ZebOS-XP®
Network Platform

Version 1.4
Extended Performance

Multicast Configuration Guide

December 2015

IP Infusion Inc.
3965 Freedom Circle, Suite 200
Santa Clara, CA 95054
+1 408-400-1900
http://www.ipinfusion.com/

For support, questions, or comments via E-mail, contact:
support@ipinfusion.com

Contents

Preface

This guide describes how to configure multicast protocols in ZebOS-XP.

Audience

This guide is intended for network administrators and other engineering professionals who configure multicast protocols.

Conventions

Table P-1 shows the conventions used in this guide.

Table P-1: Conventions

Convention	**Description**
Italics	Emphasized terms; titles of books
Note:	Special instructions, suggestions, or warnings
`monospaced type`	Code elements such as commands, functions, parameters, files, and directories

Contents

This document contains these chapters and appendices:

- Chapter 1, *PIM Sparse Mode Configuration*
- Chapter 2, *Bidirectional-PIM Configuration*
- Chapter 3, *PIM Dense Mode Configuration*
- Chapter 4, *Multicast Virtual Routing Configuration*
- Chapter 9, *IGMP Snooping Configuration*
- Chapter 5, *PIM Sparse-Dense Mode Configuration*
- Chapter 6, *PIM-ECMP Redirect Configuration*
- Appendix A, *Tunnel Interface*

Related Documents

Use this guide with these command reference for details about the commands used in the configurations.

- *Multicast Routing Information Base Command Reference*
- *Protocol Independent Multicasting Command Reference*
- *Virtual Routing Command Reference*

Note: All ZebOS-XP technical manuals are available to licensed customers at http://www.ipinfusion.com/support/document_list.

Chapter Organization

The chapters in this guide are organized into these major sections:

- An overview that explains a configuration in words
- Topology with a diagram that shows the devices and connections used in the configuration
- Configuration steps in a table for each device where the left-hand side shows the commands you enter and the right-hand side explains the actions that the commands perform
- Validation which shows commands and their output that verify the configuration

Support

For support-related questions, contact support@ipinfusion.com.

Comments

If you have comments, or need to report a problem with the content, contact techpubs@ipinfusion.com.

CHAPTER 1 PIM Sparse Mode Configuration

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

This chapter provides the following topics:

- Terminology
- Data Flow from Source to Receivers in PIM-SM Network Domain
- PIM-SM Configuration
- Anycast-RP Configuration
- Embedded RP Configuration

Terminology

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

Rendezvous Point

A Rendezvous Point (RP) router is configured as the root of a 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

The Multicast Routing Information Base (MRIB) is a multicast topology table derived from the unicast routing table. In PIM-SM, the MRIB decides 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 an optimized form of flooding, in which the router accepts a packet from `SourceA` through Interface `IF1`, only if `IF1` is the interface the router uses to reach `SourceA`. To determine if the interface is correct, it consults its unicast routing tables. The packet that arrives through interface `IF1` is forwarded because the routing table lists this interface as the shortest path. 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

The Tree Information Base (TIB) is a collection of states at a PIM router storing the state of all multicast distribution trees at that router. The TIB is created by receiving Join/Prune messages, Assert messages, and IGMP information from local hosts.

Upstream

Upstream indicates that traffic is going towards the root of the tree. The root of the tree might be either the Source or the RP.

Downstream

Downstream indicates that traffic is going away from the root of the tree. The root of tree might be either the Source or the RP.

Source-Based Trees

In Source-Based Trees, the forwarding paths are based on the shortest unicast path to the source. If the unicast routing metric used is `hop counts`, the branches of the multicast Source-Based Trees are minimum hop. If the metric used is `delay`, the branches are minimum delay. A corresponding multicast tree directly connects the source to all receivers for every multicast source. 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. 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, 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).

Note: Not all hosts are receivers.

Bootstrap Router

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

Data Flow from Source to Receivers in PIM-SM Network Domain

1. Sending out Hello Messages

PIM routers periodically send Hello messages to discover neighboring PIM routers. Hello messages are multicast using the address, 224.0.0.13 (`ALL-PIM-ROUTERS` group). Routers do not send any acknowledgement that a Hello message was received. A `holdtime` value determines the length of time for which the information is valid. In PIM-SM, a downstream receiver must join a group before traffic is forwarded on the interface.

2. Electing a Designated Router

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

3. Determining the Rendezvous Point

PIM-SM uses a 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 IP 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 IGMP for (or a data packet from) a directly connected host, for a group for which it has no entry, the designated router (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.

4. Joining the Shared Tree

To join a multicast group, a host sends an IGMP 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 PIM 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.

5. 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 de-encapsulates 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 IP 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.

6. Sending Register-Stop Messages

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

7. 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 IGMP state of the DR is deleted, and the interface is removed from the Source and Group lists of the group.

8. Forwarding Multicast Packets

PIM-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. If a downstream router has sent a join to this router or is a member of this group, then traffic that arrives on the correct interface is sent to all outgoing interfaces that lead to downstream receivers.

PIM-SM Configuration

PIM-SM is a soft-state protocol. The required steps to configure PIM-SM are the following:

- Enable IP multicast on each PIM router (see Enabling IP Multicast Routing)
- Enable PIM-SM on the desired interfaces (see Enable PIM-SM on an Interface)
- Configure the RP statically (see Configuring Rendezvous Point Statically or dynamically (see Configure Rendezvous Point Dynamically Using Bootstrap Router Method) depending on which method you use)

All multicast group states are dynamically maintained as the result of IGMP `Report/Leave` and PIM `Join/Prune` messages.

This section provides the steps to configure the PIM-SM feature. Configuration steps and examples are used for two relevant scenarios.

Topology

The following figure displays the network topology used in these examples.

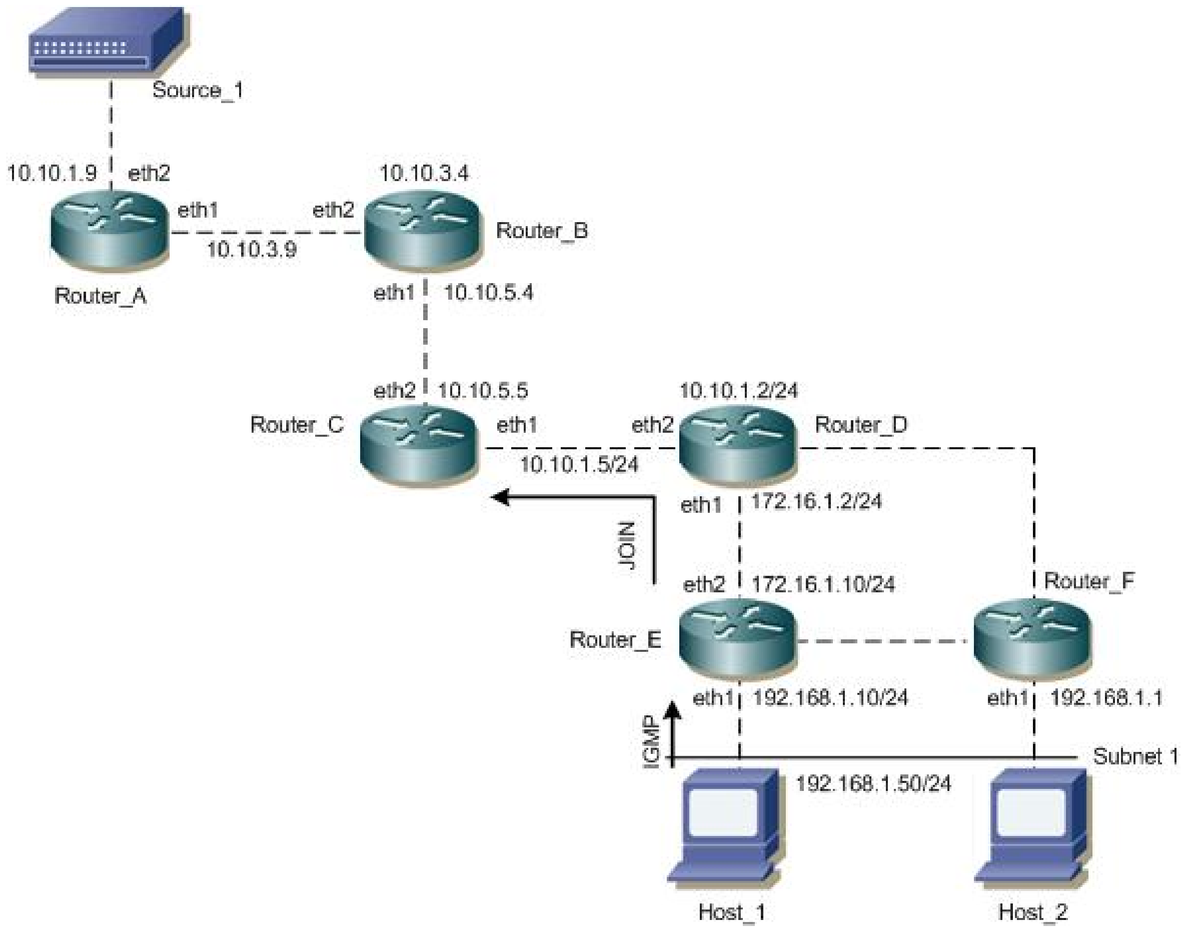

Figure 1-1: PIM-SM Topology

Enabling IP Multicast Routing

Enable IP multicast routing on all of the PIM routers inside the PIM domain:

Enable IP Multicast Routing

`#configure terminal`	Enter Configure mode.
`(config)#ip multicast-routing`	Enable IP multicast routing.
`(config)#exit`	Exit Configure mode.

Enable PIM-SM on an Interface

Enable PIM-SM on all participating interfaces within each of routers inside the PIM domain on which you want to run PIM. In the following sample configuration, both eth1 and eth2 are enabled for PIM-SM on the router.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to be configured and enter the Interface mode.
`(config-if)#ip address 10.10.12.11/24`	Configure the IP address for `eth1`.
`(config-if)#ip pim sparse-mode`	Enable PIM sparse mode on the interface.
`(config-if)#exit`	Exit Interface mode.
`(config)#interface eth2`	Specify the interface (`eth2`) to be configured and enter the Interface mode.
`(config-if)#ip address 10.10.13.11/24`	Configure the IP address for `eth2`.
`(config-if)#ip pim sparse-mode`	Enable PIM sparse mode on the interface.
`(config-if)#exit`	Exit Interface mode.

Configuring Rendezvous Point Statically

Every PIM multicast group needs to be associated with the IP address of a Rendezvous Point (RP), which is a router that resides in a multicast network domain. The address of the RP is used as the root of a group-specific distribution tree. All nodes in the domain that want to receive traffic sent to the group are aware of the address of the RP. For all senders to reach all receivers within a group, all routers in the domain must be able to map to the RP address configured for the group. There can be several RPs configured in a network deploying PIM-SM, each serving a different group.

You can statically configure a RP by specifying the RP address with in every router in the PIM domain. The use of statically configured RPs is ideal for small network environments or ones that do not require many RPs and/or require changing the assignment of the RPs often. Changing the assignment of an RP requires the re-configuration of the RP address in all of the routers in the PIM domain.

In static RP configurations, RP failover is not available.

When configuring the RP statically, do the following:

- On every router, include the `ip pim rp-address A.B.C.D` statement even if a router does not have any source or group member attached to it

- Assign only one RP address for a multicast group in the PIM domain

Using the topology depicted in Figure 1-1, Router_C is the RP, and all routers are statically configured with RP information. Host_1 and Host_2 join group 224.0.1.3 for all the sources. They send the IGMP membership report to Subnet 1. Two routers are attached to Subnet 1, Router_E and Router_F; both have default DR priority on eth1. Since Router_E has a higher IP address on interface eth1, it becomes the Designated Router, and is responsible for sending Join messages to the RP (Router_C).

Configure Static RP

#configure terminal	Enter Configure mode.
(config)#ip pim rp-address 10.10.1.5	Statically configure an RP address for multicast groups.
(config)#exit	Exit Configure mode.

Here is the sample configuration for Router_D:

```
hostname Router_D
!
interface eth0
!
interface eth1
 ip pim sparse-mode
!
interface eth2
 ip pim sparse-mode
!
interface lo
!
!
ip multicast-routing

ip pim rp-address 10.10.1.5
!
```

Validation

Enter the commands listed in this section to confirm the previous configurations.

RP Details

At Router_D, the show ip pim rp mapping command shows that 10.10.1.5 is the RP for all multicast groups 224.0.0.0/4, and is statically configured. All other routers will have a similar output:

```
Router_D#sh ip pim rp mapping
PIM Group-to-RP Mappings
Override RP cnt: 0
Group(s): 224.0.0.0/4, Static
    RP: 10.10.1.5
         Uptime: 00:01:45
```

At Router_D, use the show ip pim rp-hash command to display the selected RP for a specified group (224.0.1.3):

```
Router_D#show ip pim rp-hash 224.0.1.3
RP: 10.10.5.37
```

Interface Details

The show ip pim interface command displays the interface details for Router_E, and shows that Router_E is the Designated Router on Subnet 1.

```
Router_E#show ip pim interface
Address          Interface VIFindex Ver/   Nbr      DR    DR
                                    Mode   Count   Prior
192.168.1.10      eth1      0       v2/S   1         1     192.168.1.10
172.16.1.10       eth2      2       v2/S   1         1     172.16.1.10
```

IP Multicast Routing Table

Note: The multicast routing table displays for an RP router are different from other routers.

The show ip pim mroute command displays the IP multicast routing table. In this table, the following fields are defined:

RPF nbr Displays the unicast next-hop to reach RP.

and mask length.

RPF idx Displays the incoming interface for this (*, G) state.

RP Displays the IP address for the RP router

B Displays the bidirectional pim mode

The leading dots ....

Stand for VIF index

```
Router_E#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
(*, 224.0.1.3)
RP: 10.10.1.5
RPF nbr: 172.16.1.2
RPF idx: eth2
Upstream State: JOINED
 Local     ................................
 Joined    j...............................
 Asserted  ................................
 Outgoing  o...............................
```

At Router_E, eth2 is the incoming interface of the (*, G) entry, and eth1 is on the outgoing interface list of the (*, G) entry. This means that there is a group member through eth1, and the RP is reachable through eth2.

The 0 position on this 32-bit index is for eth1 (as illustrated in the interface display above). The j on the 0 index indicates that the Join has come from eth1.

Since Router_C is the RP, and the root of this multicast tree, the show ip pim mroute command on Router_C shows RPF nbr as 0.0.0.0 and RPF idx as none.

```
Router_C#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
```

```
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
(*, 224.0.1.3)
RP: 10.10.1.5
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 Local     ................................
 Joined    j...............................
 Asserted  ................................
 Outgoing  o...............................
```

Configure Rendezvous Point Dynamically Using Bootstrap Router Method

A static RP configuration works for a small, stable PIM network domain; however, it is not practical for a large and/or complex one. In such a network, if the RP fails or you have to change the assignment of the RP, you are required to reconfigure the static configurations on all PIM routers. Also, if you have several multicast groups mapped to several RPs, there are many repetitive configurations you are required to perform, which can be time consuming and laborious. Thus when it comes configuring RP in large and/or complex networking environments, configuring it dynamically is the best and most scalable method to use. Bootstrap router (BSR) configuration is one method of configuring the RP dynamically.

The BSR mechanism in a PIM domain uses the concept of a RP as a way for receivers to discover the sources that send to a particular multicast group. The BSR mechanism gives a way for a multicast router to learn the set of group-to-RP mappings required in order to function. The BSR’s function is to broadcast the RP set to all routers in the domain.

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

Some of the PIM routers in the domain are configured to be Candidate-BSRs (C-BSR). One C-BSR is selected to be the BSR for the domain, and all PIM routers in the domain learn the result of this election through Bootstrap messages (BSM). The C-BSR with highest value in the priority field is elected to be the BSR. The C-RPs then report their candidacies 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 using Bootstrap messages.

This section provides 2 examples to illustrate the BSR configuration for configuring RP dynamically.

Example 1

For this example, refer to Figure 1 for the topology.

To dynamically configure the RP, `Router_C` on `eth1` and `Router_D` on `eth1` are configured as a Candidate RP using the `ip pim rp-candidate` command. `Router_D` on `eth1` is also configured as the Candidate BSR. Since no other router has been configured as the candidate BSR, `Router_D` becomes the BSR router and is responsible for sending group-to-RP-mapping information to all other routers in this PIM domain.

The highest priority router (configured with lowest priority value) 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 ensure that all routers in the PIM-domain have the same RP for the same group.

To change the default priority of any candidate RP, use the `ip pim rp-candidate IFNAME PRIORITY` command. At `Router_D`, the `show ip pim rp mapping` command shows that `Router_C` is chosen as the RP for a specified group.

Configure RP Dynamically for Router C

`#configure terminal`	Enter Configure mode.
`(config)#ip pim rp-candidate eth1 priority 2`	Give this router the candidate RP status using the IP address of the specified interface.

Configure RP Dynamically for Router D

`#configure terminal`	Enter Configure mode.
`(config)#ip pim bsr-candidate eth1`	Give this router the candidate BSR status using the name the interface.
`(config)#ip pim rp-candidate eth1 priority 2`	Give this router the candidate RP status using the IP address of the specified interface.

The following output displays the complete configuration at `Router_C` and `Router_D`:

```
Router_D#show running-config
!
interface eth0
!
interface eth1
 ip pim sparse-mode
!
interface eth2
 ip pim sparse-mode
!
interface lo
!
ip multicast-routing
ip pim bsr-candidate eth1
ip pim rp-candidate eth1 priority 2
!

Router_C#show running-config
interface eth0
!
interface eth1
 ip pim sparse-mode
!
interface eth2
 ip pim sparse-mode
!
interface lo
!
!
ip multicast-routing
ip pim rp-candidate eth1
```

Validation

This section provides the steps to verify the RP configuration, interface details, and multicast routing table.

