Chapter 2
Configuring IGMP

IP hosts use Internet Group Management Protocol (IGMP) in IPv4 to report their multicast group memberships to neighboring routers. Similarly, multicast routers, such as an E-series router, use IGMP to discover which of their hosts belong to multicast groups.

This chapter describes how to configure IGMP for IP multicast on an E-series router; it contains the following sections:

IGMP Overview

The IPv4 address scheme assigns class D addresses for IP multicast. IGMP is the protocol that uses these addresses, which can be in the range 224.0.0.0 to 239.255.255.255. The following addresses have specific functions or are unavailable:

- 224.0.0.0 is reserved—you cannot assign it to a group.
- 224.0.0.1 is the all-hosts address—a packet sent to this address reaches all hosts on a subnet.
- 224.0.0.2 is the all-routers address—a packet sent to this address reaches all routers on a subnet.

This implementation of IGMP complies with IGMP versions 1, 2, and 3. IGMPv3 supports source-specific join and leave messages and is backward compatible with IGMPv1 and IGMPv2.

IGMPv2 mode interfaces exchange the following types of messages between routers and hosts:

- Group membership queries
- Group membership reports
- Leave group membership messages

IGMPv3 mode interfaces exchange the following types of messages with IGMPv3 hosts:

- Group membership queries
- IGMPv3 group membership reports

Group Membership Queries

A multicast router can be a querier or a nonquerier. Only one querier is on a network at any time. Multicast routers monitor queries from other multicast routers to determine the status of the querier. If the querier detects a query from a router with a lower IP address, it relinquishes its role to that router.

IGMPv1 and IGMPv2 mode interfaces send two types of group membership queries to hosts on the network:

- General queries to the all-hosts group address (224.0.0.1)
- Specific queries to the appropriate multicast group address

IGMPv3 mode interfaces send the following types of queries to IGMPv3 hosts:

- General queries
- Group-specific queries
- Source-specific queries

The purpose of a group membership query is to discover the multicast groups to which a host belongs.

IGMPv2 and IGMPv3 group membership queries have a Max Response Time field. This response time is the maximum amount of time that a host can take to reply to a query.

Group Membership Reports

When a host receives a group membership query, it identifies the groups associated with the query and determines to which groups the query belongs. The host then sets a timer, with a value less than the Max Response Time field in the query, for each group to which it belongs.

When the timer expires, the host sends a group membership report to the group address. When a multicast router receives a report, it adds the group to the membership list for the network and sets a timer to the *group membership interval*. The router calculates the group membership interval using the following formula of configurable IGMP values:

(query interval x robustness value) + query maximum response time

If this timer interval expires before the router receives another group membership report, the router determines that the group has no members left on the network.

IGMPv3 supports an extended report format you can use to report multiple groups and source lists in a single report.

Leave Group Membership Messages

When a host leaves a group, it sends a leave group membership message to multicast routers on the network. A host generally addresses leave group membership messages to the all-routers group address (224.0.0.2).

Platform Considerations

For information about modules that support IGMP on the ERX-7xx models, ERX-14xx models, and the ERX-310 router:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support IGMP.

For information about modules that support IGMP on the E120 router and the E320 router:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support IGMP.

References

For more information about IGMP, see the following resources:

- IGMP-based Multicast Forwarding ("IGMP Proxying")—draft-ietf-magma-igmp-proxy-00.txt (May 2002 expiration)
- RFC 2236—Internet Group Management Protocol, Version 2 (November 1997)
- RFC 2933—Internet Group Management Protocol MIB (October 2000)
- RFC 3292—General Switch Management Protocol (GSMP) V3 (June 2002)
- RFC 3376—Internet Group Management Protocol (October 2002)
- GSMP extensions for layer2 control (L2C) Topology Discovery and Line Configuration—draft-wadhwa-gsmp-l2control-configuration-00.txt (July 2006 expiration)

Before You Begin

You can configure IGMP on IPv4 multicast interfaces.

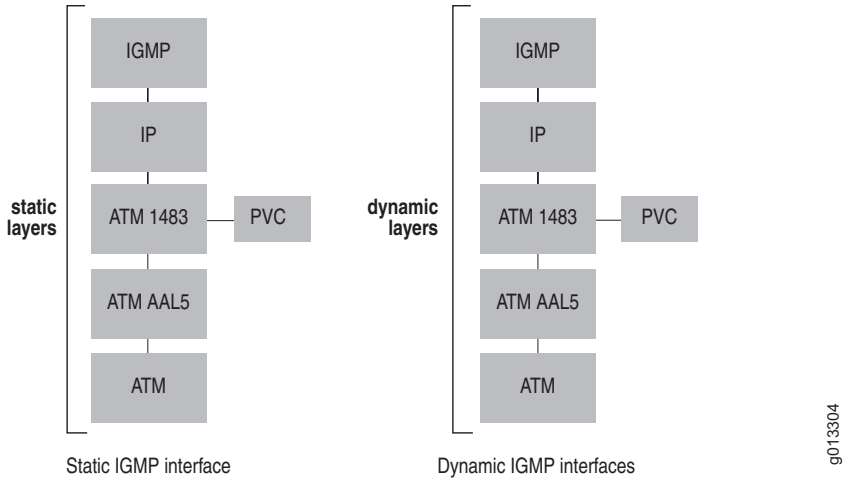
For information about IPv4 multicasting, see *Chapter 1, Configuring IPv4 Multicast*. For information about configuring IP interfaces, see *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 1, Configuring IP*. For information about configuring IPv6 interfaces, see *JUNOSe IP, IPv6, and IGP Configuration Guide, Chapter 2, Configuring IPv6*.

For information about configuring multicast on IPv6 interfaces, see *Chapter 5, Configuring IPv6 Multicast*.

Configuring Static and Dynamic IGMP Interfaces

The router supports *static* and *dynamic* IGMP interfaces. Unlike static interfaces, dynamic interfaces are not restored when you reboot the router. For some protocols, dynamic layers can build on static layers in an interface; however, in a dynamic IGMP interface, all the layers are dynamic. See Figure 5 for examples of static and dynamic IGMP interfaces.

Figure 5: Static and Dynamic IGMP Interfaces



You configure static IGMP interfaces by using software such as the CLI or an SNMP application; you configure dynamic IGMP interfaces by using a profile. A profile constitutes a set of attributes for an interface; a profile for dynamic IGMP interfaces contains attributes for configuring all the layers in the interface.

You define a profile by using the same CLI commands that you use to configure a static IGMP interface; however, the mode in which you use the commands differs. Use the commands in Interface Configuration mode to configure a static IGMP interface and in Profile Configuration mode to define a profile.

When you have defined a profile, you can apply it to an interface or a group of interfaces. Profiles provide an efficient method of creating and managing large numbers of dynamic interfaces. For detailed information about creating and assigning profiles, see *JUNOSe Link Layer Configuration Guide, Chapter 12, Configuring Dynamic Interfaces*. When you create a profile for dynamic IGMP interfaces, specify attributes for configuring all layers in the interface.

