# Content

# Chapter 1 IPv4 Multicast Protocol

## 1.1 IPv4 Multicast Protocol Overview

This chapter will give an introduction to the configuration of IPv4 Multicast Protocol.

## 1.1.1 Introduction to Multicast

Various transmission modes can be adopted when the destination of packet (including data, sound and video) transmission is the minority users in the network. One way is to use Unicast mode, i.e. to set up a separate data transmission path for each user; or, to use Broadcast mode, which is to send messages to all users in the network, and they will receive the Broadcast messages no matter they need or not. For example, if there are 200 users in a network who want to receive the same packet, then the traditional solution is to send this packet for 200 times separately via Unicast to guarantee the users who need the data can get all data wanted, or send the data in the entire domain via Broadcast. Transferring the data in the whole range of network .The users who need these data can get directly from the network. Both modes waste a great deal of valuable bandwidth resource, and furthermore, Broadcast mode goes against the security and secrecy.

The emergence of IP Multicast technology solved this problem in time. The Multicast source only sends out the message once, Multicast Routing Protocol sets up tree-routing for Multicast data packet, and then the transferred packet just starts to be duplicated and distributed in the bifurcate crossing as far as possible. Thus the packet can be sent to every user who needs it accurately and effectively.

It should be noticed that it is not necessary for Multicast source to join in Multicast group. It sends data to some Multicast groups, but it is not necessarily a receiver of the group itself. There can be more than one source sending packets to a Multicast group simultaneously. There may exist routers in the network which do not support Multicast, but a Multicast router can encapsulate the Multicast packets into Unicast IP packets with tunnel mode to send them to the Multicast router next to it, which will take off the Unicast IP header and continue the Multicast transmission process, thus a big alteration of network structure is avoided. The primary advantages of Multicast are:

1.       Enhance efficiency: reduce network traffic, lighten the load of server and CPU
2.       Optimize performance: reduce redundant traffic
3.       Distributed application: Enable Multipoint Application

## 1.1.2 Multicast Address

The destination address of Multicast message uses class D IP address with range from 224.0.0.0 to 239.255.255.255. D class address can not appear in the source IP address field of an IP message. In the process of Unicast data transmission, the transmission path of a data packet is from source address routing to destination address, and the transmission is performed with hop-by-hop principle. However, in IP Multicast environment, the destination addresses is a group instead of a single one, they form a group address. All message receivers will join in a group, and once they do, the data flowing to the group address will be sent to the receivers immediately and all members in the group will receive the data packets. The members in a Multicast group are dynamic, the hosts can join and leave the Multicast group at any time.

Multicast group can be permanent or temporary. Some of the Multicast group addresses are assigned officially; they are called Permanent Multicast Group. Permanent Multicast Group keeps its IP address fixed but its member structure can vary within. The member amount of Permanent Multicast Group can be arbitrary, even zero. The IP Multicast addresses which are not kept for use by Permanent Multicast Group can be utilized by temporary Multicast groups.

224.0.0.0 ～ 224.0.0.255 are reserved Multicast addresses (Permanent Group Address), address 224.0.0.0 is reserved but not assigned, and other addresses are used by Routing Protocol; 224.0.1.0～238.255.255.255 are Multicast addresses available to users（Temporary Group Address） and are valid in the entire domain of the network; 239.0.0.0～239.255.255.255 are local management Multicast addresses, which are valid only in specific local domain. Frequently used reserved multicast address list is as follows:

Benchmark address (reserved)
224.0.0.1 Address of all hosts
224.0.0.2 Address of all Multicast Routers
224.0.0.3 Unassigned
224.0.0.4 DVMRP Router
224.0.0.5 OSPF Router
224.0.0.6 OSPF DR
224.0.0.7 ST Router
224.0.0.8 ST host
224.0.0.9 RIP-2 Router
224.0.0.10 IGRP Router
224.0.0.11 Active Agent
224.0.0.12 DHCP Server/Relay Agent
224.0.0.13 All PIM Routers
224.0.0.14 RSVP Encapsulation
224.0.0.15 All CBT Routers
224.0.0.16 Specified SBM
224.0.0.17 All SBMS

224.0.0.18 VRRP

224.0.0.22 IGMP

When Ethernet transmits Unicast IP messages, the destination MAC address it uses is the receiver's MAC address. But in transmitting Multicast packets, the transmission destination is not a specific receiver any more, but a group with uncertain members, thus Multicast MAC address is used. Multicast MAC address is corresponding to Multicast IP address. It is prescribed in IANA (Internet Assigned Number Authority) that the higher 25 bits in Multicast MAC address is 0x01005e, and the lower 23bits in MAC address is the lower 23bits in Multicast IP address.

Since only 23bits out of the lower 28bits in IP Multicast address are mapped into MAC address, therefore there are 32 IP Multicast addresses which are mapped into the same MAC address.

## 1.1.3 IP Multicast Packet Transmission

In Multicast mode, the source host sends packets to the host group indicated by the Multicast group address in the destination address field of IP data packet. Unlike Unicast mode, Multicast data packet must be forwarded to a number of external interfaces to be sent to all receiver sites in Multicast mode, thus Multicast transmission procedure is more complicated than Unicast transmission procedure.

In order to guarantee that all Multicast packets get to the router via the shortest path, the receipt interface of the Multicast packet must be checked in some certain way based on Unicast router table; this checking mechanism is the basis for most Multicast Routing Protocol to forward in Multicast mode --- RPF (Reverse Path Forwarding) check. Multicast router makes use of the impressed packet source address to query Unicast Router Table or independent Multicast Router Table to determine if the packet ingress interface is on the shortest path from receipt site to source address. If shortest path Tree is used, then the source address is the address of source host which sends Multicast Data Packets; if Shared Tree is used, then the source address is the address of the root of the Shared-Tree. When Multicast data packet gets to the router, if RPF check passes, then the data packet is forwarded according to Multicast forward item, and the data packet will be discarded else wise.

## 1.1.4 IP Multicast Application

IP Multicast technology has effectively solved the problem of sending in single point and receiving in multipoint. It has achieved the effective data transmission from a point to multiple points, saved a great deal of network bandwidth and reduced network load. Making use of the Multicast property of network, some new value-added operations can be supplied conveniently. In Information Service areas such as online living broadcast, network TV, remote education, remote medicine, real time video/audio meeting, the following applications may be supplied:

1) Application of Multimedia and Streaming Media

2)    Data repository, finance application (stock) etc

3)    Any data distribution application of "one point to multiple points"

In the situation of more and more multimedia operations in IP network, Multicast has tremendous market potential and Multicast operation will be generalized and popularized.

# 1.2 IGMP

# 1.2.1 Introduction to IGMP

IGMP (Internet Group Management Protocol) is the protocol in TCP/IP protocol family which is responsible for IP multicast member management. It is used to set up and maintain multicast group member relationship between IP host and its neighbor multicast switches. IGMP does not include the spread and maintenance of relation information of group members among multicast switches, this work is accomplished by each multicast routing protocol. All hosts participating in multicast must implement IGMP protocol.

Hosts participating IP multicast can join in and exit multicast group at any location, any time and without limit of member total. Multicast switch does not need and not likely to save all relationships of all hosts. It only gets to know if there are receivers of some multicast group, i.e. group member, on the network segment each interface connects to. And the host only needs to save which multicast groups it joined.

IGMP is asymmetric between host and router: the host needs to respond the IGMP query messages of multicast switches, i.e. to report message response in membership; the switch sends out membership query messages periodically, and then determine if there are hosts of some specific group joining in the sub-network it belongs to based on the received response message, and send out query of specific group (IGMP version2) when receiving the report of a host exiting the group to determine if there exists no member in some specific group.

Up to now, there are three versions of IGMP: IGMP version1 (defined by RFC1112), IGMP version2 (defined by RFC2236) and IGMP version3 (defined by RFC3376).

The main improvements of IGMP version2 over version1 are:

1. The election mechanism of multicast switches on the shared network segment

Shared network segment is the situation of there is more than one multicast switch on a network segment. Under this kind of situation, since all switches which runs IGMP under this network segment can get membership report message from the host, therefore, only one switch is required to transmit membership query message, so an exchange election mechanism is required to determine a switch as query machine. In IGMP version1, the selection of query machine is determined by Multicast Routing Protocol; IGMP version2 made an improvement for it, it prescribed that when there are more than one multicast switches on the same network segment, the multicast switch with the lowest IP address will be elected as the query machine.

2. IGMP version2 added Leave Group Mechanism

In IGMP version 1, the host leaves the multicast group silently without sending any notification to any multicast switch. This causes that the multicast switch can only determine the leave of multicast member by multicast group response time-out. But in version2, when a host decides to leave a multicast group, if it is the host which gives response to the latest membership query message, then it will send out a message implying it is leaving.

