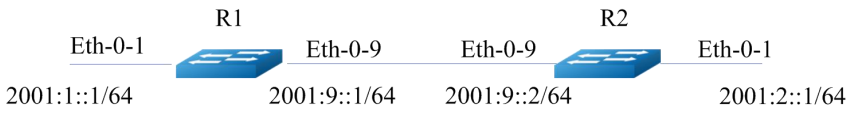

Figure 3-1 Configuring RP statically

3.4.2 Configuration

PIMv6-SM is a soft-state protocol. The main requirement is to enable PIMv6-SM on desired interfaces, and configure the RP information correctly, through static or dynamic methods. All multicast group states are maintained dynamically as the result of MLD Report/Leave and PIMv6 Join/Prune messages. Currently, we support only one RP for all multicast groups (ff00::/8).

This section provides PIMv6-SM configuration examples for two relevant scenarios. The following graphic displays the network topology used in these examples:

In this example, using the above topology, R1 is the Rendezvous Point (RP), and all routers are statically configured with RP information. While configuring the RP, make sure that:

- Every router includes the ipv6 pim rp-address 2001:1::1 statement, even if it does not have any source or group member attached to it.
- There is only one RP address for a group scope in the PIMv6 domain.

- All interfaces running PIMv6-SM must have sparse-mode enabled.

Here is a sample configuration:

Configuring R1

Switch# configure terminal	Enter the configure mode
Switch(config)# ipv6 enable	Enable ipv6
Switch(config)# interface eth-0-1	Specify the interface (eth-0-1) to be configured and enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface
Switch(config-if)# no switchport	Change this port to Layer3 interface
Switch(config-if)# ipv6 address 2001:1::1/64	Configure IPv6 address for this interface
Switch(config-if)# ipv6 pim sparse-mode	Enable ipv6 pim sparse mode
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch(config)# interface eth-0-9	Specify the interface (eth-0-9) to be configured and enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface
Switch(config-if)# no switchport	Change this port to Layer3 interface
Switch(config-if)# ipv6 address 2001:9::1/64	Configure IPv6 address for this interface
Switch(config-if)# ipv6 pim sparse-mode	Enable ipv6 pim sparse mode
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch(config)# ipv6 route 2001:2::/64 2001:9::2	Configure a static route
Switch(config)# ipv6 pim rp-address 2001:1::1	Configure the static rp address

Configuring R2

Switch# configure terminal	Enter the configure mode
Switch(config)# ipv6 enable	Enable ipv6

Switch(config)# interface eth-0-1	Specify the interface (eth-0-1) to be configured and enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface
Switch(config-if)# no switchport	Change this port to Layer3 interface
Switch(config-if)# ipv6 address 2001:2::1/64	Configure IPv6 address for this interface
Switch(config-if)# ipv6 pim sparse-mode	Enable ipv6 pim sparse mode
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch(config)# interface eth-0-9	Specify the interface (eth-0-9) to be configured and enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface
Switch(config-if)# no switchport	Change this port to Layer3 interface
Switch(config-if)# ipv6 address 2001:9::2/64	Configure IPv6 address for this interface
Switch(config-if)# ipv6 pim sparse-mode	Enable ipv6 pim sparse mode
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch(config)# ipv6 route 2001:1::/64 2001:9::1	Configure a static route
Switch(config)# ipv6 pim rp-address 2001:1::1	Configure the static rp address

3.4.3 Validation

Configure all the routers with the same ipv6 pim rp-address 2001:1::1 command as shown above. Use the following commands to verify the RP configuration, interface details, and the multicast routing table.

RP Details

At R1, the show ip pim sparse-mode rp mapping command shows that 11.1.1.1 is the RP for all multicast groups ff00::/8, and is statically configured. All other routers will have a similar output.

R1# show ipv6 pim sparse-mode rp mapping

```
PIM Group-to-RP Mappings
Group(s): ff00::/8, Static
    RP: 2001:1::1
         Uptime: 00:00:04
Embedded RP Groups:
```

Interface Details

The show ipv6 pim sparse-mode interface command displays the interface details for R1.

R1# show ipv6 pim sparse-mode interface

```
Interface    VIFindex Ver/    Nbr     DR
                      Mode    Count   Prior
eth-0-1      2        v2/S    0       1
    Address        : fe80::fc94:efff:fe96:2600
    Global Address: 2001:1::1
    DR             : this system
eth-0-9      0        v2/S    0       1
    Address        : fe80::fc94:efff:fe96:2600
    Global Address: 2001:9::1
    DR             : this system
```

IPv6 Multicast Routing Table

The show ipv6 pim sparse-mode mroute detail command displays the IPv6 multicast routing table.