PIM Group-to-RP Mappings

The `show ip pim rp mapping` command displays the group-to-RP mapping details and displays information about RP candidates. There are two RP candidates for the group range, 224.0.0.0/4. RP Candidate 10.10.1.5 has a default priority of 192, whereas, RP Candidate 172.16.1.2 has been configured to have a priority of 2. Since RP candidate 172.16.1.2 has a higher priority, it is selected as RP for the multicast group, 224.0.0.0/4.

```
Router_D#show ip pim rp mapping
This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/4
 RP: 10.10.1.5
    Info source: 172.16.1.2, via bootstrap, priority 192
         Uptime: 00:00:13, expires: 00:02:29
 RP: 172.16.1.2
    Info source: 172.16.1.2, via bootstrap, priority 2
         Uptime: 00:34:42, expires: 00:01:49
```

RP Details

To display information about the RP router for a particular group, use the following command. This output displays that 172.16.1.2 has been chosen as the RP for the multicast group 224.0.1.3.

```
Router_D#show ip pim rp-hash 224.0.1.3
Group(s): 224.0.0.0/4
    RP: 172.16.1.2
    Info source: 172.16.1.2, via bootstrap
```

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

Example 2

To dynamically configure the RP, `Router_2` on `eth1` is configured as a Candidate RP using the `ip pim rp-candidate` command. Since no other router is configured as C-RP, `Router_2` becomes the RP. `Router_1` on `eth1` and `Router_2` on `eth1` are configured as the Candidate BSRs. Since `Router_1` has a higher priority value than `Router_2`, `Router_1` becomes the BSR router and is responsible for sending group-to-RP-mapping information to all other routers in this PIM domain.

Topology

For this example, refer to Figure 1-2 for the topology.

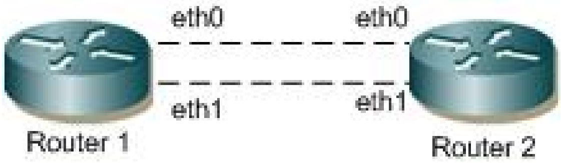

Figure 1-2: Boostrap Router Topology

Router 1

`#configure terminal`	Enter Configure mode for `eth1`.
`(config)#ip pim bsr-candidate eth1`	Configure `eth1` of Router 1 as C-BSR. The default priority is 64, so it is not necessary to designate a priority.
`(config)#exit`	Exit Configure mode.

Router 2

`#configure terminal`	Enter the Configure mode.
`(config)#ip pim bsr-candidate eth1 10 25`	Configure `eth1` of Router 2 as C-BSR with a hash mask length of 10, and a priority of 25.
`(config)#ip pim rp-candidate eth1 priority 0`	Configure interface `eth1` as C-RP with a priority of 0.
`(config)#exit`	Exit Configure mode.

Router 2 Unicast BSM

When the `ip pim unicast-bsm` command is configured on an interface that is a DR for a network, then that interface unicasts the stored copy of BSM to the new or rebooting router.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Enter the Interface mode for `eth1`.
`(config-if)#ip pim dr-priority 10`	Configure `eth1` as DR
`(config-if)#ip pim unicast-bsm`	Enable sending and receiving of Unicast BSM for backward compatibility.
`(config-if)#exit`	Exit Interface mode.

Validation

1. Verify the C-BSR state on Router 1.

```
#show ip pim bsr-router
      PIMv2 Bootstrap information
      This system is the Bootstrap Router (BSR)
        BSR address: 20.0.1.21
        Uptime:      00:37:12, BSR Priority: 64, Hash mask length: 10
        Next bootstrap message in 00:00:04
        Role: Candidate BSR
        State: Elected BSR
```

2. Verify the C-BSR state on Router 2.

   The initial state of C-BSR is P-BSR before transitioning to C-BSR. The two states are illustrated in the sample outputs from the `show ip pim bsr-router` command below.

```
#show ip pim bsr-router
PIMv2 Bootstrap information
  BSR address: 20.0.1.21
  Uptime:      00:02:39, BSR Priority: 64, Hash mask length: 10
  Expires:     00:00:03
  Role: Candidate BSR
  State: Pending BSR

#show ip pim bsr-router
PIMv2 Bootstrap information
 BSR address: 20.0.1.21
 Uptime:      00:40:20, BSR Priority: 64, Hash mask length: 10
 Expires:     00:02:07
 Role: Candidate BSR
 State: Candidate BSR
```

3. Verify RP-set information on E-BSR.

```
#show ip pim rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2)
Group(s): 224.0.0.0/4
 RP: 20.0.1.11
 Info source: 20.0.1.11, via bootstrap, priority 0
 Uptime: 00:00:30, expires: 00:02:04
```

4. Verify RP-set information on C-BSR.

```
#show ip pim rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4
RP: 20.0.1.11
Info source: 20.0.1.21, via bootstrap, priority 0
Uptime: 00:00:12, expires: 00:02:18
```

Anycast-RP Configuration

The Anycast-RP feature provides load balancing among active RPs and redundancy in a PIM-SM network domain. In a PM-SM configuration, only a single active RP for each multicast group within a domain is permitted. However, in an Anycast-RP configuration, this restriction is removed with the support of multiple active RPs for each group in a domain.

ZebOS-XP supports Anycast-RP using the PIM implementation. In PIM Anycast-RP, Multicast Source Discovery Protocol (MSDP) is not employed to share information about active sources. Instead the Register mechanism in PIM is extended to provide this same function.

The following describes Anycast-RP in PIM-SM:

- A Unicast IP address is used as the RP address. The address is statically configured, and associated with all PIM routers throughout the domain.
- A set of routers in the domain is 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 address. The loopback address is configured on all RPs for the loopback interface, then configured as the RP address (static RP), and injected into OSPF using redistribute connected. The PIM-SM implementation uses only the first non-loopback address configured on the loopback interface. Therefore, it is important to be sure that the Anycast-RP address is configured with the first non-loopback address.
- Each router in the Anycast-RP set also needs a separate IP address, which is used for communication between the RPs.
- The RP address, or a prefix that includes the RP address, is injected into the unicast routing system inside 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.

Topology

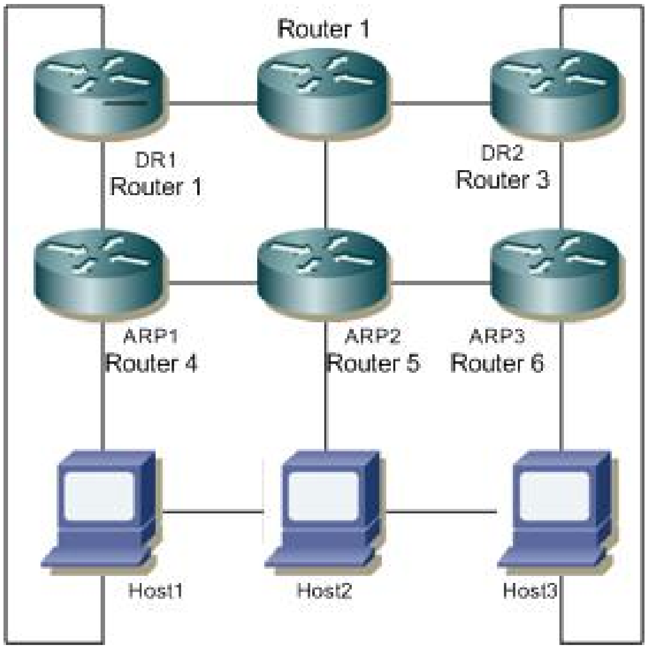

Figure 1-3: Anycast RP Topology

Host1 and Host3 act as hosts and sources for sending join and multicast data packets; Host2 acts as a host.

ARP1, ARP2 and ARP3

`#configure terminal`	Enter the Configure mode.
`(config)#interface lo`	Enter the loopback interface.
`(config)#ip address 1.1.1.152/32`	Configure the IP address for loopback
`(config)#exit`	Exit the Configure mode.
`(config)#ip pim rp-address 1.1.1.152`	Configure the static RP with the address of the loopback.
`(config)#ip pim anycast-rp 1.1.1.152 4.4.4.5`	Configure the member RP address. In this example, `4.4.4.5` is the member RP in ARP2. It is the address used for communication between all RPs.
`(config)#ip pim anycast-rp 1.1.1.152 7.7.7.1`	Configure the member RP address. In this example, `7.7.7.1` is the member RP in ARP3. It is the address used for communication between all RPs.
`(config)#ip pim anycast-rp 1.1.1.152 23.23.23.1`	Configure the member RP address. In this example, `23.23.23.1` is the member RP in ARP1. It is the address used for communication between all RPs.
`(config)#exit`	Exit the Configure mode.

Disable Anycast-RP

`#configure terminal`	Enter Configure mode.
`(config)#no ip pim anycast-rp 1.1.1.152`	Disable Anycast-RP.
`(config)#no ip pim rp-address 1.1.1.152`	Disable static RP.
`(config)#exit`	Exit Configure mode.

Validation

1. Verify RP-mapping in ARP1.

```
#show ip pim rp mapping
      PIM Group-to-RP Mappings
      Group(s): 224.0.0.0/4, Static
          RP: 1.1.1.152
               Uptime: 20:20:29
```

2. Verify RP-mapping in ARP1 after disabling anycast-RP and RP-address.

```
#show ip pim rp mapping
      PIM Group-to-RP Mappings
```

Embedded RP Configuration

RFC 3956 describes a multicast address allocation policy, in which the address of the Rendezvous Point (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.

Embedded RP Multicast Group Address Format

RFC 3956 specifies a modification to the unicast-prefix-based address format by specifying the second high-order bit (R-bit), as follows:

```
|    8   | 4  | 4  | 4  | 4  | 8  |       64       |    32    |
|11111111|flgs|scop|rsvd|RIID|plen| network prefix | group ID |
```

The `flgs` is a set of four flags: |0|R|P|T|

When the highest-order bit is 0, flag R = 1, which indicates a multicast address that embeds the address on the RP. In this case, P must be set to 1, and T must be set to 1. In effect, this implies the prefix `FF70::/12,` which means that the last 4 bits of the previously reserved field are interpreted as the embedded RP interface ID.

RP Address in Embedded RP Multicast Address

The address of the RP can only be embedded in unicast prefix-based Any Source Multicast (ASM) addresses. To identify whether an address is an embedded RP multicast address, and should be processed any further, an address must satisfy all of the following criteria:

- It must be a multicast address with `flgs` set to 0111, that is, to be of the prefix FF70::/12; or `flgs` set to 1111, for example, FFF0::/12
- `plen` must not be 0 (Source-Specific Multicast or SSM)
- `plen` must not be greater than 64

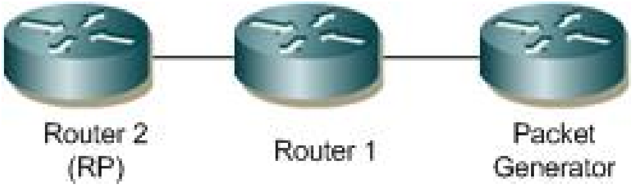

Figure 1-4: Topology

Enable Embedded RP

`#configure terminal`	Enter Configure mode.
`(config)#ipv6 multicast-routing`	Configure Multicast routing
`(config)#ipv6 pim rp embedded`	Enable embedded RP-to-group mapping.
`(config)#ipv6 access-list embedrp1 permit ff7e:240:3ffe:172:31:12::/96`	Configure an access-list to permit the multicast group.
`(config)#ipv6 pim rp-address 3ffe:172:31:12::2 embedrp1`	Configure a static RP, and limit the valid groups using an access list.
`(config)#exit`	Exit Configure mode.

Disable Embedded RP

`#configure terminal`	Enter Configure mode.
`(config)#no ipv6 pim rp embedded`	Disable embedded RP-to-group mapping.
`(config)#exit`	Exit Configure mode.

Plen bits and the RP Interface ID (RIID) from the embedded-RP group address form the embedded-RP address. Therefore, the global IPv6 address should look like the following example

```
3ffe:192:168:1::1/64 (to)
3ffe:192:168:1::15/64
```

The static-RP configuration should limit the valid groups via an access list as in this example:

```
ipv6 access-list embedrp permit ff7e:0240:3ffe:192:168:1::/96
ipv6 pim rp-address 3ffe:192:168:1::2 embedrp
```

Packets should be generated in the group range <f`f7e:0240:3ffe:192:168:1::/96`>.

Validation

The group-to-RP mapping for embedded-RP addresses is created when the group is first seen at a PIM router. This can be due to the MLD local receiver report, Join/Prune and Register message processing.

1. Verify RP-mapping in RP router.

```
#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
Group(s): ff7e:240:3ffe:172:31:12::/96, Static
    RP: 3ffe:172:31:12::2
         Uptime: 00:04:12
Embedded RP Groups:
Group(s): ff7e:240:3ffe:172:31:12::/96
    RP: 3ffe:172:31:12::2, Uptime: 00:00:33
```

2. Verify RP-mapping in non-RP router.

```
#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
Embedded RP Groups:
Group(s): ff7e:240:3ffe:172:31:12::/96
    RP: 3ffe:172:31:12::2, Uptime: 00:00:27
```

CHAPTER 2 Bidirectional-PIM Configuration

Bidirectional PIM (BIDIR-PIM) is a variant of PIM Sparse-Mode (PIM-SM) that builds bidirectional shared trees connecting multicast sources and receivers as specified in RFC5015.

BIDIR-PIM dispenses with both encapsulation and source state by allowing packets to be natively forwarded from a source to the Rendezvous Point (RP) using shared tree state.

BIDIR-PIM uses the same tree for traffic from source towards RP and from RP to receivers.

Note: BIDIR-PIM is not supported for ZebIC releases.

Designated Forwarders (DF) Election

Bidirectional Shared-Trees violates current (*, G) RPF rules, as it accepts traffic from one Reverse Path Forwarding (RPF) interface only. To avoid forwarding multicast packet looping, bidir-PIM introduces a new mechanism called the designated forwarder (DF) election.

The designated forwarder (DF) election takes place for all PIM routers on every network segment and point-to-point link. The procedure selects one router as the DF for every RP of bidirectional groups. The designated forwarder is responsible for forwarding multicast packets received on that network.

PIM-SM Configuration

For the steps to configure PIM-SM refer to PIM Sparse Mode Configuration on page 9.

Enabling BIDIR-PIM

`#configure terminal`	Enter Configure mode.
`(config)#ip pim bidir-enable`	Enable bidir-pim
`(config)#exit`	Exit Configure mode.

Configuring BIDIR Rendezvous Point Statically

Configuring Static BIDIR RP

`#configure terminal`	Enter configure mode.
`(config)#ip pim rp-address 10.10.1.5 bidir`	Statically configure an RP address for multicast groups.
`(config)#exit`	Exit configure mode.

Here is the sample configuration for `Router_D`:

```
hostname Router_D
!
interface eth0
!
```

```
interface eth1
 ip pim sparse-mode
!
interface eth2
 ip pim sparse-mode
!
interface lo
!
!
ip multicast-routing

ip pim bidir-enable
ip pim rp-address 10.10.1.5 bidir
!
```

Validation

RP Details

At Router_D, the `show ip pim rp mapping` command shows that `10.10.1.5` is the RP for all multicast groups `224.0.0.0/4`, and is statically configured. All other routers will have a similar output:

```
Router_D#sh ip pim rp mapping
PIM Group-to-RP Mappings
Override RP cnt: 0
Group(s): 224.0.0.0/4, Static
    RP: 10.10.1.5 bidir
         Uptime: 00:01:45
```

At Router_D, use the `show ip pim rp-hash` command to display the selected RP for a specified group (224.0.1.3):

```
Router_D#show ip pim rp-hash 224.0.1.3
RP: 10.10.5.37
```

Interface Details

The `show ip pim interface` command displays the interface details for `Router_E`, and shows that `Router_E` is the Designated Router on `Subnet 1.`

```
Router_E#show ip pim interface
Address          Interface VIFindex Ver/   Nbr       DR     DR
                                    Mode   Count   Prior
192.168.1.10      eth1      0       v2/S   1         1     192.168.1.10
172.16.1.10       eth2      2       v2/S   1         1     172.16.1.10
```

IP Multicast Routing Table

Note: The multicast routing table displays for an RP router are different from other routers.

The `show ip pim mroute` command displays the IP multicast routing table. In this table, the following fields are defined:

`RPF nbr` Displays the unicast next-hop to reach RP.

and mask length.

`RPF idx` Displays the incoming interface for this (*, G) state.

`RP` Displays the IP address for the RP router

B	Displays the bidirectional pim mode
The leading dots	Stand for VIF index

```
Router_E#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
(*, 224.0.1.3)B
RP: 10.10.1.5
RPF nbr: 172.16.1.2
RPF idx: eth2
 Local     ................................
 Joined    j...............................
```

At `Router_E`, `eth2` is the incoming interface of the (*, G) entry, and the RP is reachable through `eth2`. The ‘B’ flag indicates that it is in bidirectional pim mode.

Since `Router_C` is the RP, and the root of this multicast tree, the `show ip pim mroute` command on `Router_C` shows `RPF nbr` as 0.0.0.0 and `RPF idx` as none.

```
Router_C#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
(*, 224.0.1.3)B
RP: 10.10.1.5
RPF nbr: 0.0.0.0
RPF idx: None
 Local     ................................
 Joined    j...............................
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(*, 224.0.1.3), uptime 00:00:07, stat expires 00:03:23
Owner PIM, Flags: TFB
  Outgoing interface list:
    eth2 (1)
    eth1 (1)
```

Configuring BIDIR-Neighbor Filter

This section shows how to configure a bidir-neighbor filter to specify which bidirectionally capable (bidir-capable) neighbors will participate in the designated forwarder (DF) election.

`#configure terminal`	Enter configure mode
`(config)# interface eth1`	Enter interface mode
`(config-if)# ip pim bidir-neighbor-filter Acl-name/acl-no`	Configure bidir-neighbor-filter at interface
`(config-if)# no ip pim bidir-neighbor-filter acl-name/acl-no`	Unconfigure bidir-neighbor-filter at interface

Validation

Enter the commands listed in this section to confirm the previous configurations.

```
      rtr6#show ip pim neighbor
      Neighbor        Interface          Uptime/Expires            Ver     DR
      Address                                                           Priority/Mode
      192.168.1.149   eth1               00:00:44/00:01:31         v2    1 / B
      192.168.1.152   eth1               00:00:01/00:01:44         v2    1 / DR  ------
--?B Flag is removed

      rtr6#show running-config interface eth1
      !
      interface eth1
       ip address 192.168.1.57/24
       no shutdown
       no snmp trap link-status
       ip ospf cost 10
       ip pim bidir-neighbor-filter 1
       ip pim sparse-mode
       lldp-agent
       no dcbx enable
       exit
```

Configuring BIDIR PIM Offer Message Interval Time

This section shows how to configure BIDIR PIM offer message interval time.