3. IGMP version 2 added the query to specific group

In IGMP version1, a query of multicast switch is for all multicast groups on the network segment. This query is called general group query. In IGMP version2, query of specific group is added besides general group query. The destination IP address of this kind of query message is the IP address of the multicast group, the group address field part of the message is also the IP address of the multicast group. Thus it is prevented that hosts which are other multicast group members transmit response message.

4. IGMP version2 added the biggest response time field

IGMP version2 added the biggest response time field to dynamically adjust the response time of the host to group query message.

The main features of version3 is allowing the host to choose receiving from or rejecting a certain source, which is the basis of SSM （Source-Specific Multicast）multicast. For example, when a host is sending a report of INCLUDE{10.1.1.1, 10.1.1.2} to some group G, that means the host needs the router to forward the flux from 10.1.1.1 and 10.1.1.2; when a host is sending a report of EXCLUDE{192.168.1.1} to some group G, that means the host needs the flux from all sources of group G except 192.168.1.1. This makes a great difference from the previous IGMP.

The main improvements of IGMP Version3 over IGMP Version1 and Version2 are:

1.  The status to be maintained is group and source list, not only the groups in IGMPv2.
2.  The interoperations with IGMPv1 and IGMPv2 are defined in IGMPv3 status.
3.  IP service interface is modified to allow specific source list thereby.
4.  The queried includes his/her Robustness Variable and Query Interval in query group to allow the synchronization with these variables of non-queries.
5.  Max Response Time in Query Message has an exponential range, with maximum value from 25.5 secs of v2 to 53 mins, which can be used in links of great capacity.
6.  In order to increase strength, the host retransmits State-Change message.
7.  Additional data is defined to adapt future extension.
8.  Report group is sent to 224.0.0.22 to help with IGMP Snooping of Layer 2 Switch.
9.  Report group can include more than one group record, and it allows using small group to report complete current status.
10. The host does not restrain operation any more, which simplifies the implement and allows direct membership trace.
11. In querying messages, the new router side restraint process (S sign) modified the existing strength of IGMPv2.

# 1.2.2 IGMP Configuration Task List

1．Enable IGMP (Required)
2．Configure IGMP sub-parameters (Optional)
    (1) Configure IGMP group parameters
        1) Configure IGMP group filtering conditions
        2) Configure IGMP to join in group
        3) Configure IGMP to join in static group
    (2) Configure IGMP query parameters
        1) Configure the interval of IGMP sending query message
        2) Configure the maximum response time of IGMP query
        3) Configure time-out of IGMP query
    (3) Configure IGMP version
3．Disable IGMP Protocol

**1. Enable IGMP Protocol**

    There are not specific commands for enabling IGMP Protocol on the Layer 3 switch. Enabling any multicast protocol under corresponding interface will automatically enable IGMP.

| Command | Explanation |
| --- | --- |
| Global Mode | |
| **ip dvmrp multicast-routing \| ip pim multicast-routing** | To enable global multicast protocol is the prerequisite to enable IGMP protocol, the "**no ip dvmrp multicast-routing \| no ip pim multicast-routing**" commands disable multicast protocol and IGMP protocol. (Required) |

| Command | Explanation |
| --- | --- |
| Interface Configuration Mode | |
| **ip dvmrp enable\| ip pim dense-mode \| ip pim sparse-mode** | Enable IGMP Protocol, the corresponding commands "**no ip dvmrp enable\| no ip pim dense-mode \| no ip pim sparse-mode**" disable IGMP Protocol. (Required) |

**2. Configure IGMP Sub-parameters**
   **（1）Configure IGMP group parameters**
        1) Configure IGMP group filtering conditions
        2) Configure IGMP to join in group
        3) Configure IGMP to join in static group

| Command | Explanation |
| --- | --- |
| Interface Configuration Mode | |

| | |
|---|---|
| **ip igmp access-group {<*acl_num* \| *acl_name*>}**<br>**no ip igmp access-group** | Configure the filtering conditions of the interface to IGMP group; the "**no ip igmp access-group**" command cancels the filtering condition. |
| **ip igmp join-group <*A.B.C.D* >**<br>**no ip igmp join-group <*A.B.C.D* >** | Configure the interface to join in some IGMP group, the "**no ip igmp join-group <*A.B.C.D* >**" command cancels the join. |
| **ip igmp static-group <*A.B.C.D* >**<br>**no ip igmp static-group <*A.B.C.D*>** | Configure the interface to join in some IGMP static group; the "**no ip igmp static-group <*A.B.C.D* >**" command cancels the join. |

(2) **Configure IGMP Query parameters**
   1) Configure interval for IGMP to send query messages
   2) Configure the maximum response time of IGMP query
   3) Configure the time-out of IGMP query

| Command | Explanation |
|---|---|
| Interface Configuration Mode | |
| **ip igmp query-interval <*time_val*>**<br>**no ip igmp query-interval** | Configure the interval of IGMP query messages sent periodically; the "**no ip igmp query-interval**" command restores default value. |
| **ip igmp query-max-response-time <*time_val*>**<br>**no ip igmp query-max-response-time** | Configure the maximum response time of the interface for IGMP query; the "**no ip igmp query-max-response-time**" command restores default value. |
| **ip igmp query-timeout <*time_val*>**<br>**no ip igmp query-timeout** | Configure the time-out of the interface for IGMP query; the "**no ip igmp query-timeout**" command restores default value. |

(3) **Config IGMP version**

| Command | Explanation |
|---|---|
| Global Mode | |
| **ip igmp version <*version*>**<br>**no ip igmp version** | Configure IGMP version on the interface; the "**no ip igmp version**" command restores the default value. |

3. **Disable IGMP Protocol**

| Command | Explanation |
|---|---|
| Interface Configuration Mode | |
| **no ip dvmrp \| no ip pim dense-mode \| no ip pim sparse-mode \| no ip dvmrp multicast-routing \| no ip pim multicast-routing** | Disable IGMP Protocol. |

## 1.2.3 IGMP Configuration Examples

As shown in the following figure, add the Ethernet ports of Switch A and Switch B to corresponding VLAN, and start PIM-DM on each VLAN interface.
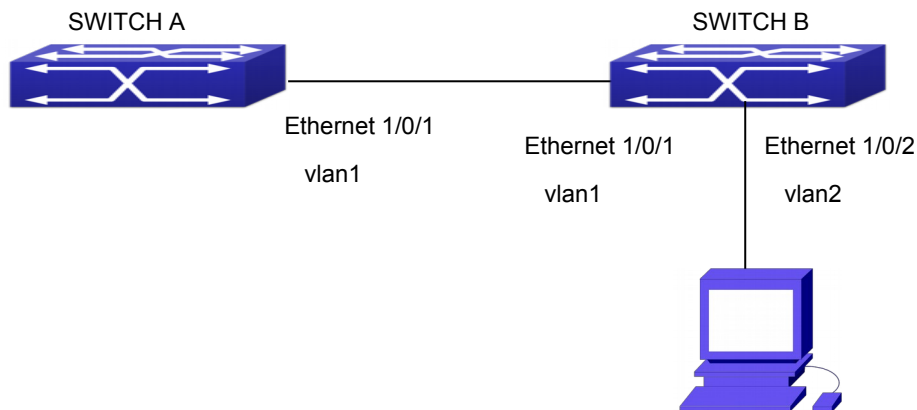


Fig 1-1 IGMP Network Topology Diagram

The configuration procedure for SwitchA and SwitchB is as follows:
(1) Configure SwitchA:
Switch(config)#ip pim multicast-routing
Switch (config)#interface vlan 1
Switch(Config-if-Vlan1)#ip address 12.1.1.1 255.255.255.0
Switch(Config-if-Vlan1)#ip pim dense-mode
(2) Configure SwitchB:
Switch(config)#ip pim multicast-routing
Switch(config)#interface vlan1
Switch(Config-if-Vlan1)#ip address 12.1.1.2 255.255.255.0
Switch(Config-if-Vlan1)#ip pim dense-mode
Switch(Config-if-Vlan1)#exit
Switch(config)#interface vlan2
Switch(Config-if-Vlan1)#ip address 20.1.1.1 255.255.255.0
Switch(Config-if-Vlan2)#ip pim dense-mode
Switch(Config-if-Vlan2)#ip igmp version 3

## 1.2.4 IGMP Troubleshooting

In configuring and using IGMP Protocol, IGMP Protocol might not operate normally caused by physical connection or incorrect configuration. Therefore, user should pay attention to the following issues:
☞  Firstly to assure that physical connection is correct;

- Next, to assure the Protocol of Interface and Link protocol is UP (use show interface command);
- Afterwards, to assure to start a kind of multicast protocol on the interface;
- Multicast Protocol requires RPF Check using unicast routing; therefore the correctness of unicast routing must be assured beforehand.