You use the following IGMP commands to configure a static IGMP interface. You also use these commands to define the attributes for the IGMP layer when you create a profile for dynamic IGMP interfaces:

Table 6: IGMP Commands

ip igmp	ip igmp query-max-response-time
ip igmp access-group	ip igmp robustness
ip igmp access-source-group	ip igmp ssm-map enable
ip igmp apply-oif-map	ip igmp ssm-map static

Table 6: IGMP Commands (continued)

ip igmp explicit-tracking	**ip igmp query-interval**
ip igmp group limit	**ip igmp static-exclude**
ip igmp immediate-leave	**ip igmp static-group**
ip igmp last-member-query-interval	**ip igmp static-include**
ip igmp promiscuous	**ip igmp version**
ip igmp querier	**multicast group port limit**
ip igmp querier-timeout	

The following sections describe the tasks associated with these and other **ip igmp** commands.

You can also use various IGMP-specific RADIUS attributes in RADIUS Access-Accept messages as an alternative method of configuring certain values. See *JUNOSe Broadband Access Configuration Guide, Chapter 3, Configuring RADIUS Attributes* for additional information.

Enabling IGMP on an Interface

You must start IGMP on each interface that you want to use the protocol. You can configure IGMP and either PIM or DVMRP on the same interface. If you configure only IGMP on an interface, IGMP owns that interface. If you configure IGMP and either PIM or DVMRP on an interface, PIM or DVMRP owns the interface.

By enabling IGMP, the router processes incoming multicast packets and creates an entry in the multicast routing table. If neither PIM nor DVMRP own the interface (for example, when only IGMP is configured), then the packets are locally routed to other interfaces on the router. PIM or DVMRP must be configured on the interface for packets to be sent to other routers.

For networks that use only IGMPv1, you can configure an interface to operate in IGMPv1 mode. However, IGMPv2 and IGMPv3 interfaces support IGMPv1 hosts. In an IGMPv1 network, you must configure one interface to act as a querier. In an IGMPv2 or IGMPv3 network, the querier is the router with the lowest IP address.

To start IGMP, complete the following steps:

1. Enable IGMP on the interface (IGMPv2 is the default version).
2. (IGMPv1 or IGMPv3) Specify the IGMP version for the interface.
3. (IGMPv1 only) Specify that the interface act as the querier for the network.

ip igmp

- Use to enable IGMP on an interface and to set the IGMP version to IGMPv2. Use the **ip igmp version** command to specify a different IGMP version.
- Example

  host1:boston(config-if)#**ip igmp**

- Use the **no** version to disable IGMP on an interface.

ip igmp querier

- Use to specify that this IGMPv1 interface acts as a querier.

NOTE: This command is valid only for interfaces on which you configured IGMPv1.

- By default, IGMPv1 interfaces act as queriers.
- Example

  host1:boston(config-if)#**ip igmp querier**

- Use the **no** version to cause the interface to not act as a querier.

ip igmp version

- Use to set the IGMP version (1, 2, or 3) for the interface or specify a passive interface with only multicast-data-forwarding capability (passive).
- Example

  host1:boston(config-if)#**ip igmp version 1**

- Use the **no** version to set the version to the default, IGMPv2.

Configuring IGMP Settings for an Interface

When you start IGMP on an interface, it operates with the default settings. You can, however, modify:

- The method that the router uses to remove hosts from multicast groups (IGMPv2 and IGMPv3 interfaces only)
- The query time interval for the querier sends group membership messages
- The time that a non-querier waits for queries from the current querier before sending query messages to assume responsibility of querier
- The time that a new querier waits before sending query messages after it assumes responsibility from another querier
- The time that a host can take to reply to a query (maximum response time)
- The number of times that the router sends each IGMP message from this interface

ip igmp immediate-leave

- Use to specify that, when the router receives a leave group membership message from a host associated with this interface, the router immediately removes that host from the multicast group.

CAUTION: Issue this command only on IGMPv2 and IGMPv3 interfaces to which one IGMP host is connected. If more than one IGMP host is connected to a LAN through the same interface, and one host sends a leave group message, the router removes all hosts on the interface from the multicast group. The router loses contact with the hosts that must remain in the multicast group until they send join requests in response to the router's next general group membership query.

- Use the IGMP-Immediate-Leave RADIUS attribute (VSA 26-97) in RADIUS Access-Accept messages as an alternative method of configuring this value. The RADIUS setting takes precedence over a CLI setting.
- Example

  host1:boston(config-if)#**ip igmp immediate-leave**

- Use the **no** version to restore the default behavior, in which the router removes a host from a multicast group if that host does not return a group membership report within a certain length of time after receiving a group membership query from the router.

ip igmp last-member-query-interval

- Use to specify the last-member-query-interval value, in the range 1–255 tenths of a second. When the router receives an IGMPv2 leave message or an IGMPv3 state change report, it sends out a query and expects a response within the time specified by this value.
- Using a lower value enables members to leave groups more quickly.
- Example

  host1:boston(config-if)#**ip igmp last-member-query-interval 90**

- Use the **no** version to restore the default, 10-tenths of a second (1 second).

ip igmp querier-timeout

- Use to set the time, in the range 1–400 seconds, that the interface waits for queries from the current querier before sending query messages to assume responsibility of querier.
- Example

  host1:boston(config-if)#**ip igmp querier-timeout 200**

- Use the **no** version to set the time to the default, twice the query interval.

ip igmp query-interval

- Use to specify how often, in the range 1–300 seconds, the interface sends group membership queries.
- Use the IGMP-Query-Interval RADIUS attribute (VSA 26-95) in RADIUS Access-Accept messages as an alternative method of configuring this value. The RADIUS setting takes precedence over a CLI setting.
- Example

  host1:boston(config-if)#**ip igmp query-interval 100**

- Use the **no** version to set the polling interval to the default, 125 seconds.

ip igmp query-max-response-time

- Use to specify the time in tenths of a second in which the host must respond to a group membership query. The possible period ranges are as follows:
  - IGMPv2: 1–255 tenths of a second
  - IGMPv3: 1–31744 tenths of a second
- IGMPv2 and IGMPv3 include this value in IGMP query messages sent out on the interface.
- You cannot set this value on interfaces running IGMPv1.
- Using a lower value enables members to join and leave groups more quickly.
- Use the IGMP-Max-Resp-Time RADIUS attribute (VSA 26-96) in RADIUS Access-Accept messages as an alternative method of configuring this value. The RADIUS setting takes precedence over a CLI setting.
- Example

  host1:boston(config-if)#**ip igmp query-max-response-time 120**

- Use the **no** version to restore the default, 100 tenths of a second (10 seconds).

ip igmp robustness

- Use to specify the number of times that the router sends each IGMP message from this interface.
- Use a higher value to ensure high reliability from IGMP.
- Specify a number in the range 1–4.
- Example

  host1:boston(config-if)#**ip igmp robustness 2**

- Use the **no** version to restore the default, 3.

