Chapter25:IGMP-SNOOPING Configuration

Table of Contents

Chapter 1 IGMP-Snooping Configuration

1.1 IGMP-Snooping Configuration Tasks

The task of IGMP-snooping is to maintain the relationship between VLAN and group address and to update simultaneously with the multicast changes, enabling the switch to forward data according to the topology structure of the multicast group. The main functions of IGMP-snooping are shown as follows:

(1) Listening IGMP message;

(2) Maintaining the relationship table between VLAN and group address;

(3) Keeping the IGMP entity of host and the IGMP entity of router in the same state to prevent flooding from occurring.

Note: Because igmp-snooping realizes the above functions by listening the query message and report message of igmp, igmp-snooping can function properly only when it works on the multicast router, that is, the switch must periodically receive the igmp query information from the router. The router age timer of igmp-snooping must be set to a time value that is bigger than the group query period of the multicast router connecting igmp-snooping. You can check the multicast router information in each VLAN by running show ip igmp-snooping. ● Enabling/Disabling IGMP-snooping of VLAN

- Adding/Deleting the Static Multicast Address of VLAN
- Configuring immediate-leave of VLAN
- Configuring the static routing port of VLAN
- Configuring IPACL of Generating Multicast Forward Table
- Configuring the function to filter multicast message without registereddestination address
- Configuring the Router Age timer of IGMP-snooping
- Configuring the Response Time timerof IGMP-snooping
- Configuring IGMP Querier of IGMP-snooping
- Configuring Querier Time Timer of IGMP-snooping
- Configuring Forward-L3-to-Mrouter of IGMP-Snooping to Forward the Data Packets to the Routing Port
- Configuring the Sensitive Mode and Value of IGMP-Snooping
- Configuring v3-leave-check of IGMP-Snooping
- Configuring forward-wrongiif-within-vlan of IGMP-Snooping.
- Configuring IPACL of IGMP-snooping

- Configuring max multicast IP address number of IGMP-snooping
- IGMP-snooping monitoringandmaintenance
- IGMP-snoopingConfiguration Example

1.1.1 Enabling/Disabling IGMP Snooping of VLAN

Run the following commands in global configuration mode.

Command	Purpose
ip igmp-snooping [**vlan** *vlan_id*]	Enabling/Disabling IGMP Snooping of VLAN
no ip igmp-snooping [**vlan** *vlan_id*]	Resumes the default settings.

If vlan is not specified, all vlans in the system, including vlans created later, can be enabled or disabled.

In the default configuration, IGMP-snooping of all VLANs is disabled.

For instance, to enable IGMP-snooping on VLAN3 and keep it after you restart the system, run command "no ip IGMP-snooping", then configure "ip IGMP-snooping VLAN 3" and save the configuration.

1.1.2 Adding/Deleting the Static Multicast Address of VLAN

Hosts that do not support IGMP can receive corresponding multicast message by configuring the static multicast address.

Run the following commands in global configuration mode.

Command	Purpose
ip igmp-snooping vlan *vlan_id* **static** *A.B.C.D* **interface** *intf*	Adds the static multicast address of VLAN.
no ip igmp-snooping vlan *vlan_id* **static** *A.B.C.D* **interface** *intf*	Deletes static multicast address of VLAN.

1.1.3 Configuring Immediate-Leave of VLAN

When the characteristic immediate-leave is configured, the switch can delete the port from the port list of the multicast group after the switch receives the leave message. The switch, therefore, does not need to enable the timer to wait for other hosts to join the multicast. If other hosts in the same port belongs to the same group and their users do not want to leave the group, the multicast communication of these users may be affected. In this case, the immediate-leave function should not be enabled.

Run the following commands in global configuration mode.

Command	Operation
ip igmp-snooping vlan *vlan_id* **immediate-leave**	Configures the immediate-leave function of the VLAN.
no ip igmp-snooping vlan *vlan_id* **immediate-leave**	Sets immediate-leave of VLAN to its default value.

The immediate-leave characteristic of VLAN is disabled by default.