# 1.3 IGMP Snooping

## 1.3.1 Introduction to IGMP Snooping

IGMP (Internet Group Management Protocol) is a protocol used in IP multicast. IGMP is used by multicast enabled network device (such as a router) for host membership query, and by hosts that are joining a multicast group to inform the router to accept packets of a certain multicast address. All those operations are done through IGMP message exchange. The router will use a multicast address (224.0.0.1) that can address to all hosts to send an IGMP host membership query message. If a host wants to join a multicast group, it will reply to the multicast address of that a multicast group with an IGMP host membership reports a message.

IGMP Snooping is also referred to as IGMP listening. The switch prevents multicast traffic from flooding through IGMP Snooping, multicast traffic is forwarded to ports associated to multicast devices only. The switch listens to the IGMP messages between the multicast router and hosts, and maintains multicast group forwarding table based on the listening result, and can then decide to forward multicast packets according to the forwarding table.

Switch provides IGMP Snooping and is able to send a query from the switch so that the user can use switch in IP multicast.

## 1.3.2 IGMP Snooping Configuration Task List

1. Enable IGMP Snooping
2. Configure IGMP Snooping

**1. Enable IGMP Snooping**

| Command | Explanation |
|---|---|
| Global Mode | |
| **ip igmp snooping**<br>**no ip igmp snooping** | Enables IGMP Snooping. The no operation disables IGMP Snooping function. |

**2. Configure IGMP Snooping**

| Command | Explanation |
|---|---|

| Global Mode | |
|---|---|
| **ip igmp snooping vlan *<vlan-id>*** <br> **no ip igmp snooping vlan *<vlan-id>*** | Enables IGMP Snooping for specified VLAN. The no operation disables IGMP Snooping for specified VLAN. |
| **ip igmp snooping proxy** <br> **no ip igmp snooping proxy** | Enable IGMP Snooping proxy function, the no command disables the function. |
| **ip igmp snooping vlan < *vlan-id* > limit {group *<g_limit>* \| source *<s_limit>*}** <br> **no ip igmp snooping vlan < *vlan-id* > limit** | Configure the max group count of vlan and the max source count of every group. The "no **ip igmp snooping vlan *<vlan-id>* limit"** command cancels this configuration. |
| **ip igmp snooping vlan <1-4094> interface (ethernet \| port-channel\|) IFNAME limit {group <1-65535>\| source <1-65535>} strategy (replace \| drop)** <br> **no ip igmp snooping vlan <1-4094> interface (ethernet \| port-channel\|) IFNAME limit group source strategy** | Configure the number of groups which are allowed joining and the maximum of the source in each group under the IGMP Snooping port. Configure the strategy when it is up to the upper limit, including "replace" and "drop". No command configures as "no limitation". |
| **ip igmp snooping vlan *<vlan-id>* l2-general-querier** <br> **no ip igmp snooping vlan *<vlan-id>* l2-general-querier** | Set this vlan to layer 2 general querier. It is recommended to configure a layer 2 general querier on a segment. The "no **ip igmp snooping vlan *<vlan-id>* l2-general-querier"command** cancels this configuration. |
| **ip igmp snooping vlan *<vlan-id>* l2-general-querier-version <version>** | Configure the version number of a general query from a layer 2 general querier. |
| **ip igmp snooping vlan *<vlan-id>* l2-general-querier-source <source>** | Configure the source address of a general query from a layer 2 general querier. |
| **ip igmp snooping vlan *<vlan-id>* mrouter-port interface *<interface – name>*** <br> **no ip igmp snooping vlan *<vlan-id>* mrouter-port interface *<interface – name>*** | Configure static mrouter port of vlan. The no form of the command cancels this configuration. |
| **ip igmp snooping vlan *<vlan-id>* mrouter-port learnpim** <br> **no ip igmp snooping vlan *<vlan-id>* mrouter-port learnpim** | Enable the function that the specified VLAN learns mrouter-port (according to pim packets), the no command will disable the function. |
| **ip igmp snooping vlan *<vlan-id>* mrpt *<value >*** <br> **no ip igmp snooping vlan *<vlan-id>* mrpt** | Configure this survive time of mrouter port. The "no **ip igmp snooping vlan *<vlan-id>* mrpt"** command restores the default value. |

| | |
|---|---|
| **ip igmp snooping vlan <*vlan-id*> query-interval <*value*>**<br>**no ip igmp snooping vlan <*vlan-id*> query-interval** | Configure this query interval. The "no **ip igmp snooping vlan <*vlan-id*> query-interval**" command restores the default value. |
| **ip igmp snooping vlan <*vlan-id*> immediately-leave**<br>**no ip igmp snooping vlan <*vlan-id*> immediately-leave** | Enable the IGMP fast leave function for the specified VLAN: the "no **ip igmp snooping vlan <*vlan-id*> immediate-leave**" command disables the IGMP fast leave function. |
| **ip igmp snooping vlan <*vlan-id*> query-mrsp <*value*>**<br>**no ip igmp snooping vlan <*vlan-id*> query-mrsp** | Configure the maximum query response period. The "no **ip igmp snooping vlan <*vlan-id*> query-mrsp**" command restores to the default value. |
| **ip igmp snooping vlan <*vlan-id*> query-robustness <*value*>**<br>**no ip igmp snooping vlan <*vlan-id*> query-robustness** | Configure the query robustness. The "no **ip igmp snooping vlan <*vlan-id*> query-robustness**" command restores to the default value. |
| **ip igmp snooping vlan <*vlan-id*> suppression-query-time <*value*>**<br>**no ip igmp snooping vlan <*vlan-id*> suppression-query-time** | Configure the suppression query time. The "no **ip igmp snooping vlan <*vlan-id*> suppression-query-time**" command restores to the default value. |
| **ip igmp snooping vlan <*vlan-id*> static-group <*A.B.C.D*> [source <*A.B.C.D*>] interface [ethernet | port-channel] <*IFNAME*>**<br>**no ip igmp snooping vlan <*vlan-id*> static-group <*A.B.C.D*> [source <*A.B.C.D*>] interface [ethernet | port-channel] <*IFNAME*>** | Configure static-group on specified port of the VLAN. The no form of the command cancels this configuration. |
| **ip igmp snooping vlan <*vlan-id*> report source-address <*A.B.C.D*>**<br>**no ip igmp snooping vlan <*vlan-id*> report source-address** | Configure forwarding IGMP packet source address, The no operation cancels the packet source address. |
| **ip igmp snooping vlan <*vlan-id*> specific-query-mrsp <value>**<br>**no ip igmp snooping vlan <*vlan-id*> specific-query-mrspt** | Configure the maximum query response time of the specific group or source, the no command restores the default value. |

# 1.3.3 IGMP Snooping Examples
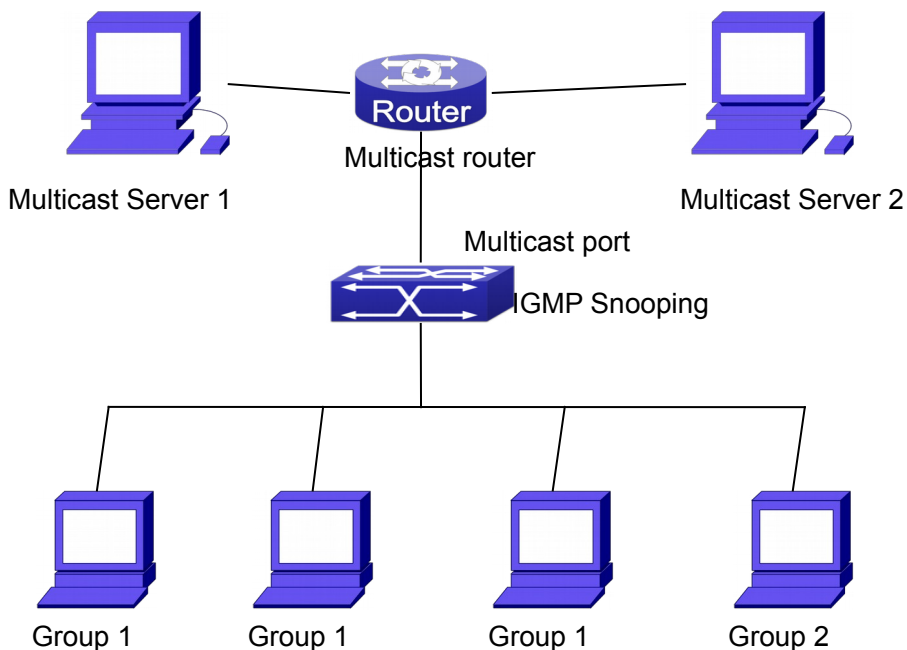
**Scenario 1:** IGMP Snooping function



Fig 1-2 Enabling IGMP Snooping function

Example: As shown in the above figure, a VLAN 100 is configured in the switch and includes ports 1, 2, 6, 10 and 12. Four hosts are connected to port 2, 6, 10 and 12 respectively and the multicast router is connected to port 1. As IGMP Snooping is disabled by default either in the switch or in the VLANs, If IGMP Snooping should be enabled in VLAN 100, the IGMP Snooping should be first enabled for the switch in Global Mode and in VLAN 100 and set port 1 of VLAN 100 to be the mrouter port.