R1# show ipv6 pim sparse-mode mroute detail

```
IPv6 Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0

*, ff0e::1234:5678
Type: (*,G)
Uptime: 00:01:37
  RP: 2001:1::1, RPF nbr: None, RPF idx: None
  Upstream:
    State: JOINED, SPT Switch: Enabled, JT: off
    Macro state: Join Desired,
  Downstream:
    eth-0-1:
      State: NO INFO, ET: off, PPT: off
      Assert State: NO INFO, AT: off
       Winner: ::, Metric: 4294967295, Pref: 4294967295, RPT bit: on
      Macro state: Could Assert, Assert Track
```

```
  Local Olist:
    eth-0-1
```

R2# show ip pim sparse-mode mroute detail

```
IPv6 Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
FCR Entries: 0

*, ff0e::1234:5678
Type: (*,G)
Uptime: 00:00:06
  RP: 2001:1::1, RPF nbr: None, RPF idx: None
  Upstream:
    State: JOINED, SPT Switch: Enabled, JT: off
    Macro state: Join Desired,
  Downstream:
    eth-0-1:
      State: NO INFO, ET: off, PPT: off
      Assert State: NO INFO, AT: off
       Winner: ::, Metric: 4294967295, Pref: 4294967295, RPT bit: on
      Macro state: Could Assert, Assert Track
  Local Olist:
    eth-0-1
```

3.5 Configuring RP dynamically

A static configuration of RP works for a small, stable PIMv6 domain; however, it is not practical for a large and not-suitable internet work. In such a network, if the RP fails, the network administrator might have to change the static configurations on all PIMv6 routers. Another reason for choosing dynamic configuration is a higher routing traffic leading to a change in the RP.

We use the BSR mechanism to dynamically maintain the RP information. For configuring RP dynamically in the above scenario, R1 on eth-0-1 and R2 on eth-0-9 are configured as Candidate RP using the ipv6 pim rp candidate command. R2 on eth-0-9 is also configured as Candidate BSR. Since no other router has been configured as Candidate BSR, the R2 becomes the BSR router, and is responsible for sending group-to-RP mapping information to all other routers in this PIMv6 domain.

The following output displays the complete configuration at R1 and R2.

3.5.1 Configuration

R1

Switch# configure terminal	Enter the configure mode
Switch(config)# ipv6 enable	Enable ipv6
Switch(config)# interface eth-0-1	Specify the interface (eth-0-1) to be configured and enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface
Switch(config-if)# no switchport	Change this port to Layer3 interface
Switch(config-if)# ipv6 address 2001:1::1/24	Configure IPv6 address for this interface
Switch(config-if)# ipv6 pim sparse-mode	Enable ipv6 pim sparse mode
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode.
Switch(config)# interface eth-0-9	Specify the interface (eth-0-9) to be configured and enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface
Switch(config-if)# no switchport	Change this port to Layer3 interface
Switch(config-if)# ipv6 address 2001:9::1/24	Configure IPv6 address for this interface
Switch(config-if)# ipv6 pim sparse-mode	Enable ipv6 pim sparse mode
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode.
Switch(config)# ipv6 route 2001:2::/4 2001:9::2/64	Configure a static route
Switch(config)# ipv6 pim rp-candidate eth-0-1	Configure the candidate rp

R2

Switch# configure terminal	Enter the configure mode
Switch(config)# ipv6 enable	Enable ipv6
Switch(config)# interface eth-0-1	Specify the interface (eth-0-1) to be configured and enter the Interface mode.

Switch(config-if)# no shutdown	Turn up the interface.
Switch(config-if)# no switchport	Change this port to Layer3 interface.
Switch(config-if)# ipv6 address 2001:2::1/64	Configure IPv6 address for this interface
Switch(config-if)# ipv6 pim sparse-mode	Enable ipv6 pim sparse mode
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode.
Switch(config)# interface eth-0-9	Specify the interface (eth-0-9) to be configured and enter the Interface mode.
Switch(config-if)# no shutdown	Turn up the interface.
Switch(config-if)# no switchport	Change this port to Layer3 interface.
Switch(config-if)# ipv6 address 2001:9::2/24	Configure IPv6 address for this interface
Switch(config-if)# ipv6 pim sparse-mode	Enable ipv6 pim sparse mode.
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode.
Switch(config)# ipv6 route 2001:1::/64 2001:9::1	Configure a static route.
Switch(config)# ipv6 pim rp-candidate eth-0-9	Configure the candidate rp.
Switch(config)# ipv6 pim bsr-candidate eth-0-9	Configure the candidate bsr.

The highest priority router is chosen as the RP. If two or more routers have the same priority, a hash function in the BSR mechanism is used to choose the RP, to make sure that all routers in the PIMv6-domain have the same RP for the same group.

Use the ipv6 pim rp-candidate IFNAME PRIORITY command to change the default priority of any candidate RP.

3.5.2 Validation

PIMv6 group-to-RP mappings

Use the show ip pim sparse-mode rp mapping command to display the group-to-RP mapping details. The output displays information about RP candidates. There are two RP candidates for

the group range ff00::/8. RP Candidate 2001:1::1 has a default priority of 192, whereas, RP Candidate 2001:9::2 has been configured to have a priority of 2. Since RP candidate 2001:1::1 has a higher priority, it is selected as RP for the multicast group ff00::/8. Only permit filters would be cared in group list.

R2# show ipv6 pim sparse-mode rp mapping

```
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): ff00::/8
  RP: 2001:9::2
    Info source: 2001:9::2, via bootstrap, priority 2
         Uptime: 00:00:32, expires: 00:02:02
  RP: 2001:1::1
    Info source: 2001:1::1, via bootstrap, priority 192
         Uptime: 00:00:31, expires: 00:02:03
Embedded RP Groups:
```

RP details

To display information about the RP router for a particular group, use the following command. This output displays that 2001:9::2 has been chosen as the RP for the multicast group ff02::1234.

