QTECH
МИР ДОСТУПНЕЕ

РУКОВОДСТВО ПОЛЬЗОВАТЕЛЯ

Оглавление

1. IGMP-SNOOPING CONFIGURATION

1.1. IGMP-snooping Configuration Task

The task of IGMP-snooping is to maintain the relationships between VLAN and group address and to update simultaneously with the multicast changes, enabling layer-2 switches 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 static multicast address of VLAN
- Configuring immediate-leave of VLAN
- Configuring the function to filter multicast message without registered destination address
- Configuring the **Router Age** timer of IGMP-snooping
- Configuring the **Response Time** timer of IGMP-snooping
- Configuring IGMP Querier of IGMP-snooping
- Monitoring and maintaining IGMP-snooping
- IGMP-snooping configuration example

1.1.1. Enabling/Disabling IGMP-Snooping of VLAN

Perform the following configuration in global configuration mode:

Command	Description
ip igmp-snooping [vlan *vlan_id*]	Enables IGMP-snooping of VLAN.

no ip igmp-snooping [vlan *vlan_id*]	Resumes the default configuration.

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 enabled, just as the **ip igmp-snooping** command is configured.

Note: IGMP-snooping can run on up to 16 VLANs.

To enable IGMP-snooping on VLAN3, you must first run **no ip IGMP-snooping** to disable IGMP-snooping of all VLANs, then configure **ip IGMP-snooping VLAN 3** and save configuration.

1.1.2. Adding/Deleting Static Multicast Address of VLAN

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

Perform the following configuration in global configuration mode:

Command	Description
ip igmp-snooping vlan *vlan_id* static *A.B.C.D* interface *intf*	Adds 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.

Perform the following configuration in global configuration mode:

Command	Description
ip igmp-snooping vlan *vlan_id* immediate-leave	Configures the immediate-leave function of the VLAN.
no ip igmp-snooping vlan *vlan_id*	Sets immediate-leave of VLAN

immediate-leave	to its default value.

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

1.1.4. Configuring Static Routing Interface 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 following commands in the 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 IPACL 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 Addresss

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	Description
ip igmp-snooping dlf-	Drops multicast message whose destination fails

drop	to be found.
no ip igmp-snooping dlf-drop	Resumes the fault configuration (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 Router Age Timer of IGMP-snooping

The **Router Age** timer is used to monitor whether the IGMP inquirer exists. IGMP inquirers maintains multicast addresses by sending **query** message. IGMP-snooping works through communication between IGMP inquier and host.

Perform the following configuration in global configuration mode:

Command	Description
ip igmp-snooping timer router-age *timer_value*	Configures the value of Router Age of IGMP-snooping.
no ip igmp-snooping timer router-age	Resumes the default value of Router Age of IGMP-snooping.

Note:
For how to configure the timer, refer to the query period setup of IGMP inquirer. The timer cannot be set to be smaller than query period. It is recommended that the timer is set to three times of the query period.

The default value of Router Age of IGMP-snooping is 260 seconds.

1.1.8. Configuring Response Time Timer of IGMP-Snooping.

The **response time** timer is the upper limit time that the host reports the multicast after IGMP inquirer sends the **query** message. If the **report** message is not received after the timer ages, the switch will delete the multicast address.

Perform the following configuration in global configuration mode:

Command	Description
ip igmp-snooping timer response-time *timer_value*	Configures the value of Response Time of IGMP-snooping.

no ip igmp-snooping timer response-time	Resumes the default value of Response Time of IGMP-snooping.

Note:
The timer value cannot be too small. Otherwise, the multicast communication will be unstable.

The value of Response Time of IGMP-snooping is set to 15 seconds.

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.

Perform the following configuration in global configuration mode:

Command	Description
[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 IGMP-snooping's Querier Time Timer

Querier Time Timer is the time interval when switch as local IGMP querier sends messages. Timer broadcasts query message within VLAN after aging.