The configuration steps are listed below:
Switch(config)#ip igmp snooping
Switch(config)#ip igmp snooping vlan 100
Switch(config)#ip igmp snooping vlan 100 mrouter interface ethernet 1/0/1

**Multicast Configuration**
Suppose two programs are provided in the Multicast Server using multicast address Group1 and Group2, three of four hosts running multicast applications are connected to port 2, 6, 10 plays program1, while the host is connected to port 12 plays program 2.
**IGMP Snooping listening result:**
The multicast table built by IGMP Snooping in VLAN 100 indicates ports 1, 2, 6, 10 in Group1 and ports 1, 12 in Group2.
All the four hosts can receive the program of their choice: ports 2, 6, 10 will not receive the traffic of program 2 and port 12 will not receive the traffic of program 1.
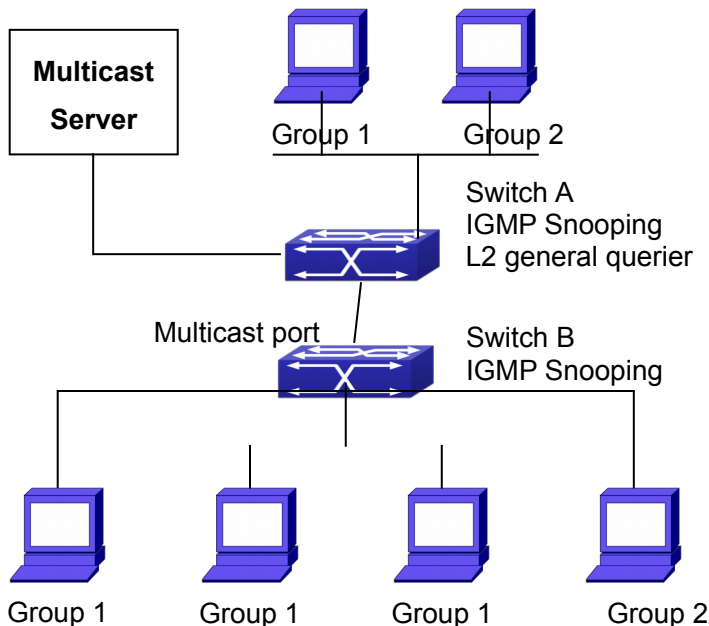
**Scenario 2:** L2-general-querier



Fig 1-3 The switches as IGMP Queries

The configuration of Switch2 is the same as the switch in scenario 1, SwitchA takes the place of Multicast Router in scenario 1. Let's assume VLAN 60 is configured in SwitchA, including ports 1, 2, 10 and 12. Port 1 connects to the multicast server, and port 2 connects to Switch2. In order to send Query at regular interval, IGMP query must enabled in Global mode and in VLAN60.

**The configuration steps are listed below:**
SwitchA#config
SwitchA(config)#ip igmp snooping
SwitchA(config)#ip igmp snooping vlan 60
SwitchA(config)#ip igmp snooping vlan 60 L2-general-querier

SwitchB#config
SwitchB(config)#ip igmp snooping
SwitchB(config)#ip igmp snooping vlan 100
SwitchB(config)#ip igmp snooping vlan 100 mrouter interface ethernet 1/0/1

**Multicast Configuration**
The same as scenario 1
**IGMP Snooping listening result:**
Similar to scenario 1

**Scenario 3:** To run in cooperation with layer 3 multicast protocols.

SWITCH which is used in Scenario 1 is replaced with ROUTER with specific configurations remains the same. And multicast and IGMP snooping configurations are the same with what it is in Scenario 1. To configure PIM-SM on ROUTER, and enable PIM-SM on vlan 100 (use the same PIM mode with the connected multicast router)

Configurations are listed as below:
switch#config
switch(config)#ip pim multicast-routing
switch(config)#interface vlan 100
switch(config-if-vlan100)#ip pim sparse-mode

IGMP snooping does not distribute entries when layer 3 multicast protocol is enabled. It only does the following tasks.
⊐    Remove the layer 2 multicast entries.
⊓    Provide query functions to the layer 3 with vlan, S, and G as the parameters.
⊓    When layer 3 IGMP is disabled, re-enable distributing layer 2 multicast entries.

By looking up the layer 3 IPMC entries, it can be found that ports can be indicated by the layer 3 multicast entries. This ensures the IGMP snooping can work in cooperation with the layer 3 multicast protocols.

# 1.3.4 IGMP Snooping Troubleshooting

On IGMP Snooping function configuration and usage, IGMP Snooping might not run properly because of physical connection or configuration mistakes. So the users should note that:
⊐    Make sure correct physical connection
⊐    Activate IGMP Snooping on whole configuration mode (use **ip igmp snooping**)
⊐    Configure IGMP Snooping at VLAN on whole configuration mode ( use **ip igmp snooping vlan <vlan-id>**)
⊐    Make sure one VLAN is configured as L2 common checker in same mask, or make sure configured static mrouter
⊐    Use **show ip igmp snooping vlan <vid>** command check IGMP Snooping information

# 1.4 IGMP Proxy Configuration

# 1.4.1 Introduction to IGMP Proxy

IGMP/MLD proxy which is introduced in rfc4605, is a simplified multicast protocol running at edge boxes. The edge boxes which runs the IGMP/MLD proxy protocol, does

not need to run complicated multicast routing protocols such as PIM/DVMRP. However they work with multicast protocol enabled network through IGMP/MLD proxy. They can simplify the implementation of multicasting on edge devices.

The IGMP/MLD proxy works between the multicast router and the client, it works as both the multicast host and router. Upstream and downstream ports should be specified in the IGMP/MLD proxy configuration. The host protocol runs at upstream ports, while the router protocol runs at downstream ports. The switch collects the join and leave messages received from downstream ports and forward them to the multicast router through upstream ports.

The IGMP proxy configuration is exclusive with PIM and DVMRP configuration.

# 1.4.2 IGMP Proxy Configuration Task List

1. Enable IGMP Proxy function
2. Enable configurations for both downstream and upstream ports for the IGMP Proxy in different interfaces
3. Configure IGMP Proxy

**1. Enable IGMP Proxy function**

| Command | Explanation |
|---|---|
| Global Mode | |
| **ip igmp proxy**<br>**no ip igmp proxy** | Enable IGMP Proxy function. The "**no ip igmp proxy**" disables this function. |

**2. Enable configurations for both downstream and upstream ports for the IGMP Proxy in different interfaces**

| Command | Explanation |
|---|---|
| Interface Configuration Mode | |
| **ip igmp proxy upstream**<br>**no ip igmp proxy upstream** | Enable IGMP Proxy upstream function. The "**no ip igmp proxy upstream**" disables this function. |
| **ip igmp proxy downstream**<br>**no ip igmp proxy downstream** | Enable IGMP Proxy downstream function. The "**no ip igmp proxy downstream**" disables this function. |

**3. Configure IGMP Proxy assistant parameter**

| Command | Explanation |
|---|---|
| Global Mode | |
| **ip igmp proxy limit {group <1-500>\|**<br>**source <1-500>}**<br>**no ip igmp proxy limit** | To configure the maximum number of groups that upstream ports can join, and the maximum number of sources in a |

| | single group. The no form of this command will restore the default value. |
|---|---|
| **ip igmp proxy unsolicited-report interval** *<1-5>*<br>**no ip igmp proxy unsolicited-report interval** | To configure how often the upstream ports send out unsolicited report. The no form of this command will restore the default configuration. |
| **ip igmp proxy unsolicited-report robustness** *<2-10>*<br>**no ip igmp proxy unsolicited-report robustness** | To configure the retry times of upstream ports' sending unsolicited reports. The no form of this command will restore the default value. |
| **ip igmp proxy aggregate**<br>**no ip igmp proxy aggregate** | To configure non-query downstream ports to be able to aggregate the IGMP operations. The no form of this command will restore the default configuration. |
| **ip multicast ssm range** *<1-99>*<br>**ip multicast ssm default**<br>**no ip mulitcast ssm** | To configure the address range for IGMP proxy ssm multicast groups; The no form of this command will remove the configuration. |
| **ip igmp proxy multicast-source**<br>**no ip igmp proxy multicast-source** | To configure the port as downstream ports for the source of multicast datagram; The no from of this command will disable the configuration. |