`#configure terminal`	Enter configure mode.
`(config)# ip pim bidir-offer-interval <1>`	Specify offer-interval in the range 1-20000
`(config-if)# no ip pim bidir-offer-interval`	Disable offer-interval

Validation

1. Verify the time set for offer message interval

```
      (config)#ip pim bidir-offer-interval 10

      #show running-config
```

```
  !
  no service password-encryption
  !
  debug nsm packet
  debug ip pim events
debug ip pim mfc
  debug ip pim packet
  debug ip pim state
  debug ip pim timer
  debug ip pim mib
  !
  ip vrf management
  !
  mpls propagate-ttl
  !
  no ip icmp-broadcast
  !
  ip multicast-routing
  !
  ip pim bidir-enable
  ip pim bidir-offer-interval 10
  ip pim rp-address 172.31.5.153 bidir
```

2. Verify neighbor information in Bidirectional PIM mode with “B” flag associated

```
rtr6#show ip pim neighbor
Neighbor        Interface          Uptime/Expires            Ver     DR
Address                                                          Priority/Mode
192.168.1.149   eth1               00:38:36/00:01:39         v2    1 / B
192.168.1.152   eth1               00:37:53/00:01:22         v2    1 / DR B
rtr6#
```

3. Verify DF status per interface

```
rtr6#show ip pim interface df
Interface RP               DF Winner        Metric
eth1      172.31.5.153     192.168.1.152    20
eth2      172.31.5.153     192.168.10.57    30
rtr6#
rtr6#show ip pim interface eth1 df 172.31.5.153

 Designated Forwarder election for eth1, 192.168.1.57, RP 172.31.5.153
 State                           Non-DF (Lose)
 Offer count is                  0
 Current DF ip address           192.168.1.152
 Last winner metric preference   110
 Last winner metric              20
rtr6#
```

Configuring BIDIR PIM Offer Interval Limit

This section shows how to configure the Protocol Independent Multicast (PIM) bidirectionally capable number of unanswered offers before it changes as the designated forwarder (DF).

`#configure terminal`	Enter Configure mode.
`(config)# ip pim bidir-offer-limit <offer packet limit>`	Configure bidir-offer-limit
`(config-if)# no ip pim bidir-offer-limit`	Disable offer-limit

Validation

```
rtr6#show  running-config
!
no service password-encryption
!
hostname rtr6
!
!
debug nsm packet
!
ip vrf management
!
mpls propagate-ttl
!
no ip icmp-broadcast
!
access-list 1 deny 192.168.1.152
access-list 1 permit any

!
ip multicast-routing
!
ip pim bidir-enable
ip pim bidir-offer-limit 5
ip pim register-rp-reachability
ip pim vrf management register-rp-reachability
!
```

Configure BIDIR Rendezvous Point Dynamically Using BSR Method

A static BIDIR RP configuration works for a small, stable PIM network domain; however, it is not practical for a large and complex one. In such a network, if the RP fails the assignment of the RP is changed and the static configurations need to be reconfigured on all PIM routers. Also, if several multicast groups are mapped to several RPs, there are many configurations which need to be redone.This is time consuming and laborious. Thus configuring BIDIR RP dynamically is the best and most scalable method to use. Bootstrap router (BSR) configuration is one method of configuring the BIDIR RP dynamically.

The BSR mechanism in PIM domain uses the concept of a RP as a way for receivers to discover the sources that send to a particular multicast group. The BSR mechanism gives a way for a multicast router to learn the set of group-to- RP mappings required in order to function. The BSR's function is to broadcast the BIDIR RP set to all routers in the domain.

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

Some of the PIM routers in the domain are configured to be Candidate-BSRs (C-BSR). One C-BSR is selected to be the BSR for the domain, and all PIM routers in the domain learn the result of this election through Bootstrap messages (BSM). The C-BSR with highest value in the priority field is elected to be the BSR. The C-RPs then report their candidacies 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 using Bootstrap messages.

This section provides two examples to illustrate dynamic BIDIR Rendezvous Point configuration through BSR (Bootstrap Router) Method

Example 1

For this example, see Figure 2-1 for the topology.

To dynamically configure the RP, Router_C on eth1 and Router_D on eth1 are configured as a Candidate BIDIR RP using the ip pim rp-candidate bidir command. Router_D on eth1 is also configured as the Candidate BSR. Since no other router has been configured as the candidate BSR, Router_D becomes the BSR router and is responsible for sending group-to-RP-mapping information to all other routers in this PIM domain.

The highest priority router (configured with lowest priority value) is chosen as the BIDIR RP. If two or more routers have the same priority, a hash function in the BSR mechanism is used to choose the BIDIR RP to ensure that all routers in the PIM- domain have the same RP for the same group.

To change the default priority of any candidate BIDIR RP, use the ip pim rp-candidate IFNAME bidir PRIORITY command. At Router_D, the show ip pim rp mapping command shows that Router_C is chosen as the BIDIR RP for a specified group

Topology

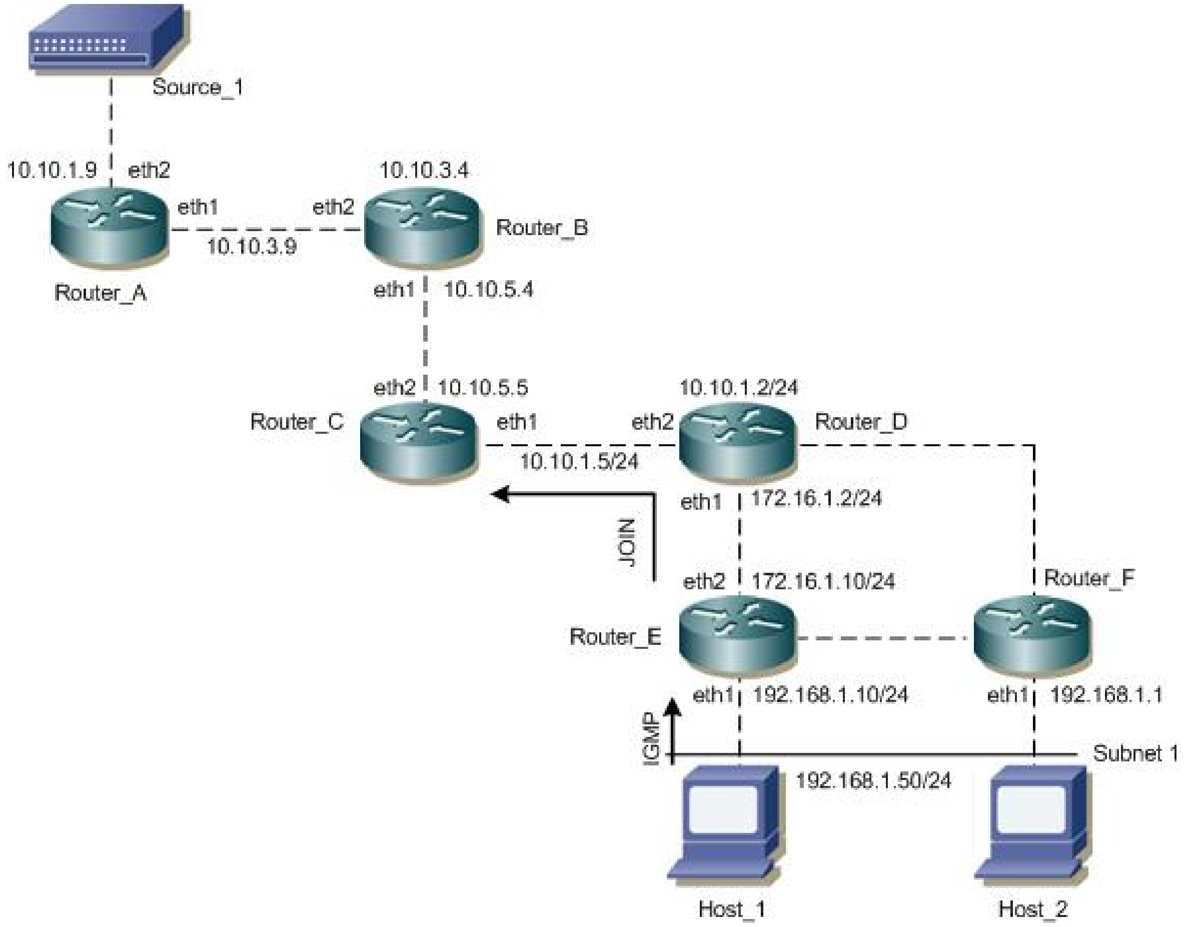

Figure 2-1: PIM-SM Topology

Configure BIDIR RP Dynamically for Router C

`#configure terminal`	Enter configure mode.
`(config)#ip pim rp-candidate eth1 bidir priority 2`	Configure the router with BIDIR RP status using the IP address of the interface
`(config)#exit`	Exit configure mode.

Configure BIDIR RP Dynamically for Router D

`#configure terminal`	Enter configure mode.
`(config)# ip pim bsr-candidate eth1`	Configure the router with BSR candidate status with the name of the interface
`(config)# ip pim rp-candidate eth1  priority 2`	Configure the router with BIDIR RP status using the IP address of the interface
`(config)#exit`	Exit configure mode.

Validation

Here is the sample configuration for `Router_D`:

```
Router_D#show running-config
!
interface eth0
!
interface eth1
ip pim sparse-mode
!
interface eth2
ip pim sparse-mode
!
interface lo
!
ip multicast-routing
!
ip pim bidir-enable
ip pim bsr-candidate eth1
ip pim rp-candidate eth1 bidir priority 2
!

Router_C#show running-config interface eth0
!
interface eth1
ip pim sparse-mode
!
interface eth2
ip pim sparse-mode
!
interface lo
!
!
ip multicast-routing
!
ip pim bidir-enable
ip pim rp-candidate eth1 bidir
!
```

PIM Group-to-RP Mappings

The `show ip pim rp mapping` command displays the group-to-RP mapping details and displays information about BIDIR RP candidates. There are two BIDIR RP candidates for the group range, 224.0.0.0/4. BIDIR RP Candidate 10.10.1.5 has a default priority of 192, whereas, BIDIR RP Candidate 172.16.1.2 has been configured to have a priority of 2. Since RP candidate 172.16.1.2 has a higher priority, it is selected as BIDIR RP for the multicast group, 224.0.0.0/4.

```
Router_D#show ip pim rp mapping
This system is the Bootstrap Router (v2) Group(s): 224.0.0.0/4
RP: 10.10.1.5, Bidir
Info source: 172.16.1.2, via bootstrap, priority 192
Uptime: 00:00:13, expires: 00:02:29
RP: 172.16.1.2, Bidir
Info source: 172.16.1.2, via bootstrap, priority 2
Uptime: 00:34:42, expires: 00:01:49
```

RP Details

To display information about the RP router for a particular group, use the following command. This output displays that 172.16.1.2 has been chosen as the RP for the multicast group 224.0.1.3.

```
Router_D#show ip pim rp-hash 224.0.1.3
Group(s): 224.0.0.0/4
RP: 172.16.1.2
Info source: 172.16.1.2, via bootstrap
```

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

Example 2

For this example, see Figure 2-2 for the topology.

To dynamically configure the BIDIR RP, router 2 on eth1 is configured as a Candidate BIDIR RP using the ip pim rp-candidate bidir command. Since no other router is configured as C-RP, router 2 becomes the BIDIR RP. Router 1 on eth1 and router 2 on eth1 are configured as the Candidate BSRs. Since router 1 has a higher priority value than router 2, router 1 becomes the BSR router and is responsible for sending group-to-RP-mapping information to all other routers in this PIM domain.

Topology

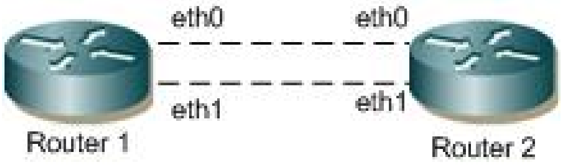

Figure 2-2: Boostrap Router Topology

Router 1

`#configure terminal`	Enter configure mode.
`(config)#ip pim bsr-candidate eth1`	Configure the router with as C-BSR.The default priority is 64 so it is not necessary to designate the priority
`(config)#exit`	Exit configure mode.

Router 2

`#configure terminal`	Enter configure mode.
`(config)# ip pim bsr-candidate eth1 0 25`	Configure the router as C-BSR with a mask length of 10 and a priority of 25
`(config)# ip pim rp-candidate eth1  bidir priority 0`	Configure interface as BIDIR C-RP with a priority of 0
`(config)#exit`	Exit configure mode.

Validation

C-BSR

Router1:

```
#show ip pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR) BSR address: 20.0.1.21
Uptime:00:37:12, BSR Priority: 64, Hash mask length: 10
Next bootstrap message in 00:00:04
Role: Candidate BSR State: Elected BSR
```

Router2:

The initial state of C-BSR is P-BSR before transitioning to C-BSR. The two states are illustrated in the sample outputs from the `show ip pim bsr-router` command below.

```
#show ip pim bsr-router
PIMv2 Bootstrap information
BSR address: 20.0.1.21
Uptime:00:02:39, BSR Priority: 64, Hash mask length: 10
Expires:00:00:03
Role: Candidate BSR State: Pending BSR

 #show ip pim bsr-router
PIMv2 Bootstrap information
BSR address: 20.0.1.21
Uptime:00:40:20, BSR Priority: 64, Hash mask length: 10
Expires:00:02:07
Role: Candidate BSR State: Candidate BSR
```

RP-set information on E-BSR

```
#show ip pim rp mapping
PIM Group-to-RP Mappings
This system is the Bootstrap Router (v2) Group(s): 224.0.0.0/4
RP: 20.0.1.11, Bidir
 Info source: 20.0.1.11, via bootstrap, priority 0
Uptime: 00:00:30, expires: 00:02:04
```

RP-set information on C-BSR

```
#show ip pim rp mapping PIM
Group-to-RP Mappings Group(s):
224.0.0.0/4
RP: 20.0.1.11, Bidir
Info source: 20.0.1.21, via bootstrap, priority 0
     Uptime: 00:00:12, expires: 00:02:18
```

CHAPTER 3 PIM Dense Mode Configuration

Protocol Independent Multicast - Dense Mode (PIM-DM) is a data-driven multicast routing protocol that builds source-based multicast distribution trees that operate on the flood-and-prune principle. PIM-DM requires unicast-reachability information, but it does not depend on a specific unicast routing protocol.

Terminology

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

Reverse Path Forwarding

Reverse Path Forwarding (RPF) is an optimized form of flooding, in which the router accepts a packet from `SourceA` through Interface `IF1`, only when `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.

Forwarding Multicast Packets

PIM-DM routers forward multicast traffic to all interfaces that lead to receivers that have explicitly joined a multicast group. Messages are sent to a group address in the local subnetwork. The router performs an RPF check, and forwards the packet. Traffic that arrives on the correct interface is sent to all outgoing interfaces that lead to downstream receivers, if the downstream router is a member of this group.

Upstream

Upstream traffic is traffic that is going towards the source.

Downstream

Downstream traffic is anything other than the upstream interface for that group.

Nexthop

PIM-DM does periodic lookups for prefixes to check router reachability. The nexthop lookup mechanism avoids periodic lookup. During start-up, PIM-DM notifies NSM (Network Services Manager) about the prefixes that pertain to them. NSM notifies the protocols if a better nexthop is available, or if a nexthop becomes unavailable. In this way, PIM-DM does not expend resources to do periodic lookups, because NSM is proactive in their maintenance.

Configuration Steps

Configuring PIM-DM requires the following steps:

- Enable IP multicast on each PIM router (see Enabling IP Multicast Routing)
- Enable PIM-DM on the desired interfaces (see Enabling PIM-DM)

This section provides the configuration steps for configuring PIM-DM and examples for a relevant scenario.

Topology

In this network topology, the Source_1 address is 10.10.1.52 and the group address is set to 224.0.1.3.

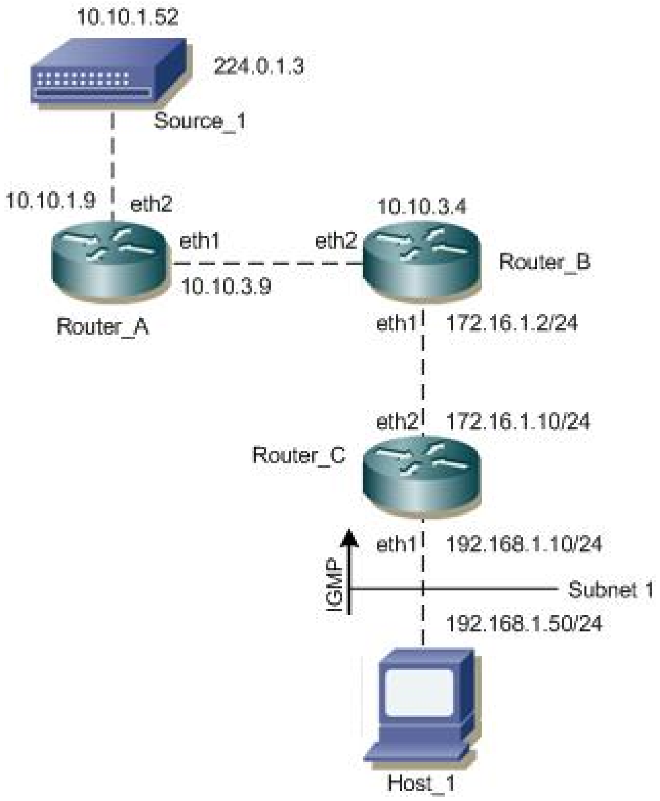

Figure 3-1: PIM-DM Configuration Topology

In this example, all routers are running PIM-DM.

1. Host_1 sends an IGMP membership report to Subnet 1.
2. After Router_C receives this report, it associates its receiving interface, `eth1`, with the group reported in the IGMP message, for example, group1.
3. Source_1 then sends a data packet for group1.
4. Every router creates an (S,G) entry in the multicast routing table.
5. When the data packet reaches `Router_C`, it forwards via the interface, `eth1`, because there is a local member on this interface for this group. `Router_C` has a downstream receiver, so it does not send a prune message to its upstream neighbor router, `Router_B`.

Enabling IP Multicast Routing

Enable IP multicast routing on all of the PIM routers inside the PIM domain:

`#configure terminal`	Enter Configure mode.