R2# show ipv6 pim sparse-mode rp-hash ff02::1234

```
    RP: 2001:9::2
    Info source: 2001:9::2, via bootstrap
```

After RP information reaches all PIMv6 routers in the domain, various state machines maintain all routing states as the result of Join/Prune from group membership. To display information on interface details and the multicast routing table, refer to the Configuring RP Statically section above.

3.6 Configuring Boostrap Router

Every PIMv6 multicast group needs to be associated with the IPv6 address of a Rendezvous Point (RP). This address is used as the root of a group-specific distribution tree whose branches extend to all nodes in the domain that want to receive traffic sent to the group. For all senders to reach all receivers, all routers in the domain use the same mappings of group

addresses to RP addresses. In order to determine the RP for a multicast group, a PIMv6 router maintains a collection of group-to-RP mappings, called the RP-Set.

The Bootstrap Router (BSR) mechanism for the class of multicast routing protocols in the PIMv6 domain use the concept of a Rendezvous Point as a means for receivers to discover the sources that send to a particular multicast group. The BSR mechanism is one way that a multicast router can learn the set of group-to-RP mappings required in order to function.

Some of the PIMv6 routers within a PIMv6 domain are configured as Candidate-RPs (C-RPs). A subset of the C-RPs will eventually be used as the actual RPs for the domain. An RP configured with a lower value in the priority field has higher a priority.

Some of the PIMv6 routers in the domain are configured to be Candidate-BSRs (C-BSRs). One of these C-BSRs is elected to be the bootstrap router (BSR) for the domain, and all PIMv6 routers in the domain learn the result of this election through BSM (Bootstrap messages). The C-BSR with highest value in priority field is Elected-BSR.

The C-RPs then reports their candidacy to the elected BSR, which chooses a subset of the C-RPs and distributes corresponding group-to-RP mappings to all the routers in the domain through Bootstrap messages.

3.6.1 Topology

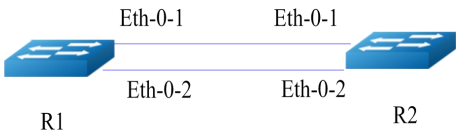

Figure 3-2 BSR Topology

3.6.2 Configuration

R1

Switch# configure terminal	Enter Configuration mode

Switch(config)# ipv6 enable	Enable ipv6
Switch(config)# ipv6 pim bsr-candidate eth-0-1	Configure eth-0-1 of rtr1 as C-BSR. The default priority is 64.

R2

Switch# configure terminal	Enter Configuration mode
Switch(config)# ipv6 enable	Enable ipv6
Switch(config)# ipv6 pim bsr-candidate eth-0-1 10 25	Configure eth-0-1 of rtr2 as C-BSR with a hash mask length 10 and a priority of 25.
Switch(config)# ipv6 pim rp-candidate eth-0-1 priority 0	Configure interface eth-0-1 as C-RP with a priority of 0.

When the command ipv6 pim unicast-bsm is configured on an interface which is a DR for that network, then that interface will unicast the stored copy of BSM to new/rebooting router.

Switch# configure terminal	Enter Configuration mode
Switch(config)# interface eth-0-1	Enter interface mode
Switch(config-if)# ipv6 pim dr-priority 10	Configure the interface (eth-0-1) as DR
Switch(config-if)# ipv6 pim unicast-bsm	Enable sending and receiving of Unicast BSM for backward compatibility.

3.6.3 Validation

Verify the C-BSR state on rtr1

Switch# show ipv6 pim sparse-mode bsr-router

```
PIM6v2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 2001:9::1 (?)
  Uptime:      00:01:27, BSR Priority: 64, Hash mask length: 126
  Next bootstrap message in 00:00:16
  Role: Candidate BSR
  State: Elected BSR
```

Verify the C-BSR state on rtr2

The initial state of C-BSR is P-BSR before transitioning to C-BSR.

Switch# show ipv6 pim sparse-mode bsr-router

```
PIM6v2 Bootstrap information
  BSR address: 2001:9::1 (?)
  Uptime:      00:01:34, BSR Priority: 64, Hash mask length: 126
  Expires:     00:01:51
  Role: Candidate BSR
  State: Candidate BSR

  Candidate RP: 2001:9::2(eth-0-9)
    Advertisement interval 60 seconds
    Next C-RP advertisement in 00:00:35
```

Verify RP-set information on E-BSR

Switch#show ipv6 pim sparse-mode rp mapping

```
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): ff00::/8
  RP: 2001:9::2
    Info source: 2001:9::2, via bootstrap, priority 0
         Uptime: 00:45:37, expires: 00:02:29
Embedded RP Groups:
```

Verify RP-set information on C-BSR

Switch#show ipv6 pim sparse-mode rp mapping

```
PIM Group-to-RP Mappings
Group(s): ff00::/8
  RP: 2001:9::2
    Info source: 2001:9::1, via bootstrap, priority 0
         Uptime: 00:03:14, expires: 00:01:51
Embedded RP Groups:
```

3.7 Configuring PIMv6-SSM feature

PIMv6-SSM can work with PIMv6-SM on the multicast router. By default, PIMv6-SSM is disabled

Switch# configure terminal	Enter Configuration mode

Switch(config)# ipv6 enable	Enable ipv6
Switch(config)# ipv6 pim ssm default	Enable pimv6-ssm on the switch and set the ssm group range as default
Switch(config)# ipv6 pim ssm range ipv6acl	Enable pimv6-ssm on the switch and set the ssm group range as group range specified in ipv6acl

4 Configuring PIMv6-DM

4.1 Overview

The Ipv6 Protocol Independent Multicasting-Dense Mode (PIMv6-DM) is a multicast routing protocol designed to operate efficiently across Wide Area Networks (WANs) with densely distributed groups. It helps network nodes that are geographically dispersed to conserve bandwidth, and reduces traffic by simultaneously delivering a single stream of information to multiple locations.

