Content

Chapter 1 AP IGMP Snooping Configuration

1.1 Introduction to AP IGMP Snooping

1.1.1 Introduction to M2U

M2U (multicast to unicast): When stack module of kernel protocol receives multicast packet, it will find the multicast table entry matching to multicast packet in multicast forwarding table according to multicast address and transform the multicast packet to unicast packet according to this matching table entry to send it to corresponding wireless interface. The wireless driving module of the wireless interface will send the unicast packet to destination host.

On the other hand, the multicast data receiver can be located accurately through M2U function, and it can avoid client to receive the multicast data which client does not want to receive to save the client bandwidth. At the same time, it avoids data information disclosure.

Multicast packet transmission does not need client to response to confirm packet (there is no retransmission mechanism), unicast packet transmission need client to response to confirm packet, and otherwise the underlying chip will retransmit. So M2U can improve the reliability of data transmission.

1.1.2 Introduction to IGMP Snooping

The layer 2 device enabled IGMP Snooping analyzes the IGMP packet received to create mapping for ports and MAC multicast address and forward multicast data according to this mapping.

When layer 2 device receives IGMP packet transmitted between host and router, IGMP Snooping analyzes packet information. When monitored IGMP host report packet from host, this host will be added into corresponding multicast table; when monitored IGMP leaving packet from host, controller will delete the multicast table corresponding to this host. Through monitoring IGMP packet constantly, mac multicast address table can be created and maintained in layer 2. Then, layer 2 device can forward the multicast packet issued from router according to mac multicast address table.

As shown in the following picture, client station 1, station 2 and station 3 are associated with VAP1 respectively. Only station 1 and station 3 are multicast demander. If enabling IGMP Snooping, AP will create multicast forwarding table according to IGMP

Report packet from demander. The multicast forwarding table is as below:

Vlan1	Group1	Vap1	station1
Vlan1	Group1	Vap1	station3

If Vap1 receives the multicast data flow from Group1, and if IGMP Snooping is not enabled on Vap1, AP will broadcast this multicast packet in Vap1 and client station 1, station 2 and station 3 will all receive this multicast data. When IGMP Snooping is enabled, AP will find corresponding multicast member in Vap1 according to vlan id and Group address. According to M2U, only receiver station 1 and station 3 can receive multicast data.