1.1.4 Configuring the Static Routing Port of VLAN

Configure the static routing interface and send the multicast packet to the routing port. The switch will send the multicast report packets to all routing ports in vlan.

Run the following commands in global configuration mode.

Command	Purpose
ip igmp-snooping vlan *vlan_id* **mrouter interface** *intf*	Add the static routing port of VLAN.
no ip igmp-snooping vlan *vlan_id* **mrouter interface** *intf*	Delete the static routing port of VLAN.

1.1.5 Configuring IP ACL of Generating Multicast Forward Table

Run following commands to configure IPACL. Thus, the rules and limitations of generating the multicast forwarding table after receiving packets of igmp report can be set.

Command	Purpose
ip igmp-snooping policy *word*	Adds IPACL in generating multicast forwarding table.
no ip igmp-snooping policy	Deletes IPACL in generating multicast forwarding table.

1.1.6 Configuring the Function to Filter Multicast Message without Registered Destination Address

When multicast message target fails to be found (DLF, the destination address is not registered in the switch chip through igmp-snooping), the default process method is to send message on all ports of VLAN. Through configuration, you can change the process method and all multicast messages whose destination addresses are not registered to any port will be dropped.

Command	Operation

ip igmp-snooping dlf-drop	Drops multicast message whose destination fails to be found.
no ip igmp-snooping dlf-drop	Resume the default settings (forward)

Note:

1) The attribute is configured for all VLANs.

2) The default method for the switch to handle this type of message is forward (message of this type will be broadcasted within VLAN).

1.1.7 Configuring the Router Age timer of IGMP-snooping

The router age timer is used to monitor whether the IGMP querier exists or not; the IGMP querier maintenance is used to maintain and manage the multicast address by sending the query packets and IGMP snooping works by independence on the communication between IGMP querier and host.

Run the following commands in global configuration mode.

Command	Operation
ip igmp-snooping timer router-age *timer_value*	Sets the value of the router age of IGMP Snooping.
no ip igmp-snooping timer router-age	Resumes the default value of the router age of IGMP Snooping.

Note:

The settings of the timer requires to refer to the query period settings of the IGMP querier for it cannot be smaller than the query period; you are recommended to set the router age timer to the triple of the query period.

By default the router age timer is set to be 260 seconds of IGMP snooping.

1.1.8 Configuring the Response Timer of IGMP Snooping

The response time timer means the threshold time for the host to report the multicast after IGMP querier sends the query packets; if this report packet is not received after the timer ages, the switch will delete this multicast address.

Run the following commands in global configuration mode.

Command	Operation
ip igmp-snooping timer response-time *timer_value*	Sets the value of the response time of IGMP Snooping.
no ip igmp-snooping timer response-time	Resumes the default value of the response time of IGMP Snooping.

Note:

The value of the timer cannot be set too small, or the multicast communication may be unstable.

By default the response time is set to be 15 seconds of IGMP snooping.

1.1.9 Configuring Querier of IGMP-snooping

If the multicast router does not exist in VLAN where IGMP-snooping is activated, the querier function of IGMP-snooping can be used to imitate the multicast router to regularly send IGMP query message. (The function is global, that is, it can be enabled or disabled in VLAN where IGMP-snooping is globally enabled)

When the multicast router does not exist in LAN and multicast flow does not need routing, the automatic query function of the switch can be activated through IGMP snooping, enabling IGMP snooping to work properly.

Run the following commands in global configuration mode.

Command	Operation
[**no**] **ip igmp-snooping querier [address** *[ip_addr*]	Configures the querier of IGMP-snooping. The optional parameter address is the source IP address of query message.

The IGMP-snooping querier function is disabled by default. The source IP address of fake query message is 10.0.0.200 by default.

Note:

If the querier function is enabled, the function is disabled when the multicast router exists in VLAN;the function can be automatically activated when the multicast router times out.

1.1.10 Configuring Querier Time Timer of IGMP-snooping

Querier Time timer is the time interval of the switch (acts as local IGMP query) forwards query packets. After aging, the timer broadcasts query packets within vlan.