PIMv6-DM assumes that when a source starts sending, all downstreamsystems want to receive multicast datagrams. Initially, multicastdatagrams are flooded to all areas of the network. PIMv6-DM uses RPF to prevent looping of multicast datagrams while flooding. If some areas of the network do not have group members, PIMv6-DM will prune off the forwarding branch by instantiating prune state.

Prune state has a finite lifetime. When that lifetime expires, datawill again be forwarded down the previously pruned branch. Prune state is associated with an (S,G) pair. When a new member for a group G appears in a pruned area, a router can "graft" toward the source S for the group, thereby turning the pruned branch back into a forwarding branch.

4.2 References

The PIMv6-DM module is based on the following IETF standard:

RFC 3973

4.3 Configuring General PIM dense-mode

4.3.1 Topology

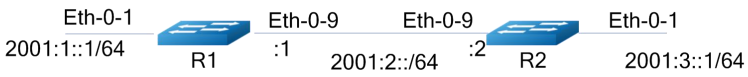

Figure 4-1 Configuring PIMv6 dense-mode

4.3.2 Configuration

PIMv6-DM is a soft-state protocol. The main requirement is to enable PIMv6-DM on desired interfaces. All multicast group states are maintained dynamically as the result of MLD Report/Leave and PIMv6 messages.

This section provides PIMv6-DM configuration examples for two relevant scenarios. The following graphic displays the network topology used in these examples:

In this example, using the above topology, multicast data stream comes to eth-0-1 of R1, host is connected to eth-0-1 of R2.

Here is a sample configuration:

Configuring R1

Switch# configure terminal	Enter the configure mode
Switch(config)# ipv6 enable	Enable ipv6
Switch(config)# interface eth-0-1	Specify the interface (eth-0-1) to be configured and enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface
Switch(config-if)# no switchport	Change this port to Layer3 interface
Switch(config-if)# ipv6 address 2001:1::1/64	Configure IPv6 address for this interface
Switch(config-if)# ipv6 pim dense-mode	Enable ipv6 pim dense mode
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode

Switch(config)# interface eth-0-9	Specify the interface (eth-0-9) to be configured and enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface
Switch(config-if)# no switchport	Change this port to Layer3 interface
Switch(config-if)# ipv6 address 2001:2::1/64	Configure IPv6 address for this interface
Switch(config-if)# ipv6 pim dense-mode	Enable ipv6 pim dense mode
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch(config)# ipv6 route 2001:3::/64 2001:2::2	Configure a static route

Configuring R2

Switch# configure terminal	Enter the configure mode
Switch(config)# ipv6 enable	Enable ipv6
Switch(config)# interface eth-0-1	Specify the interface (eth-0-1) to be configured and enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface
Switch(config-if)# no switchport	Change this port to Layer3 interface
Switch(config-if)# ipv6 address 2001:3::1/64	Configure IPv6 address for this interface
Switch(config-if)# ipv6 pim dense-mode	Enable ipv6 pim dense mode
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode
Switch(config)# interface eth-0-9	Specify the interface (eth-0-9) to be configured and enter the Interface mode
Switch(config-if)# no shutdown	Turn up the interface
Switch(config-if)# no switchport	Change this port to Layer3 interface
Switch(config-if)# ipv6 address 2001:2::2/64	Configure IPv6 address for this interface
Switch(config-if)# ipv6 pim dense-mode	Enable ipv6 pim dense mode
Switch(config-if)# exit	Exit the Interface mode and enter the Configure mode

Switch(config)# ipv6 route 2001:1::/64 2001:2::1	Configure a static route

4.3.3 Validation

Use the following commands to verify the interface details, and the multicast routing table.

Interface Details

The show ipv6 pim dense-mode interface command displays the interface details for R1.

R1# show ipv6 pim dense-mode interface

```
Neighbor Address                          Interface    VIFIndex Ver/    Nbr
                                                                Mode    Count
fe80::326f:c9ff:fef2:8200                 eth-0-1      0        v2/D    0
fe80::326f:c9ff:fef2:8200                 eth-0-9      2        v2/D    1
```

Neighbor Details

The show ip pim dense-mode neighbor command displays the neighbor details for R1.

R1# show ipv6 pim sparse-mode neighbor

```
Neighbor Address                          Interface    Uptime/Expires    Ver
fe80::ce47:6eff:feb7:1400                 eth-0-9      00:51:51/00:01:24 v2
```

IP Multicast Routing Table

The show ip pim dense-mode mroute detail command displays the IP multicast routing table.

