NETWORK SWITCHING FEATURES

IGMP Snooping

Document ID: SW-IGMP-004
Revision ID: 01 | Revision Date: 23-10-2024

Table of Contents

Glossary

The following terms are frequently used in this document.

Term	Definition
IGMP	Internet Group Management Protocol
LAN	Local Area Network
MAC	Media Access Control
VLAN	Virtual Local Area Network

Functional Description:

IGMP snooping is a technique used in network switches to optimise the delivery of multicast traffic. Internet Group Management Protocol (IGMP) is a protocol used by devices to join or leave multicast groups.

When a device wants to receive traffic from a specific multicast group, it sends an IGMP message to the router or switch. The router or switch keeps track of which devices are interested in which multicast groups.

By only forwarding multicast traffic to interested devices, IGMP snooping helps to conserve valuable network bandwidth.

Network switches use IGMP snooping to streamline how multicast traffic reaches its intended devices. Using IGMP Snooping, network devices can manage the multicast traffic database.

IGMP snooping helps optimize multicast traffic with a Local Area Network (LAN), enhancing efficiency and bandwidth utilization. IGMP snooping becomes critical in scenarios where careful management of bandwidth is required. It allows several devices to use the same IP address so they can receive the same data.

In a LAN, multicast packets must pass through Layer 2 switches between the router and multicast users. However, multicast packets may broadcast to all the hosts in the broadcast domain including non-multicast group members, as the Layer 2 switch cannot learn multicast MAC addresses. This wastes network bandwidth and threatens network information security.

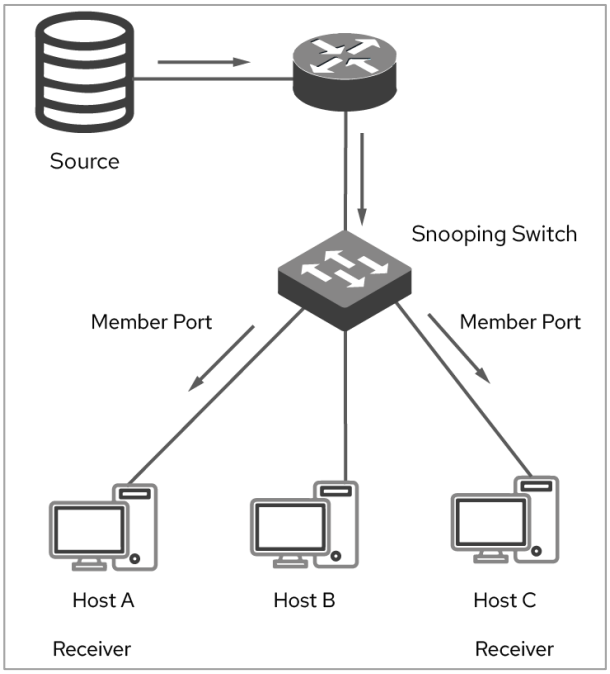

Figure 1

When IGMP snooping is enabled, the IGMP Snooping switch can listen to and analyze IGMP message and set up Layer 2 multicast forwarding entries to control multicast data forwarding. In this way, multicast packets are only multicast to multicast group members, host A and C receivers, rather than broadcast to all hosts.

IGMP Snooping in QN switches

Commands Outline

Use the ip igmp snooping command in Global Configuration mode to enable igmp snooping. Use the no form of this command to restore default.

switch(config)#ip igmp snooping

switch(config)#no ip igmp snooping

Use the ip igmp snooping vlan command in Global Configuration mode to enable igmp snooping for vlan. Use the no form of this command to restore default.

switch(config)#interface vlan

switch(config)#no interface vlan

Use the bridge multicast filtering command in Global Configuration mode to filter igmp groups. Use the no form of this command to restore default.

switch(config)#bridge multicast filtering

switch(config)#no bridge multicast filtering

Use the ip igmp snooping vlan immediate-leave command in Global Configuration mode to filter igmp groups. Use the no form of this command to restore default.

switch(config-if)#ip igmp snooping vlan immediate-leave

switch(config-if)#no ip igmp snooping vlan immediate-leave

Use the ip igmp snooping vlan querier version command in Global Configuration mode to set the version. Use the no form of this command to restore default.

switch(config)#ip igmp snooping vlan querier version

switch(config)#no ip igmp snooping vlan querier version

Configuration Steps:

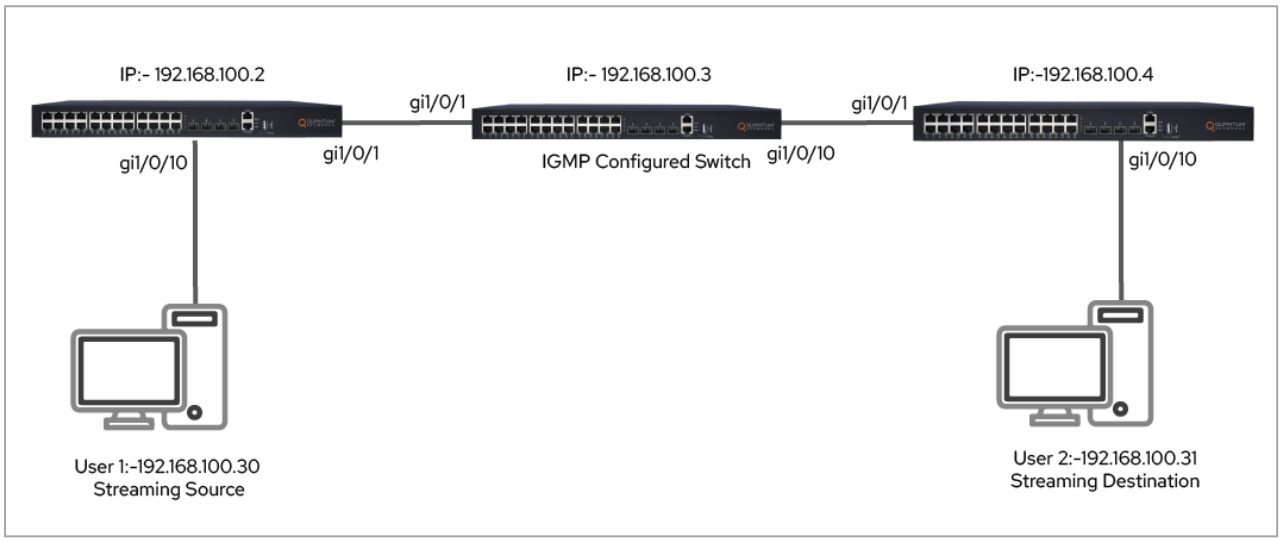

Figure 2

As shown in Figure 2, User-2 wants to join a channel which is streaming by User-1 with multicast ip 225.0.0.10. So, we have to configure IGMP Snooping in one of the three switches. In above Figure, IGMP Snooping is configured in the middle switch.

To enable the filtering of Multicast addresses, use the bridge multicast filtering Global Configuration mode command. This command does not have any arguments or keywords. When this feature is enabled, unregistered Multicast traffic (as opposed to registered) will still be flooded.

switch(config)#bridge multicast filtering

To enable Internet Group Management Protocol (IGMP) snooping, use the ip igmp snooping command in Global Configuration mode.

switchconfig)#ip igmp snooping

To enable IGMP snooping on a specific VLAN (Here, specified vlan is vlan1), use the ip igmp snooping vlan command in Global Configuration mode. To return to the default, use the no form of this command.

switch(config)#ip igmp snooping vlan 1

To enable the IGMP Snooping Immediate-Leave processing on a VLAN, use the ip igmp snooping vlan immediate-leave Global Configuration mode command in Global Configuration mode. The command can be executed before the vlan is created.

switch(config-if)#ip igmp snooping vlan 1 immediate-leave

To configure the IGMP version of an IGMP Snooping querier on a specific VLAN, use the ip igmp snooping vlan querier version command in Global Configuration mode. Here, querier version 3 specifies that the IGMP version is IGMPv3. By default it is IGMPv2.

switch(config)#ip igmp snooping vlan 1 querier version 3

Verifying configuration:

Now Join the streaming channel in User-2 and check the IGMP Snooping groups in middle switches as below.

switch#sh ip igmp snooping groups

Vlan	Group Address	Source Address	Include Ports	Exclude Ports	Comp.
1	225.0.0.10	*	gig1/0/1		V3

IGMP Reporters that are forbidden statically:

Vlan	Group Address	Source Address	Ports
1	225.0.0.10	*	No Forbidden ports

Notes & Limitations

- Malicious actors could exploit IGMP snooping to launch Denial-of-Service (DoS) attacks. By sending fake IGMP messages claiming interest in a specific group, they could flood the network with unnecessary traffic.
- Enabling IGMP snooping addresses some processing overhead to the switch as it needs to monitor IGMP messages and maintain group membership tables.
- IGMP snooping only works on Layer 2 networks (Ethernet). It cannot track multicast traffic across routers which operate at Layer 3.