FSOS

IGMP Snooping Configuration

Contents

1. IGMP Snooping

1.1 Brief Introduction to IGMP Snooping

IGMP (Internet Group Management Protocol) is a part of IP protocol which is used to support and manage the IP multicast between host and multicast router. IP multicast allows transferring IP data to a host collection formed by multicast group. The relationship of multicast group member is dynamic and host can dynamically add or exit this group to reduce network load to the minimum to realize the effective data transmission in network.

IGMP Snooping is used to monitor IGMP packet between host and routers. It can dynamically create, maintain, and delete multicast address table according to the adding and leaving of the group members. At that time, multicast frame can transfer packet according to his own multicast address table.

1.2 IGMP Snooping Configuration

1.2.1 Brief Configuration to IGMP Snooping

Table 1-1 Brief configuration of IGMP Snooping

Configuration Task		Remark	Detailed configuration
IGMP Snooping basic configuration	Enable IGMP Snooping	required	3.2.2
Modify and optimize IGMP Snooping configuration	Configure IGMP Snooping multicast interface aging time	optional	3.2.3
	Configure IGMP Snooping max-response-time	optional	3.2.3
	Configure IGMP Snooping interface fast-leave	optional	3.2.4
	Configure the number of the multicast group allowed learning	optional	3.2.5
	Configure IGMP-Snooping multicast learning strategy	optional	3.2.6
	Configure IGMP-Snooping CSS	optional	3.2.7
	Configure route-port	optional	3.2.8

	Configure IGMP Snooping multicast VLAN	optional	3.2.9
	Configure port record host MAC	optional	3.2.10
	Configure port whether waive research packets or not	optional	3.2.11
	Configure port whether waive report packets or not	optional	3.2.12
	Configure multicast preview	optional	3.2.13
	Configure IGMP Snooping profile name list	optional	3.2.14
Display and maintain IGMP Snooping		optional	3.2.15

1.2.2 Enable IGMP Snooping

Table 1-2 Brief configuration of IGMP Snooping

Command	Operation	Remark
Enter global configuration mode	**configure terminal**	-
Enable IGMP Snooping	**igmp-snooping**	

1.2.3 Configuring IGMP Snooping Timer

Table 1-3 Configure IGMP Snooping timer

Command	Operation	Remark
Enter global configuration mode	**configure terminal**	-
Configure IGMP Snooping multicast interface aging time	**igmp-snooping** ***host-aging-time*** time	optional By default, dynamic interface aging time is300S
Configure maximum leave time	**igmp-snooping** ***max-response-time*** time	optional by default, maximum leave time is 10S

1.2.4 Configuring Port Fast-leave

Under normal circumstances, IGMP-Snooping on IGMP leave message is received directly will not remove the port from the multicast group, but to wait some time before the port from the multicast group.

Enabling quickly delete function, IGMP-Snooping IGMP leave packet received, directly to the port from the multicast group. When the port is only one user, can be quickly removed to save bandwidth

Table 1-4 Configure port fast-leave

Command	Operation	Remark
Enter global configuration mode	**configure terminal**	-
Enter port configuration	**interface ethernet** *interface-num*	-
Configure port fast-leave	**igmp-snooping fast-leave**	optional By default, port fast-leave disables

1.2.5 Configuring Number of Multicast Group Allowed Learning

Use igmp-snooping group-limit command to configure the number of the multicast group allowed learning.

Table 1-5 Configure the number of the multicast group allowed learning

Command	Operation	Remark
Enter global configuration mode	**configure terminal**	-
Enter port configuration	**interface ethernet** *interface-num*	-
Configure the number of the multicast group allowed learning	**igmp-snooping group-limit** *number*	optional By default, the number of the multicast group allowed learning is NUM_MULTICAST_GROUPS

1.2.6 Configuring IGMP Snooping Querier

In an IP multicast network running IGMP, a multicast router or Layer 3 multicast switch is responsible for sending IGMP general queries, so that all Layer 3 multicast devices can establish and maintain multicast forwarding entries, thus to forward multicast traffic correctly at the network layer .This router or Layer 3 switch is called IGMP querier.

However, a Layer 2 multicast switch does not support IGMP, and therefore cannot send general queries by default. By enabling IGMP Snooping on a Layer 2 switch in a VLAN where multicast traffic needs to be Layer-2 switched only and no multicast routers are present, the Layer 2 switch will act as the IGMP Snooping querier to send IGMP queries, thus allowing multicast forwarding entries to be established and maintained at the data link layer.

