Contents

1 Configuring IGMP

1.1 Introduction

1.1.1 Overview

Multicast devices in a multicast network must maintain members in a multicast group that are connected to the same network segment with the multicast devices. Hosts need to be added to the multicast group dynamically so that a multicast packet can be correctly transmitted to the hosts that need the packet. With the development of multicast applications and ever growing of the multicast network, a protocol is needed to manage the members in the multicast group.

The Internet Group Management Protocol (IGMP) is a TCP/IP protocol that manages members in an IPv4 multicast group and runs on the multicast devices and hosts residing on the stub of the multicast network, creating and maintaining membership of the multicast group between the hosts and connected multicast devices. At present, IGMP is available in three versions: IGMPv1, IGMPv2, and IGMPv3. The three versions support the Any-Source Multicast (ASM) and Source-Specific Multicast (SSM) models as follows:

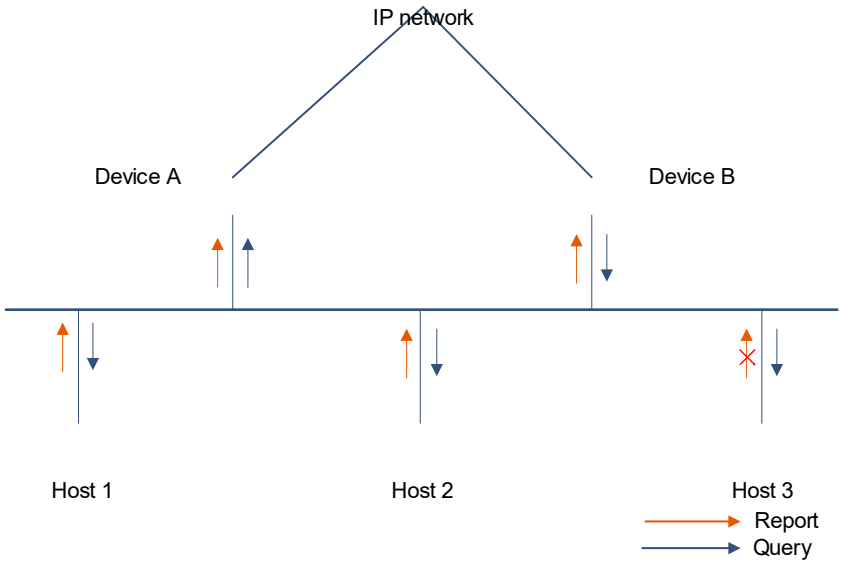
- The three versions of IGMP support the ASM model.
- IGMPv3 can be directly applied to the SSM model.
- IGMPv1 and IGMPv2 can be applied to the SSM model only when the IGMP SSM mapping technology is configured.

1.1.2 Basic Principles of IGMPv1

IGMPv1 runs on multicast devices and hosts, and manages members in a multicast group by communication between the multicast devices and hosts. The IGMP behavior of a multicast device is referred to as device behavior, and the IGMP behavior of a host is referred to as host behavior.

1. Basic Structure of IGMPv1

Figure 1-1 Basic Topology of IGMP



As shown in Figure 1-1, IGMP runs on hosts (host 1, host 2, and host 3) that need to be added to a multicast group and multicast devices (device A and device B) that are directly connected to the hosts.

A host sends an IGMP Report packet to a multicast device to report that the host joins the multicast group. The multicast device sends an IGMP Query packet to the host to discover the membership of the multicast group.

There are two important concepts involved in IGMPv1 running:

- Querier

  A querier is a multicast device that sends query packets and receives packets of a host. The querier is used to discover members of a multicast group on a connected network segment.

  If multiple multicast devices running IGMP reside on a network segment, one of the multicast devices is selected as a querier, and other devices function as non-queriers. In IGMPv1, a designated router (DR) elected based on the multicast routing protocols functions as a querier. For more information about DR, see *Configuring PIM-SM*.