# 1.4.3 IGMP Proxy Examples
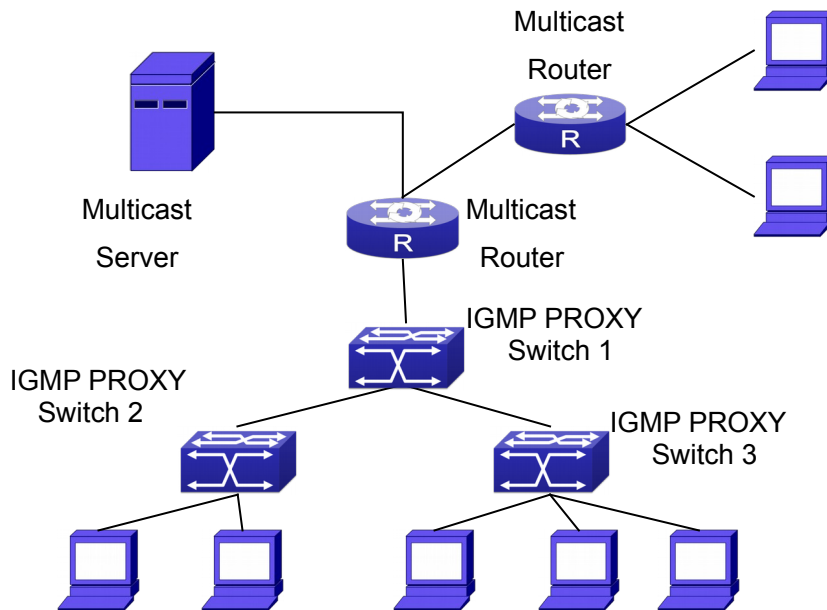
**Example 1:** IGMP Proxy function.

Fig 1-4 IGMP Proxy Topology Diagram

As it is show in the figure above, the switch functions as IGMP Proxy in a network of topology of tree, the switch aggregates the multicast dataflow from upstream port and redistributes them to the downstream ports, while the IGMP membership reports flow from downstream ports to upstream ports. Three IGMP Proxy enabled switches which are connected in tree topology, respectively have one port connected to multicast routers, and no less than one ports connected to hosts or upstream ports from other IGMP Proxy enabled switches.

**The configuration steps are listed below:**
Switch#config
Switch(config)#ip igmp proxy
Switch(Config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp proxy upstream
Switch(Config)#interface vlan 2
Switch(Config-if-Vlan2)#ip igmp proxy downstream

**Multicast Configuration:**
Suppose the multicast server offers some programs through 224.1.1.1. Some hosts subscribe that program at the edge of the network. The IGMP multicast members report themselves to the downstream ports of IGMP Proxy enabled Switch 2 and Switch 3. Switch 2 and Switch 3 then aggregate the group membership information and send them through the upstream ports. Switch 1 finally forward these membership information to the multicast router when receiving the group membership information through upstream

ports, and deliver the multicast dataflow through downstream ports.

**Example2:** IGMP Proxy for multicast sources from downstream ports.
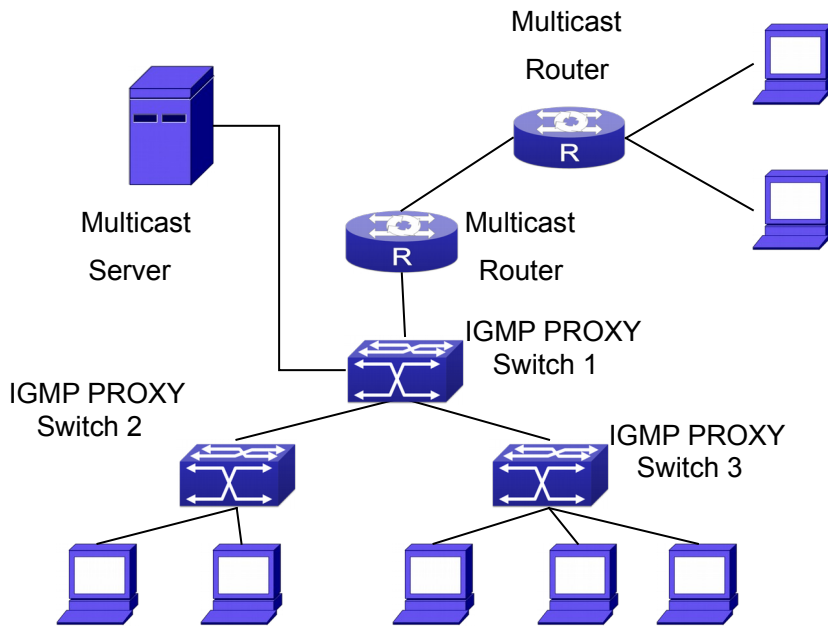


Fig 1-5 IGMP Proxy for multicast sources from downstream ports

As it is show in the figure above, IGMP Proxy enabled switches connected to the network in tree topology. The multicast source server connects to the downstream port of Switch1, the multicast dataflow is distributed through the upstream port and other downstream ports. Three IGMP Proxy enabled switches which are connected in tree topology, respectively have one port connected to multicast routers, and no less than one ports connected to hosts or upstream ports from other IGMP proxy enabled switches.

**The configuration steps are listed below:**
IGMP PROXY Switch1 configuration：
Switch#config
Switch(config)#ip igmp proxy
Switch(Config)#interface vlan 1
Switch(Config-if-Vlan1)#ip igmp proxy upstream
Switch(Config)#interface vlan 2
Switch(Config-if-Vlan2)#ip igmp proxy downstream
Switch(Config-if-Vlan2)#ip igmp proxy multicast-source
Route1 configuration:
Switch#config
Switch(config)#ip pim multicast
Switch(Config)#interface vlan 1
Switch(Config-if-Vlan1)#ip pim sparse-mode

Switch(Config-if-Vlan1)#ip pim bsr-border

**Multicast Configuration:**

Suppose the server provides programs through the multicast address 224.1.1.1, and some hosts subscribe that program on the edge of the network. The host reports their IGMP multicast group membership to Switch 2 and Switch 3 through downstream ports. Switch 2 and Switch 3 then aggregate and forward them to Switch 1 which then forwards the information to multicast router. When multicast dataflow arrives, the IGMP Proxy enabled switches re-distribute the group membership through upstream ports and downstream ports. When the multicast router receives the multicast dataflow from IGMP proxy, it will consider the multicast data source is directly connected to the router, and determine the identity of DR and ORIGINATOR. The multicast dataflow will be redistributed according to the PIM protocol.

# 1.4.4 IGMP Proxy Troubleshooting

When IGMP Proxy function configuration and usage, IGMP Proxy might not run properly because of physical connection or configuration mistakes. So the users should note that:
- Make sure physical connection correctly;
- Activate IGMP Proxy on whole Global mode (use **ip igmp proxy**);
- Make sure configure one upstream port and at least one downstream port under interface configuration mode (Use **ip igmp proxy upstream**, **ip igmp proxy downstream**);
- Use **show ip igmp proxy** command to check if the IGMP Proxy information is correct.

If the IGMP Proxy problem remains unsolved, please use debug IGMP Proxy and other debugging command and copy the DEBUG message within three minutes, send the recorded message to the technical service center of our company.

# Chapter 2 IPv6 Multicast Protocol

## 2.1 MLD

### 2.1.1 Introduction to MLD

MLD (Multicast Listener Discovery) is the multicast group member (receiver) discovery protocol serving IPv6 multicast. It is similar to IGMP Protocol in IPv4 multicast application. Correspondingly, MLD Protocol version1 is similar to IGMP Protocol version2, and MLD Protocol version2 is similar to IGMP Protocol version3. Current firmware  supports MLDv1/ MLDv2.

The IPv6 multicast hosts can join or leave from multicast group at any location, any time, regardless of the total number of group members. It is unnecessary and impossible for multicast switch to store the relationship among all host members. Multicast switch simply finds out via MLD protocol if there are receivers of certain multicast group on the network segment connected to each port. The only thing host need to do is to keep the record of which multicast groups it joined.

MLD is unsymmetrical between host and switch: the host needs to respond the MLD query message of multicast switch with membership report message; the switch periodically sends membership query message and determines if there is host joining a specific group in its subnetworks according to the response message received, and after it receives the report of a host quitting from the group, it sends out the query for the group to confirm if there is no member left in it.

There are three types of protocol messages of MLD Protocol, that is, Query, Report and Done (which is corresponding to Leave of IGMPv2). Like IGMPV2, the Query messages include General Query and Specific Group Query. General Query uses the multicast address FF02::1 of hosts as destination address, the group address is 0; and Specific Group Query use its group address as destination address. The multicast addresses of MLD use 130, 131 and 132 as data types denoting the three kinds of messages mentioned above. Other logic is basically same as IGMPv2.
MLD protocol version2 use FF02::16 as destination address of membership report, and 143 as data type. The other logic of MLD Protocol version2 is similar to IGMP Protocol version3.