Configure as following under global configuration mode:

Command	Operation

ip igmp-snooping querier querier-timer *timer_value*	Configures the value of IGMP-snooping's Querier Time
no ip igmp-snooping querier querier-timer	Recovers IGMP-snooping's Querier Time as default

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

Notice:

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 filter of IGMP-snooping

The command is used to enable IGMP-snooping filter, the switch only enables the configured multicast group in the filter to add group.

Configure as following under port configuration mode:

Command	Purpose
[no] ip igmp-snooping filter [address [ip_addr]	Configures filter of IGMP-snooping, the optional parameter: address is the multicast group address.

By default the function "IGMP-snooping filter" is disabled. All multicast addresses can add groups.

Note:

Only an arbitrary address is configured can the filter function takes effect. Delete all addresses and the filter function is disabled.

1.1.12. Configuring clear-group of IGMP-snooping

The command is used to delete all multicast groups recorded by igmp-snooping in the switch.

Configure as following under global configuration mode:

Command	Purpose
ip igmp-snooping	Delete all multicast groups manually

clear-group	

Note:

The command is used to delete all multicast groups in non-service condition.

1.1.13. Configuring quick-query of IGMP-snooping

If enable quick of IGMP-snooping, there is port up, send igmp query packets to the port directly.

Configure as following under global configuration mode:

Command	Purpose
[no] ip igmp-snooping quick-query	Enables the command and if there is port up, send igmp query packets to port up.

Note:

If quick-query is enabled, send query to the new port when there is up of the port. The function is applicable to the downstream host of not actively sending join packets.

1.1.14. Configuring decrease-query-report-for-mvc of IGMP-snooping

If to enable descrease-query-report of IGMP-snooping, the command works after enabling mvc. The command is used to decrease igmp-snooping forwarding or protocol packets of the broadcast in mvc mode.

Configure as following under global configuration mode:

Command	Purpose
[no] ip igmp-snooping decrease-query-report-for-mvc	Configures decrease-query-report-for-mvc of IGMP-snooping. Decrease the number of protocol packet in the mode of mvc after the command is enabled.

By default, igmp-snooping and mvc will collaboratively send igmp protocol packets, which will increase the number of packets.

Note: If the function is enabled, it is not applicable to the condition of igmp-snooping and mvc working collaboratively.

1.1.15. Configuring no-send-special-query of IGMP-snooping

If no-send-special-query of IGMP-snooping is enabled and querier is disabled, special query will not be forwarded after receiving leave packets.

Configure as following under global configuration mode:

Command	Purpose
[no] ip igmp-snooping no-send-special-query	Configure no-send-special-query of IGMP-snooping

By default, special-query packets will be forwarded only leave packets are received.

Note:

If Querier is enabled, the command will not take effect.

1.1.16. 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 intiated, 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	Purpose
[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.

1.1.17. Configuring sensitive mode and value for IGMP-snooping

If IGMP-snooping's sensitive mode is enabled, when port at trunk mode is shut down, set router-age time of mrouter at active status as sensitive value, and send out query message quickly.

Configure as following under global configuration mode:

Command	Purpose
[no] ip igmp-snooping sensitive [value [3-30]]	Configuring IGMP-snooping's sensitive and value could be router-age time of currently active mrouter.

By default IGMP-snooping sensitive is disabled.

Notice:

When it is sensitive mode, sensitive value is used to update router-age aiming at current one time period. Next time, route-age is recovered as configured time router-age time.

1.1.18. Configuring IGMP-snooping's v3-leave-check function

If IGMP-snooping's v3-leave-check feature is enabled, send special query message after receiving v3's leave message. Otherwise, no operation is processed.

Configure as following under global configuration mode:

Command	Purpose
[no] ip igmp-snooping v3-leave-check	Configuring IGMP-snooping's v3-leave-check. Send special query message after receiving v3 leave message.。

1.1.19. Configuring IGMP-snooping's forward-wrongiif-within-vlan function

If IGMP-snooping's forward-wrongiif-within-vlan function is enabled, do L2 forwarding of the multicast data message received from wrong vlan interface port within source vlan. Forward messages to the group member ports in the vlan. Otherwise, drop messages.