- IGMPv1 packet

  IGMPv1 packets are classified into IGMP Query packets and IGMP Report packets.

  - IGMP Query packet: A packet sent by a multicast device to a host to query members of a multicast group on the connected network segment.
  - IGMP Report packet: A packet sent by a host to a multicast device to join a multicast group.

2. Work Process of IGMPv1

Management of multicast group members is divided into host joining a multicast group and host leaving from the multicast group.

- Host joining a multicast group

  Communication after a host joins a multicast group falls into active joining and response query.

- Active joining steps are as follows:

  When a host initiates a join request, the host sends an IGMP Report packet to the network segment it resides, to report that it joins a multicast group.

  The querier receives the IGMP Report packet, and creates a forwarding entry for the members in the multicast group.

- Response query steps are as follows:

  The querier periodically sends an IGMP Query packet to all hosts in the local network segment in multicast mode.

  The host that joins the multicast group replies an IGMP Report packet to the querier in multicast mode. Other hosts that do not join the multicast group do not respond.

  The querier creates and maintains forwarding entries for the members in each multicast group.

- Host leaving a multicast group

  a A host leaves a multicast group without notifying the querier (types of packets for leaving a multicast group are not defined in IGMPv1).

  a The querier does not receive an IGMP Report packet from a multicast group in a specified period and removes the forwarding entry of this multicast group after the specified timer times out.

1.1.3 Basic Principles of IGMPv2

On the basis of the features of IGMPv1, IGMPv2 comes with a querier election mechanism and a group leaving mechanism.

1. Querier Election Mechanism

In IGMPv1, no querier election rule exists, a DR is selected as a querier using multicast routing protocols. In IGMPv2, a querier election mechanism is developed. The main communication process is as follows:

(1) A multicast device running IGMPv2 considers itself a querier and sends an IGMP Query (common group) packet (with destination address 224.0.0.1) to the connected network segment.

(2) Upon receiving the query packet, another multicast device compares the source IP address in the packet with the local IP address. If the source IP address is smaller than the local IP address, the querier changes to a non-querier. In this way, only one querier survives finally on the connected network segment.

(3) After the multicast device changes to a non-querier, a timer starts. The timeout time of the timer is referred to as "survival period of other querier". After timer times out, the multicast device considers itself a querier and re-initiates a querier election process. If the multicast device receives an IGMP Query packet from the querier before the timer times out, the timer is reset.

2. Group Leaving Mechanism

In IGMPv1, a host leaves a multicast group without notifying the multicast device. The multicast device detects the leaving of the host in hindsight only after the timer times out. In IGMPv2, an IGMP Leave packet is developed. When a host leaves the multicast group, the host sends an IGMP Leave packet to notify the multicast device. The main communication process is as follows:

(1) When a host leaves a multicast group, the host sends an IGMP Leave packet to all multicast devices (destination address 224.0.0.2) on the connected network segment.

(2) Upon receiving the packet, the querier sends a query packet (the destination address is the multicast group address that the host resides) of the specified multicast group to the connected network segment.

(3) If this multicast group contains other hosts, the hosts reply an IGMP Report packet to the querier within the maximum response time upon receiving the query packet.

(4) If the querier receives replies from the hosts of the multicast group within the maximum response time, there are members in the multicast group. The querier continues maintaining the forwarding entry of this multicast group. Otherwise, the querier clears the entry of this multicast group.

1.1.4 Basic Principles of IGMPv3

On the basis of the features of IGMPv1 and IGMPv2, IGMPv3 comes with a multicast source filtering function and enhanced IGMP Query packet and IGMP Report packet.

1. Multicast Source Filtering Function

The multicast source filtering function requires the cooperation of the querier and a host.

- Host action

  A host supports filtering of a specific multicast source. When the host tries to join a multicast group, it adds information of one or multiple sources to an IGMP Report packet and sets the mode of the multicast sources to INCLUDE or EXCLUDE. In INCLUDE mode, the host receives packets from this multicast source. In EXCLUDE mode, the host rejects packets from this multicast source.

