

Chapter 6

IGMP Configuration Guidelines

To configure IGMP, you include statements at the [edit protocols igmp] hierarchy level of the configuration:

```
[edit]
protocols {
  igmp {
    interface interface-name {
      disable;
      static {
        group group {
          source source;
        }
      }
      version version;
    }
    query-interval seconds;
    query-last-member-interval seconds;
    query-response-interval seconds;
    robust-count number;
    traceoptions {
      file name <replace> <size size> <files number> <no-stamp>
        <(world-readable | no-world-readable)>;
      flag flag <flag-modifier> <disable>;
    }
  }
}
```

By default, IGMP is automatically enabled on all broadcast interfaces on which you configure DVMRP or PIM.

This chapter describes the following tasks for configuring IGMP:

Minimum IGMP Configuration on page 38

Enable IGMP on page 38

Modify the IGMP Host-Query Message Interval on page 38

Modify the IGMP Query Response Interval on page 39

Modify the Last-Member Query Interval on page 39

Modify the Robustness Variable on page 39

Change the IGMP Version on page 40

Enable IGMP Static Group Membership on page 40

Trace IGMP Protocol Traffic on page 41

Disable IGMP on page 42

Minimum IGMP Configuration

IGMP is automatically enabled on all broadcast interfaces when you configure PIM or DVMRP. All IGMP configuration statements are optional.

Enable IGMP

IGMP is automatically enabled on all broadcast interfaces when you configure PIM or DVMRP.

To enable IGMP explicitly, include the `igmp` statement at the [edit protocols] hierarchy level. Optionally, you can specify the interface or interfaces on which to enable IGMP. If you do not specify any interfaces, IGMP is enabled on all interfaces.

```
[edit protocols]
igmp {
  interface interface-name;
}
```

For information about specifying interface names, see interface naming in the *JUNOS Internet Software Configuration Guide: Network Interfaces and Class of Service*.

Modify the IGMP Host-Query Message Interval

The IGMP querier router periodically sends general host-query messages. These messages solicit group membership information and are sent to the all-systems multicast group address, 224.0.0.1.

By default, host-query messages are sent every 125 seconds. You can change this interface to change the number of IGMP messages sent on the subnet.

To modify this interval, include the `query-interval` statement at the [edit protocols igmp] hierarchy level:

```
[edit protocols igmp]
query-interval seconds;
```

The query interval value can range from 1 through 1024 seconds.

Modify the IGMP Query Response Interval

The query response interval is the maximum amount of time that can elapse between when the querier router sends a host-query message and when it receives a response from a host. Varying this interval allows you to adjust the burstiness of IGMP messages on the subnet.

By default, the query response interval is 10 seconds. To modify this interval, include the `query-response-interval` statement at the `[edit protocols igmp]` hierarchy level:

```
[edit protocols igmp]
query-response-interval seconds;
```

The query response interval can range from 1 through 1024 seconds. It must be less than the host-query message interval.

Modify the Last-Member Query Interval

The last-member query interval is the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You can lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group.

The default last-member query interval is 1 second. To modify this interval, include the `query-last-member-interval` statement at the `[edit protocols igmp]` hierarchy level:

```
[edit protocols igmp]
query-last-member-interval seconds;
```

The last-member query interval can range from 1 through 1024 seconds.

Modify the Robustness Variable

The IGMP robustness variable provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals:

Group member interval—Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: $(\text{robustness variable} \times \text{query interval}) + (1 \times \text{query response interval})$.

Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: $(\text{robustness variable} \times \text{query interval}) + (0.5 \times \text{query response interval})$.

Last member query count—Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable.

By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to be lossy. To change the value of the robustness variable, include the robust-count statement at the [edit protocols igmp] hierarchy level:

```
[edit protocols igmp]
robust-count number;
```

The number can be from 2 through 10.

Change the IGMP Version

By default, the router runs IGMP version 2. To change to version 3 (for SSM functionality), include the version statement at the [edit protocols igmp interface *interface-name*] hierarchy level:

```
[edit protocols igmp interface interface-name]
version 3;
```

To enable SSM functionality, version 3 must be configured on the host and the host's directly connected router.



Note

Routers running different versions of IGMP negotiate the lowest common version of IGMP that is supported by hosts on their subnet and operate in that version.

If you have already configured the router to use IGMP version 1 and then configure it to use IGMP version 2, the router continues to use IGMP version 1 for up to 6 minutes and then use IGMP version 2.

Enable IGMP Static Group Membership

You can create IGMP static group membership to test multicast forwarding without a receiver host. When you enable IGMP static group membership, data is forwarded to an interface without receiving membership reports from host members.

To configure IGMP static membership, include the static statement at the [edit protocols igmp interface *interface-name*] hierarchy level. Then specify the group, or the group and its source(s).

```
[edit protocols igmp interface interface-name]
static {
  group group {
    source source;
  }
}
```



Note

You must specify a unique address for each group.

Example: IGMP Static Group Membership

Configure IGMP static membership on the interface where the data is to be forwarded, and specify the groups 239.255.0.1 and 232.1.1.1 with the sources 10.1.1.1 and 10.1.1.2:

```
[edit]
protocols {
  igmp {
    interface ge-1/1/1.0 {
      static {
        group 239.255.0.1;
        group 232.1.1.1 {
          source 10.1.1.1;
          source 10.1.1.2;
        }
      }
    }
  }
}
```

Trace IGMP Protocol Traffic

To trace IGMP protocol traffic, you can specify options in the global traceoptions statement at the [edit routing-options] hierarchy level, and you can specify IGMP-specific options by including the traceoptions statement at the [edit protocols igmp] hierarchy level:

```
[edit protocols igmp]
traceoptions {
  file name <replace> <size size> <files number> <no-stamp>
    <(world-readable | no-world-readable)>;
  flag flag <flag-modifier> <disable>;
}
```

You can specify the following IGMP-specific options in the IGMP flag statement:

leave—Trace leave-group messages (for IGMP Version 2 only).

mtrace—Trace mtrace packets. Use the mtrace command to troubleshoot the software.

packets—Trace all IGMP packets.

query—Trace IGMP membership query messages, including general and group-specific queries.

report—Trace membership report messages.

To trace the paths of multicast packets, use the mtrace command, as described in the *JUNOS Internet Software Operational Mode Command Reference: Protocols, Class of Service, Chassis, and Management* .

For information about tracing and global tracing options, see the *JUNOS Internet Software Configuration Guide: Routing and Routing Protocols* .

Example: Trace IGMP Protocol Traffic

Trace only unusual or abnormal operations to routing-log, and trace all IGMP packets to igmp-log:

```
[edit]
routing-options {
  traceoptions {
    file routing-log;
    flag errors;
  }
}
protocols {
  igmp {
    traceoptions {
      file igmp-log;
      flag packets;
    }
  }
}
```

Disable IGMP

To disable IGMP on an interface, include the disable statement at the [edit protocols igmp interface *interface-name*] hierarchy level:

```
[edit protocols]
igmp {
  interface interface-name;
  disable;
}
```

For information about specifying interface names, see the sections about interface naming in the *JUNOS Internet Software Configuration Guide: Network Interfaces and Class of Service*.