Run the following commands in global configuration mode.

Command	Operation
ip igmp-snooping querier querier-timer *timer_value*	Configuring the value of IGMP-snooping's Querier Time
no ip igmp-snooping querier querier-timer	Recovering IGMP-snooping's Querier Time as default

The IGMP-snooping querier function is disabled by default. By default IGMP-snooping querier is shut down. The default time interval of Query messages is 200 seconds.

Note:

If Querier function is initiated, querier-timer should not be set as too long. In subnet if there are other switches with querier initiated, long querier-timer (longer than other switch's router-age) would lead to the instablization of querier selection in subnet.

1.1.11 Configuring Forward-L3-to-Mrouter of IGMP-Snooping to Forward the Data Packets to the Routing Port

If L3 multicast feature is initiated and igmp-snooping does not join messages to downstream port, only downstream vlan port can be learnt by multicast route. If forward-l3-to-mrouter function is initiated, all the downstream router ports can be learned. Data messages could be sent to multicast router pot registered by PIM-SM message not broadcasting messages to all downstream physical port. The command is mainly used under the following conditions.

When L3 multicast is enabled in multiple switch cascading, the upstream devices can only learn the downstream vlan ports through the multicast routing protocol and there is no IGMP packet exchange between the upstream and downstream devices. Hence the snooping of the upstream devices cannot learn the specific physical ports that the downstream devices connect and the upstream devices will send the multicast packets to all physical ports in the local vlan. After this command is enabled, the upstream devices can forward the multicast packets to the physical ports that the downstream devices connect, preventing the multicast packets to be broadcast in the downstream vlan.

Run the following commands in global configuration mode.

Command	Operation
[**no**] **ip igmp-snooping forward-l3-to-mrouter**	Sets the forward-l3-to-mrouter function of IGMP-snooping.

By default, the IGMP-snooping forward-l3-to-mrouter is disabled.

Note:

This command can be used to send the data packets to the multicast routing port, but the switchchip can limit the source-data-port, so the data packets will not be sent to the port of source data, but to the downstream multicast routing port that is registered on PIM-SM.

1.1.12 Configuring the Sensitive Mode and Value of IGMP-Snooping

If IGMP-snooping sensitive is enabled, the router-age of mrouter in active state will be set to sensitive value when the port in trunk mode is shut down, and then the query packets will be sent out rapidly.

Run the following commands in global configuration mode.

Command	Operation
[**no**] **ip igmp-snooping sensitive** [value [3-30]]	Sets IGMP-snooping sensitive. The value parameter is the current router-age of mrouter in active state.

By default, IGMP-snooping sensitive is disabled.

Note:

When it is in sensitive mode, the update of router-age through sensitive value is only for the current period; the next router-age will resume to the time router-age.

1.1.13 Configuring v3-leave-check of IGMP-Snooping

If v3-leave-check of IGMP-snooping is enabled, the special query packet will be sent after the v3-leave packet is received; otherwise, no following actions will be taken after the v3-leave packet is received.

Run the following commands in global configuration mode.

Command	Operation
[**no**] **ip igmp-snooping v3-leave-check**	Sets v3-leave-check of IGMP-Snooping. After the v3-leave packet is received, the special query packet will be sent.

1.1.14 Configuring forward-wrongiif-within-vlan of IGMP-Snooping.

If forward-wrongiif-within-vlan of IGMP-snooping is enabled, the multicast packets that are received from the incorrect vlan interface will be taken to carry out L2 forward in the source VLAN and then forwarded to the relative group ports in the local vlan; otherwise, the multicast will be dropped.

Run the following commands in global configuration mode.

Command	Operation
[**no**] **ip igmp-snooping forward-wrongiif-within-vlan**	Sets forward-wrongiif-within-vlan of IGMP-snooping.

By default, IGMP-snooping forward-wrongiif-within-vlan is enabled.