Table 1-6 Configure IGMP Snooping querier

Command	Operation	remark
Enter global configuration	**configure terminal**	-

mode		
Configuration is not black and white list in the multicast group to learn the rules of the default	**igmp-snooping {permit | deny} {group all | vlan *vid}***	optional By default, not black and white list in the multicast group to learn the rules for the learning of all multicast group
Enter port configuration	**interface ethernet** *interface-num*	-
Configure the port multicast black list	**igmp-snooping {permit | deny} group-range** *MAC* **multi-count** *num* **vlan** *vid*	optional Configure the port to learn (not learn) VID of the start of continuous num mac multicast groups
	igmp-snooping {permit | deny} group *MAC* **vlan** *vid*	optional By default, any multicast group are not black and white list are added

1.2.7 Configuring IGMP Snooping Multicast Learning Strategy

Configured multicast learning strategies, the administrator can control the router only to learn the specific multicast group. If a multicast group is added to the blacklist, then the router will not learn the multicast group; the contrary, in the white list in the router can learn multicast group.

Table 1-7 Configuring IGMP Snooping multicast learning strategy

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Open the IGMP-Snooping querier	**igmp-snooping querier**	
Configuring VLAN general query messages	**igmp-snooping querier-vlan** *vid*	Optional
Configured to send general query message interval	***igmp-snooping query-interval*** *intervaltime*	Optional
Configuration is generally the maximum query response time of message	**igmp-snooping query-max-respond** *time*	Optional
Configured to send	**igmp-snooping general-query source-ip** *IP*	Optional

general inquiries packet source IP address		

1.2.8 Configuring IGMP Snooping Router-Port

You can configure the router port will be automatically added to the dynamic IGMP Snooping Multicast learn to make routing port also has a multicast packet forwarding capability.
When the switch receives a host membership report sent packets, the port will be forwarded to the route.

Table 1-8 Configuring Routing port

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Configure hybrid routing port	**igmp-snooping route-port forward**	Optional
Configure dynamic routing port aging time	***igmp-snooping router-port-age*** **{on | off |** ***age-time}***	Optional
Configure static routing port	***igmp-snooping route-port*** **vlan** *vid* ***interface*** **{All | ethernet** ***interface-num}***	Optiona

1.2.9 Configuring IGMP Snooping Port Multicast VLAN

Multicast VLAN on the port function, regardless of the port receiving the IGMP messages belong to which VLAN, the switch will be modified as a multicast VLAN.

Table 1-9 Configure IGMP Snooping port multicast VLAN

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Enter port configuration mode	***interface*** **ethernet** ***interface-num***	-
Configure IGMP Snooping port multicast VLAN	**igmp-snooping multicast vlan** *vid*	Optional

1.2.10 Configuring Host Port Record MAC Functions

When this feature is enabled on the port, the switch will record the source packet IGMP report MAC address.

Table 1-10 Configure the host port record MAC functions

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Enter port configuration mode	***interface* ethernet *interface-num***	-
Configure the host port record MAC	**igmp-snooping record-host**	Optional

1.2.11 Configuring Port of Dropped Query Packets or Not

When this feature is enabled on a port, the switch drops the IGMP query message. Default port to receive all IGMP packets.

Table 1-11 Configure port of dropped query packets or not

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Enter port configuration mode	***interface* ethernet *interface-num***	-
Discard the query message to the configuration port	**igmp-snooping drop query**	Optional
Configure the port to receive the query message	**no igmp-snooping drop query**	Optional

1.2.12 Configuring Port of Discarded Packets Report or Not

When this feature is enabled on a port, the switch drops the IGMP report message. Default port to receive all IGMP packets.

Table 1-12 Configure port of discarded packets report or not

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Enter port configuration mode	***interface* ethernet *interface-num***	-
Configure the port discarded packets report	**igmp-snooping drop report**	Optional
Configure the port to receive a report with	**no igmp-snooping drop report**	Optional

1.2.13 Configuring Multicast Preview

Multicast IGMP Snooping provides preview feature, users can configure the multicast channel preview, you can configure a single multicast length preview, preview interval, duration, and reset to allow preview times.