- Querier action

  When receiving multicast source information in INCLUDE mode, the multicast device acts as follows:

  - If this multicast source is active, the multicast device forwards the packet from this multicast source.
  - If this multicast source is inactive, the multicast device does not forward the packet from this multicast source.

  When receiving multicast source information in EXCLUDE mode, the multicast device acts as follows:

  - If other hosts need packets from this multicast source, the multicast device continues forwarding the packet from this multicast source.
  - If this multicast source is inactive, the multicast device does not forward the packet from this multicast source.
  - For other multicast sources not in EXCLUDE mode, the multicast device needs to forward the packets.

2. Enhanced IGMP Query Packet and IGMP Report Packet

- Enhanced IGMP Query Packet

  IGMPv1 supports common group query, and IGMPv2 supports specific group query. On the basis of the features of IGMPv1 and IGMPv2, IGMPv3 supports specific source and group query.

  - Common group query: No multicast source or group is specified.
  - Specific group query: A multicast group is specified.
  - Specific source and group query: A multicast source and a multicast group are specified.

- Enhanced IGMP Report Packet

  In IGMPv3, an IGMP Report packet carries records of one or multiple groups. The group records include the multicast source addresses and multicast group addresses.

Group records are divided into the following types:

- IS_IN: The filtering mode of a multicast source is INCLUDE, indicating that only packets from this specified multicast source to this multicast group are received.
- IS_EX: The filtering mode of a multicast source is EXCLUDE, indicating that packets from this specified multicast source to this multicast group are rejected.
- TO_IN: The filtering mode is changed from EXCLUDE to INCLUDE.
- TO_EX: The filtering mode is changed from INCLUDE to EXCLUDE.
- ALLOW: Multicast packets from specified multicast sources to this multicast group are received. If the filtering mode is INCLUDE, these multicast sources are added to the original source list. If the filtering mode is EXCLUDE, these multicast sources are removed from the original source list.
- BLOCK: Multicast packets from specified multicast sources to this multicast group are rejected. If the filtering mode is INCLUDE, these multicast sources are removed from the original source list. If the filtering mode is EXCLUDE, these multicast sources are added to the original source list.

1.1.5 IGMP SSM Mapping

In actual network environment, most multicast devices support IGMPv3. However, there are a great number of old multicast devices that support only IGMPv1 or IGMPv2. Consequently, these old multicast devices cannot provide hosts with the multicast services in the SSM model using IGMPv3. After the IGMP SSM mapping technology is applied, the multicast devices can provide hosts with the multicast services in the SSM model without upgrading to IGMPv3.

The IGMP SSM mapping technology enables the multicast devices to support IGMPv3 by mapping the multicast group information in IGMPv1 Report packets and IGMPv2 Report packets to the multicast group information that carries specific multicast sources. After an SSM mapping rule is configured on the multicast devices, upon receiving IGMPv1 Report packets and IGMPv2 Report packets, the multicast devices process the packets based on the multicast group information in the packets.

- If a multicast group is not in the SSM group address range, the multicast services are provided in the ASM model.
- If the multicast group is in the SSM group address range and no SSM mapping rule corresponding to this multicast group is configured on the multicast device, the multicast device cannot provide multicast services in the SSM model and then discards the packets.
- If the multicast group is in the SSM group address range and an SSM mapping rule corresponding to this multicast group is configured on the multicast device, the multicast group information in the packets is converted to the multicast group information that carries specific multicast sources and the multicast device provides the multicast services in the SSM model.

1.1.6 IGMP Proxy

In a simple tree network topology, a border multicast device does not need to run complex multicast routing protocols such as Protocol Independent Multicast (PIM), you can configure the IGMP proxy function on this multicast device. This multicast device functions as an intermediate proxy between upstream IGMP querier and downstream hosts.