`(config)#ip multicast-routing`	Enable IP multicast routing.
`(config)#exit`	Exit Configure mode.

Enabling PIM-DM

Enable PIM-DM on all participating interfaces within each of routers inside the PIM domain on which you want to run PIM.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip address 10.10.15.12/24`	Configure the IP address for `eth1`.
`(config-if)#ip pim dense-mode`	Enable PIM dense mode on the interface.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth2`	Enter interface mode.
`(config-if)#ip address 10.10.14.12/24`	Configure the IP address for `eth1`.
`(config-if)#ip pim dense-mode`	Enable PIM dense mode on the interface.
`(config-if)#exit`	Exit interface mode.

The following is a sample configuration for `Router_C`:

```
hostname Router_C
!
interface eth0
!
interface eth1
 ip pim dense-mode
!
interface eth2
 ip pim dense-mode
!
interface lo
!
!
ip multicast-routing
!
```

Validation

The `show ip pim interface` command displays the interface details for `Router_C`.

```
Router_C#show ip pim interface
Address          Interface VIFindex Ver/   Nbr
                                    Mode   Count
192.168.1.10      eth1      0       v2/D   0
172.16.1.10       eth2      2       v2/D   1
```

The `show ip mroute` command displays the IP multicast routing table.

```
Router_C#show ip mroute
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)
(10.10.1.52, 224.0.1.3), uptime 00:00:15
Owner PIM-DM, Flags: F
 Incoming interface: eth2
 Outgoing interface list:
    eth1 (1)
```

The `show ip pim mroute` displays the IP PIM-DM multicast routing table.

```
Router_C#show ip pim mroute
PIM-DM Multicast Routing Table
(10.10.1.52, 224.0.1.3)
 RPF Neighbor: 172.16.1.2, Nexthop: 172.16.1.2, eth2
 Upstream IF: eth2
    Upstream State: Forwarding
    Assert State: NoInfo
 Downstream IF List:
    eth1, in 'olist':
      Downstream State: NoInfo
      Assert State: NoInfo
```

CHAPTER 4 Multicast Virtual Routing Configuration

This chapter contains Multicast Virtual Routing configuration examples.

Note: For ZebIC releases, multicast VRs/VRFs are supported only in Agema and Trident 2.

Configuration Steps

The basic VR configuration can be divided into the following steps:

1. Log on as a Global Administrator
2. Create a VR and Assign a User
3. Bind an Interface to the VR
4. Configure the VR
5. Log in as VR Administrator
6. Save VR Configuration
7. Proceed to one of the following:
   - Enable PIM on a VR
   - Enable PIM-SMv6 on a VR

Log on as a Global Administrator

1. Launch the ZebOS-XP daemons: (`nsm`, `ospfd`, `bgpd`, `imi`).
2. Start IMISH.
3. Use the `enable` command to enter Privileged Exec mode.

Create a VR and Assign a User

`#configure terminal`	Enter Configure mode.
`(config)#virtual-router VR1`	Enter the VR mode.
`(config-vr)#description VR1 for customer A`	Enter a description for the VR.
`(config-vr)#username user-A password abc12`	Add a user name for the VR.
`(config-vr)#configuration file VR-A.conf`	(Optional) Set the VR configuration file.
`(config-vr)#exit`	Exit VR mode.

Validation

```
#show virtual-router
Virtual Router vr1
  Description: vr1 for customer-A
  Loaded Protocols:
  VR-ID: 1
  Router-ID: Unset
  Interfaces:
```

Bind an Interface to the VR

`#configure terminal`	Enter Configure mode.
`(config)#interface eth0`	Specify the interface (`eth2`) to be configured and enter the Interface mode.
`(config-if)#virtual-router forwarding VR1`	Bind an interface to the VR, `VR1`.This command binds an interface, and informs all ZebOS-XP clients about it.
`(config-if)#exit`	Exit interface mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to be configured and enter the Interface mode.
`(config-if)#virtual-router forwarding VR1`	Bind an interface to the VR, `VR1`.

Validation

Use the `show interface` command to validate the configuration.

Configure the VR

`#login virtual-router VR1`	From the Global Management Authority (GMA), enter the VR Management Authority (MA)
`#configure terminal`	Enter Configure mode.
`(config)#router ospf`	Enter router mode.
`(config-router)#neighbor 10.10.10.48`	Define the interface on which OSPF runs,
`(config-router)#network 172.16.1.0/24 area 5`	Associate the area ID (5) with the interface. Area ID 0 is the backbone.

Validation

Use the `how ip ospf` command to verify the OSPF configuration.

```
#show ip ospf
  Routing Process "ospf 1" with ID 10.10.11.49
  Process bound to VRF default
  Process uptime is 0 minute
  ...
         SPF algorithm executed 0 times
         Number of LSA 0. Checksum Sum 0x000000
```

Note: A relevant section of the above show output is displayed, the rest is replaced by ellipsis (**...**).

Log in as VR Administrator

Log in as a VR administrator using one of the following two methods:

- From the GMA, run the following command:

```
login virtual-router VR1
#
```

- From the UNIX shell, type the following:

```
imish -v VR1
#
```

Save VR Configuration

By default, GMA configuration statements are stored in the `ZebOS.conf` file in the `/usr/local/etc` directory.

By default, VR configuration statements are stored in the `ZebOS.conf` file in the `/usr/local/etc/<VR-Name>` directory. In this location, `<VR-Name>` is the name of the specific VR configured. A directory for each VR is created automatically whenever a new VR is initiated.

To store a configuration in a different file, enter the file name using the `configuration file` command, which creates a new file in the directory related to the VR. No other directory can be specified for storing configuration.

```
configuration file First.conf
```

where `First.conf` is the name of the file to store the configuration statements.

To display the current running configuration for each VR, execute the following command in the VR context:

```
show running-config
```

To save the running configuration to startup configuration, execute the following command in the VR context:

```
write file
```

or

```
write memory
```

The configuration is saved to the file specified using the `configuration file` command (`First.conf` in the example above) or in the default `ZebOS.conf` file.

Enable PIM on a VR

The configuration that follows shows how PIM-SM can be configured on an IPv4 VR.

Topology

In this example:

- R3 is capable of Virtual Routing, and has two VRs:
  - VR1 has interfaces Eth1 and Eth2
  - VR2 has interfaces Eth3 and Eth4
  - VR1 and VR2 are both configured to run PIM-SM
  - VR1 and VR2 have different neighbors
  - Eth4 of VR2 is the Rendezvous Point (RP).
- R1 is the multicast receiver
- R2 is the source

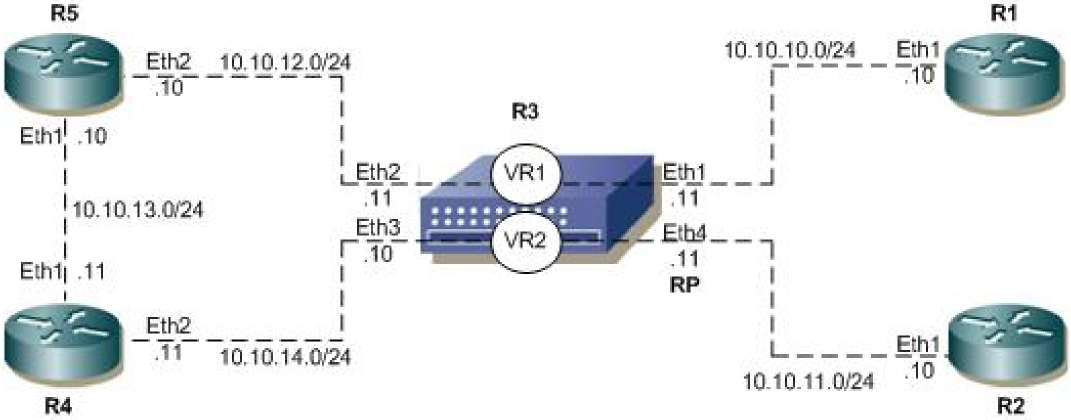

Figure 4-1: Configuration Topology

Create VR1 and VR2

`#configure terminal`	Enter Configure mode.
`(config)#virtual-router VR1`	Create a VR on R3, and specify the VR name `VR1`.
`(config-vr)#load pim`	Load the PIM-SM protocol module on this VR.
`(config-vr)#exit`	Exit the VR Management Authority (MA).
`(config)#virtual-router VR2`	Create a VR on R3, and specify the VR name `VR2`.
`(config-vr)#load pim`	Load the PIM-SM protocol module on this VR.
`(config-vr)#end`	Exit the virtual router mode.

Bind Interfaces to VR1 and VR2

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Enter the Interface mode for `eth1`.
`(config-if)#virtual-router forwarding VR1`	Bind interface `eth1` to `VR1`.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface eth2`	Enter the Interface mode for `eth2`.
`(config-if)#virtual-router forwarding VR1`	Bind interface `eth2` to `VR1`.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface eth3`	Enter the Interface mode for `eth3`.
`(config-if)#virtual-router forwarding VR2`	Bind interface `eth3` to `VR2`.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface eth4`	Enter the Interface mode for `eth4`.
`(config-if)#virtual-router forwarding VR2`	Bind interface `eth4` to `VR2`.
`(config-if)#end`	Exit the Interface mode and return to Configure mode.

Enable PIM-SM on VR1

`#login virtual-router VR1`	In Global Configuration mode, execute this command to jump to Configure mode for `VR1`.
`#configure terminal`	Enter Configure mode.
`(config)#ip multicast-routing`	Enable multicast routing.
`(config)#interface eth1`	Enter the Interface mode for `eth1`.
`(config-if)#ip address 10.10.10.11/24`	Configure the IP address for `eth1`.
`(config-if)#ip pim sparse-mode`	Enable PIM-SM on the interface.
`(config-if)#exit`	Exit Interface mode and return to Configure mode.
`(config)#interface eth2`	Enter the Interface mode for `eth2`.
`(config-if)#ip address 10.10.12.11/24`	Configure the IP address for `eth2`.
`(config-if)#ip pim sparse-mode`	Enable PIM-SM on the interface.
`(config-if)#end`	Exit the Interface mode and return to Configure mode.

Enable PIM-SM on VR2

`#login virtual-router VR2`	In Global Configuration mode, run this command to jump to Configure mode on `VR2`.
`#configure terminal`	Enter Configure mode.
`(config)#ip multicast-routing`	Enable multicast routing.
`(config)#interface eth3`	Enter the Interface mode for `eth3`.
`(config-if)#ip address 10.10.14.10/24`	Configure the IP address for `eth3`.
`(config-if)#ip pim sparse-mode`	Enable PIM-SM on the interface.

(config-if)#exit	Exit Interface mode and return to Configure mode.
(config)#interface eth4	Enter the Interface mode for eth4.
(config-if)#ip address 10.10.11.11/24	Configure the IP address for eth4.
(config-if)#ip pim sparse-mode	Enable PIM-SM on the interface.
(config-if)#end	Exit the Interface mode and return to Configure mode.

Configure RP on VR1

#login virtual-router VR1	From Global Configuration mode, run this command to jump to Configure mode on VR1.
#configure terminal	Enter Configure mode.
(config)#ip pim rp-address 10.10.11.11	Configure the RP address.
(config)#end	Exit the Configure mode.

Configure RP on VR2

#login virtual-router VR2	From Global Configuration mode, run this command to jump to Configure mode on VR2.
#configure terminal	Enter the Configure mode.
(config)#ip pim rp-address 10.10.11.11	Configure the RP address.
(config)#end	Exit the Configure mode.

Validation

Use the following commands to validate the configuration.

Display the global running configuration on the router:

```
#show running-config
!
no service password-encryption
!
no service dhcp
hostname ZebOS-XP
!
ip domain-lookup
!
virtual-router VR1
 load ospf
 load pim
!
virtual-router VR2
 load ospf
 load pim
!
mpls propagate-ttl
```

```
!
spanning-tree mode provider-rstp
!
vrrp vmac enable
!
interface lo
 ipv6 address::1/128
!
interface eth0
 ip address 10.11.3.50/16
!
interface svlan0.1
!
interface eth1
 virtual-router forwarding VR1
!
interface eth2
 virtual-router forwarding VR1
!
interface lo1
 virtual-router forwarding VR1
!
interface eth3
 virtual-router forwarding VR2
!
interface eth4
 virtual-router forwarding VR2
!
interface lo2
 virtual-router forwarding VR2
!
line con 0
 login
line vty 0 4
 login
!
end
```

Display the running configuration at VR1:

```
#show running-config
!
no service password-encryption
!
no service dhcp
hostname VR1
!
ip domain-lookup
!
mpls propagate-ttl
!
ip multicast-routing
```

```
!
vrrp vmac enable
!
ip pim rp-address 10.10.11.11
!
interface eth1
 ip address 10.10.10.11/24
 ip pim sparse-mode
!
interface eth2
 ip address 10.10.12.11/24
 ip pim sparse-mode
!
interface lo1
 ip address 127.0.0.1/8
 ipv6 address ::1/128
!
router ospf 1
 redistribute connected
 network 10.10.10.0/24 area 0
 network 10.10.12.0/24 area 0
!
line con 0
 login
line vty 0 4
 login
!
end
```

Display the running configuration at VR2:

```
#show running-config
!
no service password-encryption
!
no service dhcp
hostname VR2
!
ip domain-lookup
!
mpls propagate-ttl
!
ip multicast-routing
!
vrrp vmac enable
!
ip pim rp-address 10.10.11.11
!
interface eth3
 ip address 10.10.14.10/24
 ip pim sparse-mode
!
```

```
interface eth4
 ip address 10.10.11.11/24
 ip pim sparse-mode
!
interface lo2
 ip address 127.0.0.1/8
 ipv6 address ::1/128
 shutdown
!
router ospf 1
 redistribute connected
 network 10.10.11.0/24 area 0
 network 10.10.14.0/24 area 0
!
line con 0
 login
line vty 0 4
 login
!
end
```

Display PIM-SM interface information:

```
#show ip pim interface
Address          Interface VIFindex Ver/   Nbr    DR    DR
                                    Mode   Count  Prior
10.10.10.11      eth1      0        v2/S   1      1     10.10.10.11
10.10.12.11      eth2      2        v2/S   1      1     10.10.12.11
```

Display PIM-SM RP information:

```
#show ip pim rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4, Static
    RP: 10.10.11.11
         Uptime: 00:04:57
```

Display PIM-SM neighbor information:

```
#show ip pim neighbor
Neighbor          Interface          Uptime/Expires    Ver   DR
Address                                                      Priority/Mode
10.10.10.10       eth1               00:17:33/00:01:30 v2    1 /
10.10.12.10       eth2               00:17:23/00:01:44 v2    1 /
```

Display the IP multicast routing table summary:

```
#show ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(10.10.11.10, 224.0.1.3), uptime 00:00:07, stat expires 00:03:23
Owner PIM-SM, Flags: TF
```

```
  Incoming interface: eth2
  Outgoing interface list:
    eth1 (1)
```

Display the IP multicast routing table details:

```
#show ip pim mroute
IP Multicast Routing Table

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

(*, 224.0.1.3)
RP: 10.10.11.11
RPF nbr: 10.10.12.10
RPF idx: eth2
Upstream State: JOINED
 Local     i................................
 Joined    ................................
 Asserted  ................................
FCR:
Source: 10.10.11.10
 Outgoing  o...............................
 KAT timer running, 196 seconds remaining
 Packet count 1
```

Display PIM-SM interface information:

```
#show ip pim interface
Address          Interface VIFindex Ver/   Nbr    DR     DR
                                    Mode   Count  Prior
10.10.14.10      eth3      0        v2/S   1      1      10.10.14.11
10.10.11.11      eth4      2        v2/S   0      1      10.10.11.11
```

Display PIM-SM neighbor information:

```
#show ip pim neighbor
Neighbor          Interface          Uptime/Expires    Ver   DR
Address                                                      Priority/Mode
10.10.14.11       eth3               00:14:30/00:01:45 v2    1 / DR
```

Display the IP multicast routing table:

```
#show ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(10.10.11.10, 224.0.1.3), uptime 00:02:05, stat expires 00:02:06
Owner PIM-SM, Flags: TF
  Incoming interface: eth4
  Outgoing interface list:
    eth3 (1)
```

Display the IP multicast routing table details:

```
#show ip pim mroute
IP Multicast Routing Table

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

(*, 224.0.1.3)
RP: 10.10.11.11
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 Local     ................................
 Joined    j...............................
 Asserted  ................................
FCR:

(10.10.11.10, 224.0.1.3)
RPF nbr: 0.0.0.0
RPF idx: None
SPT bit: 1
Upstream State: JOINED
 Local     ................................
 Joined    ................................
 Asserted  ................................
 Outgoing  o...............................

(10.10.11.10, 224.0.1.3, rpt)
RP: 10.10.11.11
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: NOT PRUNED
 Local     ................................
 Pruned    ................................
 Outgoing  o...............................
```

Enable PIM-SMv6 on a VR

This configuration shows how PIM-SMv6 (IPv6) can be configured on an IPv6 Virtual Router (VR).

Topology

In this example:

- R3 is capable of Virtual Routing and has two VRs:
    - VR1 has interfaces eth1 and eth2
    - VR2 has interfaces eth3 and eth4
    - Both VR1 and VR2 run PIM-SMv6
    - eth4 of VR2 is the Rendezvous Point (RP)
    - VR1 and VR2 have different neighbors.
- R1 is the multicast receiver
- R2 is the source

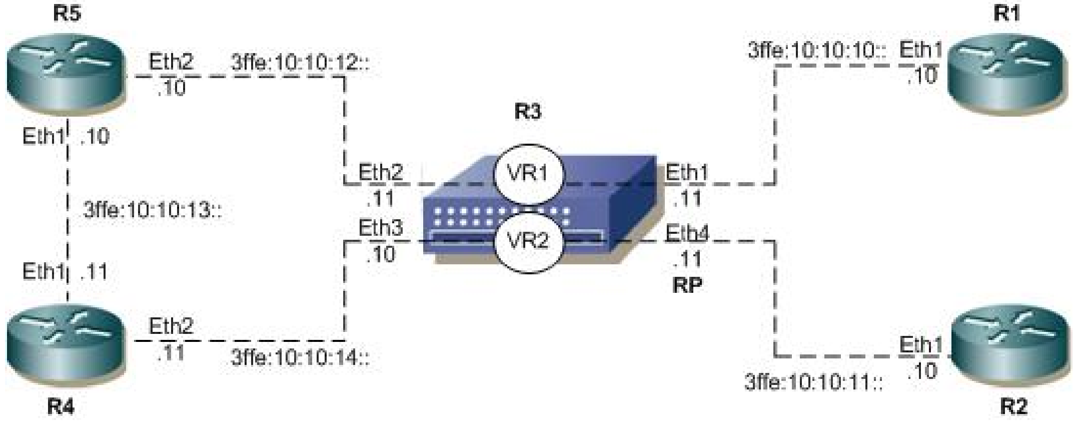

Figure 4-2: Configuration Topology

Create VR1 and VR2

`#configure terminal`	Enter Configure mode.
`(config)#virtual-router VR1`	Create a VR on R3, and specify the VR name (VR1).
`(config-vr)#load pim`	Load the PIM-SM protocol module on this VR.
`(config-vr)#exit`	Exit the Virtual Router Management Authority (MA).
`(config)#virtual-router VR2`	Create a VR on R3, and specify the VR name (VR2).
`(config-vr)#load pim`	Load the PIM-SM protocol module on this VR.
`(config-vr)#end`	Exit the virtual router mode.

