IGMP-SNOOPING Configuration

Model: S5900-24S4T2Q

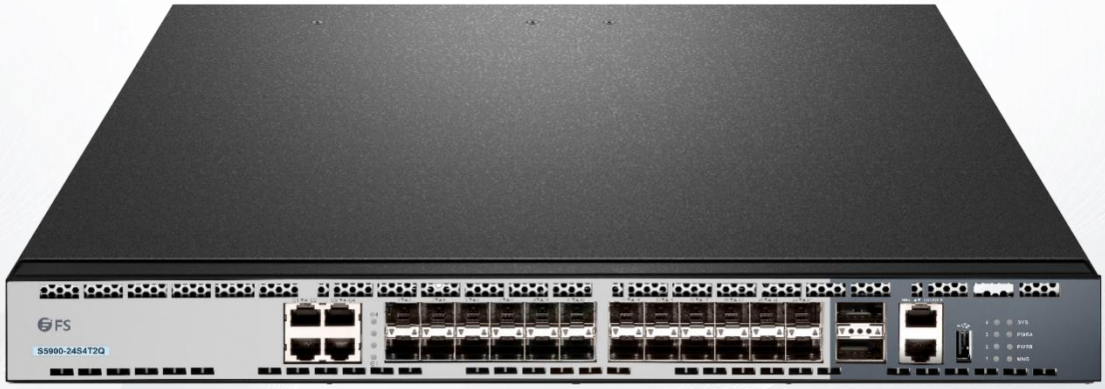

Table of Contents

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:

- Listening IGMP message;
- Maintaining the relationship table between VLAN and group address;
- 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 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 Function to Filter Multicast Message Without Registered Destination Address

When multicast message target fails to be found (DHL, 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-frames filter	Drops multicast message whose destination fails to be found.
no ip igmp-snooping dlf-frames	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).

1.1.5 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.

1.1.6 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 ten seconds.

1.1.7 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.

1.1.8 Monitoring and Maintaining IGMP-Snooping

Perform the following operations in management mode:

Command	Description
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 he 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
igmp-snooping response time:10 s
vlan 1
------------
   running
   Router: 90.0.0.120(F0/2)
```

Display information about the multicast group of IGMP-snooping:

```
switch#show ip igmp-snooping groups
Vlan Source              Group              Type Port(s)
---- --------------- --------------- ---- ---------------------------------------
    1 0.0.0.0          234.5.6.6          IGMP F0/2
    1 0.0.0.0          239.255.255.250 IGMP F0/2
```

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
rx: s_ip:90.0.0.3, d_ip:224.0.8.9   Source and destination IP addresses where packets are received
          type:16(V2-Report), max resp:00, group address:224.0.8.9   Type and content of packet
rx: s_ip:90.0.0.90, d_ip:224.0.0.1
          type:11(Query), max resp:64, group address:0.0.0.0
rx: s_ip:90.0.0.3, d_ip:224.0.8.9
```

```
        type:16(V2-Report), max resp:00, group address:224.0.8.9
rx: s_ip:90.0.0.3, d_ip:224.0.0.2
        type:17(V2-Leave), max resp:00, group address:224.0.8.9
rx: s_ip:90.0.0.90, d_ip:224.0.8.9
        type:11(Query), max resp:0a, group address:224.0.8.9
```

Debug the message timer of IGMP-snooping:

```
switch#debug ip igmp-snooping timer
tm: vlan 1 igmp router age expiry at port 2(F0/2)
tm: multicast item 0.0.0.0->224.0.8.9(0100.5e00.0809) response time expiry at port F0/4
Inquerying the response timer expiry
```

1.1.9 IGMP-Snooping Configuration Example

Figure 1 shows network connection of the example.

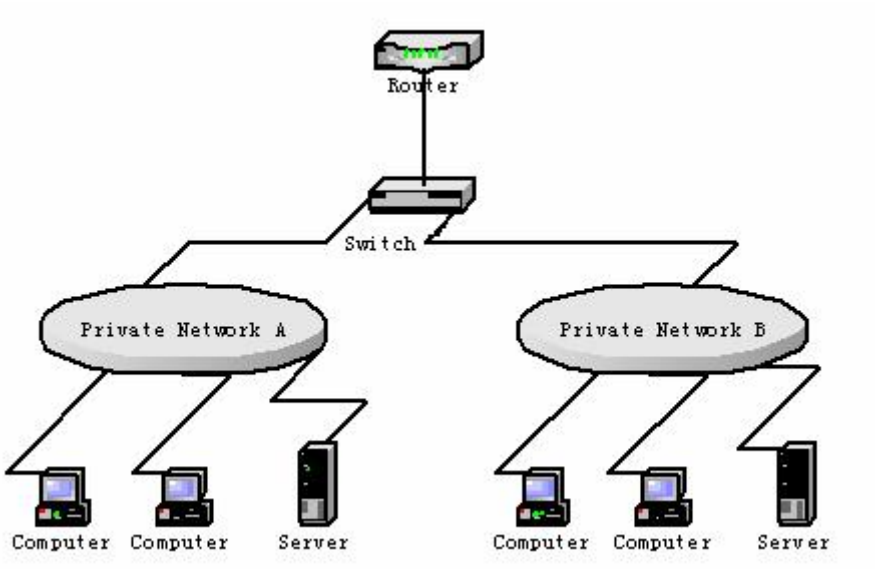

Figure 1 Configuring Switch

(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