R1# show ipv6 pim dense-mode mroute

```
PIM-DM Multicast Routing Table
(2001:1::2, ff0e::1)
  Source directly connected on eth-0-1
  State-Refresh Originator State: Originator
  Upstream IF: eth-0-1
    Upstream State: Forwarding
    Assert State: NoInfo
  Downstream IF List:
    eth-0-9, in 'olist':
      Downstream State: NoInfo
      Assert State: NoInfo
```

R2# show ipv6 pim dense-mode mroute

```
PIM-DM Multicast Routing Table
```

```
(2001:1::2, ff0e::1)
  RPF Neighbor: none
  Upstream IF: eth-0-9
    Upstream State: AckPending
    Assert State: Loser
  Downstream IF List:
    eth-0-1, in 'olist':
      Downstream State: NoInfo
      Assert State: NoInfo
```

5 Configuring MLD Snooping

5.1 Overview

Layer 2 switches can use MLD snooping to constrain the flooding of multicast traffic by dynamically configuring Layer 2 interfaces so that multicast traffic is forwarded only to those interfaces associated with IPv6 multicast devices. As the name implies, MLD snooping requires the LAN switch to snoop on the MLD transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an MLD report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an MLD Leave Group message from a host, it removes the host port from the table entry. It also deletes entries per entry if it does not receive MLD membership reports from the multicast clients. The multicast router sends out periodic general queries to all VLANs. All hosts interested in this multicast traffic send report and are added to the forwarding table entry. The switch forwards only one report per IPv6 multicast group to the multicast router. It creates one entry per VLAN in the Layer 2 forwarding table for each MAC group from which it receives an MLD report.

Layer 2 multicast groups learned through MLD snooping are dynamic. If you specify group membership for a multicast group address statically, your setting supersedes any automatic manipulation by MLD snooping. Multicast group membership lists can consist of both user-defined and MLD snooping-learned settings.

5.2 Enable Globally Or Per Vlan

5.2.1 Configuration

MLD Snooping can be enabled globally or per vlan. If MLD Snooping is disabled globally, it can't be active on any vlan even it's enabled on the vlan. If MLD snooping is enabled globally, it can be disabled on a vlan. On the other hand, the global configuration can overwrite the per vlan configuration. By default, MLD snooping is enabled globally and per vlan.

Switch# configure terminal	Enter Configuration mode
Switch(config)# ipv6 enable	Enable ipv6
Switch(config)# ipv6 mld snooping	Enable mld snooping globally
Switch(config)# ipv6 mld snooping vlan 1	Enable mld snooping on vlan 1
Switch# show ipv6 mld snooping vlan 1	Verify ipv6 mld snooping configuration

5.2.2 Validation

Switch# show ipv6 mld snooping vlan 1

```
Global Mld Snooping Configuration
------------------------------------------------
Mld Snooping                                :Enabled
Mld Snooping Fast-Leave                     :Disabled
Mld Snooping Version                        :1
Mld Snooping Max-Member-Number              :4096
Mld Snooping Unknown Multicast Behavior     :Flood
Mld Snooping Report-Suppression             :Enabled
Vlan 1
-----------
Mld Snooping                                :Enabled
Mld Snooping Fast-Leave                     :Disabled
Mld Snooping Report-Suppression             :Enabled
Mld Snooping Version                        :1
Mld Snooping Max-Member-Number              :4096
Mld Snooping Unknown Multicast Behavior     :Flood
Mld Snooping Group Access-list              :N/A
Mld Snooping Mrouter Port                   :
Mld Snooping Mrouter Port Aging Interval(sec) :255
```

5.3 Configuring Fast Leave

5.3.1 Configuration

When MLD Snooping fast leave is enabled, the mld snooping group will be removed at once upon receiving a corresponding mld report. Otherwise the switch will send out specified mld specific query, if it doesn't get response in specified period, it will remove the group. By default, mld snooping fast-leave is disabled globally and per vlan.

Switch# configure terminal	Enter Configuration mode
Switch(config)# ipv6 mld snooping fast-leave	Enable mld snooping fast-leave globally
Switch(config)# ipv6 mld snooping vlan 1 fast-leave	Enable mld snooping fast-leave on vlan 1
Switch# show ipv6 mld snooping vlan 1	Verify ipv6 mld snooping configuration.

5.3.2 Validation

Switch# show ipv6 mld snooping vlan 1

```
Global Mld Snooping Configuration
------------------------------------------------
Mld Snooping                            :Enabled
Mld Snooping Fast-Leave                 :Enabled
Mld Snooping Version                    :1
Mld Snooping Max-Member-Number          :4096
Mld Snooping Unknown Multicast Behavior  :Flood
Mld Snooping Report-Suppression         :Enabled
Vlan 1
-----------
Mld Snooping                            :Enabled
Mld Snooping Fast-Leave                 :Enabled
Mld Snooping Report-Suppression         :Enabled
Mld Snooping Version                    :1
Mld Snooping Max-Member-Number          :4096
Mld Snooping Unknown Multicast Behavior  :Flood
Mld Snooping Group Access-list          :N/A
Mld Snooping Mrouter Port               :
Mld Snooping Mrouter Port Aging Interval(sec) :255
```

5.4 Configuring Querior Parameters

5.4.1 Configuration

In order for MLD, and thus MLD snooping, to function, a multicast router must exist on the network and generate MLD queries. The tables created for snooping (holding the member ports for a each multicast group) are associated with the querier. Without a querier the tables are not created and snooping will not work.