A device running the IGMP proxy functions as a multicast device and a host at the same time. For an upstream IGMP querier, this device plays the role of a host and executes host actions. For a downstream host, this device plays the role of an IGMP querier and executes querier actions.

1.1.7 Protocols and Standards

- RFC 1112: Host Extensions for IP Multicasting
- RFC 2236: Internet Group Management Protocol, Version 2
- RFC 3376: Internet Group Management Protocol, Version 3
- RFC 4605: Internet Group Management Protocol (IGMP)/Multicast Listener Discovery

1.2 Configuration Task Summary

IGMP configuration includes the following tasks:

- Configuring Basic Functions of IGMP
- (Optional) Configuring IGMP Parameters. All the configuration tasks below are optional. Select the configuration tasks as required.
  - Configuring an IGMP Version
  - Configuring the Maximum Response Time for Query Packets
  - Configuring Common Group Query
  - Configuring Specific Group Query
  - Configuring Survival Period of Other Querier
- (Optional) Configuring IGMP Group Filtering
- (Optional) Configuring the IGMP Proxy Function
- (Optional) Configuring the IGMP SSM Mapping Function
- (Optional) Configuring the Router Alert Option of IGMP Packets
- (Optional) Enabling Source Address Checking for IGMP Report Packets
- (Optional) Enabling Fast Leave
- (Optional) Configuring the Querier Robustness Variable
- (Optional) Adding a Static Interface to a Group
- (Optional) Simulating a Host to Join a Group

1.3 Configuring Basic Functions of IGMP

1.3.1 Overview

Basic functions of IGMP lay a foundation for other functions, enable multicast devices to run IGMP, and help collect and manage members in a multicast group.

You cannot directly enable the basic functions of IGMP. You need to enable the multicast routing function on a device to make the basic functions of IGMP take effect.

1.3.2 Restrictions and Guidelines

Before the basic functions of IGMP are enabled, you must enable the Protocol Independent Multicast Sparse Mode (PIM-SM) or Protocol Independent Multicast Dense Mode (PIM-DM) function on an interface to make the basic functions of IGMP take effect. To disable the basic functions of IGMP take effect, you need to remove the configuration of the PIM-SM or PIM-DM function.

1.3.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable IPv4 multicast routing.

ip multicast-routing

The multicast routing is disabled by default.

(4) Enter the interface configuration mode.

interface *interface-type interface-number*

(5) Enable the PIM-SM or PIM-DM function on an interface. Select at least one of them to configure.

- Enable PIM-DM on an interface.

  ip pim dense-mode

  The PIM-DM function is disabled on an interface by default.

- Enable PIM-SM on an interface.

  ip pim sparse-mode

  The PIM-SM function is disabled on an interface by default.

1.4 Configuring IGMP Parameters

1.4.1 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Configuring an IGMP Version
- Configuring the Maximum Response Time for Query Packets
- Configuring Common Group Query
- Configuring Specific Group Query
- Configuring Survival Period of Other Querier

1.4.2 Configuring an IGMP Version

1. Overview

IGMP comes with three versions: IGMPv1, IGMPv2, and IGMPv3. A later version corresponds to stronger protocol functions. You can select an IGMP version based on network requirements and IGMP support of upstream and downstream devices.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure an IGMP version.

ip igmp version { **1** | **2** | **3** }

IGMPv2 runs on an interface by default.

After this command is run, the IGMP function module automatically restarts.

1.4.3 Configuring the Maximum Response Time for Query Packets

1. Overview

After sending a query packet, the querier needs to receive a reply packet from a host in the specified time. Otherwise, the querier considers that no member exists in the corresponding multicast group and deletes the group information. This specified time is referred to as the maximum response time for a query packet, and it can be set to a proper time value based on actual network topology.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the maximum response time for query packets on an interface.

ip igmp query-max-response-time *query-max-response*

The maximum response time for query packets on an interface is **10** seconds by default.

1.4.4 Configuring Common Group Query

1. Overview

Common group query means querying members in a multicast group. You can configure an interval for sending common group query packets.

2. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the interval for querying a common group member.

ip igmp query-interval *query-interval*

The interval for querying a common group member is **125** seconds by default.

1.4.5 Configuring Specific Group Query

1. Overview

Specific group query means querying members in a specified multicast group. You can configure an interval and times for sending specific group query packets.

Upon receiving an IGMP Leave packet on an interface, the querier continuously sends specific group query packets and waits for responses from hosts. If no host replies in the specified time, the querier considers that this multicast group does not contain any member, and deletes this interface from the IGMP group member records. Then, this interface does not forward packets from this multicast group. The timeout time is a product of the number of specific group query packets and the times for sending the specific group query packets.

2. Restrictions and Guidelines

The parameter of specific group query can be configured in IGMPv2 and IGMPv3. The parameter is not supported in IGMPv1.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the parameters of specific group query. Select at least one of them to configure.

- Configure the interval for sending specific group query packets.

  ip igmp last-member-query-interval *last-member-query-interval*

  The interval for sending specific group query packets is **1** second by default.

- Configure the times for sending specific group query packets.

  ip igmp last-member-query-count *last-member-query-count-number*

  Specific group query packets are sent twice by default.

1.4.6 Configuring Survival Period of Other Querier

1. Overview

A querier election mechanism is introduced in IGMPv2. Based on the mechanism, non-queriers maintain a timer and the timeout time of the timer is referred to as "survival period of other querier". If the timer times out, a multicast device considers itself a querier and re-initiates a querier election request. During networking, you can determine proper survival period of other querier based on network topology configuration.

2. Restrictions and Guidelines

The querier election mechanism can be configured in IGMPv2 and IGMPv3. It is not supported in IGMPv1.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure survival period of other querier.

ip igmp query-timeout *query-timeout*

The survival period of other querier is **255** seconds by default.

1.5 Configuring IGMP Group Filtering

1.5.1 Configuration Tasks

All the configuration tasks below are optional. Select the configuration tasks as required.

- Filtering a Multicast Group
- Configuring the Maximum Number of Group Members

1.5.2 Filtering a Multicast Group

1. Overview

If you do not want hosts in the network segment where an interface resides to join a multicast group, you can configure access control list (ACL) rules on the interface as a filter. The interface filters IGMP Report packets of the hosts based on the ACL rules and allows the hosts to join specific groups.

2. Restrictions and Guidelines

- For more information about ACL, see *Configuring ACL*.
- Extended ACL rules can be configured in IGMPv3. When a received IGMP Report packet is (S1, S2, S3…Sn, G), an ACL rule is used to match (0, G). Therefore, to normally filter (S1, S2, S3…Sn, G), a (0, G) extended ACL rule must be configured.

3. Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Filter out groups that you do not want a host to join.

ip igmp access-group { *acl-name* | *acl-number* }

Hosts can join any group by default.

1.5.3 Configuring the Maximum Number of Group Members

1. Overview

To configure the maximum number of group members means configuring the maximum number of multicast groups that a host can join.

The configuration can be completed in interface or global mode. If the configuration is completed in global mode, the number of group members for a multicast device is limited. If the configuration is completed in interface mode, the number of group members on an interface is limited. If the number of group member records exceeds the interface limit or global limit, subsequent received IGMP Report packets are ignored.

2. Restrictions and Guidelines

- Group member records that are generated in EXCLUDE mode list are not counted in the group members.
- Interface and global limits can be configured separately. If the global limit is smaller than the interface limit, the global limit prevails.

3. Procedure (Global Configuration Mode)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure the maximum number of IGMP group members in global configuration mode.

ip igmp limit *limit-number* [**except** *acl-name* | **except** *acl-number*]

The maximum number of IGMP group members is **64000** in global configuration mode by default.