Table 1-13 Configure multicast preview

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Configuring Multicast preview	**igmp-snooping preview**	-
Configure multicast channel preview	**igmp-snooping preview group-ip *IP* vlan** *vid* ***interface ethernet interface-num***	Optional
Configuration when the long single preview, preview interval, duration and allows preview preview reset the number of	***igmp-snooping*** **preview** ***{time-once*** **time-once** ***time-interval*** **time-interval** ***time-reset*** **time-reset permit-times** *preview-times* **}**	Optional

1.2.14 Configuring Profile of Black and White List

IGMP Snooping provides the way black and white list feature profile, first in global configuration mode to create a number of profile, then the port configuration mode to configure the port reference profile list. Users can configure the IGMP Snooping profile of the type and scope, which refers to the type of permit / deny, you can use the multicast IP address range or MAC address to configure. IGMP Snooping profile only the port referenced to take effect, the configuration port reference profile, the more the type of profile must be the same between that port can only refer to the same type (permit or deny) the profile. When the port is referenced permit the profile, the profile can only learn the definition of the corresponding multicast group; when the port reference deny the profile, the profile can be defined in addition to learning outside of all multicast group; when the port does not refer to any profile, in accordance with Normally learning multicast group.

Table 1-14 Configure profile of black and white list

Operation	Command	Remarks
Enter global configuration mode	**configure terminal**	-
Create a profile, and enter profile	***igmp-snooping profile*** *profile-id*	-

configuration mode		
Configuration profile types	**profile limit {permit | deny}**	Optional
Configuration profile ip range	**ip range start-ip end-ip [vlan vlan-id]**	Optional
Range of configuration profile mac	**mac range start-mac end-mac [vlan vlan-id]**	Optional
Enter port configuration mode	***interface* ethernet *interface-num***	-
Reference configuration profile	**igmp-snooping profile refer** *profile-list*	Optional

1.2.15 Displaying and Maintenance of IGMP Snooping

After completing the above configuration, can use the following command to view configuration.

Table 1-14 Configure displaying and maintenance of IGMP Snooping

Operation	Command	Remarks
See the related configuration IGMP Snooping	**show igmp-snooping**	Performs either of the commands
See dynamic routing port	**show igmp-snooping router-dynamic**	
Display static router port configuration	**show igmp-snooping router-static**	
Display Record in host MAC	**show *igmp-snooping* record-host *[interface* ethernet *interface-num]***	
Display information about multicast preview	**show igmp-snooping preview**	
Display the current state of multicast channel preview	**show igmp-snooping preview status**	
Display profile configuration information	**show *igmp-snooping profile [interface* ethernet *interface-num] [profile-list]***	
Display multicast group	**show multicast *[interface* ethernet *interface-num]***	

1.3 IGMP Snooping Configuration Examples

IGMP Snooping configuration examples as below:

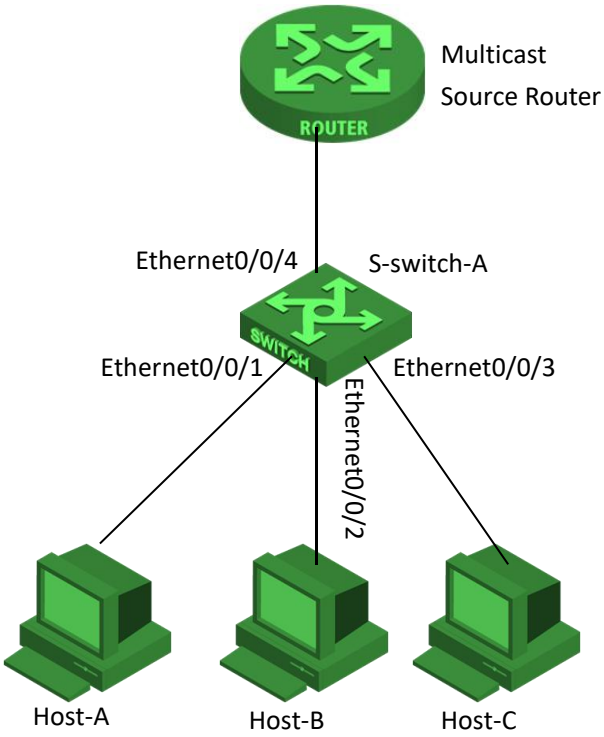

Figure 1-1

1. Network requirements

As shown in the figure 1-1, Host-A, Host-B, Host-C hosts separately belong to VLAN2, VLAN3, VLAN4.Three hosts separately receive the data of the multicast address 224.0.1.1-224.0.1.3 per configuring.