Switch# configure terminal	Enter Configuration mode
Switch(config)# ipv6 enable	Enable ipv6
Switch(config)# ipv6 mld snooping query-interval 100	Set mld snooping query interval globally
Switch(config)# ipv6 mld snooping query-max-response-time 5	Set mld snooping max query response time globally
Switch(config)# ipv6 mld snooping last-member-query-interval 2000	Set mld snooping last member query interval globally
Switch(config)# ipv6 mld snooping vlan 1 querier address fe80::1	Configure mld snooping querier IPv6 address on vlan 1
Switch(config)# ipv6 mld snooping vlan 1 querier	Enable mld snooping querier on vlan 1
Switch(config)# ipv6 mld snooping vlan 1 query-interval 200	Set mld snooping query interval on vlan 1
Switch(config)# ipv6 mld snooping vlan 1 query-max-response-time 5	Set mld snooping max response time on vlan 1
Switch(config)# ipv6 mld snooping vlan 1 querier-timeout 100	Set mld snooping querier timeout value on vlan 1
Switch(config)# ipv6 mld snooping vlan 1 last-member-query-interval 2000	Set mld snooping last member query interval on vlan 1
Switch(config)# ipv6 mld snooping vlan 1 discard-unknown	Discard all unknown multicast packet in vlan 1
Switch(config)# ipv6 mld snooping discard-unknown	Discard all unknown multicast packet globally

5.4.2 Validation

Switch# show ipv6 mld snooping querier

```
Global Mld Snooping Querier Configuration
-------------------------------------------------
Version                          :1
Last-Member-Query-Interval (msec) :2000
Max-Query-Response-Time (sec)     :5
Query-Interval (sec)              :100
Global Source-Address             :::
TCN Query Count                   :2
TCN Query Interval (sec)          :10

Vlan 1:   MLD snooping querier status
-----------------------------------------
Elected querier is : fe80::1
-----------------------------------------
Admin state                       :Enabled
Admin version                     :1
Operational state                 :Querier
Querier operational address       :fe80::1
Querier configure address         :fe80::1
Last-Member-Query-Interval (msec) :2000
Max-Query-Response-Time (sec)     :5
Query-Interval (sec)              :200
Querier-Timeout (sec)             :100
```

5.5 Configuring Mrouter Port

5.5.1 Configuration

An MLD Snooping mrouter port is a switch port which is assumed to connect a multicast router. The mrouter port is configured on the vlan or learnt dynamic. When MLD general query packet or PIMv6 hello packet is received on port of speficified VLAN, this port becomes mrouter port of this vlan. All the mld queries received on this port will be flooded on the belonged vlan. All the mld reports and leaves received on this vlan will be forwarded to the mrouter port, directly or aggregated, depending on the report-suppression configuration. In addition, all the multicast traffic on this vlan will be forwarded to this mrouter port.

Switch# configure terminal	Enter Configuration mode
Switch(config)# ipv6 enable	Enable ipv6

Switch(config)# ipv6 mld snooping report-suppression	Enable mld snooping report suppression globally
Switch(config)# ipv6 mld snooping vlan 1 mrouter interface eth-0-1	Configure mrouter port on vlan 1
Switch(config)# ipv6 mld snooping vlan 1 report-suppression	Enable mld snooping report suppression on vlan 1
Switch(config)# ipv6 mld snooping vlan 1 mrouter-aging-interval 200	Set mld snooping dynamic mrouter port aging interval

5.5.2 Validation

Switch# show ipv6 mld snooping vlan 1

```
Global Mld Snooping Configuration
------------------------------------------------
Mld Snooping                            :Enabled
Mld Snooping Fast-Leave                 :Enabled
Mld Snooping Version                    :1
Mld Snooping Max-Member-Number          :4096
Mld Snooping Unknown Multicast Behavior  :Discard
Mld Snooping Report-Suppression         :Enabled
Vlan 1
-----------
Mld Snooping                            :Enabled
Mld Snooping Fast-Leave                 :Enabled
Mld Snooping Report-Suppression         :Enabled
Mld Snooping Version                    :1
Mld Snooping Max-Member-Number          :4096
Mld Snooping Unknown Multicast Behavior  :Discard
Mld Snooping Group Access-list          :N/A
Mld Snooping Mrouter Port               :eth-0-1(static)
Mld Snooping Mrouter Port Aging Interval(sec) :200
```

5.6 Configuring Querier Tcn

5.6.1 Configuration

Switch# configure terminal	Enter Configuration mode
Switch(config)# ipv6 enable	Enable ipv6
Switch(config)# ipv6 mld snooping querier tcn query-count 5	Set mld snooping querier tcn query-count globally

Switch(config)# ipv6 mld snooping querier tcn query-interval 20	Set ip mld snooping querier tcn query-interval globally

5.6.2 Validation

Switch# show ipv6 mld snooping querier

```
Global Mld Snooping Querier Configuration
-------------------------------------------------
Version                          :1
Last-Member-Query-Interval (msec) :2000
Max-Query-Response-Time (sec)     :5
Query-Interval (sec)              :100
Global Source-Address             :::
TCN Query Count                   :5
TCN Query Interval (sec)          :20

Vlan 1:   MLD snooping querier status
-----------------------------------------
Elected querier is : fe80::1
-----------------------------------------
Admin state                       :Enabled
Admin version                     :1
Operational state                 :Querier
Querier operational address       :fe80::1
Querier configure address         :fe80::1
Last-Member-Query-Interval (msec) :2000
Max-Query-Response-Time (sec)     :5
Query-Interval (sec)              :200
Querier-Timeout (sec)             :100
```