Bind interfaces to VR1 and VR2

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Specify the interface (`eth1)` to be configured.
`(config-if)#virtual-router forwarding VR1`	Bind interface `eth1` to `VR1`.
`(config-if)#exit`	Exit Interface mode.
`(config)#interface eth2`	Specify the interface (`eth2)` to be configured.
`(config-if)#virtual-router forwarding VR1`	Bind interface `eth2` to `VR1`.
`(config-if)#exit`	Exit Interface mode.
`(config)#interface eth3`	Specify the interface (`eth3)` to be configured.

(config-if)#virtual-router forwarding VR2	Bind interface eth3 to VR2.
(config-if)#exit	Exit Interface mode.
(config)#interface eth4	Specify the interface (eth4) to be configured.
(config-if)#virtual-router forwarding VR2	Bind interface eth4 to VR2.
(config-if)#end	Exit the Interface mode.

Enable PIM-SMv6 on VR1

#login virtual-router VR1	From Global Configuration mode, run this command to jump to Configure mode on VR1.
#configure terminal	Enter Configure mode.
(config)#ipv6 multicast-routing	Enable multicast routing.
(config)#interface eth1	Specify the interface (eth1) to be configured.
(config-if)#ipv6 address 3ffe:10:10:10::11/64	Configure the IPv6 address for the interface (eth1).
(config-if)#ipv6 address fe80::70/64	Configure the link local address for the interface (eth1).
(config-if)#ipv6 pim sparse-mode	Enable PIM-SMv6 on the interface.
(config-if)#exit	Exit Interface mode.
(config)#interface eth2	Specify the interface (eth2) to be configured.
(config-if)#ipv6 address 3ffe:10:10:12::11/64	Configure the IPv6 address for the interface (eth2).
(config-if)#ipv6 address fe80::50/64	Configure the link local address for the interface (eth2).
(config-if)#ipv6 pim sparse-mode	Enable PIM-SMv6 on the interface.
(config-if)#end	Exit the Interface mode.

Enable PIM-SMv6 on VR2

#login virtual-router VR2	From Global Configuration mode, run this command to jump to Configure mode on VR2.
#configure terminal	Enter Configure mode.
(config)#ipv6 multicast-routing	Enable multicast routing.
(config)#interface eth3	Specify the interface (eth3) to be configured.
(config-if)#ipv6 address 3ffe:10:10:14::10/64	Configure the IPv6 address for the interface (eth3).
(config-if)#ipv6 address fe80::20/64	Configure the link local address for the interface (eth3).
(config-if)#ipv6 pim sparse-mode	Enable PIM-SMv6 on the interface.
(config-if)#exit	Exit Interface mode.
(config)#interface eth4	Specify the interface (eth4) to be configured.
(config-if)#ipv6 address 3ffe:10:10:11::11/64	Configure the IPv6 address for the interface (eth4).
(config-if)#ipv6 address fe80::30/64	Configure the link local address for the interface (eth4).
(config-if)#ipv6 pim sparse-mode	Enable PIM-SMv6 on the interface.
(config-if)#end	Exit the Interface mode.

Configure RP on VR1

`#login virtual-router VR1`	From Global Configuration mode, run this command to jump to Configure mode on `VR1`.
`#configure terminal`	Enter Configure mode.
`(config)#ipv6 pim rp-address 3ffe:10:10:11::11`	Configure the RP address.
`(config)#end`	Exit the Configure mode.

Configure RP on VR2

`#login virtual-router VR2`	From Global Configuration mode, run this command to jump to Configure mode on `VR2`.
`#configure terminal`	Enter Configure mode.
`(config)#ipv6 pim rp-address 3ffe:10:10:11::11`	Configure the RP address.
`(config)#end`	Exit the Configure mode.

Verify Configurations

Use the following validation commands to verify the configurations.

Display the global running configuration at the router:

```
#show running-config
```

Display the running configuration at VR1:

```
#show running-config
```

Display the running configuration at VR2:

```
#show running-config
```

Display PIM-SMv6 interface information:

```
#show ipv6 pim interface
```

Display PIM-SM RP information:

```
#show ipv6 pim rp mapping
```

Display PIM-SMv6 neighbor information:

```
#show ipv6 pim neighbor
```

Display the IPv6 multicast routing table summary:

```
#show ipv6 mroute
```

Display the IPv6 multicast routing table details:

```
#show ipv6 pim mroute
```

Display PIM-SMv6 interface information:

```
#show ipv6 pim interface
```

Display PIM-SMv6 neighbor information:

```
#show ipv6 pim neighbor
```

Display the IPv6 multicast routing table:

```
#show ipv6 mroute
```

Display the IPv6 multicast routing table details:

```
#show ipv6 pim mroute
```

CHAPTER 5 PIM Sparse-Dense Mode Configuration

PIM-SMDM is an integrated protocol which handles both sparse groups and dense groups at the same time. In sparse-dense mode, if the group is in dense mode, the interface will be treated as dense mode. If the group is in sparse mode, the interface will be treated in sparse mode. The group is sparse if the router knows about an RP for that group.

Note: PIM-SMDM is not supported for ZebIC releases.

Configuration Steps

The required steps to configure PIM-SMDM are the following:

- Enable IP multicast on each PIM router (see Enabling IP Multicast Routing)
- Enable PIM-SMDM on the desired interfaces (see Enabling PIM-SMDM)
- Example for the group operating in sparse-mode having Static RP (see Configuring Rendezvous Point Statically for PIM-SMDM
- Example for the group operating in dense-mode having no RP

All multicast group states are dynamically maintained as the result of IGMP Report/Leave and PIM Join/Prune messages.

This section provides the steps to configure the PIM-SMDM feature. Configuration steps and examples are used for two relevant scenarios. The following figure displays the network topology used in these examples:

Enabling IP Multicast Routing

Enable IP multicast routing on all of the PIM routers inside the PIM domain:

`#configure terminal`	Enter Configure mode.
`(config)#ip multicast-routing`	Enable IP multicast routing.
`(config)#exit`	Exit Configure mode.

Enabling PIM-SMDM

Enable PIM-SMDM on all participating interfaces within each of routers inside the PIM domain on which you want to run PIM. In the following sample configuration, both eth1 and eth2 are enabled for PIM-SMDM on the router.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Specify the interface (`eth1`) to be configured and enter the Interface mode.
`(config-if)#ip pim sparse-dense-mode`	Enable PIM sparse-dense mode on the interface.
`(config-if)#exit`	Exit Interface mode.

`(config)#interface eth2`	Specify the interface (`eth2`) to be configured and enter the Interface mode.
`(config-if)# ip pim sparse-dense-mode`	Enable PIM sparse -dense mode on the interface.
`(config-if)#exit`	Exit Interface mode.

Validation

Here is the sample configuration for `Router_C`:

```
hostname Router_C
!
interface eth0
!
interface eth1
 ip pim sparse-dense-mode
!
interface eth2
 ip pim sparse-dense-mode
!
interface lo
!
!
ip multicast-routing
```

The `show ip pim interface` command displays the interface details for Router_C.

```
Router_C#show ip pim interface

Address            Interface          VIFindex Ver/  Nbr
                                               Mode  Count
192.168.1.10        eth1                 0      v2/SD  0
172.16.1.10         eth2                 2      v2/SD  1
```

Sparse Mode Operation versus Dense Mode Operation

The following examples differentiates the group operating in sparse mode versus dense mode:

- Sparse mode operation when the RP is present for the group
- Dense mode operation when there is no RP for the group

Sparse Mode Operation

Configuring Rendezvous Point Statically for PIM-SMDM

Every PIM multicast group needs to be associated with the IP address of a Rendezvous Point (RP), which is a router that resides in a multicast network domain. The address of the RP is used as the root of a group-specific distribution tree. All nodes in the domain that want to receive traffic sent to the group are aware of the address of the RP. For all senders to reach all receivers within a group, all routers in the domain must be able to map to the RP address configured for the group. There can be several RPs configured in a network deploying PIM-SM, each serving a different group.

You can statically configure a RP by specifying the RP address in every router in the PIM domain. The use of statically configured RPs is ideal for small network environments or ones that do not require many RPs and/or require changing the assignment of the RPs often. Changing the assignment of an RP requires the re-configuration of the RP address in all of the routers in the PIM domain.

In static RP configurations, RP failover is not available.

When configuring the RP statically, do the following:

- On every router, include the `ip pim rp-address A.B.C.D` statement even if a router does not have any source or group member attached to it
- Assign only one RP address for a multicast group in the PIM domain

Using the topology depicted in Figure 5-1, `Router_C` is the RP, and all routers are statically configured with RP information. Host_1 and Host_2 join group 224.0.1.3 for all the sources. They send the IGMP membership report to Subnet 1. Two routers are attached to Subnet 1, `Router_E` and `Router_F`; both have default DR priority on `eth1`. Since `Router_E` has a higher IP address on interface `eth1`, it becomes the Designated Router, and is responsible for sending Join messages to the RP (`Router_C`).

Topology

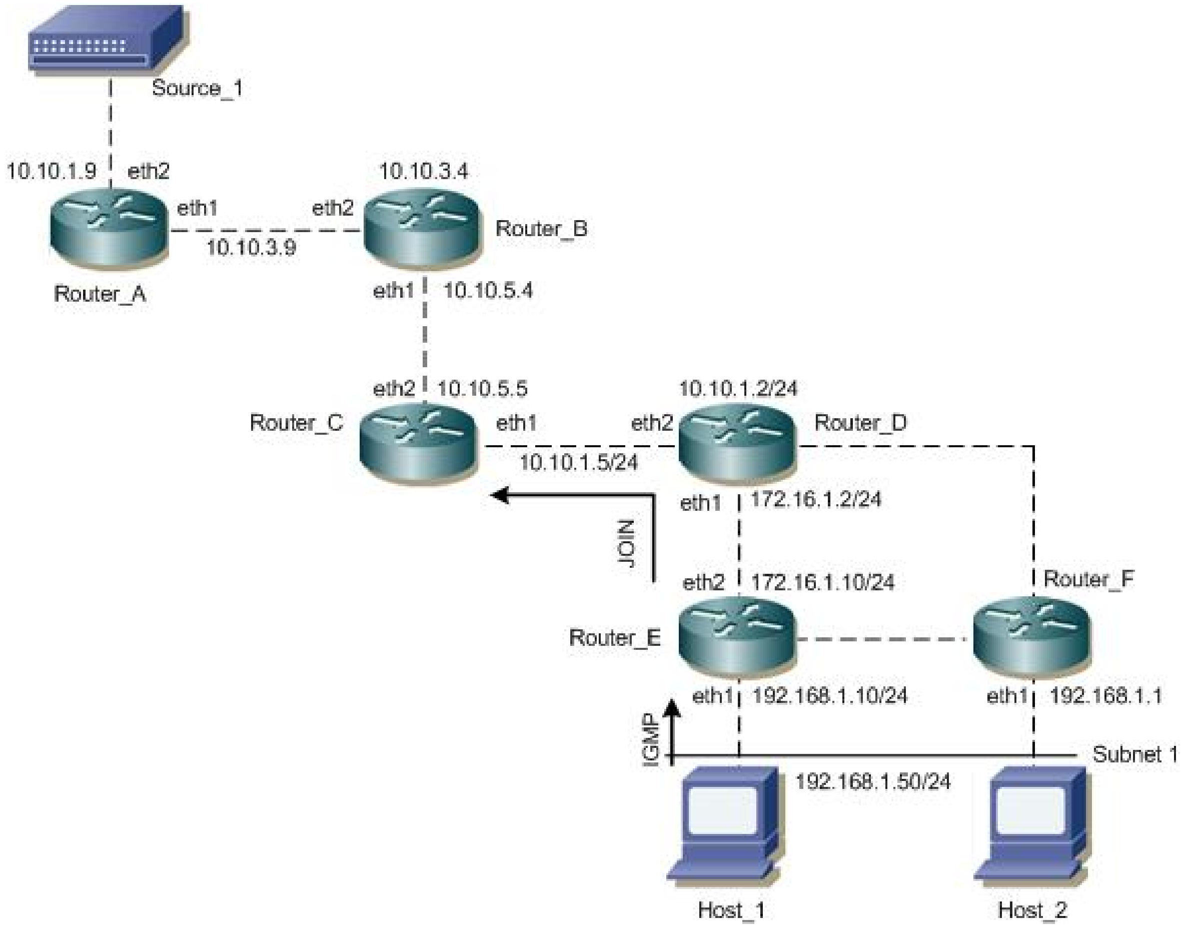

Figure 5-1: PIM-SMDM Configuration Topology (a)

Configure Static RP

`#configure terminal`	Enter Configure mode.
`(config)#ip pim rp-address 10.10.1.5`	Statically configure an RP address for multicast groups.
`(config)#exit`	Exit Configure mode.

Validation

Here is the sample configuration for `Router_D`:

```
hostname Router_D
!
interface eth0
!
interface eth1
 ip pim sparse-dense-mode
!
interface eth2
 ip pim sparse-dense-mode
!
interface lo
!
!
ip multicast-routing
ip pim rp-address 10.10.1.5
!
```

RP Details

At Router_D, the `show ip pim rp mapping` command shows that `10.10.1.5` is the RP for all multicast groups `224.0.0.0/4`, and is statically configured. All other routers will have a similar output:

```
Router_D#sh ip pim rp mapping
PIM Group-to-RP Mappings
Override RP cnt: 0
Group(s): 224.0.0.0/4, Static
    RP: 10.10.1.5
         Uptime: 00:01:45
```

At Router_D, use the `show ip pim rp-hash` command to display the selected RP for a specified group (224.0.1.3):

```
Router_D#show ip pim rp-hash 224.0.1.3
RP: 10.10.5.37
```

Interface Details

The `show ip pim interface` command displays the interface details for `Router_E`, and shows that `Router_E` is the Designated Router on `Subnet 1`.

```
Router_E#show ip pim interface
Address          Interface VIFindex Ver/   Nbr      DR    DR
                                    Mode   Count   Prior
192.168.1.10      eth1      0       v2/SD   1         1     192.168.1.10
172.16.1.10       eth2      2       v2/SD   1         1     172.16.1.10
```

IP Multicast Routing Table

Note: The multicast routing table displays for an RP router are different from other routers.

The `show ip pim mroute` command displays the IP multicast routing table. In this table, the following fields are defined:

`RPF nbr` Displays the unicast next-hop to reach RP.

and mask length.

`RPF idx` Displays the incoming interface for this (*, G) state.

`RP` Displays the IP address for the RP router

`B` Displays the bidirectional pim mode

`The leading dots ....`

Stand for VIF index

```
Router_E#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
(*, 224.0.1.3)
RP: 10.10.1.5
RPF nbr: 172.16.1.2
RPF idx: eth2
Upstream State: JOINED
 Local     ................................
 Joined    j...............................
 Asserted  ................................
 Outgoing  o...............................
```

At `Router_E`, `eth2` is the incoming interface of the (*, G) entry, and `eth1` is on the outgoing interface list of the (*, G) entry. This means that there is a group member through `eth1`, and the RP is reachable through `eth2`.

The 0 position on this 32-bit index is for `eth1` (as illustrated in the interface display above). The `j` on the 0 index indicates that the `Join` has come from `eth1`.

Since `Router_C` is the RP, and the root of this multicast tree, the `show ip pim mroute` command on `Router_C` shows `RPF nbr` as 0.0.0.0 and `RPF idx` as none.

```
Router_C#show ip pim mroute
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
(S,G,rpt) Entries: 0
(*, 224.0.1.3)
RP: 10.10.1.5
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 Local     ................................
```

```
      Joined    j..............................
      Asserted  ...............................
      Outgoing  o..............................
```

For configuring Rendezvous point dynamically refer Configure Rendezvous Point Dynamically Using Bootstrap Router Method and Configuring Rendezvous Point Statically

Dense-mode Operation

Topology

In this network topology, the Source_1 address is 10.10.1.52 and the group address is set to 224.0.1.3.

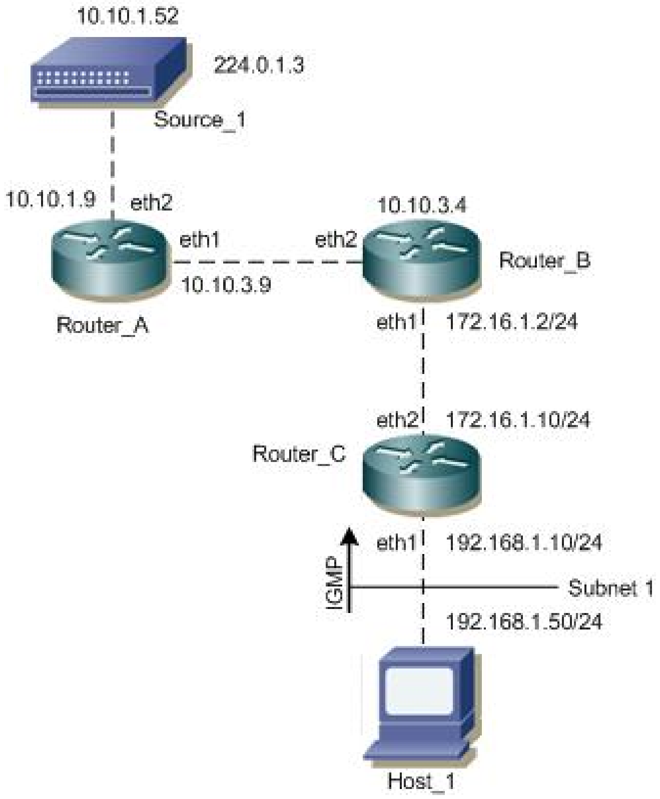

Figure 5-2: PIM-SMDM Configuration Topology (b)

In this network topology, the Source_1 address is 10.10.1.52 and the group address is set to 224.0.1.3

In this example all routers are running PIM-SMDM

1. Host_1 sends an IGMP membership report to Subnet 1
2. After Router_C receives this report, it associates its receiving interface, eth1, with the group reported in the IGMP message, for example, group1.
3. Source_1 then sends a data packet for group1.
4. Every router creates an (S,G) entry in the multicast routing table.
5. When the data packet reaches Router_C, it forwards via the interface, eth1, because there is a local member on this interface for this group. Router_C has a downstream receiver, so it does not send a prune message to its upstream neighbor router, Router_B.