4. Procedure (Interface Configuration Mode)

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the maximum number of IGMP group members on an interface.

ip igmp limit *limit-number* [**except** *acl-name* | **except** *acl-number*]

The maximum number of IGMP group members on an interface is **4000** by default.

1.6 Configuring the IGMP Proxy Function

1.6.1 Overview

In a simple tree network topology, you can configure the IGMP proxy function and use it as an intermediate proxy between upstream IGMP querier and downstream hosts without running complex multicast routing protocols such as PIM.

On the device that runs the IGMP proxy, interfaces are classified into proxy service interfaces and MRoute proxy interfaces.

The proxy service interfaces execute host behaviors, receive IGMP packets from upstream devices, and forward the packets to the MRoute proxy interfaces.

The MRoute proxy interfaces execute device behaviors, receive IGMP Report packets from downstream devices, and forward the packets to the proxy service interfaces.

1.6.2 Restrictions and Guidelines

- The basic functions of IGMP must be configured.
- The interfaces connected to upstream devices must be configured as proxy service interfaces and the interfaces connected to hosts must be configured as MRoute proxy interfaces. The two types of interfaces must be used at the same time. If only one type of interfaces are configured, the IGMP proxy function will be abnormal.
- If the proxy service interfaces are switched over from L3 to L2, the routing proxy configured on the MRoute proxy interfaces is automatically disabled.

1.6.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the IGMP proxy function. The configuration steps below are mutually exclusive. Please configure only one task.

- Configure an interface as a proxy service interface.

  ip igmp proxy-service

  No interface is configured as a proxy service interface by default.

  The interface directly connected to an upstream device can be configured as a proxy service interface unless otherwise specified. A device supports 32 proxy service interfaces at most. When a proxy service interface receives an IGMP Report packet, the proxy service interface makes response based on the IGMP group member records.

- Configure an interface as an MRoute proxy interface.

  ip igmp mroute-proxy *interface-type interface-number*

No interface is configured as an MRoute proxy interface by default.

The interface directly connected to a downstream device can be configured as an MRoute proxy interface unless otherwise specified.

1.7 Configuring the IGMP SSM Mapping Function

1.7.1 Overview

At present, the SSM multicast model (supporting filtering multicast sources) is supported in IGMPv3 only. To enable the SSM multicast model to be supported in IGMPv1 and IGMPv2, you can configure the IGMP SSM mapping function on a device, and add multicast group information of specified multicast sources to IGMPv1 and IGMPv2 packets so that the hosts can use the SSM multicast services provided by the device on the basis of running IGMPv1 or IGMPv2.

1.7.2 Restrictions and Guidelines

- When a device receives an IGMPv1 or IGMPv2 Report packet, the device adds the static mapping source address.
- The IGMP SSM mapping function applies to only IGMPv1 and IGMPv2 packets. You are advised to enable IGMPv3 on an interface to ensure that IGMP packets of different versions can obtain the SSM multicast services.

1.7.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable the IGMP SSM mapping function.

ip igmp ssm-map enable

The IGMP SSM mapping function is disabled by default.

(4) Configure a static mapping entry.

ip igmp ssm-map static { *acl-name* | *acl-number* } *source-address*

No static mapping entry is configured by default.

1.8 Configuring the Router Alert Option of IGMP Packets

1.8.1 Overview

The Router Alert option in an IP packet header is used to warn a router device to check content in the IP packet. The router device can determine whether to add this option to a packet to be sent and whether to check this option in a received packet. The device does not check this option by default.

After the Router Alert option is configured, if an IGMP packet carries the Router Alert option, the multicast device checks the IGMP packet carefully and updates the controlled content. If the IGMP packet does not

carry the Router Alert option, the multicast device does not check the content in the packet and directly forwards the packet.

1.8.2 Restrictions and Guidelines

After the Router Alert option is configured, the multicast device must add this option to a packet to be sent and check this option in a received packet. Otherwise, an error occurs in IGMP packet receiving.

1.8.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Configure to check the Router Alert option in an IGMP packet.

ip igmp enforce-router-alert

The Router Alert option in an IGMP packet is not checked by default.