### 2.1.2 MLD Configuration Task List

1、 Start MLD (Required)
2、 Configure MLD auxiliary parameters (Required)
    （1）Configure MLD group parameters
        1）Configure MLD group filter conditions

(2) Configure MLD query parameters

    1) Configure the interval of MLD sending query message

    2) Configure the maximum response time of MLD query

    3) Configure overtime of MLD query

3、Shut down MLD Protocol

**1. Start MLD Protocol**

There is no special command for starting MLD Protocol on EDGECORE series layer 3 switches. MLD Protocol will automatically start up as long as any IPv6 multicast protocol is started on corresponding interface.

| Command | Explanation |
| --- | --- |
| Global Mode | |
| **Ipv6 pim multicast-routing** | To start Global IPv6 Multicast Protocol, the precondition of starting MLD Protocol. The NO operation of corresponding command shuts ipv6 multicast protocol and MLD Protocol. (Required) |

| Command | Explanation |
| --- | --- |
| Port Configuration Mode | |
| **ipv6 pim dense-mode | ipv6 pim sparse-mode** | Start MLD Protocol. The NO operation of corresponding command shuts MLD Protocol. (Required) |

**2. Configure MLD auxiliary parameters**

**(1) Configure MLD group parameters**

  1) Configure MLD group filter conditions

| Command | Explanation |
| --- | --- |
| Port Configuration Mode | |
| **ipv6 mld access-group**   *<acl_name>* **no ipv6 mld access-group** | Configure the filter conditions of interface for MLD group; the NO operation of this command cancels filter conditions. |

**(2) Configure MLD Query parameters**

  1) Configure interval time for MLD to send query messages

  2) Configure the maximum response time of MLD query

  3) Configure the overtime of MLD query

| Command | Explanation |
| --- | --- |
| Port Configuration Mode | |
| **ipv6 mld query-interval** *<time_val>* **no ipv6 mld query-interval** | Configure the interval of MLD query messages sent periodically; the NO operation of this command restores the default value. |

| | |
|---|---|
| **ipv6 mld query-max-response-time <*time_val*>**<br>**no ipv6 mld query-max-response-time** | Configure the maximum response time of the interface for MLD query; the NO operation of this command restores the default value. |
| **ipv6 mld query-timeout <*time_val*>**<br>**no ipv6 mld query-timeout** | Configure the overtime of the interface for MLD query; the NO operation of this command restores the default value. |

3. **Shut down MLD Protocol**

| Command | Explanation |
|---|---|
| Port Configuration Mode | |
| **no ipv6 pim dense-mode \| no ipv6 pim sparse-mode \| no ipv6 pim multicast-routing (Global Mode)** | Shut down MLD Protocol |

# 2.1.3 MLD Typical Application

As shown in the following figure, add the Ethernet interfaces of Switch A and Switch B to corresponding vlan, and start PIM6 on each vlan interface.
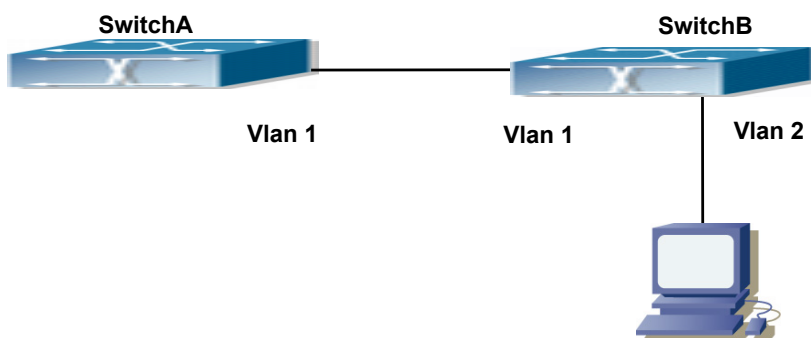


Fig 2-1 Network Topology Diagram

The configuration procedure for SwitchA and SwitchB is as below:
(1) Configure SwitchA:
Switch (config) #ipv6 pim multicast-routing
Switch (config) #ipv6 pim rp-address 3FFE::1
Switch (config) #interface vlan 1
Switch (Config-if-Vlan1) #ipv6 address 3FFE::1/64
Switch (Config-if-Vlan1) #ipv6 pim sparse-mode
(2) Configure SwitchB:
Switch (config) #ipv6 pim multicast-routing
Switch (config) #ipv6 pim rp-address 3FFE::1
Switch (config) #interface vlan1
Switch (Config-if-Vlan1) #ipv6 address 3FFE::2/64

Switch (Config-if-Vlan1) #ipv6 pim sparse-mode
Switch (Config-if-Vlan1) #exit
Switch (config) #interface vlan2
Switch (Config-if-Vlan2) #ipv6 address 3FFA::1/64
Switch (Config-if-Vlan2) #ipv6 pim sparse-mode
Switch (Config-if-Vlan2) #ipv6 mld query-timeout 150

# 2.1.4 MLD Troubleshooting Help

When configuring and using MLD protocol, MLD protocol may fail to work normally due to physical connections, incorrect configuration and so on. So, users shall note the following points:
- Assure the physical connection is correct.
- Assure the protocol of interface and link is UP (use show interface command)
- Assure to start one kind of multicast protocol on the interface
- Assure the time of the timers of each router on the same network segment is consistent; usually we recommend the default setting.
- Unicast route shall be used to carry out RPF examination for multicast protocol. So the correctness of unicast route shall be guaranteed above all.

If all attempts fail to solve the problems on MLD, please use debug commands such as debug ipv6 MLD event/packet, and copy DEBUG information in 3 minutes and send to Technology Service Center.

# 2.2 MLD Snooping

# 2.2.1 Introduction to MLD Snooping

MLD, the Multicast Listener Discovery Protocol, is used to realize multicasting in the IPv6. MLD is used by the network equipments such as routers which supports multicast for multicast listener discovery, also used by listeners looking forward to join certain multicast group informing the router to receive data packets from certain multicast address, all of which are done through MLD message exchange. First the router send an MLD Multicast listener Query message through a multicast address which can address all the listeners (namely ff02::1). Once there is a listener who wishes to join the multicast address, it will send a MLD Multicast listener Report back through the multicast address.

MLD Snooping is namely the MLD listening. The switch restricts the multicast traffic from flooding through MLD Snooping, and forward the multicast traffic to ports associated to multicast devices only. The switch listens to the MLD messages between multicast routers and listeners, and maintains the multicast group forwarding list based on the listening result. The switches forwards multicast packets according to the multicast forwarding list

The switch realizes the MLD Snooping function while supporting MLD v2. This way,

the user can acquire IPv6 multicast with the switch.

# 2.2.2 MLD Snooping Configuration Task

1. Enable the MLD Snooping function
2. Configure the MLD Snooping

**1. Enable the MLD Snooping function**

| Command | Explanation |
|---|---|
| Global Mode | |
| **ipv6 mld snooping**<br>**no ipv6 mld snooping** | Enable global MLD Snooping, the "**no ipv6 mld snooping**" command disables the global MLD snooping. |

**2. Configure MLD Snooping**

| Command | Explanation |
|---|---|
| Global Mode | |
| **ipv6 mld snooping vlan *&lt;vlan-id&gt;***<br>**no ipv6 mld snooping vlan *&lt;vlan-id&gt;*** | Enable MLD Snooping on specific VLAN. The "no" form of this command disables MLD Snooping on specific VLAN. |
| **ipv6 mld snooping vlan *&lt;vlan-id&gt;* limit {group *&lt;g_limit&gt;* | source *&lt;s_limit&gt;*}**<br>**no ipv6 mld snooping vlan *&lt;vlan-id&gt;* limit** | Configure the number of the groups in which the MLD Snooping can join, and the maximum number of sources in each group. The "no" form of this command restores to the default. |
| **ipv6 mld snooping vlan *&lt;vlan-id&gt;* l2-general-querier**<br>**no ipv6 mld snooping vlan *&lt;vlan-id&gt;* l2-general-querier** | Set the VLAN level 2 general querier, which is recommended on each segment. The "no" form of this command cancels the level 2 general querier configuration. |
| **ipv6 mld snooping vlan *&lt;vlan-id&gt;* mrouter-port interface *&lt;interface –name&gt;***<br>**no ipv6 mld snooping vlan *&lt;vlan-id&gt;* mrouter-port interface *&lt;interface –name&gt;*** | Configure the static mrouter port in specific vlan. The "no" form of this command cancels the mrouter port configuration. |
| **ipv6 mld snooping vlan *&lt;vlan-id&gt;* mrouter-port learnpim6**<br>**no ipv6 mld snooping vlan *&lt;vlan-id&gt;* mrouter-port learnpim6** | Enable the function that the specified VLAN learns mrouter-port (according to pimv6 packets), the no command will disable the function. |
| **ipv6 mld snooping vlan *&lt;vlan-id&gt;* mrpt *&lt;value&gt;***<br>**no ipv6 mld snooping vlan *&lt;vlan-id&gt;* mrpt** | Configure the keep-alive time of the mrouter port. The "no" form of this command restores to the default. |