Specifying Multicast Groups

You can use a standard-format or extended-format IP access list to specify the multicast groups that a host can join.

ip igmp access-group

- Use to restrict hosts on this subnetwork to join only multicast groups that appear on the specified IP access list.
- When this feature is configured, the access list is queried whenever the router receives an IGMPv2 report requesting membership of a group, and IGMPv3 ChangeToInclude or IsExclude reports. The request is rejected if the access list query fails.
- The **ip igmp access-group** command accepts standard or extended-format access lists. Because the extended format enables you to specify both the source address and the destination group address, the source address must be set to any. For example, **access-list test permit ip host 224.128.64.32 any**.
- Note that in the access list specified when you issue this command, the group is specified before the source.
- Example

  host1:boston(config-if)#**ip igmp access-group boston-list**

- Use the **no** version to dissociate the interface from an access list and to enable hosts on the interface to join any multicast group.

ip igmp access-source-group

- Use to restrict hosts on this subnetwork to membership in those (S,G) pairs (also known as *channels*) included on the specified IP access list.
- When this feature is configured, both source and group addresses query the associated access list whenever the router receives an IGMPv3 report requesting membership of the (S,G) pairs (that is, the router receives an IGMPv3 ChangeToInclude, IsInclude, or AllowNewSource group report). The request is rejected if the access list query fails.
- The **ip igmp access-source-group** command accepts standard or extended-format access lists. The extended format enables you to specify both the source address and the destination group address; for example, **access-list test permit ip host 10.1.1.1 host 224.128.64.32**. Typically, you use the extended-format access list. If you instead use the standard-format access list, you explicitly specify the source address to create the access list, but the group address is implicitly assumed to be **any**,
- Note that in the access list specified when you issue this command, the source is specified before the group.
- Example

  host1:boston(config-if)#**ip igmp access-source-group dallas-list**

- Use the **no** version to remove any access list restriction.

Assigning a Multicast Group to an Interface

You can assign an interface to send and receive all traffic for a particular multicast group. This feature enables you to control the IGMP traffic and to test the behavior of multicast protocols in the network.

ip igmp static-group

- Use to send and receive all traffic for a multicast group from a specific interface.
- The interface sets no timers for this group.
- Example

  host1:boston(config-if)#**ip igmp static-group 225.1.2.3**

- Use the **no** version to stop the interface from sending all traffic for the group.

Configuring Group Outgoing Interface Mapping

You can configure an IGMP interface to use a different outgoing interface (OIF) for multicast-date-forwarding by applying an OIF map. When you configure an OIF map on an IGMP interface, the map is applied to all IGMP membership requests that the interface receives.

To configure OIF mapping on an interface:

1. Create an OIF map using the **ip igmp oif-map** command at the global level.
2. Apply the OIF map to an interface using the **ip igmp apply-oif-map** command.

To properly configure an interface used in the OIF map for multicast-data-forwarding capability, you must configure the interface version as passive with the **ip igmp version** command. You can either specify a passive interface as the OIF or specify the OIF as *self* (to use the IGMP interface as the OIF) in the **ip igmp oif-map** command.

ip igmp apply-oif-map

- Use to apply the specified outgoing interface (OIF) map to the current interface.
- Example

  host1(config-subif)#**ip igmp apply-oif-map OIFMAP**

- Use the **no** version to remove the outgoing interface map association from the interface.

ip igmp oif-map

- Use to create an OIF map.
- Example

  host1(config)#**ip igmp oif-map OIFMAP atm 3/0.1 232.0.0.1/32 51.0.0.1/32**
  host1(config)#**ip igmp oif-map OIFMAP atm 3/0.2 232.0.0.1/32 51.0.0.2/32**
  host1(config)#**ip igmp oif-map OIFMAP atm 3/0.3 233.0.0.1/32**
  host1(config)#**ip igmp oif-map OIFMAP atm 3/0.4 233.0.0.0/24 51.0.0.1/32**
  host1(config)#**ip igmp oif-map OIFMAP atm 3/0.5 233.0.0.0/24 51.0.0.2/32**
  host1(config)#**ip igmp oif-map OIFMAP self 0.0.0.0/0 51.0.0.0/24**

- Use the **no** version to remove an outgoing interface map attribute.

ip igmp version

- Use to set the IGMP version (1, 2, or 3) for the interface or specify a passive interface with only multicast-data-forwarding capability (passive).
- Example

  host1:dallas(config-if)#**ip igmp version passive**

- Use the **no** version to set the version to the default, IGMPv2.

Configuring Access Node Control Protocol for IGMP

By using ANCP, IGMP is no longer terminated or proxied at the access node. Instead, IGMP passes through the access node transparently. B-RAS terminates both the data PVC and IGMP. After possible user permission verification, B-RAS may instruct the access node, by using GSMP, to establish a multicast branch for the subscriber port.

L2C works with a special IGMP session to collect OIF mapping events in a scalable manner. For additional information about configuring L2C for IGMP, see *JUNOSe IP Services Configuration Guide, Chapter 8, Configuring ANCP*.

For additional information about OIF mapping, see *Configuring Group Outgoing Interface Mapping* on page 53.

Configuring SSM Mapping

Source-specific multicast (SSM) mapping enables the router to determine one or more source addresses for group G. The mapping effectively translates IGMPv1 or IGMPv2 membership reports to an IGMPv3 report, enabling the router to continue as if it had initially received an IGMPv3 report. After the router is joined to these groups, it sends out PIM join messages and continues to enable joining from these groups, as long as it continues to receive IGMPv1 and IGMPv2 membership reports and no change occurs to the SSM mapping for the group.

When you statically configure SSM mapping, the router can discover source addresses from a statically configured table.

The following conditions apply when you configure SSM mapping:

- When SSM mapping is enabled, and either you have not configured a static SSM map or the router cannot find any matching access lists, the router continues to accept (*,G) groups. The PIM SSM range must deny any unacceptable SSM group addresses.
- When you issue the **no ip igmp ssm-map enable** command, the router removes all SSM map (S,G) states and establishes a (*,G) state.
- You can enter multiple **ssm-map static** commands for different access lists. Also, you can enter multiple **ssm-map static** commands for the same access list, as long as the access list uses different source addresses.
- SSM maps do not process statically configured groups.

ip igmp ssm-map enable

- Use to enable SSM mapping on the router. SSM mapping statically assigns sources to IGMPv1 and IGMPv2 groups. You must use SSM mapping for IGMPv1 and IGMPv2 hosts to interoperate with PIM SSM. SSM mapping enables the router to use a statically configured list to translate (*,G) memberships to (S,G) memberships.
- Example

  host1:boston(config)#**ip igmp ssm-map enable**

- Use the **no** version to disable SSM mapping on the router.

ip igmp ssm-map static

- Use to specify an access list and source address for use in SSM mapping. SSM mapping statically assigns sources to IGMPv1 and IGMPv2 groups. You must use SSM mapping for IGMPv1 and IGMPv2 hosts to interoperate with PIM SSM. SSM mapping enables the router to use a statically configured list to translate (*,G) memberships to (S,G) memberships.
- Example

  host1:boston(config)#**ip igmp ssm-map static boston-list 51.0.0.1**

- Use the **no** version to remove the SSM map association.

Limiting the Number of Accepted IGMP Groups

By default, there is no limit on the number of IGMP groups that an IGMP interface can accept. However, you can manage multicast traffic on the router by restricting the number of IGMP groups accepted by:

- A specific port on an I/O module
- A specific IGMP interface

If you set limits for both a port and interfaces on that port, the router uses the lower of the two limits when determining how many IGMP groups an interface can accept. For example, if you set a limit of 10 groups for the port and 15 groups for each interface, only 10 groups can be accepted among the interfaces.