5.7 Configuring Report Suppression

5.7.1 Configuration

The switch uses MLD report suppression to forward only one MLD report per multicast router query to multicast devices. When MLD router suppression is enabled (the default), the switch sends the first MLD report from all hosts for a group to all the multicast routers. The switch does not send the remaining MLD reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

Switch# configure terminal	Enter Configuration mode
Switch(config)# ipv6 enable	Enable ipv6

Switch(config)# ipv6 mld snooping report-suppression	Enable mld snooping report suppression globally
Switch(config)# ipv6 mld snooping vlan 1 report-suppression	Enable mld snooping report suppression on vlan 1

5.7.2 Validation

Switch# show ipv6 mld snooping

```
Global Mld Snooping Configuration
------------------------------------------------
Mld Snooping                              :Enabled
Mld Snooping Fast-Leave                   :Enabled
Mld Snooping Version                      :1
Mld Snooping Max-Member-Number            :4096
Mld Snooping Unknown Multicast Behavior   :Discard
Mld Snooping Report-Suppression           :Enabled
Vlan 1
-----------
Mld Snooping                              :Enabled
Mld Snooping Fast-Leave                   :Enabled
Mld Snooping Report-Suppression           :Enabled
Mld Snooping Version                      :1
Mld Snooping Max-Member-Number            :4096
Mld Snooping Unknown Multicast Behavior   :Discard
Mld Snooping Group Access-list            :N/A
Mld Snooping Mrouter Port                 :eth-0-1(static)
Mld Snooping Mrouter Port Aging Interval(sec) :200
```

5.8 Configuring Static group

5.8.1 Configuration

The switch can build MLD Snooping Group when receiving MLD report packet on Layer 2 port of specified VLAN. We also support configure static MLD Snooping Group by specifying MLD group, Layer 2 port and VLAN.

Switch# configure terminal	Enter Configuration mode
Switch(config)# ipv6 enable	Enable ipv6
Switch(config)# ipv6 mld snooping vlan 1 static-group ff0e::1234 interface eth-0-2	Configure static group on port eth-0-2 of vlan2

5.8.2 Validation

Switch# show ipv6 mld snooping groups

```
VLAN  Interface  Group Address                          Uptime      Expire-time
1     eth-0-2    ff0e::1234                             00:00:02    stopped
```

5.9 Limitations And Configuration Guidelines

VRRP, RIPng and OSPFv3 used multicast IPv6 address, so you need to avoid use such multicast IPv6 addresses, which have same multicast MAC address with multicast IPv6 address reserved by VRRP, RIPng and OSPFv3.

VRRP used multicast group address ff02::12, so when mld snooping and VRRP are working, you need to avoid using multicast group address that matched same mac address with group address ff02::12.

OSPFv3 used multicast group address ff02::5, so when mld snooping and OSFPv3 are working, you need to avoid using multicast group address that matched same mac address with group address ff02::5.

RIPng used multicast group address ff02::9, so when mld snooping and RIPng are working, you need to avoid using multicast group address that matched same mac address with group address ff02::9.

6 Configuring MVR6

6.1 Overview

Multicast VLAN Registration for IPv6 (MVR6) is designed for applications using wide-scale deployment of IPv6 multicast traffic across an Ethernet ring-based service provider network (for example, the broadcast of IPv6 multiple television channels over a service-provider network). MVR6 allows a subscriber on a port to subscribe and unsubscribe to a IPv6 multicast stream on the network-wide multicast VLAN. It allows the single multicast VLAN to be shared in the network while subscribers remain in separate VLANs. MVR6 provides the ability to continuously send IPv6 multicast streams in the multicast VLAN, but to isolate the streams from the subscriber VLANs for bandwidth and security reasons.

MVR6 assumes that subscriber ports subscribe and unsubscribe (join and leave) these multicast streams by sending out MLD join and leave messages. These messages can originate from an MLD version-1-compatible host with an Ethernet connection. Although MVR6 operates on the underlying mechanism of MLD snooping, the two features operation affect with each other. One can be enabled or disabled with affecting the behavior of the other feature. If MLD snooping and MVR6 are both enabled, MVR6 reacts only to join and leave messages from IPv6 multicast groups configured under MVR6. The switch CPU identifies the MVR6 IPv6 multicast streams and their associated MAC addresses in the switch forwarding table, intercepts the MLD messages, and modifies the forwarding table to include or remove the subscriber as a receiver of the multicast stream, and the receivers must be in a different VLAN from the source. This forwarding behavior selectively allows traffic to cross between different VLANs.

6.2 Terminology

MVR6: Multicast Vlan Registration for IPv6.

Source vlan: The vlan for receiving multicast traffic for MVR6.

Source port: The port in the source vlan for sending report or leave to upstream.

Receiver port: The port not in source vlan for receiving report or leave for downstream.

6.3 Topology

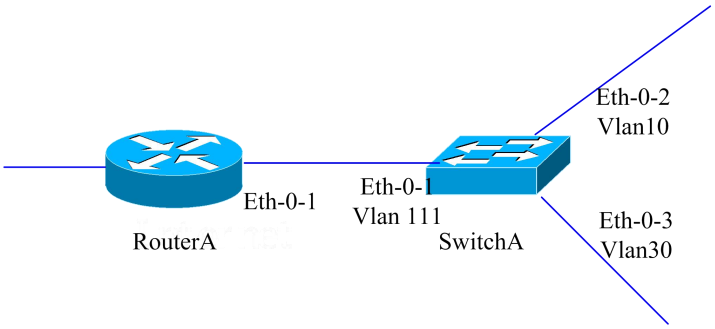

Figure 6-1 MVR6 Topology

6.4 Configurations

Purpose

Enable MLD&PIMv6-SM in the interface of eth-0-1 of Router A.