| | |
|---|---|
| **ipv6 mld snooping vlan** *<vlan-id>* **query-interval** *<value>*<br>**no ipv6 mld snooping vlan** *<vlan-id>* **query-interval** | Configure the query interval. The "no" form of this command restores to the default. |
| **ipv6 mld snooping vlan** *<vlan-id>* **immediate-leave**<br>**no ipv6 mld snooping vlan** *<vlan-id>* **immediate-leave** | Configure immediate leave multicast group function for the MLD Snooping of specific VLAN. The "no" form of this command cancels the immediate leave configuration. |
| **ipv6 mld snooping vlan** *<vlan-id>* **query-mrsp** *<value>*<br>**no ipv6 mld snooping vlan** *<vlan-id>* **query-mrsp** | Configure the query maximum response period. The "no" form of this command restores to the default. |
| **ipv6 mld snooping vlan** *<vlan-id>* **query-robustness** *<value>*<br>**no ipv6 mld snooping vlan** *<vlan-id>* **query-robustness** | Configure the query robustness, the "no" form of this command restores to the default. |
| **ipv6 mld snooping vlan** *<vlan-id>* **suppression-query-time** *<value>*<br>**no ipv6 mld snooping vlan** *<vlan-id>* **suppression-query-time** | Configure the suppression query time. The "no" form of this command restores to the default |
| **lpv6 mld snooping vlan** *<vlan-id>* **static-group** *<X:X::X:X>* **[source** *<X:X::X:X>***] interface [ethernet \| port-channel]** *<IFNAME>*<br>**no ipv6 mld snooping vlan** *<vlan-id>* **static-group** *<X:X::X:X>* **[source** *<X:X::X:X>***] interface [ethernet \| port-channel]** *<IFNAME>* | Configure static-group on specified port of the VLAN. The no form of the command cancels this configuration. |

## 2.2.3 MLD Snooping Examples

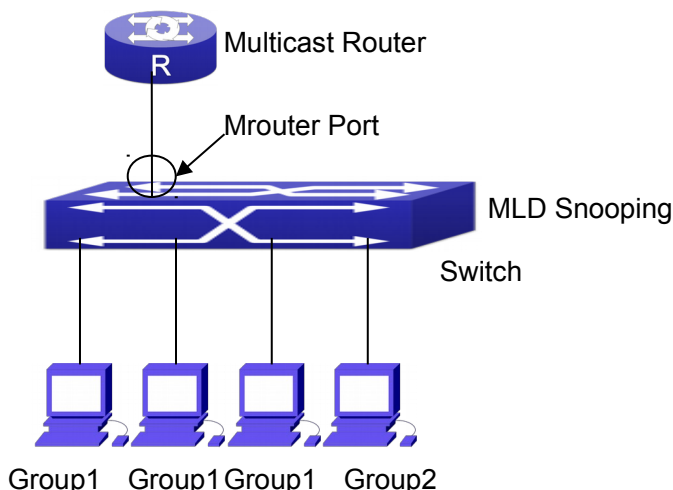**Scenario 1: MLD Snooping Function**

Fig 2-2 Open the switch MLD Snooping Function figure

As shown above, the vlan 100 configured on the switch consists of ports 1, 2, 6, 10 and 12. Four hosts are respectively connected to 2, 6, 10 and 12 while the multicast router on port 1. Suppose we need MLD Snooping on VLAN 100, however by default, the global MLD Snooping as well as the MLD Snooping on each VLAN are, therefore first we have to enable the global MLD Snooping at the same time enable the MLD Snooping on VLAN 100, furthermore we need to set the port 1 of VLAN 100 as a mrouter port.

Configuration procedure is as follows.

Switch#config

Switch(config)#ipv6 mld snooping

Switch(config)#ipv6 mld snooping vlan 100

Switch(config)#ipv6 mld snooping vlan 100 mrouter-port interface ethernet 1/0/1

Multicast configuration:

Assume there are two multicast servers: the Multicast Server 1 and the Multicast Server 2, amongst program 1 and 2 are supplied on the Multicast Server 1 while program 3 on the Multicast server 2, using group addresses respectively the Group 1, Group 2 and Group 3. Concurrently multicast application is operating on the four hosts. Two hosts connected to port 2, 6 are playing program 1 while the host connected to port 10 playing program 2, and the one to port 12 playing program 3.

**MLD Snooping interception results:**

The multicast table on vlan 100 shows: port 1, 2, 6 are in （Multicasting Server 1, Group1）, port1, 10 are in (Multicasting Server 1,Group2), and port1, 121, 12 are in (Multicasting Server 2, Group3）

All the four hosts successfully receive programs they are interested in. port2, 6 receives no traffic from program2 and 3; port10 receives no traffic from program 1 and 3, and port12 receives no traffic from program1 and 2.
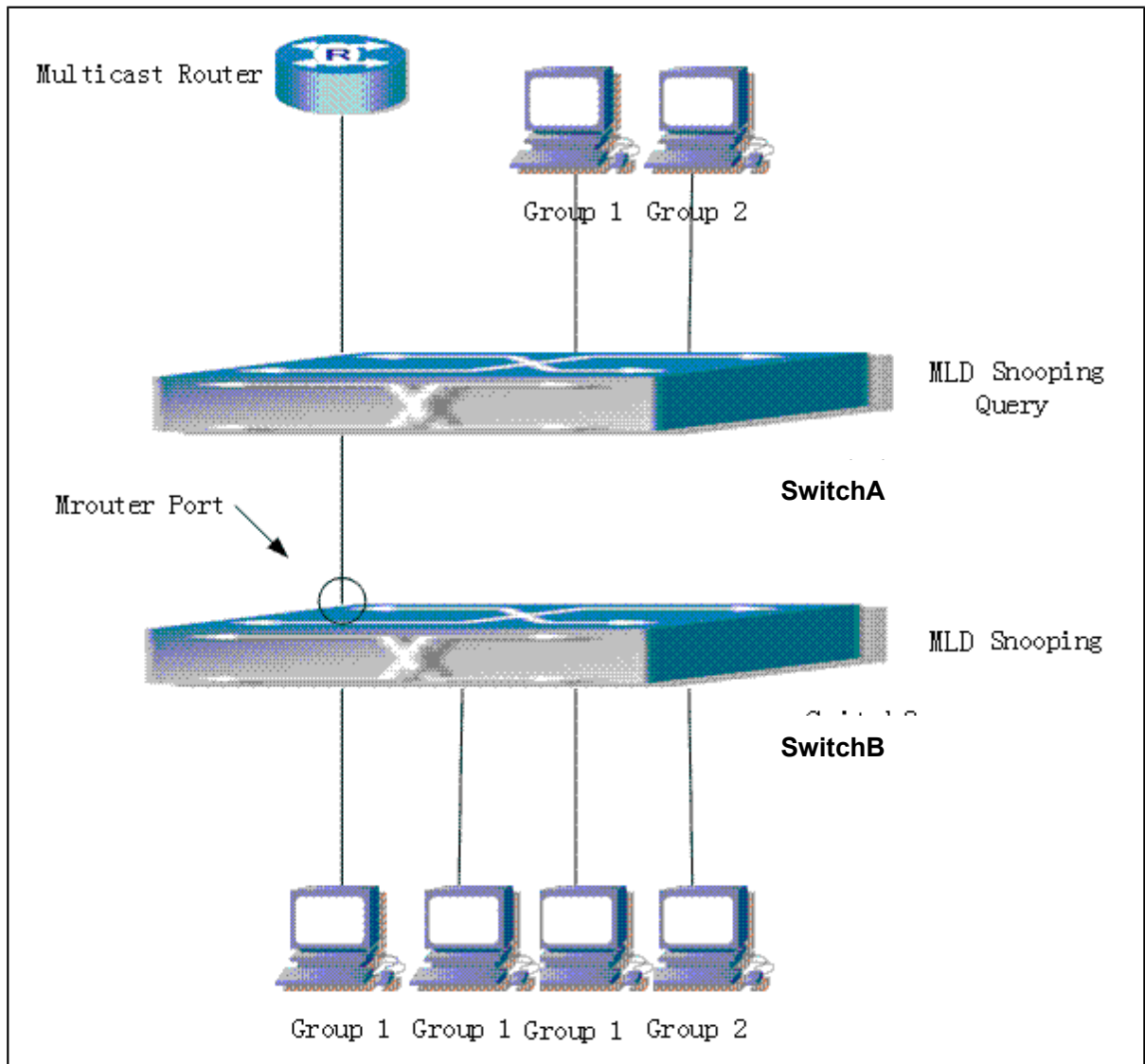
**Scenario 2: MLD L2-general-querier**



Fig 2-3 Switch as MLD Querier Function figure

Configuration of switch B is the same as the switches in case 1, and here the switch 1 replaces the Multicast Router in case 1. Assume the vlan 60 configured on it contains port 1, 2, 10 and 12, amongst port 1 is connected to multicast server, port 2 to switch2. To send Query periodically, global MLD Snooping has to be enabled while executing the mld snooping vlan 60 l2-general-querier, setting the vlan 60 to a Level 2 General Querier. Configuration procedure is as follows:

