Multicast Routing Overview

The FWSM supports both Stub Multicast Routing and PIM multicast routing. However, you cannot configure both concurrently on a single FWSM.

Note

Only the UDP transport layer is supported for multicast routing.

Stub multicast routing provides dynamic host registration and facilitates multicast routing. When configured for Stub Multicast Routing, the FWSM acts as an IGMP proxy agent. Instead of fully participating in multicast routing, the FWSM forwards IGMP messages to an upstream multicast router, which sets up delivery of the multicast data. When configured for Stub Multicast Routing, the FWSM cannot be configured for PIM.

The FWSM supports both PIM-SM and bi-directional PIM. PIM-SM is a multicast routing protocol that uses the underlying unicast routing information base or a separate multicast-capable routing information base. It builds unidirectional shared trees rooted at a single Rendezvous Point per multicast group and optionally creates shortest-path trees per multicast source.

Bi-directional PIM is a variant of PIM-SM that builds bi-directional shared trees connecting multicast sources and receivers. Bi-directional trees are built using a DF election process operating on each link of the multicast topology. With the assistance of the DF, multicast data is forwarded from sources to the Rendezvous Point, and therefore along the shared tree to receivers, without requiring source-specific state. The DF election takes place during Rendezvous Point discovery and provides a default route to the Rendezvous Point.
Enabling Multicast Routing

Enabling multicast routing lets the FWSM forward multicast packets. Enabling multicast routing automatically enables PIM and IGMP on all interfaces. To enable multicast routing, enter the following command.

```
hostname(config)# multicast-routing
```

**Note**

If the FWSM is the PIM RP, use the untranslated outside address of the FWSM as the RP address.

**Enabling Multicast Routing**

Multicast routing on the FWSM is limited to eight outgoing interfaces.

The number of entries in the multicast routing tables are limited by the amount of RAM on the system. Table 9-1 lists the maximum number of entries for specific multicast tables based on the amount of RAM on the FWSM. Once these limits are reached, any new entries are discarded.

**Table 9-1  Entry Limits for Multicast Tables**

<table>
<thead>
<tr>
<th>Table</th>
<th>16 MB</th>
<th>128 MB</th>
<th>128+ MB</th>
</tr>
</thead>
<tbody>
<tr>
<td>MFIB</td>
<td>1000</td>
<td>3000</td>
<td>5000</td>
</tr>
<tr>
<td>IGMP Groups</td>
<td>1000</td>
<td>3000</td>
<td>5000</td>
</tr>
<tr>
<td>PIM Routes</td>
<td>3000</td>
<td>7000</td>
<td>12000</td>
</tr>
</tbody>
</table>

**Configuring IGMP Features**

IP hosts use IGMP to report their group memberships to directly connected multicast routers. IGMP uses group addresses (Class D IP address) as group identifiers. Host group address can be in the range 224.0.0.0 to 239.255.255.255. The address 224.0.0.0 is never assigned to any group. The address 224.0.0.1 is assigned to all systems on a subnet. The address 224.0.0.2 is assigned to all routers on a subnet.

When you enable multicast routing on the FWSM, IGMP Version 2 is automatically enabled on all interfaces.

**Note**

Only the `no igmp` command appears in the interface configuration when you use the `show run` command. If the `multicast-routing` command appears in the device configuration, then IGMP is automatically enabled on all interfaces.

This section describes how to configure optional IGMP setting on a per-interface basis. This section includes the following topics:

- Disabling IGMP on an Interface, page 9-3
- Configuring Group Membership, page 9-3
- Configuring a Statically Joined Group, page 9-3
Disabling IGMP on an Interface

You can disable IGMP on specific interfaces. This is useful if you know that you do not have any multicast hosts on a specific interface and you want to prevent the FWSM from sending host query messages on that interface.

To disable IGMP on an interface, enter the following command:

`hostname(config-if)# no igmp`

To reenable IGMP on an interface, enter the following command:

`hostname(config-if)# igmp`

Note: Only the `no igmp` command appears in the interface configuration.

Configuring Group Membership

You can configure the FWSM to be a member of a multicast group. Configuring the FWSM to join a multicast group causes upstream routers to maintain multicast routing table information for that group and keep the paths for that group active.

To have the FWSM join a multicast group, enter the following command:

`hostname(config-if)# igmp join-group group-address`

Configuring a Statically Joined Group

Sometimes a group member cannot report its membership in the group, or there may be no members of a group on the network segment, but you still want multicast traffic for that group to be sent to that network segment. You can have multicast traffic for that group sent to the segment in one of two ways:

- Using the `igmp join-group` command (see Configuring Group Membership, page 9-3). This causes the FWSM to accept and to forward the multicast packets.
- Using the `igmp static-group` command. The FWSM does not accept the multicast packets but rather forwards them to the specified interface.