However, if you set a limit for a port and that limit is lower than the number of groups currently accepted by the interfaces on that port, the router does not dissociate the groups from the interfaces. The router enforces the new limit on the port when the number of groups associated with the interfaces falls to that limit. For example, if the interfaces on the port have accepted a total of 15 groups, and you set a limit of 10 groups on the port, the router does not disconnect any of the groups and prevents the interfaces from accepting any more groups. Over time, some groups leave the interfaces and, eventually, a maximum of ten groups remain connected.

ip igmp group limit

- Use to limit the number of IGMP groups that an interface can accept.

NOTE: This command is deprecated and might be removed completely in a future release. The function provided by this command has been replaced by the updated by limiting bandwidth of multicast streams using the **ip multicast admission-bandwidth-limit** command.

- Example

  host1:boston(config-if)#**ip igmp group limit 5**

- Use the **no** version to restore the default behavior, in which there is no limit on the number of IGMP groups that an interface can accept.

multicast group port limit

- Use to limit the number of IGMP groups that a port can accept.

NOTE: This command is deprecated and might be removed completely in a future release. The function provided by this command has been replaced by the updated by limiting bandwidth of multicast streams using the **mroute port admission-bandwidth-limit** command.

- Specify the identifier for the port in *slot/port* format (ERX routers) or in *slot/adapter/port* format (E320 router).
  - *slot*—Number of the chassis slot in the range 0–6 (ERX-7xx models), 0–13 (ERX-14xx models), or 0–16 (E320)
  - *adapter*—Adapter number on the E320 IOA module
  - *port*—Port number on the I/O or IOA module
- Specify the maximum number of IGMP groups that interfaces can accept.
- Example 1—ERX models

  host1(config)#**multicast group port 3/0 limit 5**

- Example 2—E320 router

  host1(config)#**multicast group port 3/1/0 limit 5**

- Use the **no** version to restore the default behavior, in which there is no limit on the number of IGMP groups that a port can accept.

Including and Excluding Traffic

IGMPv3 extends IGMPv2 functionality with the ability to include or exclude specific multicast traffic sources. That is, with IGMPv3, hosts signal (S,G) pairs to be included or excluded.

For hosts that cannot signal group membership dynamically, you can use the **ip igmp static-include** or **ip igmp static-exclude** command to statically include or exclude multicast traffic, respectively.

IGMPv3 is the industry-designated standard protocol for hosts to signal channel subscriptions in SSM. For additional information about SSM, see *PIM Source-Specific Multicast* on page 83.

ip igmp static-exclude

- Use to statically exclude the IGMP (S,G) membership for a host that is not capable of dynamically signaling group membership.
- Example

  host1:boston(config-if)#**ip igmp static-exclude 10.1.1.5 225.1.2.3**

- Use the **no** version to remove the static designation.

ip igmp static-include

- Use to statically include the IGMP (S,G) membership for a host that is not capable of dynamically signaling group membership.
- Example

  host1:boston(config-if)#**ip igmp static-include 10.1.1.1 225.1.2.3**

- Use the **no** version to remove the static designation.

Configuring Explicit Host Tracking

Explicit host tracking enables the router to explicitly track each individual host that is joined to a group or channel on a particular multi-access network.

Explicit host tracking provides the following:

- Minimal leave latency when a host leaves a multicast group or channel. When the router receives a leave message for a group or channel on an interface, it accesses a list of hosts and immediately stops forwarding traffic if the sender is the last host to request traffic for that group or channel. The leave latency is bound only by the packet transmission latencies in the multi-access network and the processing time in the router.
- Ability to change channels quickly in networks where bandwidth is constrained between a multicast-enabled router and hosts.
- Ability to determine what multicast hosts are joined to particular multicast groups or channels, which is useful for accounting purposes.
- Reduction of control message traffic on the network because, when it receives a leave message, the router no longer needs to send out IGMP queries to verify membership. As a result, interested hosts also do not need to respond to these queries with reports.
- Tracking based on the IGMP reports for hosts in both include and exclude modes for every multicast group or channel on an interface.

When the router is configured for explicit host tracking and starts immediate leave using the host information collected, every leave message received for a group or channel is treated as follows:

- The router checks the number of hosts that receive traffic from the group or channel.
- If the host sending the leave message is the only host, it starts immediate leave for that group or channel on that interface. The router removes the interface from the multicast group or channel immediately, without sending out a group or group-source-specific query and waiting for the last member query interval.
- If the host sending the leave message is not the only host receiving traffic for that group or channel, the router removes the host from the list of hosts on that interface, but keeps the interface in the outgoing interface list for the multicast group or channel. No group or group-source-specific queries are sent.

If one or more hosts that support only IGMP V1 are present on a network, the leave latencies for the multicast groups to which those hosts are joined revert to the IGMP V1 leave latency. This affects only the multicast groups to which these legacy hosts are actually joined at any point in time.

You cannot configure explicit host tracking on passive IGMP interfaces or on IGMP V1 interfaces. When you enable IGMP V2 or V3 on an interface, explicit host tracking is not enabled by default.

When you enable explicit host tracking on an interface that has a membership state, the router does not immediately start performing immediate leave. For a maximum of group membership interval seconds, the router only performs host tracking. Any leave messages that the router receives during this period receive normal leave processing. Any leave messages received after this interval has elapsed receive immediate leave processing, when appropriate.

When explicit host tracking has been enabled on an IGMP V3 interface, even if a group has to downgrade to IGMP V2 due to the presence of an IGMP V2 host, explicit host tracking continues for that group. To avoid this, you can use the **disable-if-igmp-v2-detected** keyword. If you select this option, the router turns off explicit host tracking for the group when IGMP V2 host reports are received for the group on that interface. This option does not have any significance on an interface configured for IGMP V2 and is ignored if provided. Because IGMP V1 does not support leave messages, explicit host tracking is turned off for a group that downgrades to IGMP V1 due to the presence of IGMP V1 hosts.

Explicit host tracking cannot be enabled on an interface that has immediate-leave configured and vice versa. Any attempt to configure immediate-leave on an interface that has explicit host tracking enabled or to configure explicit host tracking on an interface that has immediate-leave enabled is rejected and an error message logged on the screen.

The following example enables IGMP V3 explicit host tracking on interface 3/0.101 with the default configuration where the router continues to perform explicit host tracking for IGMP V2 groups. To override this default configuration, you must use the **ip igmp explicit-tracking disable-if-igmp-v2-detected** command.

```
interface 3/0.101
ip igmp version 3
ip igmp explicit-tracking
end
```

ip igmp explicit-tracking

- Use to set explicit host tracking for IP IGMP interfaces.
- To disable explicit host tracking if IGMP V2 hosts are detected, use the **disable-if-igmp-v2-detected** keyword.
- Example

  host1(config)#**ip igmp explicit-tracking**

- Use the **no** version to disable explicit host tracking on the interface. Use the **no** version with the **disable-if-igmp-v2-detected** keyword to revert to the default explicit host tracking behavior.

Accepting IGMP Reports from Remote Subnetworks

By default, IGMP interfaces accept IGMP reports only from associated subnetworks. You can configure the router to accept IGMP reports from subnetworks that are not associated with its interfaces. The **igmp promiscuous** command in Router Configuration mode specifies whether interfaces on the router can accept IGMP reports from indirectly connected subnets. To override this global setting on a particular interface, use the **ip igmp promiscuous** command in Interface Configuration mode.