2. Configuration steps

Configuring S-switch-A

#Configure VLAN2 to 4, and add the ports separately into VlAN2,3,4 of Ethernet0/0/1, Ethernet0/0/2 and Ethernet0/0/3.

```
S-switch-A(config)#vlan 2
S-switch-A(config-if-vlan)#switchport ethernet 0/0/1
S-switch-A(config-if-vlan)#exit
S-switch-A(config)#vlan 3
S-switch-A(config-if-vlan)#switchport ethernet 0/0/2
S-switch-A(config-if-vlan)#exit
S-switch-A(config)#vlan 4
S-switch-A(config-if-vlan)#switchport ethernet 0/0/3
S-switch-A(config-if-vlan)#exit
```

#Enable igmp snooping

```
S-switch-A(config)#igmp-snooping
```

When Host-A, Host-B, Host-C forward IGMP report to S-switch-A, S-switch-A will

learn corresponding multicast table entry port; When the Multicast Source Router send igmp query time to the S-switch-A message, S-switch-A will learn the appropriate router port entry.

Show the switch learned multicast group

S-switch-A(config)#show multicast

show multicast table information

MAC Address : 01:00:5e:00:01:01
VLAN ID : 2
Static port list :.
IGMP port list : e0/0/1
Dynamic port list :

MAC Address : 01:00:5e:00:01:02
VLAN ID : 3
Static port list :.
IGMP port list : e0/0/2
Dynamic port list :

MAC Address : 01:00:5e:00:01:03
VLAN ID : 4
Static port list :
IGMP port list : e0/0/3.
Dynamic port list :

Total entries: 3 .

S-switch-A(config)#show igmp-snooping router-dynamic

Port	VID	Age	Type
e0/0/4	2	284	{ STATIC }
e0/0/4	3	284	{ STATIC }
e0/0/4	4	284	{ STATIC }

Total Record: 3

When Multicast Source Router sends 224.0.1.1-224.0.1.3 multicast serve data flow, S-switch-A will forward corresponding to Host-A, Host-B, Host-C.

Static multicast configuration examples:

Configuration steps:

Configuring S-switch-A

#configure VLAN 2 to 4, and add the ports into VLAN2, 3, 4 of Ethernet0/0/1, Ethernet0/0/2 and Ethernet0/0/3.

S-switch-A(config)#vlan 2
S-switch-A(config-if-vlan)#switchport ethernet 0/0/1
S-switch-A(config-if-vlan)#exit

S-switch-A(config)#vlan 3
S-switch-A(config-if-vlan)#switchport ethernet 0/0/2
S-switch-A(config-if-vlan)#exit
S-switch-A(config)#vlan 4
S-switch-A(config-if-vlan)#switchport ethernet 0/0/3
S-switch-A(config-if-vlan)#exit

#Add the ports into the VLAN2 to VLAN4 of Ethernet0/0/4, configure Ethernet0/0/4 as static router port.
S-switch-A(config)#vlan 2-4
S-switch-A(config-if-vlan)#switchport ethernet 0/0/4
S-switch-A(config-if-vlan)#exit
S-switch-A(config)#igmp-snooping route-port vlan 2 interface ethernet 0/0/4
S-switch-A(config)#igmp-snooping route-port vlan 3 interface ethernet 0/0/4
S-switch-A(config)#igmp-snooping route-port vlan 4 interface ethernet 0/0/4

#configure static multicast group
S-switch-A(config)#multicast mac-address 01:00:5e:00:01:01 vlan 2
S-switch-A(config)#multicast mac-address 01:00:5e:00:01:01 vlan 2 interface ethernet 0/0/1
S-switch-A(config)#multicast mac-address 01:00:5e:00:01:02 vlan 3
S-switch-A(config)#multicast mac-address 01:00:5e:00:01:02 vlan 3 interface ethernet 0/0/2
S-switch-A(config)#multicast mac-address 01:00:5e:00:01:03 vlan 4
S-switch-A(config)#multicast mac-address 01:00:5e:00:01:03 vlan 4 interface ethernet 0/0/3

Show the switch learned multicast groups
S-switch-A(config)#show multicast
show multicast table information
MAC Address : 01:00:5e:00:01:01
VLAN ID : 2
Static port list :.e0/0/1
IGMP port list :
Dynamic port list :

MAC Address : 01:00:5e:00:01:02
VLAN ID : 3
Static port list : e0/0/2
IGMP port list :
Dynamic port list :

MAC Address : 01:00:5e:00:01:03
VLAN ID : 4

Static port list : e0/0/3
IGMP port list :
Dynamic port list :

Total entries: 3 .

S-switch-A(config)#show igmp-snooping router-static

Port	VID	Age	Type
e0/0/4	2	no age	{ STATIC }
e0/0/4	3	no age	{ STATIC }
e0/0/4	4	no age	{ STATIC }

Total Record: 3

When Multicast Source Router sends 224.0.1.1-224.0.1.3 multicast serve data flow, S-switch-A will forward corresponding to Host-A, Host-B, Host-C.