Validation

Enter the commands listed in this section to confirm the previous configurations.

IP Multicast Routing Table

The `show ip pim mroute` command displays the IP multicast routing table.

```
Router_C#show ip mroute
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
Timers: Uptime/Stat Expiry Interface State:
Interface (TTL) (10.10.1.52,   224.0.1.3), uptime 00:00:15
Owner PIM-DM, Flags: F
Incoming interface: eth2
Outgoing interface list:
eth1 (1)
```

IP PIM-SMDM Multicast Routing Table

The `show ip pim dense-mode mroute` command displays the IP PIM-DM multicast routing table

```
Router_C#show ip pim mroute
PIM-DM Multicast Routing Table (10.10.1.52, 224.0.1.3)
RPF Neighbor: 172.16.1.2, Nexthop: 172.16.1.2, eth2
Upstream IF: eth2
Upstream State: Forwarding
Assert State: NoInfo
Downstream IF List:
eth1, in 'olist': Downstream State: NoInfo Assert State: NoInfo
```

CHAPTER 6 PIM-ECMP Redirect Configuration

A Protocol Independent Multicast (PIM) router uses Reverse Path Forwarding (RPF) procedure to select an upstream interface and router in order to build forwarding state. When there are equal-cost multipaths (ECMPs), existing implementations often use hash algorithms to select a path. Such algorithms do not allow the spread of traffic among the ECMPs according to administrative metrics. This usually leads to inefficient or ineffective use of network resources. PIM ECMP Redirect (RFC 6754) provides a mechanism to improve the RPF procedure over ECMPs. It allows ECMP selection to be based on administratively selected metrics, such as data transmission delays, path preferences, and routing metric. An interface identifier option is used in PIM hello messages as a tiebreaker during ECMP path selection.

Note: PIM ECMP Redirect is not supported for Bidirectional PIM, PIM-DM and PIM-SMDM.

Note: PIM-ECMP feature is not supported for ZebIC.

Terminology

Following is a brief description of terms and concepts used to describe the PIM-ECMP Redirect protocol:

Equal Cost Multipath (ECMP)

ECMP refers to parallel, single-hop, equal-cost links between adjacent nodes.

ECMP Bundle

An ECMP bundle is a set of PIM-enabled interfaces on a router, where all interfaces belonging to the same bundle share the same routing metric. The next hops for the ECMP are all one hop away. There can be one or more ECMP bundles on any router, while one individual interface can only belong to a single bundle. ECMP bundles are created on a router via configuration.

Reverse Path Forwarding

Reverse Path Forwarding (RPF) is an optimized form of flooding, in which the router accepts a packet from `SourceA` through Interface `IF1`, only if `IF1` is the interface the router uses to reach `SourceA`. To determine if the interface is correct, it consults its unicast routing tables. The packet that arrives through interface `IF1` is forwarded because the routing table lists this interface as the shortest path. 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.

Upstream

Towards the root of the multicast forwarding tree. An upstream router refers to a router that is forwarding, or potentially capable of forwarding, data packets onto interfaces in an ECMP bundle. When there are multiple routers forwarding packets onto interfaces in the ECMP bundle, all these routers are called upstream routers.

Downstream

Away from the root of the multicast forwarding tree. A downstream router is a router that uses an interface in the ECMP bundle as an RPF interface for a multicast forwarding entry

When a PIM router downstream of the ECMP interfaces creates a new (*,G) or (S,G) entry, it will populate the RPF interface and RPF neighbor information according to the rules specified by [RFC4601]. This router will send its initial PIM Joins to that RPF neighbor. When the RPF neighbor router receives the Join message and finds that the receiving interface is one of the ECMP interfaces, it will check if the same flow is already being forwarded out of another ECMP interface. If so, this RPF neighbor router will send a PIM ECMP Redirect message onto the interface the Join was received on. The PIM ECMP Redirect message contains the address of the desired RPF neighbor, an Interface ID [RFC6395], and the other parameters used as tiebreakers. In essence, a PIM ECMP Redirect message is sent by an upstream router to notify downstream routers to redirect PIM Joins to the new RPF neighbor via a different interface. When the downstream routers receive this message, they SHOULD trigger PIM Joins toward the new RPF neighbor specified in the packet.

This PIM ECMP Redirect message has similar functions as the existing PIM Assert message:

- It is sent by an upstream router.
- It is used to influence the RPF selection by downstream routers.
- A tiebreaker metric is used

However, the existing Assert message is used to select an upstream router within the same multi-access network (such as a LAN), while the Redirect message is used to select both a network and an upstream router.

Sending ECMP Redirect

ECMP Redirects are sent by an upstream router under either of the following conditions:

- It detects a PIM Join on a non-desired outgoing interface.
- It detects multicast traffic on a non-desired outgoing interface.

In both cases, an ECMP Redirect is sent to the non-desired interface. An outgoing interface is considered non-desired when:

- The upstream router is already forwarding the same flow out of another interface belonging to the same ECMP bundle.
- The upstream router is not yet forwarding the flow out any interfaces of the ECMP bundle, but there is another interface with more desired attributes.

Receiving ECMP Redirect

When a downstream router receives an ECMP Redirect, and detects that the desired RPF path from its upstream router's point of view is different from its current one, it should choose to join the newly suggested path and prune from the current path.

If a downstream router receives multiple ECMP Redirects sent by different upstream routers, it SHOULD use the Preference, Metric, or other fields as specified below as the tiebreakers to choose the most preferred RPF interface and neighbor. The tie-break procedure is the same as that used in PIM Assert processing described by [RFC4601].

If an upstream router receives an ECMP Redirect, it SHOULD NOT change its forwarding behavior even if the ECMP Redirect makes it a less preferred RPF neighbor on the receiving interface.

PIM-ECMP Configuration

This section provides the configuration steps for configuring PIM ECMP Redirect and examples for a relevant scenario.

Note: Configure PIM SM on the routers. For steps to configure PIM-SM refer to Chapter 1, *PIM Sparse Mode Configuration*

Topology

In this network topology, the source address is 172.31.1.52 and the group address is set to 224.0.1.3.

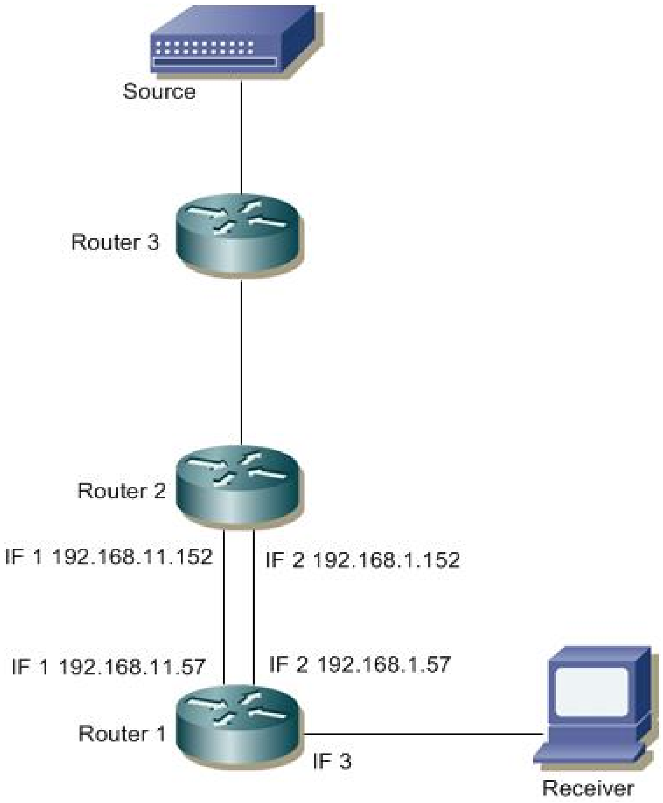

Figure 6-1: PIM ECMP Redirect Topology

Configure PIM Router-ID

Configure PIM router-id on all of the PIM routers inside the PIM domain:

`# configure terminal`	Enter Configure mode.
`(config)# ip pim router-id 1.1.1.1`	Configure PIM router-id
`(config)#exit`	Exit Configure mode.

Validation

```
#show running-config
!
ip multicast-routing
!
ip pim router-id 1.1.1.1
```

Configure PIM ECMP Bundle

Configure PIM ECMP Bundle on all of the PIM routers inside the PIM domain:

`# configure terminal`	Enter Configure mode.
`(config)# ip pim ecmp-bundle <bundle-name>`	Configure PIM ECMP Bundle
`(config)#exit`	Exit Configure mode.

Validation

```
#show running-config
!
ip multicast-routing
!
```

Bind PIM ECMP Bundle

Bind an ECMP Bundle to an interface on the PIM routers inside the PIM domain:

`# configure terminal`	Enter Configure mode.
`(config)# interface eth1`	Enter Interface mode
`(config-if)# ip pim bind ecmp-bundle ecmpbundle`	Bind PIM ECMP Bundle to an interface
`(config-if)#exit`	Exit Interface mode.

Validation

Validation 1

Enter the commands listed in this section to confirm the previous configurations.

```
router_1#show running-config interface eth2
 interface eth2
 ip address 192.168.1.57/24
 no shutdown
 ip ospf cost 10
 ip pim bind ecmp-bundle ecmpbundle
 ip pim sparse-mode
 lldp-agent
 no dcbx enable
 exit
```

Validation 2

The following output displays the bundle information:

```
 router_1#show ip pim ecmp-bundle
Name        : ecmpbundle1
Interface   : <ECMP REDIRECT status>
       eth2 : allowed
       eth3 : allowed

router_1#show ip pim ecmp-bundle ecmpbundle1
Name       : ecmpbundle1
```

```
    Interface   : <ECMP REDIRECT status>
           eth2 : allowed
           eth3 : allowed
     exit
```

Validation 3

The following output displays the interface details:

```
router_1#show ip pim interface detail
 eth1 (vif 0):
 Address 192.168.10.57, Mode: Sparse
 DR 192.168.10.57, DR's priority: 1
 Hello period 30 seconds, Next Hello in 22 seconds
 Triggered Hello period 5 seconds
 PIM GenID sent in Hellos: 56e71c93
 Propagation delay is 1000 milli-seconds
 Interface ID: Router-ID:1.1.1.1 Local-ID 3
 Neighbors:
  192.168.10.52
 PIM neighbor count: 1
 PIM neighbor holdtime: 105
 PIM configured DR priority: 1
 PIM border interface: no
 PIM Neighbor policy: not configured

 eth2 (vif 2):
 Address 192.168.1.57, Mode: Sparse
 DR 192.168.1.152, DR's priority: 1
 Hello period 30 seconds, Next Hello in 23 seconds
 Triggered Hello period 5 seconds
 PIM GenID sent in Hellos: 5f2ebb37
 Propagation delay is 1000 milli-seconds
 Interface ID: Router-ID:1.1.1.1 Local-ID 4
 ECMP REDIRECT, bundle : ecmpbundle1, status :  allowed
 Neighbors:
  192.168.1.149
  192.168.1.150
  192.168.1.152
 PIM neighbor count: 3
 PIM neighbor holdtime: 105
 PIM configured DR priority: 1
 PIM border interface: no
 PIM Neighbor policy: not configured
```

IP Multicast Routing Table for ECMP Redirect

Note: The multicast routing table displays for an RP router are different from other routers.

Validation 1:

Initially router_1 sends the (*, G) to Router_2 eth2, as Router_2 eth2 is RIB indicated RPF neighbor.The RIB indicated RPF neighbor can be checked using command `show ip rpf`

```
router_1#show ip rpf 172.31.5.153
RPF information for 172.31.5.153
  RPF interface: eth3
  RPF neighbor: 192.168.11.152
  RPF route: 172.31.5.0/24
  RPF type: unicast (ospf)
  RPF recursion count: 0
  Doing distance-preferred lookups across tables
  Distance: 110
  Metric: 30
```

Validation 2:

The `show ip pim mroute` command displays the IP multicast routing table. In this table, the following fields are defined:

`RPF nbr` Displays the unicast next-hop to reach
RP. and mask length.

`RPF idx` Displays the incoming interface for this (*, G) state.

`RP` Displays the IP address for the RP router

`B` Displays the bidirectional pim mode

`The leading dots` ....Stand for VIF index

Router-2 upon receiving (*, G) on eth2, which is rib indicated RPF, sends an ECMP redirect message to Router-1 eth2 to intimate that, subsequent joins should be sent to eth1 being the desired path with a (*,G). Since, Router-2 eth1 already has a (*, G), the `show ip pim mroute` command output suggests 192.168.1.152 as the RPF neighbor, which is ECMP redirected RPF neighbor.

```
router_1#show ip pim mroute
IP Multicast Routing Table

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

(*, 224.1.1.1)
RP: 172.31.5.153
RPF nbr: 192.168.1.152
RPF idx: eth2
Upstream State: JOINED
 Local     i...............................
 Joined    ................................
 Asserted  ................................
FCR:
0
```

The below output displays (*,G) at router_2 eth1 using the command `show ip pim mroute detail`:

```
router_2#show ip pim mroute detail
IP Multicast Routing Table

(*,*,RP) Entries: 0
(*,G) Entries: 1
(S,G) Entries: 0
```

```
(S,G,rpt) Entries: 0
FCR Entries: 0

(*, 224.1.1.1) Uptime: 00:30:45
RP: 172.31.5.153, RPF nbr: 172.31.12.153, RPF idx: eth1
  Upstream:
   State: JOINED, SPT Switch: Disabled, JT Expiry: 15 secs
   Macro state: Join Desired,
  Downstream:
   eth1:
     State: JOINED, ET Expiry: 176 secs, PPT: off
     Assert State: NO INFO, AT: off
      Winner: 0.0.0.0, Metric: 4294967295, Pref: 4294967295, RPT bit: on
     Macro state: Could Assert, Assert Track
  Local Olist:
   eth1
  Join Olist:
   eth1
```

CHAPTER 7 IGMP Configuration

This chapter describes how to configure Internet Group Management Protocol (IGMP).

The Internet Group Management Protocol (IGMP) is used by IP hosts to report their multicast group memberships to any immediately-neighboring multicast routers.

Using the information obtained through IGMP, the router maintains a list of multicast group on a per-interface basis. The routers that receive these IGMP packets send multicast data that they receive for requested groups out the network segment of the known receivers.

By default, when PIM is enabled on an interface, IGMP version 3 is enabled. IGMP can be enabled on an interface explicitly.

IGMP Versions

ZebOS-XP supports IGMPv2 and IGMPv3, as well as IGMPv1 report reception. By default, ZebOS-XP enables IGMPv3 when PIM is enabled on an interface.

IGMPv3 includes the following key changes from IGMPv2:

- Support for Source-Specific Multicast (SSM), which builds shortest path trees from each receiver to the source, through the following feature:
  - Host messages that can specify both the group and the source.
  - The multicast state that is maintained for groups and sources, not just for groups as in IGMPv2.
- Hosts no longer perform report suppression, which means that hosts always send IGMP membership reports when an IGMP query message is received.

IGMP Operation

IGMP works on the premise of three major packets exchange between IGMP enabled routers and hosts, interested in joining a particular group.

IGMP Query Operation

Once IGMP is enabled or pim is enabled (which enables igmpv3), on any interface it starts sending Query message, which is called general query to the all-hosts multicast group at 224.0.0.1 periodically to discover whether any hosts want to receive multicast data.

ZebOS-XP elects a router as the IGMP querier on a subnet if it has the lowest IP address. As long as a router continues to receive query messages from a router with a lower IP address, it resets a timer that is based on its querier timeout value. If the querier timer of a router expires, it becomes the designated querier. If that router later receives a host query message from a router with a lower IP address, it drops its role as the designated querier and sets its querier timer again.

In the figure above Router-1 eth2 sends query every query-interval. Since Router1-eth2 IP address is less than Router-2 eth2, Router-1 eth2 becomes querier on the LAN.

IGMP Membership Report Operation

When a host receives a query from the local router it sends a Host Membership Report for all the multicast groups for which it wants to receive multicast traffic. This is called solicited membership report.

When a host joins a new group, the host immediately sends a Membership Report to inform a local router that it wants to receive multicast traffic for the group it has just joined without waiting to receive a Query. This is called unsolicited membership report.

In the figure above Host-1 and Host-2 sends membership reports to Router-1 eth2 for all the multicast groups for which they want to receive multicast traffic. Upon reception of membership report Router-1 maintains an IGMP group table containing multicast group-address, interface name on which it receives the report.

IGMP Leave Operation

When a multicast host leaves a group, a host that runs IGMPv2 or later sends an IGMP leave message. To check if this host is the last host to leave the group, the router sends an IGMP query (Called as Group-specific-query) message and starts a timer that you can configure called the last member query response interval. If no reports are received before the timer expires, the software removes the group state. The router continues to send multicast traffic for a group until its state is removed.

In the figure above Host-1 and Host-2 sends leave message to Router-1 eth2 for all the multicast groups for which they don’t want to receive multicast traffic. In response to leave message Router-1 eth2 sends an group-specific-query message before removing the multicast group address from the IGMP table.