To configure a statically joined multicast group on an interface, enter the following command:

`hostname(config-if)# igmp static-group group-address`
Controlling Access to Multicast Groups

To control the multicast groups that hosts on the FWSM interface can join, perform the following steps:

**Step 1** Create an access list for the multicast traffic. You can create more than one entry for a single access list. You can use extended or standard access lists.

- To create a standard access list, enter the following command:

  ```
  hostname(config)# access-list name standard [permit | deny] ip_addr mask
  ```

  The `ip_addr` argument is the IP address of the multicast group being permitted or denied.

- To create an extended access list, enter the following command:

  ```
  hostname(config)# access-list name extended [permit | deny] protocol src_ip_addr src_mask dst_ip_addr dst_mask
  ```

  The `dst_ip_addr` argument is the IP address of the multicast group being permitted or denied.

**Step 2** Apply the access list to an interface by entering the following command:

```
hostname(config-if)# igmp access-group acl
```

The `acl` argument is the name of a standard or extended IP access list.

Limiting the Number of IGMP States on an Interface

You can limit the number of IGMP states resulting from IGMP membership reports on a per-interface basis. Membership reports exceeding the configured limits are not entered in the IGMP cache and traffic for the excess membership reports is not forwarded.

To limit the number of IGMP states on an interface, enter the following command:

```
hostname(config-if)# igmp limit number
```

Valid values range from 0 to 500, with 500 being the default value. Setting this value to 0 prevents learned groups from being added, but manually defined memberships (using the `igmp join-group` and `igmp static-group` commands) are still permitted. The `no` form of this command restores the default value.

Modifying the Query Interval and Query Timeout

The FWSM sends query messages to discover which multicast groups have members on the networks attached to the interfaces. Members respond with IGMP report messages indicating that they want to receive multicast packets for specific groups. Query messages are addressed to the all-systems multicast group, which has an address of 224.0.0.1, with a time-to-live value of 1.

These messages are sent periodically to refresh the membership information stored on the FWSM. If the FWSM discovers that there are no local members of a multicast group still attached to an interface, it stops forwarding multicast packet for that group to the attached network and it sends a prune message back to the source of the packets.

By default, the PIM designated router on the subnet is responsible for sending the query messages. By default, they are sent once every 125 seconds. To change this interval, enter the following command:
hostname(config-if)# `igmp query-interval seconds`

If the FWSM does not hear a query message on an interface for the specified timeout value (by default, 255 seconds), then the FWSM becomes the designated router and starts sending the query messages. To change this timeout value, enter the following command:

hostname(config-if)# `igmp query-timeout seconds`

**Note**
The `igmp query-timeout` and `igmp query-interval` commands require IGMP Version 2.

### Changing the Query Response Time

By default, the maximum query response time advertised in IGMP queries is 10 seconds. If the FWSM does not receive a response to a host query within this amount of time, it deletes the group.

To change the maximum query response time, enter the following command:

hostname(config-if)# `igmp query-max-response-time seconds`

### Changing the IGMP Version

By default, the FWSM runs IGMP Version 2, which enables several additional features such as the `igmp query-timeout` and `igmp query-interval` commands.

All multicast routers on a subnet must support the same version of IGMP. The FWSM does not automatically detect version 1 routers and switch to version 1. However, a mix of IGMP Version 1 and 2 hosts on the subnet works; the FWSM running IGMP Version 2 works correctly when IGMP Version 1 hosts are present.

To control which version of IGMP is running on an interface, enter the following command:

hostname(config-if)# `igmp version {1 | 2}`

### Configuring Stub Multicast Routing

An FWSM acting as the gateway to the stub area does not need to participate in PIM. Instead, you can configure it to act as an IGMP proxy agent and forward IGMP messages from hosts connected on one interface to an upstream multicast router on another. To configure the FWSM as an IGMP proxy agent, forward the host join and leave messages from the stub area interface to an upstream interface.

To forward the host join and leave messages, enter the following command from the interface attached to the stub area:

hostname(config-if)# `igmp forward interface if_name`

**Note**
Stub Multicast Routing and PIM are not supported concurrently.
Configuring a Static Multicast Route

When using PIM, the FWSM expects to receive packets on the same interface where it sends unicast packets back to the source. In some cases, such as bypassing a route that does not support multicast routing, you may want unicast packets to take one path and multicast packets to take another.