Example In the following example, the router is configured to accept IGMP reports from indirectly connected subnets on all interfaces. The interface on port 0 of the line module in slot 4 is then configured to accept IGMP reports only from directly connected subnets.

```
host1(config)#virtual-router boston
host1:boston(config)#router igmp
host1:boston(config-router)#igmp promiscuous
host1:boston(config-router)#exit
host1:boston(config)#interface serial 4/0
host1:boston(config-if)#ip igmp promiscuous off
```

igmp promiscuous

- Use to enable all IGMP interfaces on the router to accept IGMP reports from hosts on any subnetwork.
- Example

  ```
  host1:boston(config-router)#igmp promiscuous
  ```

- Use the **no** version to enable IGMP interfaces on the router to accept IGMP reports only from hosts on their associated subnetworks.

ip igmp promiscuous

- Use to specify whether the interface accepts IGMP reports from hosts on any subnetwork.
  - Use the **on** keyword to enable the interface to accept IGMP reports from hosts on any subnetwork.
  - Use the **off** keyword to enable the interface to accept IGMP reports only from hosts on subnetworks associated with this interface.
- Example

  ```
  host1:boston(config-if)#ip igmp promiscuous on
  ```

- Use the **no** version to configure an IGMP interface to use the Router Configuration mode setting to determine the subnetworks from which it can accept IGMP reports.

Disabling and Removing IGMP

You can disable and reenable IGMP on the VR. You can also remove IGMP from the VR and recreate it on the VR.

igmp disable

- Use to disable IGMP on a VR.
- Example

  host1(config)#**virtual-router boston**
  host1:boston(config)#**router igmp**
  host1:boston(config-router)#**igmp disable**

- Use the **no** version to enable IGMP on a VR.

router igmp

- Use to create and enable IGMP on a VR or to access IGMP Router Configuration mode.
- Example

  host1(config)#**virtual-router boston**
  host1:boston(config)#**router igmp**

- Use the **no** version to remove IGMP and the IGMP proxy from the VR.

Monitoring IGMP

You can establish a reference point for IGMP statistics by setting the statistics counters to zero.

To display IGMP parameters, use the **show** commands described in this section.

NOTE: The E120 router and E320 router output for **monitor** and **show** commands is identical to output from other E-series routers, except that the E120 and E320 router output also includes information about the adapter identifier in the interface specifier (*slot/adapter/port*).

baseline ip igmp

- Use to set the counters for IGMP statistics to zero, to establish a baseline.
- Example

  (host1)#**baseline ip igmp**

- There is no **no** version.

show ip igmp

- Use to display IGMP information for a VR.
- Field descriptions
  - Routing Process—Routing process for this VR (IGMP)
  - Administrative state—Status of IGMP in the software: enabled or disabled
  - Operational state—Status of IGMP on the VR: enabled or disabled
  - Total interfaces—Number of interfaces on which you started IGMP
  - enabled—Number of interfaces on which IGMP is enabled
  - disabled—Number of interfaces on which IGMP is disabled
  - learnt groups—Number of multicast groups that the VR has discovered
  - IGMP graceful restart duration—Restart interval in seconds
  - IGMP Statistics Rcvd—Statistics for IGMP messages received
    - total—Total number of IGMP messages received
    - checksum errors—Number of IGMP messages received with checksum errors
    - unknown types—Number of IGMP messages received that are not group membership queries, group membership reports, or leave group membership messages
    - queries—Number of group membership queries
    - reports—Number of group membership reports
    - leaves—Number of leave group membership messages
  - IGMP Statistics Sent—Statistics for IGMP messages sent
    - Total number of group membership queries sent
- Example

```
host1:boston#show ip igmp
Routing Process IGMP, Administrative state enabled, Operational state
enabled
    2 total interfaces, 2 enabled, 0 disabled
    0 enabled interfaces performing graceful restart
    2 learnt groups
IGMP Statistics:
    Rvcd: 1 total, 0 checksum errors, 0 unknown types
          0 queries, 1 reports, 0 leaves
    Sent: 11 total
```

show ip igmp groups

- Use to display statically joined and directly connected groups learned through IGMP.
- Field descriptions
  - Grp Address—Address of the multicast group
  - Interface—Interface that discovered the multicast group
  - oif-map—Name of the OIF map and the mapped OIF interface, when a group or source has been mapped to an OIF

- State—IGMP version on the interface
- ExpTim—Time, in seconds, at which the router stops polling for more members of this group
- oldHTo—Time at which the router stops polling for more IGMPv1 members of a group. If this value is 0, the interface has received no IGMPv1 reports for the group.
- Included Sources—Sources included in the multicast group
- Excluded Sources—Sources excluded from the multicast group
- Counts—Number of source-group mappings by version and state

- Example 1—Without OIF mapping

```
host1:boston#show ip igmp groups
Grp Address     Interface       State       Reporter        ExpTim oldHTo
--------------- --------------- ----------- --------------- ------ ------
228.1.1.1       FastEthernet1/1 Version3    17.0.0.2            44      0
228.1.1.2       FastEthernet1/1 Version3    17.0.0.2            50      0
228.1.1.3       FastEthernet1/1 Version3    17.0.0.2            48      0
230.1.1.1       FastEthernet1/1 Version3    17.0.0.2            44      0
  Included Sources:
    51.0.0.1                                                    44
    51.0.0.2                                                    44
    51.0.0.3                                                    44
231.1.1.1       FastEthernet1/1 Version3    17.0.0.2            44      0
  Excluded Sources:
    51.0.0.1                                                     0
    51.0.0.2                                                     0
    51.0.0.3                                                     0

Counts: 5 version-3, 0 version-2, 0 version-1, 0 check state, 0 disabled
       (5 total)
        0 excluded
        Source-groups: 3 included, 3 excluded
```

- Example 2—With OIF mapping

```
host1:boston#show ip igmp groups
Grp Address     Interface       State       Reporter        ExpTim oldHTo
--------------- --------------- ----------- --------------- ------ ------
232.1.1.1       ATM5/0.12       Version3    1.1.1.2            371      0
                    oif-map OIFMAP ATM5/0.121
232.1.1.1       ATM5/0.13       Version3    1.1.1.3            375      0
                    oif-map OIFMAP ATM5/0.121
232.1.1.2       ATM5/0.12       Version3    1.1.1.2            373      0
  Included Sources:
    10.1.1.2        oif-map OIFMAP self                        373
    10.1.1.10       oif-map OIFMAP ATM5/0.120                  373
    10.1.1.11       oif-map OIFMAP ATM5/0.121                  373
232.1.1.2       ATM5/0.13       Version3    1.1.1.3            375      0
  Included Sources:
    10.1.1.2        oif-map OIFMAP self                        375
    10.1.1.10       oif-map OIFMAP ATM5/0.120                  375
    10.1.1.11       oif-map OIFMAP ATM5/0.121                  375

Counts: 4 version-3, 0 version-2, 0 version-1, 0 check state, 0 disabled
       (4 total)
        0 excluded
        Source-groups: 6 included, 0 excluded
```