After this option is configured, IGMP packets that do not carry the Router Alert option are discarded.

(4) Add the Router Alert option to an IGMP packet to be sent.

ip igmp send-router-alert

The Router Alert option is not added to an IGMP packet to be sent by default.

1.9 Enabling Source Address Checking for IGMP Report Packets

1.9.1 Overview

To prevent false packets, you can enable the source address checking function for IGMP packets so that a multicast device receives only IGMP Report packets whose source addresses are on the same network segment as the receiving interface.

1.9.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enable source address checking for IGMP Report packets.

ip igmp enforce-source-subnet

The source address checking function for IGMP Report packets is disabled by default.

1.10 Enabling Fast Leave

1.10.1 Overview

After the fast leave function is enabled, if a device receives an IGMP Leave packet of a specified group, the device directly deletes this interface from the group member records to shorten the leave latency.

1.10.2 Restrictions and Guidelines

This function applies to an interface that runs IGMPv2 or IGMPv3 and that is connected to only one host.

1.10.3 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Enable the fast leave function.

ip igmp immediate-leave group-list { *acl-name* | *acl-number* }

The fast leave function on an interface is disabled by default.

1.11 Configuring the Querier Robustness Variable

1.11.1 Overview

The querier robustness variable is used to calculate the aging time of a forwarding entry after a device receives an IGMP Report packet. Aging time = Query interval × Robustness variable + 10

1.11.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Configure the querier robustness variable.

ip igmp robustness-variable *robustness-variable-number*

The default querier robustness variable is **2**.

1.12 Adding a Static Interface to a Group

In normal cases, an interface can join a multicast group only after the interface receives an IGMP Report packet from the multicast group.

If you manually add an interface to a group, the interface can be added to the group and exchanges multicast group information with the PIM router without IGMP packet exchange.

1.12.1 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Add a static interface to a group.

ip igmp static-group *group-address*

No static interface is added to a group by default.

1.13 Simulating a Host to Join a Group

1.13.1 Overview

By simulating a host to join a group, you can simulate host behaviors and send a Join packet to the upstream devices to join the group. This function is used to test the multicast function.

1.13.2 Procedure

(1) Enter the privileged EXEC mode.

enable

(2) Enter the global configuration mode.

configure terminal

(3) Enter the interface configuration mode.

interface *interface-type interface-number*

(4) Simulate a host to join a group.

ip igmp join-group *group-address*

The behavior of simulating a host to join a group is not performed by default.

1.14 Monitoring

Run the **show** command to check the running status of a configured function to verify the configuration effect.

Run the **debug** command to output debugging information.

Caution

The output debugging information of the **debug** command occupies system resources. Therefore, disable the debugging function immediately after use.

Run the **clear** commands to clear information.

Caution

Running the **clear** commands may lose vital information and thus interrupt services.

Table 1-1 Monitoring

Command	Purpose
clear ip igmp group	Clears dynamic group member records in the IGMP cache.
clear ip igmp interface *interface-type interface-number*	Clears all IGMP statistics and group member records on the interface.
show ip igmp groups [*interface-type interface-number*] [*group-address*] [**detail**]	Displays groups directly connected to the device and group information learned from IGMP.
show ip igmp interface [*interface-type interface-number*]	Displays IGMP configurations of the interface.
show ip igmp ssm-mapping [*group-address*]	Displays IGMP SSM mapping information.
show debugging	Displays the status of the IGMP debugging switch.
debug ip igmp all	Debugs all IGMP information.
debug ip igmp decode	Debugs IGMP packet resolution.
debug ip igmp encode	Debugs IGMP packet encoding.
debug ip igmp events	Debugs IGMP event information.
debug ip igmp fsm	Debugs IGMP Finite State Machine (FSM).
debug ip igmp tib	Debugs IGMP state machine information.
debug ip igmp warning	Debugs IGMP warning.