Note:

The ip igmp-snooping forward-wrongiif-within-vlan command takes its importance only when L3 multicast is enabled.

1.1.15 Configuring IPACL of IGMP-snooping

Enable IPACL function of IGMP-snooping and determine the packets of some multicast IP address are to be deleted or ignored.

Run the following commands in physical interface configuration mode.

Command	Operation

ip igmp-snooping policy *word*	Adding multicast message's IPACL which need to be dealt with port.
no ip igmp-snooping policy	Deleting multicast message's IPACL which need to be dealt with port.

1.1.16 Configuring max multicast IP address number of IGMP-snooping

If configuring the maximum multicast IP address quantity at IGMP-snooping port, the quantity of applied groups at the port would be judged whether it is beyond the configured maximum quantity when IGMP-snooping generates forwarding entry. If it is beyond the maximum quantity, the port's entry would not be generated.

Run the following commands in physical interface configuration mode.

Command	Operation
[**no**] **ip igmp-snooping limit** [value [1-2048]]	Configuring the maximum multicast IP address quantity at IGMP-snooping port

By default the maximum quantity is 2048 at IGMP-snooping.

1.1.17 IGMP-snooping monitoring and maintenance

Run the following commands in EXEC mode:

Command	Operation
show ip igmp-snooping	Displays IGMP-snooping configuration information.
show ip igmp-snooping timer	Displays the clock information of IGMP-snooping.
show ip igmp-snooping groups	Displays information about the multicast group of IGMP-snooping.
show ip igmp-snooping statistics	Displays statistics information about IGMP-snooping.
[**no**] **debug ip igmp-snooping** [**packet** | **timer** | **event** | **error**]	Enables and disables packet/clock debug/event/mistake print switch of IGMP-snooping. If the debug switch is not specified, all debug switches will be enabled or disabled.

Display VLAN information about IGMP-snooping running:

```
switch # show ip igmp-snooping
Global IGMP snooping configuration:
-----------------------------------
Globally enable          : Enabled
```

```
VLAN nodes                : 1,50,100,200,400,500
```

```
Dlf-frames filtering : Disabled
Sensitive                 : Disabled
Querier                   : Enabled
Querier address           : 10.0.0.200
Querier interval          : 140 s
Router age                : 260 s
Response time             : 15 s

vlan_id       Immediate-leave     Ports     Router Ports
-----------------------------------------------------------------
      1             Disabled          5-10       SWITCH(querier);
     50             Disabled          1-4        SWITCH(querier);
    100             Disabled          NULL       SWITCH(querier);G0/1(static);
    200             Disabled          NULL       SWITCH(querier);
    400             Disabled          NULL       SWITCH(querier);
    500             Disabled          NULL       SWITCH(querier);
```

Displays information about the multicast group of IGMP-snooping.

```
switch# show ip igmp-snooping groups
          The total number of groups          2

Vlan Group            Type Port(s)
---- --------------- ---- -----------------------------------------------------
1 226.1.1.1           IGMP G0/1                  G0/3
1 225.1.1.16          IGMP G0/1                  G0/3
```

The following example shows the timers of IGMP snooping:

switch#**show ip igmp-snooping timers** vlan 1 mrouter on port 3: 251 means the timeout time of the aging timer of the router.

vlan 1 multicast address 0100.5e00.0809 response time : 1 Indicating the period from when the last multicast group query message is received to the current time; if no host on the port respond when the timer times out, the port will be deleted.