show ip igmp interface

- Use to display IGMP information for interfaces on which you enabled IGMP.
- Specify the **brief** keyword to see a summary of the information.
- Specify the **count** keyword to see the number of IGMP interfaces.
- Specify the **group** address keyword to see information for interfaces that belong to that group.
- Field descriptions
  - Interface—Type of interface and interface specifier. For details about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.
  - address—IP address of the interface
  - Administrative state—Status of the interface in the software: enabled or disabled
  - Operational state—Physical status of the interface: enabled or disabled
  - Version—IGMP version
  - State—Function of the interface: querier or nonquerier
  - Query Interval—Time interval in seconds at which this interface sends query messages
  - Other querier present interval—Time in seconds that the interface waits before declaring itself as the querier
  - Maximum response time—Time interval, in tenths of a second, during which this interface waits for a host to respond
  - Last member query interval—Time, in tenths of a second, that this interface waits before sending a new query to a host that sends a group leave message
  - Robustness—Number of times this interface sends IGMP messages
  - Information about whether the interface accepts IGMP reports from hosts on any subnetwork
    - Interface defaults to global promiscuous mode—Interface uses the setting of the **igmp promiscuous** command to determine whether it accepts IGMP reports from hosts on any subnetwork
  - Information about standard IP access lists configured with the **ip igmp access-group** command
    - Inbound access group—Access list specified
    - No inbound access group—No access list specified
  - Information about IP access lists configured with the **ip igmp access-source-group** command
    - Inbound access source-group—Access list specified
    - No inbound access source-group—No access list specified

- Information about OIF maps configured with the **ip igmp apply-oif-map** command
  - Inbound apply-oif-map—Map name specified
  - No inbound apply-oif-map—No map name specified
- Immediate Leave—Setting of the **ip igmp immediate-leave** command: enabled or disabled
- Explicit Host Tracking—Setting of the **ip igmp explicit-tracking** command: enabled or disabled
- Max-Group limit—Number of IGMP groups that the interface can accept, as configured with the **ip igmp group limit** command
- Admission-Bandwidth limit—Value of the admission-bandwidth limit set for an interface that accepts IGMP groups, or No Limit
- Group Count—Number of IGMP groups that the interface has accepted
- IOA packet replication—Hardware multicast packet replication interface to which egress multicast packets on this interface are redirected
- Interface statistics Rcvd—Information about IGMP messages received on this interface
  - reports—Number of group membership reports received
  - leaves—Number of group leave messages received
  - wrong version queries—Number of group membership queries received from devices running a different version of IGMP
- Interface statistics Sent—Number of IGMP messages this interface has sent
- Interface statistics Groups learned—Number of groups this interface has discovered
- Counts—Breakdown of IGMP interfaces
  - down—Number of interfaces down
  - init state—Number of interfaces in the initialization state
  - querier—Number of querier interfaces
  - non-querier—Number of non-querier interfaces
  - Total—Total number of IGMP interfaces

- Example 1

```
host1:boston#show ip igmp interface
Interface ATM2/1.15 address 15.0.0.2/255.255.255.0
Administrative state enabled, Operational state enabled
Interface parameters:
    Version 2
    State Querier
    Query Interval 125 secs, 53 secs before the next query
    Other querier present interval 250 secs
    Maximum response time 100 (in 10ths of a second)
    Last member query interval 10 (in 10ths of a second)
    Robustness 3
    Interface defaults to global promiscuous mode
    No inbound access group
    No inbound access source-group
    No inbound apply-oif-map
```

```
    Immediate Leave: disabled
    Explicit Host Tracking: enabled
    Max-Group limit: No Limit
    Admission-Bandwidth limit: No Limit
    Group Count: 1
Interface statistics:
    Rcvd: 0 reports, 0 leaves, 0 wrong version queries
    Sent: 1 queries
    Groups learned: 1

Counts: 0 down, 0 init state, 1 querier, 0 non-querier, 1 Total
Counts: 0 down, 0 init state, 1 querier, 0 non-querier, 1 Total
```

- Example 2

```
host1#show ip igmp interface gigabitEthernet 3/0.0
Interface GigabitEthernet3/0.0 address 10.1.1.1/255.255.255.0
Administrative state enabled, Operational state disabled
Interface parameters:
    Version 2
    State Down
    Query Interval 125 secs
    Other querier present interval 250 secs
    Maximum response time 100 (in 10ths of a second)
    Last member query interval 10 (in 10ths of a second)
    Robustness 3
    Interface defaults to global promiscuous mode
    No inbound access group
    No inbound access source-group
    No inbound apply-oif-map
    Immediate Leave: disabled
    Explicit Host Tracking: enabled
    Max-Group limit: No Limit
    Admission-Bandwidth limit: No Limit
    Group Count: 0
    IOA packet replication gigabitEthernet 3/8.1
Interface statistics:
    Rcvd: 0 reports, 0 leaves, 0 wrong version queries
    Sent: 0 queries
    Groups learned: 0
```

show ip igmp interface brief

- Use to display a summary of IGMP information for interfaces on which you enabled IGMP.
- Field descriptions
  - Interface—Type of interface and interface specifier. For details about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.
  - Intf Address—IP address of the interface
  - Ver—IGMP version
  - State—Function of the interface: querier or nonquerier
  - Querier—IP address of the querier on the network to which this interface connects

- QTime—Time interval, in seconds, at which this interface sends query messages
- QPTime—Time in seconds that the interface waits before declaring itself as the querier
- Count—Total number of IGMP interfaces

- Example

```
host1:boston#show ip igmp interface brief
Interface        Intf Address      Ver  State    Querier         QTime  QPTime
--------------   ----------        ---  ------   -------------   -----  ---
fastEthernet0/0  192.168.1.250/24  2    Querier  192.168.1.250   28     0
atm3/0.2         21.1.1.1/8        2    Querier  21.1.1.1        26     0
Count: 2 interfaces
```

show ip igmp mapped-oif

- Use to display the current mappings to all mapped outgoing interfaces or to the specified mapped outgoing interface.
- Field descriptions
  - OIF—Outgoing interface used in an OIF map
  - Oper—Operation status of the outgoing interface
  - Group Address—Multicast group IP address associated with the OIF
  - Source Address—Source IP address associated with the OIF
  - Join I/F—IGMP interface associated with the OIF
  - Map Name—Name of the map associated to the OIF
  - Counts—Number of source-group mappings to OIFs
- Example

```
host1#show ip igmp mapped-oif
      OIF       Oper  Group Address  Source Address     Join I/F      Map Name
--------------- ---- --------------- --------------- --------------- ----------
ATM5/0.120      Up   232.1.1.2       10.1.1.10       ATM5/0.12       OIFMAP
                                                     ATM5/0.13       OIFMAP
ATM5/0.121      Up   232.1.1.1       *               ATM5/0.12       OIFMAP
                                                     ATM5/0.13       OIFMAP
                     232.1.1.2       10.1.1.11       ATM5/0.12       OIFMAP
                                                     ATM5/0.13       OIFMAP

Counts: 3 source-group mappings
```

show ip igmp membership

- Use to display IGMP membership information for multicast groups and (S, G) channels.
- Specify the **tracked** keyword to see interface information only for interfaces where explicit host tracking is enabled.