Configure as following under global configuration mode:

Command	Purpose
[no] ip igmp-snooping forward-wrongiif-within-vlan	Configuring IGMP-snooping's forward-wrongiif-within-vlan and forwarding relative group member ports within the vlan

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

Notice:

Command ip igmp-snooping forward-wrongiif-within-vlan is only meaningful when L3 multicast is enabled.

1.1.20. Configuring IGMP-snooping's IPACL function at port

If IGMP-snooping's IPACL function at port is enabled, use IPACL at port to assign whether messages of some multicast IP address need to be dealt with or ignored.

Configure as following under physical port configuration mode:

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

1.1.21. Configuring maximum multicast IP address quantity function at IGMP-snooping's port

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.

Configure as following under physical port configuration mode:

Command	Purpose
[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.

1.1.22. Monitoring and Maintaining IGMP-Snooping

Perform the following operations in management mode:

Command	Purpose
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);
```

Display 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
```

Display IGMP-snooping timer:

```
switch#show ip igmp-snooping timers
vlan 1 router age : 251 Indicating the timeout time of the router age
timer
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..
```

Display IGMP-snooping statistics:

```
switch#show ip igmp-snooping statistics
vlan 1
------------
    v1_packets:0       IGMP v1  packet number
    v2_packets:6       IGMP v2  packet number
    v3_packets:0       IGMP v3  packet number
    general_query_packets:5    General query of the packet number
    special_query_packets:0    Special query of the packet number
    join_packets:6     Number of report packets
    leave_packets:0    Number of Leave packets
    send_query_packets:0     Rserved statistics option
    err_packets:0     Number of incorrect packets
```

Debug the message timer of IGMP-snooping:

```
switch#debug ip igmp-snooping packet
Jan  1 02:22:28 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:22:28 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan  1 02:22:29 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:22:29 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan  1 02:22:38 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:22:38 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan  1 02:22:39 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:22:39 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan  1 02:23:11 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:23:11 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
Jan  1 02:23:12 IGMP-snooping: Receive IGMPv3 report from F0/1, vlan 1:
Jan  1 02:23:12 IGMP-snooping: Flood packet from F0/1 to vlan 1 rc = 0.
```

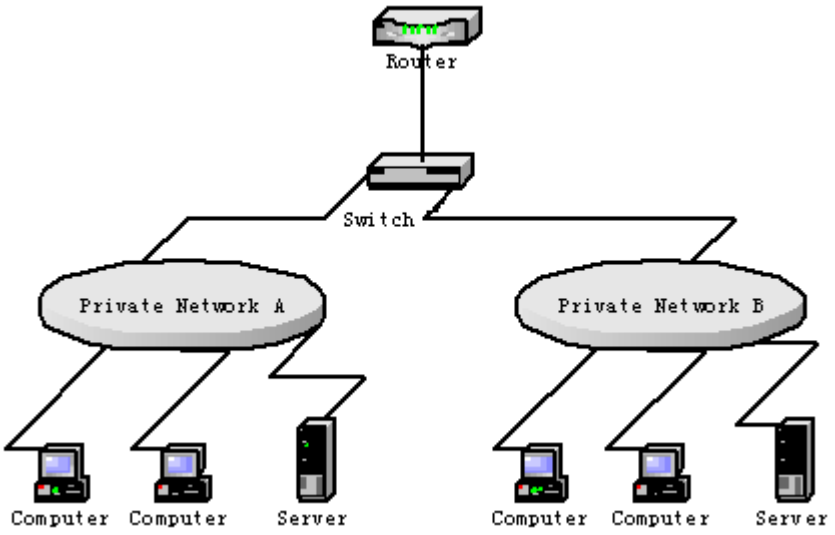
Debug the message timer of IGMP-snooping:

```
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
```

1.1.23. IGMP-Snooping Configuration Example

Figure 1 shows network connection of the example.



Configuring Switch

1. Enable IGMP-snooping of VLAN 1 connecting Private Network A.
    i. Switch_config#ip igmp-snooping vlan 1
2. Enable IGMP-snooping of VLAN 2 connecting Private Network B.
    i. Switch_config#ip igmp-snooping vlan 2