Static multicast routes are not advertised or redistributed.

To configure a static multicast route for PIM, enter the following command:

```
hostname(config)# mroute src_ip src_mask (input_if_name | rpf_neighbor) [distance]
```

For example:

```
hostname(config)# mroute 10.1.1.1 255.255.255.255 192.168.1.2
```

where 10.1.1.1 is the server that is sending out the multicast traffic, and 192.168.1.2 is the RPF neighbor for FWSM.

**Note**

You can specify the interface or the RPF neighbor, but not at the same time.

To configure a static multicast route for a stub area, enter the following command:

```
hostname(config)# mroute src_ip src_mask input_if_name [dense output_if_name] [distance]
```

**Note**

The `dense output_if_name` keyword and argument pair is only supported for Stub Multicast Routing.

Configuring PIM Features

Routers use PIM to maintain forwarding tables for forwarding multicast diagrams. When you enable multicast routing on the FWSM, PIM and IGMP are automatically enabled on all interfaces.

**Note**

PIM is not supported with PAT. The PIM protocol does not use ports and PAT only works with protocols that use ports.

This section describes how to configure optional PIM settings. This section includes the following topics:

- Disabling PIM on an Interface, page 9-6
- Configuring a Static Rendezvous Point Address, page 9-7
- Configuring the Designated Router Priority, page 9-7
- Filtering PIM Register Messages, page 9-7
- Configuring PIM Message Intervals, page 9-8

Disabling PIM on an Interface

You can disable PIM on specific interfaces. To disable PIM on an interface, enter the following command:
Configuring PIM Features

Configuring Multicast Routing

Configuring PIM Features

Hostname(config-if)# no pim

To reenable PIM on an interface, enter the following command:

Hostname(config-if)# pim

Note

Only the no pim command appears in the interface configuration.

Configuring a Static Rendezvous Point Address

All routers within a common PIM sparse mode or bidir domain require knowledge of the PIM RP address. The address is statically configured using the **pim rp-address** command.

Note

The FWSM does not support Auto-RP or PIM BSR; you must use the **pim rp-address** command to specify the RP address.

You can configure the FWSM to serve as RP to more than one group. The group range specified in the access list determines the PIM RP group mapping. If an access list is not specified, then the RP for the group is applied to the entire multicast group range (224.0.0.0/4).

To configure the address of the PIM PR, enter the following command:

```
hostname(config)# pim rp-address ip_address [acl] [bidir]
```

The **ip_address** argument is the unicast IP address of the router to be a PIM RP. The **acl** argument is the name or number of an access list that defines which multicast groups the RP should be used with. Excluding the **bidir** keyword causes the groups to operate in PIM sparse mode.

Note

The FWSM always advertises the bidir capability in the PIM hello messages regardless of the actual bidir configuration.

Configuring the Designated Router Priority

The DR is responsible for sending PIM register, join, and prune messages to the RP. When there is more than one multicast router on a network segment, there is an election process to select the DR based on DR priority. If multiple devices have the same DR priority, then the device with the highest IP address becomes the DR.

By default, the FWSM has a DR priority of 1. You can change this value by entering the following command:

```
hostname(config-if)# pim dr-priority num
```

The **num** argument can be any number from 1 to 4294967294.

Filtering PIM Register Messages

You can configure the FWSM to filter PIM register messages. To filter PIM register messages, enter the following command:
hostname(config)# **pim accept-register** *(list acl | route-map map-name)*

**Configuring PIM Message Intervals**

Router query messages are used to elect the PIM DR. The PIM DR is responsible for sending router query messages. By default, router query messages are sent every 30 seconds. You can change this value by entering the following command:

```
hostname(config-if)# **pim hello-interval** seconds
```

Valid values for the `seconds` argument range from 1 to 3600 seconds.

Every 60 seconds, the FWSM sends PIM join/prune messages. To change this value, enter the following command:

```
hostname(config-if)# **pim join-prune-interval** seconds
```

Valid values for the `seconds` argument range from 10 to 600 seconds.

**For More Information About Multicast Routing**

The following RFCs from the IETF provide technical details about the IGMP and multicast routing standards used for implementing the SMR feature:

- RFC 2236 IGMPv2
- RFC 2362 PIM-SM
- RFC 2588 IP Multicast and Firewalls
- RFC 2113 IP Router Alert Option
- IETF draft-ietf-idmr-igmp-proxy-01.txt