The IGMP snooping statistics information is displayed below:

```
switch#show ip igmp-snooping statistics vlan
1
------------
    v1_packets:0IGMP v1packet number v2_packets:6
        IGMP v2packet number v3_packets:0        IGMP v3
        packet number
    general_query_packets:5        Quantity of general query
    packets special_query_packets:0        Quantity of special
    query packets join_packets:6   Number of report packets
    leave_packets:0        Number of Leave packets
    send_query_packets:0           Rserved statistics option
    err_packets:0          Quantity of error packets
```

The information about IGMP snooping debug is shown below:

switch#**debug ip igmp-snooping packet**

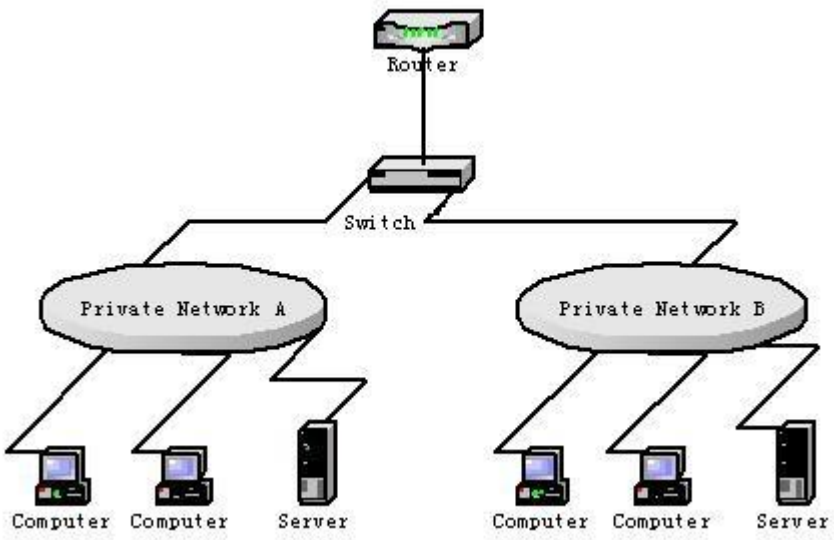
```
Jan 1 02:22:28 IGMP-snooping: Receive IGMPv3 report from G0/1, vlan 1: Jan
1 02:22:28 IGMP-snooping: Flood packet from G0/1 to vlan 1 rc = 0.
Jan  1 02:22:29 IGMP-snooping: Receive IGMPv3 report from G0/1, vlan 1:
Jan  1 2:22:29 AM IGMP-snooping: Flood packet from G0/1 to vlan 1 rc = 0.
Jan        1 2:22:38 AM IGMP-snooping: Receive IGMPv3 report from G0/1,
vlan 1: Jan1 2:22:38 AM IGMP-snooping: Flood packet from G0/1 to vlan 1 rc =
0.
Jan        1 2:22:39 AM IGMP-snooping: Receive IGMPv3 report from G0/1,
vlan 1: Jan1 2:22:39 AM IGMP-snooping: Flood packet from G0/1 to vlan 1 rc =
0.
Jan        1 2:23:11 AM IGMP-snooping: Receive IGMPv3 report from G0/1,
vlan 1: Jan1 2:23:11 AM IGMP-snooping: Flood packet from G0/1 to vlan 1 rc =
0.
Jan        1 2:23:12 AM IGMP-snooping: Receive IGMPv3 report from G0/1,
vlan 1: Jan1 2:23:12 AM IGMP-snooping: Flood packet from G0/1 to vlan 1 rc =
0.
```

The information about IGMP snooping debug timer is shown below:

```
switch#debug ip igmp-snooping timer
Jan  1 02:30:36 IGMP-snooping: Vlan 1 router on interface (null) expiry.
Jan  1 02:30:36 IGMP-snooping: Vlan 100 router on interface (null) expiry.
Jan  1 02:30:36 IGMP-snooping: Vlan 200 router on interface (null) expiry.
Jan  1 02:30:36 IGMP-snooping: Vlan 400 router on interface (null) expiry.
Jan 1 02:30:36 IGMP-snooping: Vlan 500 router on interface (null) expiry.
Inquerying the response timer expiry
```

1.1.18 IGMP-Snooping Configuration Example

The network topology is shown in figure 1.



Configuring Switch

(1) Enable IGMP-snooping of VLAN 1 connecting Private Network A.

Switch_config#ip igmp-snooping vlan 1

(2) Enable IGMP-snooping of VLAN 2 connecting Private Network B.

Switch_config#ip igmp-snooping vlan 2