Configure switch A: eth-0-1 in vlan111, eth-0-2 in vlan10, and eth-0-3 vlan30.

Enable MVR6 in the switchA, it is required that only one copy of IPv6multicast traffic from Router A is sent to switch A, but HostA and HostC can both receive this IPv6 multicast traffic.

Router A

Enable ipv6 pim-sm and mld in the eth-0-1.

RouterA# configure terminal	Enter the configure mode
RouterA(config)# ipv6 enable	Enable ipv6
RouterA (config)# interface eth-0-1	Enter the Interface mode
RouterA (config-if)# no switchport	Configure on physical port only, change this port to Layer3 interface
RouterA (config-if)# no shutdown	Enable this interface
RouterA (config-if)# ipv6 address 2001:1::1/64	Configure IPv6 address to 2001:1::1/64
RouterA (config-if)# ipv6 pim sparse-mode	Enable IPv6 pim sparse-mode on interface
RouterA (config-if)# end	Return to privileged EXEC mode

Switch A

Eth-0-1 in vlan111, eth-0-2 in vlan10, and eth-0-3 vlan30.

SwitchA# configure terminal	Enter the configure mode
SwitchA(config)# vlan database	Enter VLAN database mode
SwitchA(config-vlan)# vlan 111,10,30	Creat vlan 111,10,30
SwitchA(config-vlan)# quit	Quit the VLAN database mode and return to Configure mode to configure the next interface.
SwitchA(config)# interface vlan 111	Create Source VLAN interface
SwitchA(config-if)# exit	Return to Config mode
SwitchA(config)# interface vlan 10	Create Receiver VLAN interface
SwitchA(config-if)# exit	Return to Config mode
SwitchA(config)# interface vlan 30	Create Receiver VLAN interface
SwitchA(config-if)# exit	Return to Config mode
SwitchA(config)# interface eth-0-1	Enter the Interface mode
SwitchA(config-if)# switchport access vlan111	Enable VLAN port access by specifying the VLAN ID 111 on this interface
SwitchA(config)# interface eth-0-2	Enter the Interface mode.

SwitchA(config-if)# switchport access vlan10	Enable VLAN port access by specifying the VLAN ID 10 on this interface
SwitchA(config)# interface eth-0-3	Enter the Interface mode.
SwitchA(config-if)# switchport access vlan30	Enable VLAN port access by specifying the VLAN ID 30 on this interface
SwitchA(config-if)# end	Return to privileged EXEC mode

Eanble MVR6 in the switchA, it is required that only one copy of IPv6 multicast traffic from Router A is sent to switchA, but HostA and HostC can both receiver this IPv6 multicast traffic.

SwitchA # configure terminal	Enter the configure mode
SwitchA(config)# no ipv6 multicast-routing	Disable ipv6 multicast-routing
SwitchA(config)# mvr6	Enable Multicast Vlan Registration for IPv6
SwitchA(config)# mvr6 vlan 111	Configure mvr6 vlan
SwitchA(config)# mvr6 group ff0e::1234 64	Configure mvr6 group address
SwitchA(config)# mvr6 source-address fe80::1111	Configure mvr6 source-address
SwitchA(config)# interface eth-0-1	Enter the Interface mode
SwitchA(config-if)# mvr6 type source	Configure the port to mvr6 type source
SwitchA(config)# interface eth-0-2	Enter the Interface mode
SwitchA(config-if)# mvr6 type receiver vlan 10	Configure the port to mvr6 type receiver
SwitchA(config)# interface eth-0-3	Enter the Interface mode
SwitchA(config-if)# mvr6 type receiver vlan 30	Configure the port to mvr6 type receiver
SwitchA(config-if)# end	Return to privileged EXEC mode

6.5 Validation

Router A

RouterA # show ipv6 mld groups

```
MLD Connected Group Membership
Group Address                           Interface            Expires
ff0e::1234                              eth-0-2              00:03:01
ff0e::1235                              eth-0-2              00:03:01
ff0e::1236                              eth-0-2              00:03:01
ff0e::1237                              eth-0-2              00:03:01
ff0e::1238                              eth-0-2              00:03:01
.....
ff0e::1273                              eth-0-2              00:03:01
```

Switch A

SwitchA# show mvr6

```
MVR6 Running: TRUE
MVR6 Multicast VLAN: 111
MVR6 Source-address: fe80::111
MVR6 Max Multicast Groups: 1024
MVR6 Hw Rt Limit: 224
MVR6 Current Multicast Groups: 64
```

SwitchA# show mvr6 groups

```
VLAN   Interface   Group Address                          Uptime      Expire-time
10      eth-0-2    ff0e::1234                             00:03:23    00:02:03
10      eth-0-2    ff0e::1235                             00:03:23    00:02:03
10      eth-0-2    ff0e::1236                             00:03:23    00:02:03
10      eth-0-2    ff0e::1237                             00:03:23    00:02:03
10      eth-0-2    ff0e::1238                             00:03:23    00:02:03
10      eth-0-2    ff0e::1239                             00:03:23    00:02:03
.....
10      eth-0-2    ff0e::1273                             00:03:23    00:02:03
```