Topology

The procedures in this section use the topology in Figure 7-1

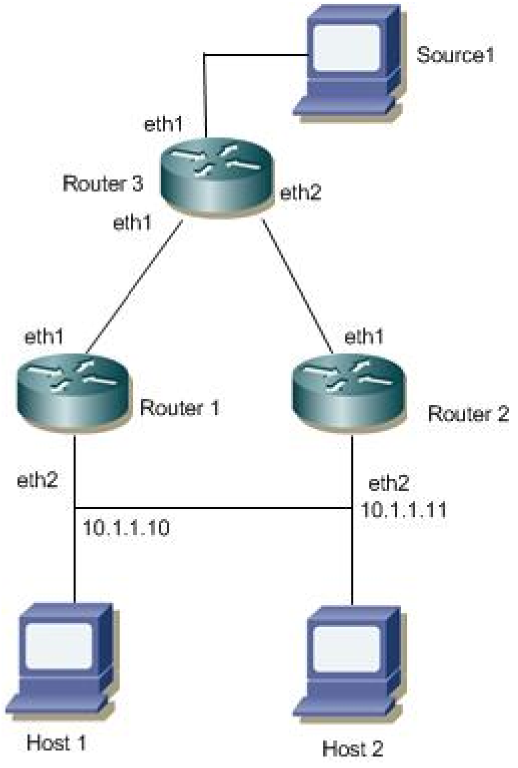

Figure 7-1: IGMP Topology

IGMP Configuration

The following example shows IGMP configuration.

Configuring IGMP Version

The configuration that follows shows how IGMP version can be configured.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip igmp version`	Enable IGMP version.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit Configure mode.

Validation

Enter the commands listed in this section to confirm the previous configurations.

```
#show  running-config
!
no service password-encryption
!
hostname rtr1
!
!
!
ip multicast-routing
!
!
interface eth2
 ip address 192.168.10.57/24
 no shutdown
 ip ospf cost 10
 ip igmp version 2
 ip pim sparse-mode
```

Configuring IGMP Parameters

The configuration that follows shows how IGMP parameters can be configured.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Enter Interface mode
`(config-if)#ip igmp access-group 1`	Configures a access-list policy to control the multicast groups that hosts on the subnet serviced by an interface can join.
`(config-if)#ip igmp immediate-leave group-list 1`	Enables the device to remove the group entry from the multicast routing table immediately upon receiving a leave message for the group.
`(config-if#ip igmp  join-group 224.1.1.1`	Statically binds a multicast group to the outgoing interface

(config-if)# ip igmp last-member-query-count 7	Sets the query count used when the software starts up.
(config-if)# ip igmp last-member-query-interval 25500	Sets the query interval used when the software starts up.
(config-if)#ip igmp limit 100	Configure Max Allowed State on this interface
(config-if)#ip igmp querier-timeout 300	Sets the querier timeout that the router uses when deciding to take over as the querier.
(config-if)#ip igmp query-interval 200	Sets the frequency at which the router sends IGMP host query messages.
(config-if)#ip igmp query-max-response-time 150	Sets the response time advertised in IGMP queries.
(config-if)#ip igmp ra-option	Enable ra-option.
(config-if)#ip igmp robustness-variable 4	Sets the robustness variable.
(config-if)#ip igmp startup-query-count 4	Sets the query count used when the router starts up.
(config-if)# ip igmp startup-query-interval 50	Sets the query interval used when the router starts up.
(config-if)# ip igmp static-group 255.1.1.1	Statically binds a multicast group to the outgoing interface.
(config-if)#exit	Exit Interface mode.
(config)#exit	Exit Configure mode.

Validation

Enter the commands listed in this section to confirm the previous configurations.

```
Rtr1#show  running-config
!
no service password-encryption
!
hostname rtr1
!
!
ip multicast-routing
!
!
interface eth2
 ip address 10.1.1.10/24
 no shutdown
 ip ospf cost 10
 ip igmp access-group 1
 ip igmp immediate-leave group-list 1
 ip igmp last-member-query-count 7
 ip igmp limit 100
 ip igmp join-group 224.1.1.1
 ip igmp static-group 225.1.1.1
 ip igmp last-member-query-interval 25500
 ip igmp querier-timeout 300
 ip igmp query-interval 200
 ip igmp query-max-response-time 150
 ip igmp startup-query-interval 50
 ip igmp startup-query-count 4
 ip igmp robustness-variable 4
 ip igmp ra-option
 ip igmp version 2
 ip pim sparse-mode
!!

Rtr1#show  ip igmp   interface  eth2
Interface eth2 (Index 4)
 IGMP Enabled, Active, Querier, Configured for version 2
 Internet address is 10.1.1.10
 IGMP interface limit is 100
 IGMP interface has 2 group-record states
 IGMP activity: 0 joins, 0 leaves
 IGMP querying router is 0.0.0.0
 IGMP query interval is 200 seconds
 IGMP Startup query interval is 50 seconds
 IGMP Startup query count is 4
 IGMP querier timeout is 300 seconds
 IGMP max query response time is 150 seconds
 Group Membership interval is 950 seconds
 IGMP Last member query count is 7
 Last member query response interval is 25500 milliseconds
```

Here is the sample configuration on Router-1 with all the IGMP related commands configured.

```
Rtr1#show  running-config
!
no service password-encryption
!
hostname rtr1
!
!
debug nsm packet
debug ip pim events
debug ip pim mfc
debug ip pim packet
debug ip pim state
debug ip pim timer
debug ip pim mib
!
ip domain-lookup
no ip icmp-broadcast
!
ip multicast-routing
!
ip pim register-rp-reachability
ip pim crp-cisco-prefix
!
interface lo
 ip address 127.0.0.1/8
 ip address 1.1.1.57/32 secondary
 ipv6 address ::1/128
 no shutdown
!
interface eth0
 ip address 10.12.48.179/24
 no shutdown
!
interface eth1
```

```
 ip address 192.168.1.27/24
 no shutdown
 ip ospf cost 10
 ip igmp version 3
 ip pim sparse-mode
!
interface eth2
 ip address 10.1.1.10/24
 no shutdown
 ip ospf cost 10
 ip igmp access-group 1
 ip igmp immediate-leave group-list 1
 ip igmp last-member-query-count 7
 ip igmp limit 100
 ip igmp join-group 224.1.1.1
 ip igmp static-group 225.1.1.1
 ip igmp last-member-query-interval 25500
 ip igmp querier-timeout 300
 ip igmp query-interval 200
 ip igmp query-max-response-time 150
 ip igmp startup-query-interval 50
 ip igmp startup-query-count 4
 ip igmp robustness-variable 4
 ip igmp ra-option
 ip igmp version 2
 ip pim sparse-mode
!
!
router ospf 100
 network 192.168.1.0/24 area 0.0.0.0
 network 10.1.1.0/24 area 0.0.0.0
!
line con 0
 login
line vty 0 16
 exec-timeout 0 0
 login
line vty 17 39
 login
!
End
```

IGMP Group Table after IGMPV2 Membership Report is received

IGMP group table is populated at router by virtue of either static join is configured on interface or dynamic report is being received on the interface.

The `show ip igmp group` command displays the IGMP group table. In this table, the following fields are defined.

Table 7-1: IGMP group table after IGMPV2 membership report

Group address	Displays the Multicast Group for which report is received.
Interface	Interface name on which Membership report is received.
Uptime	Duration since the report is received.
Expiry	Time frame in which the multicast group is going to expire.
Last Reporter	Host address from where the report is generated.

```
Rtr1#show  ip igmp groups
IGMP Connected Group Membership
Group Address    Interface            Uptime     Expires      Last Reporter
224.0.1.3            eth2                    00:10:06   00:03:43     10.1.1.52
224.1.1.1            eth2                    01:54:53   static         0.0.0.0
225.1.1.1            eth2                    00:17:22   static         0.0.0.0

Rtr1#show  ip igmp groups detail
IGMP Connected Group Membership Details

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          224.0.1.3
Flags:          R
Uptime:         00:10:06
Group mode:     Exclude (Expires: 00:03:43)
Last reporter:  10.1.1.52
Source list is empty

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          224.1.1.1
Flags:          L
Uptime:         01:54:59
Group mode:     Exclude (Static)
Last reporter:  0.0.0.0
Source list is empty

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          225.1.1.1
Flags:          SG
Uptime:         00:17:28
Group mode:     Exclude (Static)
Last reporter:  0.0.0.0
```

```
Source list is empty
```

IGMP Group Table after IGMPV3 Membership report is received

IGMP group table is populated at router by virtue of either static join is configured on interface or dynamic report is being received on the interface.

The `show ip igmp group` command displays the IGMP group table. In this table, the following fields are defined.

Table 7-2: IGMP group table after IGMPV3 membership

Group address	Displays the Multicast Group for which report is received.
Interface	Interface name on which Membership report is received.
Uptime	Duration since the report is received.
Expiry	Time frame in which the multicast group is going to expire.
Last Reporter	Host address from where the report is generated.

```
rtr6#show  ip igmp  groups
IGMP Connected Group Membership
Group Address    Interface            Uptime   Expires  Last Reporter
224.0.1.3        eth2                 00:08:50 00:02:10 192.168.10.52
rtr6#show  ip igmp  groups detail
IGMP Connected Group Membership Details

Flags: (M - SSM Mapping, R - Remote, L - Local,
        SG - Static Group, SS - Static Source)
Interface:      eth2
Group:          224.0.1.3
Flags:          R
Uptime:         00:08:50
Group mode:     Exclude (Expires: 00:04:57)
Last reporter:  192.168.10.52
Group source list: (R - Remote, M - SSM Mapping, S - Static, L - Local)

Exclude Source List :
  Source Address  Uptime    v3 Exp    Fwd  Flags
  1.2.3.4         00:08:50  stopped   No   R

For IGMPV3 report source list specifies which source to be included or exclude
based on the membership report sent by the hosts.

In the above show command, Source address 1.2.3.4 is excluded to send
Multicast data  for group 224.0.1.3
```

CHAPTER 8 IGMP Proxy Configuration

In some simple tree topologies, it is not necessary to configure complex multicast routing protocols, such as PIM, on the boundary devices. It is sufficient to learn and proxy the group membership information and simply forward multicast packets based upon that information. Using IGMP forwarding (RFC 4605) to replicate multicast traffic on devices such as the edge boxes can greatly simplify the design and implementation of those devices. By not supporting more complicated multicast routing protocol such as Protocol Independent Multicast (PIM), it reduces not only the cost of the devices but also the operational overhead. Another advantage is that it makes the proxy devices independent of the multicast routing protocol used by the core network routers.

IGMP proxy can be used in such topologies instead of PIM. With IGMP proxy configured, the device serves as a proxy for the downstream hosts to send IGMP messages, maintain group memberships, and implement multicast forwarding based on the memberships. In this case, each boundary device configured with IGMP proxying is a host but no longer a PIM neighbor to the upstream device.

A device with IGMP proxy configured maintains a group membership database, which stores the group memberships on all the downstream interfaces. Each entry comprises the multicast address, filter mode, and source list. Such an entry is a collection of members in the same multicast group on each downstream interface.

A proxy device performs host functions on the upstream interface based on the database. It responds to queries according to the information in the database or sends join/leave messages when the database changes. On the other hand, the proxy device performs router functions on the downstream interfaces by participating in the querier election, sending queries, and maintaining memberships based on the reports.

Terminology

Following is a brief description of terms and concepts used to describe the IGMP Proxy:

Upstream interface

Also referred to as the proxy interface. A proxy interface is an interface on which IGMP proxy service is configured. It is in the direction toward the root of the multicast forwarding tree. An upstream interface acts as a host running IGMP; therefore, it is also called host interface.

Downstream interface

An interface that is running IGMP and in the direction contrary to the root of the multicast forwarding tree. A downstream interface acts as a router running IGMP; therefore, it is also called router interface.

Member State

State of the associated group address and interface.

- Idle - Interface has not yet responded to a group membership query or general query for this group.
- Delay - Interface has responded to the latest group membership query or general query for this group.

IGMP-Proxy Configuration Steps

This section provides the configuration steps for configuring IGMP Proxy and example for a relevant scenario.

- Enable IP multicast on each router (see Enabling IP Multicast Routing)
- Enable IGMP Proxy service on the upstream interface.
- Enable IGMP mrouter configuration on the downstream interface.
- Enable IGMP proxy unsolicited report interval on the proxy interface. The proxy group membership reports are forwarded to the upstream router in this unsolicited report interval time. This is an optional parameter in which the default value of 1 sec is considered for forwarding proxy groups to upstream router.

Note: Configure IP addresses on all the interfaces used in the topology.

Unicast routing protocol should be configured in the PIM domain.

Topology

In this network topology, Router 1 acts as a proxying router to the upstream router Router 2 in which PIM domain is present. Also the source address is 172.31.1.52 and the group address is set to 224.0.1.3.

Note: Any PIM mode (PIM-SM,PIM-DM,PIM-SMDM) should be enabled on all the interfaces in the PIM domain.

Here in this example default value for unsolicited report interval is considered.

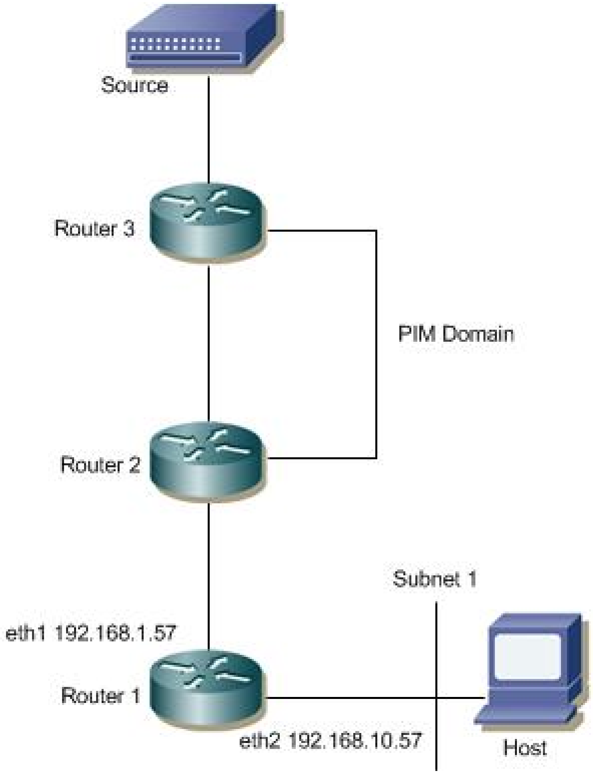

Figure 8-1: IGMP Proxy Topology

In this example, Routers 2 and 3 are running PIM and Router1 is the IGMP Proxying router.

- Host ends an IGMP membership report to Subnet 1.
- Downstream interface on Router1 received IGMP reports from host and updates the proxy interface.
- IGMP Proxying router (Router1) maintains the group membership information and forwards the received report to the upstream router (Router2).
- Source then sends a data packet for group.
- When the data packet reaches Router1, it forwards via the interface, eth2, because it has an IGMP join requested for Multicast traffic.

Enabling IP Multicast Routing

Enable IP multicast routing on all of the PIM routers inside the PIM domain:

`#configure terminal`	Enter Configure mode.
`(config)# ip multicast-routing`	Enable IP multicast routing.
`(config)#exit`	Exit Configure mode.

Enabling Proxy upstream interface

Enable IGMP proxy service on the interface in which the interface is in the direction toward the root of the multicast forwarding tree. In this example eth1 is the upstream interface which acts as an IGMP host.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Enter interface mode.
`(config-if)#ip igmp proxy-service`	Enable IGMP proxy service on the upstream interface.
`(config-if)#exit`	Exit interface mode.
`(config)#exit`	Exit Configure mode.

Enabling Proxy downstream interface

Enable IGMP mrouter proxy on the interface in which the interface is in the direction contrary to the root of the multicast forwarding tree. In this example eth2 is the downstream interface which is connected to receiver.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Enter Interface mode
`(config-if)#ip igmp mrouter-proxy eth1`	Enable IGMP mrouter proxy on the downstream interface and specify the upstream proxy interface name.
`(config-if)#exit`	Exit Interface mode.
`(config)#exit`	Exit Configure mode.

Validation

Here is the same configuration for IGMP Proxying router.

```
hostname Router1
!
interface eth0
!
interface eth1
ip igmp proxy-service
!
interface eth2
ip igmp mrouter-proxy eth1
!
interface lo
!
!
ip multicast-routing
!
```

IGMP proxy interface

The following output displays the IGMP Proxy interface information.

```
Router1#show ip igmp interface

Interface eth1 (Index 3)
 IGMP Enabled, Active, Version 3 (default), proxy-service
 IGMP host version 3
 Internet address is 192.168.1.57
 Unsolicited Report Interval is 1000 milliseconds


Interface eth2 (Index 4)
 IGMP Enabled, Active, Querier, Version 3 (default)
 IGMP mroute-proxy interface is eth1
 Internet address is 192.168.10.57
 IGMP interface has 1 group-record states
 IGMP activity: 1 joins, 0 leaves
 IGMP query interval is 125 seconds
 IGMP Startup query interval is 31 seconds
 IGMP Startup query count is 2
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Group Membership interval is 260 seconds
 IGMP Last member query count is 2
 Last member query response interval is 1000 milliseconds
```

IGMP proxy

The following output displays the IGMP proxy information.

```
Router1#show ip igmp proxy

Interface eth2 (Index 4)
Administrative status: enabled
```

```
    Operational status: up
    Upstream interface is eth1
    Number of multicast groups: 1
```

IGMP proxy groups

The following output displays the IGMP proxy group membership information.

```
    Router1#show ip igmp proxy groups

    IGMP Connected Proxy Group Membership
    Group Address    Interface            State     Member state
    224.0.1.3        eth1                 Active    Delay
```

IP Multicast Routing Table

The `show ip mroute` command displays the IP multicast routing table.

```
    Router1#show ip mroute

    IP Multicast Routing Table
    Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
           B - BIDIR
    Timers: Uptime/Stat Expiry
    Interface State: Interface (TTL)

    (172.31.1.52, 224.0.1.3), uptime 00:00:05
    Owner IGMP-Proxy-Service, Flags: F
      Incoming interface: eth1
      Outgoing interface list:
        eth2 (1)
```

Enabling Unsolicited report interval

Enable IGMP proxy unsolicited report interval on the upstream interface. The proxy group membership reports are forwarded to the upstream router in this unsolicited report interval time.