SwitchA#config

SwitchA(config)#ipv6 mld snooping

SwitchA(config)#ipv6 mld snooping vlan 60

SwitchA(config)#ipv6 mld snooping vlan 60 l2-general-querier

SwitchB#config

SwitchB(config)#ipv6 mld snooping

SwitchB(config)#ipv6 mld snooping vlan 100

SwitchB(config)#ipv6 mld snooping vlan 100 mrouter interface ethernet 1/0/1

Multicast configuration:

Same as scenario 1

**MLD Snooping** interception results:

Same as scenario 1


**Scenario 3: To run in cooperation with layer 3 multicast protocols**

SWITCH which is used in Scenario 1 is replaced with ROUTER with specific configurations remains the same. And multicast and IGMP snooping configurations are the same with what it is in Scenario 1. To configure PIM-SM6 on ROUTER, and enable PIM-SM6 on vlan 100 (use the same PIM mode with the connected multicast router)

The configurations are listed as below:

switch#config

switch(config)#ipv6 pim multicast-routing

switch(config)#interface vlan 100

switch(config-if-vlan100)#ipv6 pim sparse-mode

MLD snooping does not distribute entries when layer 3 multicast protocol is enabled. It only does the following tasks.

⊐   To remove the layer 2 multicast entries.

⊐   To provide query functions to the layer 3 with vlan, S, and G as the parameters.

⊐   When layer 3 MLD is disabled, re-enable distributing layer 2 multicast entries.

By looking up the layer 3 IP6MC entries, it can be found that ports can be indicated by the layer 3 multicast entries. This ensures the MLD Snooping can work in cooperation with the layer 3 multicast protocols.

# 2.2.4 MLD Snooping Troubleshooting

In configuring and using MLD Snooping, the MLD Snooping server may fail to run properly due to physical connection failure, wrong configuration, etc. The user should ensure the following:

⊒   Ensure the physical connection is correct

⊒   Ensure the MLD Snooping is enabled under global mode (using ipv6 mld snooping)

⊒   Ensure the MLD Snooping is configured on the vlan under global mode (using ipv6 mld snooping vlan <vlan-id>)

⊒   Ensure there is a vlan configured as a L2 general querier, or there is a static mrouter configured in a segment,

⊒   Use command to check if the MLD snooping information is correct

# Chapter 3 Multicast VLAN

## 3.1 Introductions to Multicast VLAN

Based on current multicast order method, when orders from users in different VLAN, each VLAN will copy a multicast traffic in this VLAN, which is a great waste of the bandwidth. By configuration of the multicast VLAN, we add the switch port to the multicast VLAN, with the IGMP Snooping/MLD Snooping functions enabled, users from different VLAN will share the same multicast VLAN. The multicast traffic only exists within a multicast VLAN, so the bandwidth is saved. As the multicast VLAN is absolutely separated from the user VLAN, security and bandwidth concerns can be met at the same time, after the multicast VLAN is configured, the multicast traffic will be continuously sent to the users.

## 3.2 Multicast VLAN Configuration Task List

1. Enable the multicast VLAN function
2. Configure the IGMP Snooping
3. Configure the MLD Snooping

**1. Enable the multicast VLAN function**

| Command | Explanation |
|---|---|
| VLAN configuration mode | |
| **multicast-vlan** <br> **no multicast-vlan** | Configure a VLAN and enable the multicast VLAN on it. The "**no multicast-vlan**" command disables the multicast function on the VLAN. |
| **multicast-vlan association <*vlan-list*>** <br> **no multicast-vlan association <*vlan-list*>** | Associate a multicast VLAN with several VLANs. The no form of this command deletes the related VLANs associated with the multicast VLAN. |
| **multicast-vlan association interface (ethernet \| port-channel\|) IFNAME** <br> **no multicast-vlan association interface (ethernet \| port-channel\|) IFNAME** | Associate the specified port with the multicast VLAN, so the associated ports are able to receive the multicast flow. The no command cancels the association between the ports and the multicast VLAN. |
| **multicast-vlan mode {dynamic\| compatible}** <br> **no multicast-vlan mode {dynamic\|** | Configure the two modes of multicast vlan. The no command cancels the mode configuration. |

| compatible} | |

**2. Configure the IGMP Snooping**

| Command | Explanation |
| --- | --- |
| Global Mode | |
| **ip igmp snooping vlan *<vlan-id>*** <br> **no ip igmp snooping vlan *<vlan-id>*** | Enable the IGMP Snooping function on the multicast VLAN. The no form of this command disables the IGMP Snooping on the multicast VLAN. |
| **ip igmp snooping** <br> **no ip igmp snooping** | Enable the IGMP Snooping function. The no form of this command disables the IGMP snooping function. |

**3. Configure the MLD Snooping**

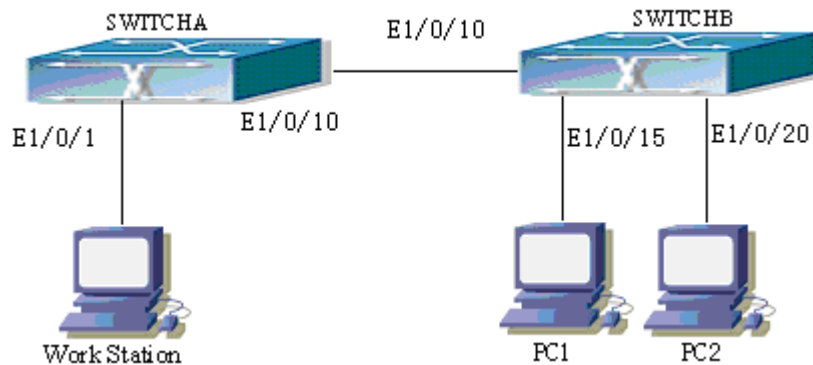| **ipv6 mld snooping vlan *<vlan-id>*** <br> **no ipv6 mld snooping vlan *<vlan-id>*** | Enable MLD Snooping on multicast VLAN; the no form of this command disables MLD Snooping on multicast VLAN. |
| --- | --- |
| **ipv6 mld snooping** <br> **no ipv6 mld snooping** | Enable the MLD Snooping function. The no form of this command disables the MLD snooping function. |

# 3.3 Multicast VLAN Examples



Fig 3-1 Function configuration of the Multicast VLAN

As shown in the figure, the multicast server is connected to the layer 3 switch switchA through port 1/0/1 which belongs to the VLAN10 of the switch. The layer 3 switch switchA is connected with layer 2 switches through the port 1/0/10, which configured as trunk port. On the switchB the VLAN100 is configured set to contain port 1/0/15, and VLAN101 to contain port 1/0/20. PC1 and PC2 are respectively connected to port 1/0/15 and 1/0/20. The switchB is connected with the switchA through port 1/0/10, which configured as trunk port. VLAN 20 is a multicast VLAN. By configuring multicast vlan, the PC1 and PC2 will receives the multicast data from the multicast VLAN.

Following configuration is based on the IP address of the switch has been configured and all the equipment are connected correctly.

**Configuration procedure**

SwitchA#config

SwitchA(config)#vlan 10

SwitchA(config-vlan10)#switchport access ethernet 1/0/1

SwitchA(config-vlan10)exit

SwitchA(config)#interface vlan 10

Switch(Config-if-Vlan10)#ip pim dense-mode

Switch(Config-if-Vlan10)#exit

SwitchA(config)#vlan 20

SwitchA(config-vlan20)#exit

SwitchA(config)#interface vlan 20

SwitchA(Config-if-Vlan20)#ip pim dense-mode

SwitchA(Config-if-Vlan20)#exit

SwitchA(config)#ip pim multicast

SwitchA(config)# interface ethernet1/0/10

SwitchA(Config-If-Ethernet1/0/10)switchport mode trunk


SwitchB#config

SwitchB(config)#vlan 100

SwitchB(config-vlan100)#Switchport access ethernet 1/0/15

SwitchB(config-vlan100)exit

SwitchB(config)#vlan 101

SwitchB(config-vlan101)#Switchport access ethernet 1/0/20

SwitchB(config-vlan101)exit

SwitchB(config)# interface ethernet 1/0/10

SwitchB(Config-If-Ethernet1/0/10)#switchport mode trunk

SwitchB(Config-If-Ethernet1/0/10)#exit

SwitchB(config)#vlan 20

SwitchB(config-vlan20)#multicast-vlan

SwitchB(config-vlan20)#multicast-vlan association 100,101

SwitchB(config-vlan20)#exit

SwitchB(config)#ip igmp snooping

SwitchB(config)#ip igmp snooping vlan 20


When multicast VLAN supports IPv6 multicast, usage is the same with IPv4, but the difference is using with MLD Snooping, so does not give an example.