- Field descriptions
  - Group—Multicast group or (S, G) channel
  - Source—(S, G) entries that are forwarding traffic
  - Reporter—Hosts that requested including sources or have not requested excluding sources. If listed under a group, host that sent exclude reports for the group. If listed under a source, host that requested traffic from this source for the group. For any (S, G), if listed under a source, indicates hosts interested in the traffic for this (S, G).
  - ExpTim—Expiration time.
  - Flags
    - M—Uses Oifmap
    - S—SSM mapped
    - T—Tracked
    - 1, 2, 3—IGMP version that the group is in
  - Interface—Type of interface and interface specifier. For details about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.
- Example

```
host1#show ip igmp membership
Flags: M - Uses Oifmap  S- SSM mapped  T - tracked
       1,2,3 - The version of IGMP the group is in
Reporter:
    <ip-address> - last reporter if the group is not explicitly tracked
    <n>/<m> - <n> reporters include mode, <m> reporters in exclude

Group           Source            Reporter         ExpTim    Flags     Interface
--------------  ---------------   -------------    ------    ------    ---------------
224.0.1.40          *             10.10.1.1        02:41     2S        FastEthernet2/1
224.0.1.50                        1/2              02:56     3MT       FastEthernet2/2
                                  11.10.0.21       02:56
                                  11.10.2.22       02:30
                  20.30.0.11
                                  11.10.0.23       02:48
                  20.30.0.12
                                  11.10.0.21       02:56
                  20.30.0.13
                                  11.10.0.21       02:56
                                  11.10.0.22       02:30
                                  11.10.0.23       02:48
224.0.1.60                        20.20.0.1        01:56     3         FastEthernet2/3
                  10.30.0.100                      02:45
                  10.30.0.101                      02:35
                  10.30.0.102                      02:15
                  10.30.0.104                      stop
224.0.1.70                        30.20.0.1        stop      3         FastEthernet2/4
                  40.30.0.100                      01:10
                  40.30.0.101                      01.24
239.0.1.80                        2/0              stop      3T        FastEthernet2/5
                  50.30.0.100
                                  10.10.0.10       02:48
```

```
                50.30.0.101
                                    10.10.0.20       02:56
                                    10.10.0.10       02:48
                50.30.0.102         10.10.0.20       02:56
235.0.1.90                          0/3              02:56     2T       FastEthernet2/6
                     *
                                    12.10.0.10       02:48
                                    12.10.0.20       02:56
                                    12.10.0.30       02:48
```

show ip igmp oif-map

- Use to display all outgoing interface (OIF) maps or the OIF map for the specified map name.
- Field descriptions
  - Map Name—Name of the map associated to the show output
  - Group Prefix—Multicast group IP prefix
  - Source Prefix—Source IP prefix
  - OIF—Outgoing interface associated with the group and source prefix
- Example

```
host1#show ip igmp oif-map

     Map Name         Group Prefix      Source Prefix           OIF
------------------ ------------------ ------------------ ------------------
OIFMAP             232.1.1.0/24       0.0.0.0/0          ATM5/0.121
                   232.1.1.0/24       10.1.1.2/32        self
                   232.1.1.0/24       10.1.1.10/32       ATM5/0.120
                   232.1.1.3/32       0.0.0.0/0          ATM5/0.130
                   232.1.1.4/32       0.0.0.0/0          ATM5/0.130
```

show ip igmp oif-mapping

- Use to display the mapped OIF that is assigned to a given map-name, group address, and source address.
- Field descriptions
  - OIF-MAP Name—Name of the map requested
  - Group Address—Multicast group IP address requested
  - Source Address—Source IP address requested
  - Mapped OIF—Interface associated with the OIF map
- Example

```
host1#show ip igmp oif-mapping OIFMAP 232.1.1.1 10.1.1.10

    OIF Mapping
    OIF-MAP Name   : OIFMAP
    Group Address  : 232.1.1.1
    Source Address : 10.1.1.10
    Mapped OIF     : ATM5/0.120
```

show ip igmp ssm-mapping

- Use to display the SSM mapping state and the source list mapping associated with a multicast group address.
- Field descriptions
  - SSM Mapping—Status of SSM mapping on the interface: Enabled or Disabled
  - Group Address—Multicast group address requested
  - Source List—List of sources mapped to the multicast group address
- Example

```
host1:boston#show ip igmp ssm-mapping 232.1.1.1

    SSM Mapping   : Enabled
    Group Address : 232.1.1.1
    Source List   : 172.1.1.1
                  : 172.1.1.2
```

show multicast group limit

- Use to display the number of IGMP groups that ports have accepted and, if configured, the maximum number of groups that ports can accept.
- A value of –1 indicates that no port group limit is configured.
- Only ports that have accepted IGMP groups and ports for which you have configured a limit for the number of IGMP groups appear in this display.
- Field descriptions
  - Port—Identifier of the port in *slot*/*port* format
    - *slot*—Number of the chassis slot in the range 0–6 (ERX-7xx models) and 0–13 (ERX-14xx models)
    - *port*—Port number on the I/O module
  - limit—Maximum number of IGMP groups that the port can accept. A value of –1 indicates that no limit has been specified.
  - count—Actual number of IGMP groups that the port has accepted
- Example

```
host1:boston#show multicast group limit
Port      limit count
--------- ----- -----
2/0           5     0
2/1          -1     1
```

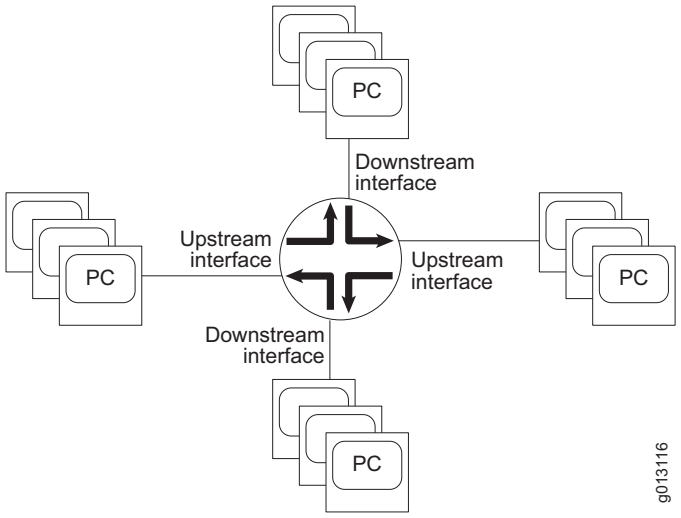
IGMP Proxy Overview

IGMP proxy enables the router to issue IGMP host messages on behalf of hosts that the router discovered through standard IGMP interfaces. The router acts as a *proxy* for its hosts. E-series routers support IGMP proxy versions 2 and 3.

Figure 6 shows a router in an IGMP proxy configuration. You enable IGMP proxy on one interface, which connects to a router closer to the root of the tree. This interface is the *upstream interface*. The router on the upstream interface is running IGMP.

You enable IGMP on the interfaces that connect the router to its hosts that are farther away from the root of the tree. These interfaces are known as *downstream interfaces*.