`#configure terminal`	Enter Configure mode.
`(config)#interface eth1`	Enter Interface mode
`(config-if)#ip igmp proxy unsolicited-report-interval 20000`	Enable IGMP proxy unsolicited report interval value on the upstream interface.
`(config-if)#exit`	Exit Interface mode.
`(config)#exit`	Exit Configure mode.

Validation

Here is the same configuration for IGMP Proxying router.

```
    hostname Router1
    !
    interface eth0
    !
```

```
interface eth1
ip igmp proxy-service
ip igmp proxy unsolicited-report-interval 20000
!
interface eth2
ip igmp mrouter-proxy eth1
!
interface lo
!
!
ip multicast-routing
!
```

IGMP proxy Unsolicited report interval

The following output displays the IGMP proxy unsolicited report interval information.

```
Router1#show ip igmp interface eth1

Interface eth1 (Index 3)
 IGMP Enabled, Active, Version 3 (default), proxy-service
 IGMP host version 3
 Internet address is 192.168.1.57
 Unsolicited Report Interval is 20000 milliseconds
```

IGMP proxy group with unsolicited report interval

The following output displays the IGMP proxy group membership information when the proxy unsolicited report interval is configured to specific value.

```
Router1#show ip igmp proxy groups

IGMP Connected Proxy Group Membership
Group Address    Interface            State     Member state
224.0.1.3        eth1                 Active    Idle
```

IP Multicast Routing Table

The `show ip mroute` command displays the IP multicast routing table.

```
Router1#show ip mroute

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder installed
       B - BIDIR
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(172.31.1.52, 224.0.1.3), uptime 00:00:05
Owner IGMP-Proxy-Service, Flags: F
  Incoming interface: eth1
  Outgoing interface list:
    eth2 (1)
```

CHAPTER 9 IGMP Snooping Configuration

This chapter describes how to configure Internet Group Management Protocol (IGMP) Snooping.

Note: This example assumes you are running the Layer-2 module. If using the ZebOS-XP Hybrid Layer-2/Layer-3 module, run the `switchport` command on each port to change to Layer-2 mode.

Without IGMP, Layer-2 switches handle IP multicast traffic in the same manner as broadcast traffic and forwards frames received on one interface to all other interfaces. This creates excessive traffic on the network, and affects network performance. IGMP Snooping allows switches to monitor network traffic, and determine hosts to receive multicast traffic. Only one membership report is relayed from a group, instead of a report from each host in the group. To achieve this, IGMP proxy is enabled on the switches.

Topology

This example describes the configuration on switch S1. The eth1 interface is configured as a multicast router port.

Because IGMP Snooping is used in bridged LAN environments, router R1 does not require running IGMP Snooping, and can run any multicast protocol (such as PIM-SM). Thus, the configuration on R1 is not included in this example.

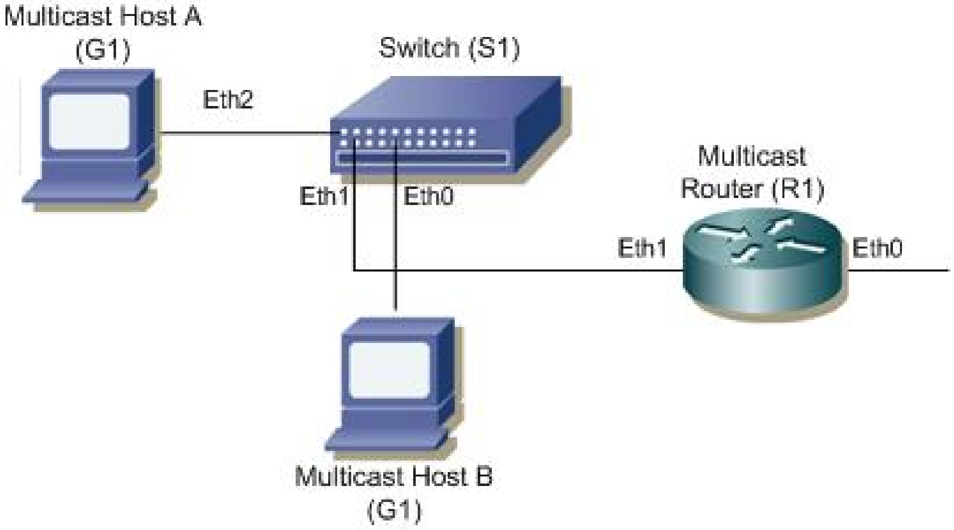

Figure 9-1: IGMP Snooping Topology

As a result of this configuration:

- The switch itself replies with membership report messages in response to queries received on interface eth1. However, if you do not enable report suppression on the switch, when it receives an IGMP Query message on eth1, it forwards it to both Host A and Host B. As a result, both hosts reply with a Membership report (as Layer-2 IGMP is running on the hosts).
- Because Host A and Host B are members of the same multicast group, the router is not notified when A leaves the group, because the group still has another member. When Host B leaves the group, the switch will send a Leave message to the Router with the destination address as 224.0.0.2 (All Router Destination Address).

Configuration Steps

To enable IGMP Snooping on an interface:

1. Add a bridge to the spanning-tree table
2. Specify the interface to be configured
3. Associate the interface with bridge group
4. Enable IGMP Snooping globally
5. Enable IGMP Snooping on the bridge group
6. Configure ports that are connected to routers as multicast router ports
7. By default, IGMP report suppression is enabled on the switch

S1

#configure terminal	Enter the Configure mode.
(config)#bridge 1 protocol ieee vlan-bridge	Add bridge 1 to the spanning-tree table.
(config)#interface eth0	Specify the interface eth0 to be configured, and enter the Interface mode.
(config-if)#shutdown	Shut down the interface.
(config-if)#switchport	Configure the interface as a switch port.
(config-if)#bridge-group 1	Associate the interface eth1 with bridge-group 1.
(config-if)#switchport mode access	Configure the port as an access port.
(config-if)#no shutdown	Bring up the interface.
(config-if)#exit	Exit the Interface mode.
(config)#interface eth1	Specify interface eth1 to be configured.
(config-if)#shutdown	Shut down the interface.
(config-if)#switchport	Configure the interface as a switch port.
(config-if)#bridge-group 1	Associate interface eth1 with bridge-group 1.
(config-if)#switchport mode access	Configure the port as an access port.
(config-if)#no shutdown	Bring up the interface.
(config-if)#exit	Exit the Interface mode.
(config)#interface eth2	Specify interface eth2 to be configured.
(config-if)#shutdown	Shut down the interface.
(config-if)#switchport	Configure the interface as a switch port.
(config-if)#bridge-group 1	Associate interface eth2 with bridge-group 1.
(config-if)#switchport mode access	Configure the port as an access port.
(config-if)#no shutdown	Bring up the interface.
(config-if)#exit	Exit the Interface mode.

`(config)#igmp snooping`	Enable IGMP Snooping globally.
`(config)#interface vlan1.1`	Specify interface `vlan1.1` to be configured.
`(config-if)# igmp snooping mrouter interface eth1`	Configure this port as a multicast router port
`(config-if)#exit`	Exit the `Interface` mode

CHAPTER 10 MSDP Configuration

Multicast Source Discovery Protocol (MSDP) is used to exchange multicast source information between BGP-enabled PIM-SM domains. Using MSDP, routers in a PIM-SM domain can rely on their own RP to reach a source in a different PIM-SM domain.

Overview

MSDP routers in a PIM-SM domain have a MSDP peering relationship with MSDP peers in another domain using a TCP connection. MSDP peering is the first step towards exchanging inter-domain multicast source information using MSDP SA (Source-Active) messages.

When an RP in a PIM-SM domain first learns of a new sender (via PIM register messages), it constructs an SA message and sends it to its MSDP peers.

All RPs which intend to originate or receive SA messages must establish MSDP peering with other RPs, either directly or via an intermediate MSDP peer.

An SA message contains these fields:

- Source address of the data source
- Group address the data source sends to
- IP address of the RP

Each SA message received from a MSDP peer goes through an RPF check. The peer-RPF check compares the RP address carried in the SA message with the MSDP peer from which the message was received:

- If the MSDP peer receives an SA from a non-RPF peer towards the originating RP, it drops the message.
- Otherwise, it forwards the message to all its MSDP peers (except the one from which it received the SA message).

When an RP receives a new SA message from a peer in another domain, it checks if there are any receivers interested in the traffic. An RP checks for a (*, G) entry with a non-empty outgoing list. If the outgoing list is non-empty, the RP sends a (S,G) join towards the source.

Caching SA state

If a member joins a group soon after a SA message is received by the local RP, that member needs to wait until the next SA message to learn about the source. MSDP SA caching is done at MSDP peers to reduce join latency for new receivers. The SA cache is populated as soon an MSDP peer receives a SA message from its peer.

MSDP Mesh Group

MSDP Mesh groups are used inside a PIM-SM domain to ease RPF checking and SA forwarding within the domain. Any SA messages received from a peer in a mesh group are not forwarded to other peers in the same mesh group. This reduces SA message flooding and simplifies peer-RPF flooding.

MSDP Default Peer

An MSDP default peer is used when MSDP peers are not BGP peers. SA messages coming from a default peer do not go through an RPF check and are always accepted.

Configure PIM-SM

For the MSDP topology in Figure 10-1, you must enable PIM-SM on all the routers in both PIM domains and make RTR-1 a rendezvous point (RP) in Domain-1 and RTR-2 an RP in Domain-2. For the steps to configure PIM-SM and RPs, see Chapter 1, *PIM Sparse Mode Configuration*.

Configure MSDP

In the topology in Figure 10-1, an MSDP session is established between RTR-1 and RTR-2 in both domains. The following sample configuration on RTR-1 shows how to enable MSDP peering between RTR-1 and RTR-2.

Topology

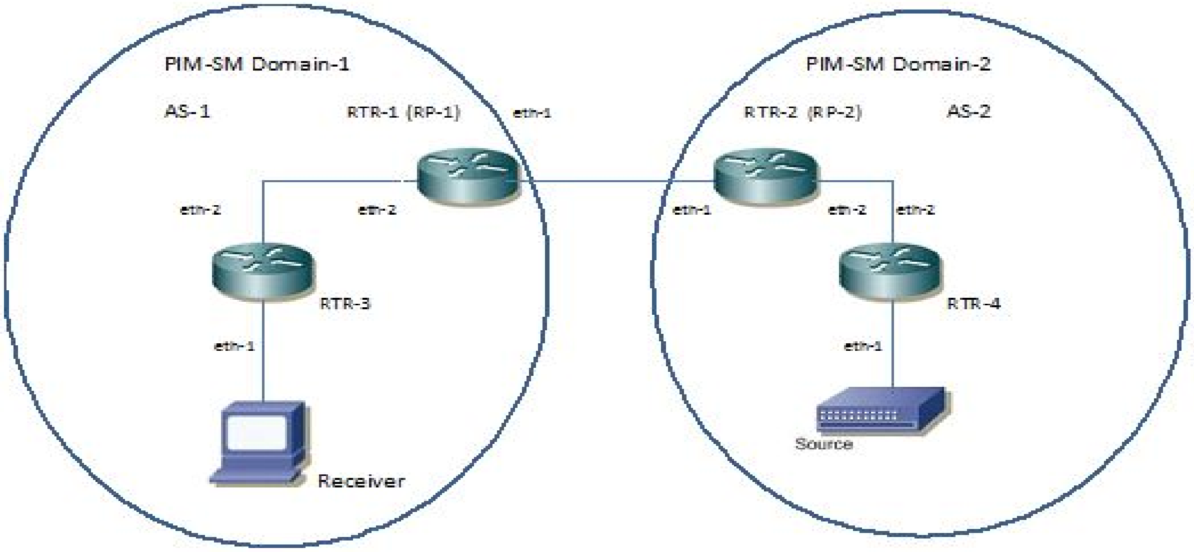

Figure 10-1: MSDP topology

IP addresses:

RTR-1 eth1: 11.1.1.11

RTR-1 eth2: 10.1.1.11

RTR-2 eth1: 11.1.1.12

RTR-2 eth2: 12.1.1.12

RTR-4 eth1: 12.1.1.14

RTR-4 eth2: 20.1.1.14

RTR-3 eth1: 13.1.1.13

RTR-3 eth2: 10.1.1.13

Source: 20.1.1.10

Multicast group: 224.1.1.1

RTR-1

`#configure terminal`	Enter configure mode.

`(config)#ip msdp peer 11.1.1.12`
--or--
`(config)#ip msdp peer 11.1.1.12 connect source eth1`
	Configure a MSDP peer.
	Use the connect-source option to specify the primary IP address of the interface to use as the source IP address of the MSDP TCP connection.

`(config)#ip msdp password zebos peer 11.1.1.12`	Configure an MSDP password for the peer. You must specify the same command at RTR-2. The password must match at both the routers.
`(config)#ip msdp default-peer 11.1.1.12`	Configure MSDP default peer.
`(config)#ip msdp mesh-group mesh1 11.1.1.12`	Configure MSDP mesh group.
`(config)#ip msdp originator-id eth2`	Configure MSDP originator identifier.
`(config)#exit`	Exit configure mode.

Validation

RTR-1

```
#show running-config

ip msdp peer 11.1.1.12
ip msdp default-peer 11.1.1.12
ip msdp mesh-group mesh1 11.1.1.12
ip msdp password zebos peer 11.1.1.12
ip msdp originator-id eth2
ip multicast-routing
!
ip pim register-rp-reachability
ip pim bsr-candidate eth2
ip pim rp-candidate eth2
ip pim vrf management register-rp-reachability
!
interface lo
 ip address 127.0.0.1/8
 ipv6 address ::1/128
 no shutdown
!
interface eth0
 ip address 10.12.48.175/24
 no shutdown
!
interface eth1
```

```
 ip address 11.1.1.11/24
no shutdown
 ip pim sparse-mode
ip pim bsr-border
!
interface eth2
 ip address 10.1.1.11/24
 no shutdown
ip pim sparse-mode
!
interface eth3
 no shutdown
!
interface pimreg
 no multicast
 no shutdown
!
router ospf 100
 network 10.1.1.0/24 area 0.0.0.0
 cspf disable-better-protection
!
router bgp 1
neighbor 11.1.1.12 remote-as 2
!
line con 0
 login
line vty 0 39
 login
!
```

This command shows the MSDP peer information at RTR-1:

```
#show ip msdp peer
MSDP Peer 11.1.1.12
Connection status
 State: Up (Established)
 Keepalive sent: 1
 Keepalive received: 1
 Number of connect retries: 0
```

In the MSDP topology in Figure 10-1, when a source sends multicast traffic for group 224.1.1.1, RTR-4 (the DR) sends a register packet towards RTR-2 which is the RP in the domain. RTR-2 receives the register packet and sends an MSDP SA message to its MSDP peer (RTR-1). RTR-1 receives the SA message and creates an entry in the SA cache containing the source, group, and RP information.

This command at RTR-1 shows the SA information with source address, group address, and RP address:

```
#show ip msdp sa-cache
MSDP Source-Active Cache:
(20.1.1.11, 224.1.1.1), RP 10.1.1.11, RPF-Peer 11.1.1.12 Uptime  00:00:02 Exptime
00:03:28P
```

RTR-3 receives an IGMP join for group 224.1.1.1 and joins the shared tree path toward the RP (RTR-1).

When RTR-1 receives an SA message from RTR-2, because it has a receiver, it sends an (S,G) join towards the source. Now traffic from the source is received at RTR-1 via the shortest path tree formed between RTR-1 and the source. RTR-1 distributes traffic downstream towards the receiver.

This command shows the PIM state at RTR-1 upon receiving an SA message and joining towards the source:

```
#show ip pim mroute
IP Multicast Routing Table

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

(*, 224.1.1.1)
RP: 10.1.1.11
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: JOINED
 Local     ..i.............................
 Joined    ................................
 Asserted  ................................
FCR:

(20.1.1.10, 224.1.1.1)
RPF nbr: 11.1.1.12
RPF idx: eth1
SPT bit: 0
Upstream State: JOINED
 Local     ................................
 Joined    ................................
 Asserted  ................................
 Outgoing  ..o.............................

(20.1.1.10, 224.0.1.3, rpt)
RP: 10.1.1.11
RPF nbr: 0.0.0.0
RPF idx: None
Upstream State: NOT PRUNED
 Local     ................................
 Pruned    ................................
 Outgoing  ..o.............................
```

RTR-2

This command shows the MSDP peer information at RTR-2.

```
#show  ip msdp  peer
MSDP Peer 11.1.1.11
Connection status
 State: Up (Established)
 Keepalive sent: 2
 Keepalive received: 2
```

Appendix A Tunnel Interface

To tunnel multicast traffic through intermediate routers which do not support multicast routing, a multicast tunnel can be created between two multicast routers (PIM-SM, PIM-DM) in IP-in-IP (IPIP) or Generic Routing Encapsulation (GRE) tunnel encapsulation mode. The following provides examples to create this tunnel.

Note: Tunnel interfaces are supported only on Linux.

Configuring Interface Tunnel between Two PIM-SM Routers

The following shows the commands to create an interface tunnel between two PIM-SM routers in IPIP mode.

`#configure terminal`	Enter Configure mode.
`(config)#interface tunnel 2`	Create a new tunnel interface and enter the Interface mode.
`(config-if)#tunnel source 10.10.1.52`	Specify the tunnel source address.
`(config-if)#tunnel destination 10.10.3.35`	Specify the tunnel destination address.
`(config-if)#tunnel ttl 23`	Set the time-to-live for the tunnel to 23.
`(config-if)#tunnel mode ipip`	Configure the tunnel mode.
`(config-if)#ip pim sparse-mode`	Enable PIM sparse mode on the interface.

PIM-DM

The following shows commands to create an interface tunnel between two PIM-DM routers in GRE mode.

`#configure terminal`	Enter Configure mode.
`(config)#interface tunnel 2`	Create a new tunnel interface and enter the Interface mode.
`(config-if)#tunnel source 10.10.1.52`	Specify the tunnel source address.
`(config-if)#tunnel destination 10.10.3.35`	Specify the tunnel destination address.
`(config-if)#tunnel ttl 23`	Set the time-to-live for the tunnel to 23.
`(config-if)#tunnel mode gre`	Configure the tunnel in Generic Routing Encapsulation (GRE) mode. Configure a Generic Routing Encapsulation (GRE) tunnel mode.
`(config-if)#ip pim dense-mode`	Enable PIM dense mode on the interface.

Index