Figure 6: Upstream and Downstream Interfaces



As described in *IGMP Overview*, earlier in this chapter, hosts interact with the router through the exchange of IGMP messages. Similarly, when you configure IGMP proxy, the router interacts with the router on its upstream interface through the exchange of IGMP messages. However, when acting as the proxy, the router performs the host portion of the IGMP task on the upstream interface, as follows:

- When queried, sends group membership reports to the group.
- When one of its hosts joins a multicast address group to which none of its other hosts belong, sends unsolicited group membership reports to that group.
- When the last of its hosts in a particular multicast group leaves the group, sends an unsolicited leave group membership report to the all-routers group (244.0.0.2).

Configuring IGMP Proxy

To configure a downstream interface, enable IGMP on that interface. To configure IGMP proxy on the router, complete the following tasks:

1. Enable IP multicast.

   host1(config)#**ip multicast-routing**

2. Identify the interface that you want to act as the upstream interface.

3. Enable IGMP proxy on that interface.

   host1(config-if)#**ip igmp-proxy**

4. (Optional) Specify how often the router sends unsolicited reports to routers on the upstream interface.

   host1(config-if)#**ip igmp-proxy unsolicited-report-interval 600**

5. (Optional) Specify how long the router calculates an IGMPv1 querier router to exists on the subnetwork after the router receives an IGMPv1 query on this interface.

   host1(config-if)#**ip igmp-proxy V1-router-present-time 600**

ip igmp-proxy

- Use to enable IGMP proxy on an interface.
- The interface for which you enable IGMP proxy is the upstream interface.

NOTE: You can enable only one upstream interface.

- You can specify either IGMP proxy version 2 or 3. The default is version 2.
- Example

  host1(config)#**ip multicast-routing**
  host1(config-if)#**ip igmp-proxy**

- Use the **no** version to disable IGMP proxy on an interface.

ip igmp-proxy unsolicited-report-interval

- Use to specify the interval, in tenths of a second, at which the upstream interface transmits unsolicited reports.

NOTE: Issue this command only on the upstream interface. Otherwise, this command has no effect.

- Example

  host1(config-if)#**ip igmp-proxy unsolicited-report-interval 600**

- Use the **no** version to transmit unsolicited reports using the default value, 400 tenths of a second.

ip igmp-proxy V1-router-present-time

- Use to specify how long, in seconds, the router calculates an IGMPv1 querier router to exist on the subnetwork after the router receives an IGMP V1 query on this interface.

NOTE: Issue this command only on the upstream interface. Otherwise, this command has no effect.

- Example

  host1(config-if)#**ip igmp-proxy V1-router-present-time 600**

- Use the **no** version to set the time to the default value, 10 seconds.

Establishing the IGMP Proxy Baseline

You can set the counters for the number of queries received and reports sent on the upstream interface to zero. This feature enables you to establish a reference point, or baseline, for IGMP proxy statistics.

baseline ip igmp-proxy interface

- Use to set the counters for the number of queries received and reports sent on the upstream interface to zero.

NOTE: Issue this command only on the upstream interface. Otherwise, this command has no effect.

- Example

  (host1)#**baseline ip igmp-proxy interface**

- There is no **no** version.

Monitoring IGMP Proxy

To display IGMP proxy parameters, use the following **show** commands.

show ip igmp-proxy

- Use to display IGMP proxy parameters for a VR.
- Field descriptions
  - Routing Process—IGMP proxy protocol
  - Administrative state—State of IGMP proxy in the software: enabled or disabled

- Operational state—Operational state of IGMP proxy: enabled or disabled
- total interface—Number of IGMP proxy interfaces on the VR; currently only one upstream interface per VR
- state—Operational state of the IGMP proxy interfaces: enabled or disabled
- multicast group—Number of multicast groups associated with IGMP proxy interfaces

- Example

```
host1#show ip igmp-proxy
Routing Process IGMP Proxy, Administrative state enabled, Operational state
enabled
total 1 upstream interface, state enabled
    6 multicast group
```

show ip igmp-proxy groups

- Use to display information about multicast groups that IGMP proxy reported.
- Field descriptions
  - Grp Address—Address of the multicast group
  - Interface—Type and specifier of the upstream interface associated with the multicast group
  - Member State—State of the associated group address and interface
    - Idle—Interface is going to send a group membership report to respond to a group membership query for this group
    - Delay—Interface has responded to the latest group membership query for this group
  - count—Total number of multicast groups associated with this interface
- Example 1

```
host1#show ip igmp-proxy groups

Grp Address     Interface       Member State
--------------- --------------- --------------
225.1.1.1       atm3/0.2          Idle
225.1.1.2       atm3/0.2          Idle
225.1.1.3       atm3/0.2          Idle
225.1.1.4       atm3/0.2          Idle
225.1.1.5       atm3/0.2          Idle
225.1.1.6       atm3/0.2          Idle
count 6
```

- Example 2

```
host1#show ip igmp-proxy group 225.1.1.1
Grp Address     Interface       Member State
--------------- --------------- --------------
225.1.1.1       atm3/0.2        Idle
```

- Example 3

```
host1#show ip igmp-proxy group count
Count: 6 groups
```

show ip igmp-proxy interface

- Use to display information about the interface on which you configured IGMP proxy.
- To view information about a particular interface, enter an interface type and specifier, such as atm 3/0. For details about interface types and specifiers, see *JUNOSe Command Reference Guide, About This Guide*.
- Specify the **brief** keyword to display a summary rather than a detailed description.
- Field descriptions
  - Interface—Type of upstream interface. For details about interface types, see *JUNOSe Command Reference Guide, About This Guide*.
  - address—Address of upstream interface
  - Administrative state—State of upstream interface in the software: enabled or disabled
  - Operational state—Physical state of upstream interface: enabled or disabled
  - Version—IGMP version on this interface
  - State—Presence of IGMPv1 routers on the same subnet as this upstream interface
  - Unsolicited report interval—Time interval, in tenths of a second, at which this upstream interface sends an unsolicited group membership report
  - Version 1 router present timeout—How long, in seconds, that the upstream interface calculates an IGMPv1 router to exist on the subnet after that interface receives an IGMPv1 group membership query
  - multicast group—Number of multicast groups associated with this upstream interface
  - Interface statistics Rcvd—Statistics for messages received on this interface
    - v1 queries—Number of IGMPv1 group membership queries received
    - v2 queries—Number of IGMPv2 group membership queries received
    - v1 reports—Number of IGMPv1 group membership reports received
    - v2 reports—Number of IGMPv2 group membership reports received
  - Interface statistics Sent—Statistics for messages sent from this interface
    - v1 reports—Number of IGMPv1 leave group reports sent
    - v2 reports—Number of IGMPv2 leave group reports sent
    - leaves—Number of leave group membership messages sent
- Example

```
host1#show ip igmp-proxy interface atm 3/0.2
Interface atm3/0.2 address 21.1.1.1/255.0.0.0
Administrative state enabled, Operational state enabled
Interface parameters:
    Version 2
    State No v1 Router Present
    Unsolicited report interval 10 secs
    Version 1 router present timeout 400 secs
```

```
    0 multicast group
Interface statistics:
    Rcvd:  0 v1 query, 6 v2 queries
           0 v1 report, 0 v2 report
    Sent:  0 v1 report, 48 v2 reports, 0 leave
```