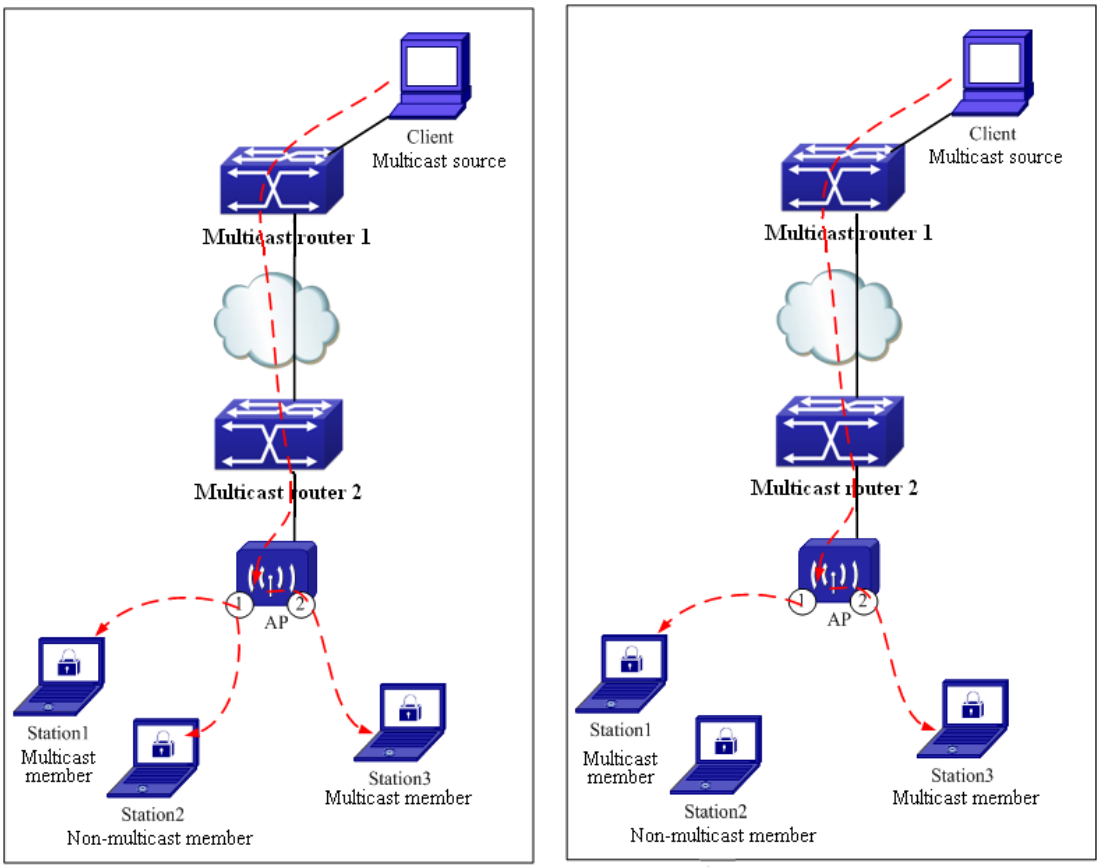

Fig 1-1 multicast forwarding principle

IGMP Snooping only forward information to receiver who need it through layer 2 multicast, it can bring some benefit as below:

- Reduce broadcast packet in layer 2 network and save network bandwidth.
- Increase security of multicast information.

1.2 AP IGMP Snooping Configuration

AP IGMP Snooping configuration task list is as below:

1. Enable/disable global IGMP Snooping function on AP
2. Enable/disable M2U function

3. Configure/recover multicast member number threshold disabled by M2U function
4. Enable/disable “broadcast to unicast” function on AP

1. Enable/disable global IGMP Snooping function on AP

Command	Explanation
Wireless Global Mode	
igmp snooping **no igmp snooping**	Enable AP global igmp snooping function. The no command will disable this function.

2. Enable/disable M2U function

Command	Explanation
Network Configuration Mode	
igmp snooping m2u **no igmp snooping m2u**	Enable the m2u function of the VAP configured igmp snooping. If configured this function, when the multicast packet received from the VAP, it will be transformed to be unicast packet to send to multicast members. The no command will disable the m2u function of the VAP.

3. Configure/recover multicast member number threshold disabled by M2U function

Command	Explanation
Network Configuration Mode	
m2u threshold <*2-255*> **no m2u threshold <*2-255*>**	Set the access station maximum number of each multicast group allows when the multicast groups support m2u, if the number of members of a multicast group exceeds the threshold value, m2u will be turned off. The no command will restore the default threshold value of 6.

4. Enable/disable “broadcast to unicast” function on AP

Command	Explanation
Network Configuration Mode	
b2u enable **no b2u enable**	Enable the AP function of transform broadcast to be unicast. If enabled this function, the AP will transform the broadcast packet to be unicast packet, and then send to the clients. The no command will disable this function.

1.3 AP IGMP Snooping Examples

Case：

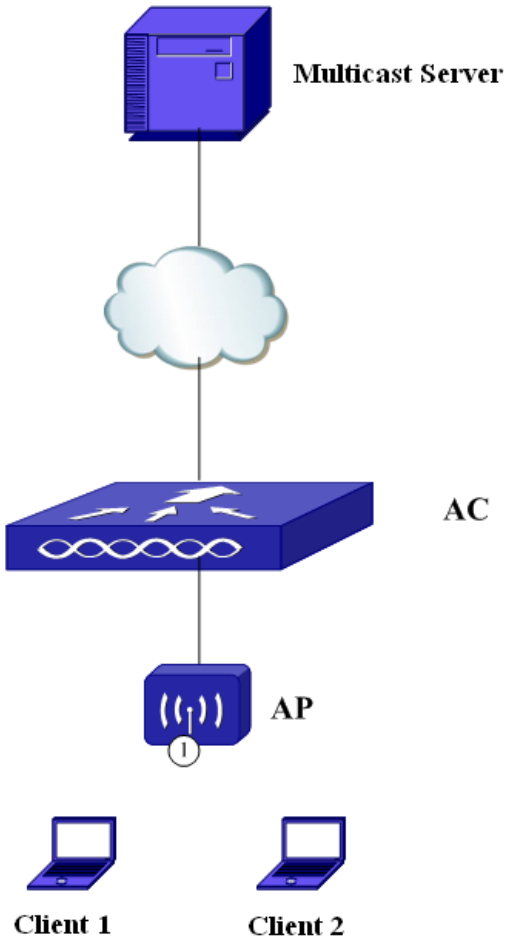

Fig 1-2 Typical application environment of AP IGMP Snooping

AC is connected to multicast server through layer 3 network, client 1 and client 2 are associated with VAP1. VAP1 belongs to vlan 10. Multicast server sends multicast flow and

enables IGMP Snooping and M2U function of AP. Client 1 and client 2 demand multicast flow. AC configures AP to use profile 1. Notice: the system of Windows2000/XP does not support the inquiry of source address 0.0.0.0. So IGMP Snooping function is needed to be enabled on AC to make sure client to continue to demand flow. Configure the inquiry source address as the layer 3 interface address corresponding to vlan of enabling IGMP Snooping on AC. Version of inquiry packet is 3. The configuration on AC is as below:

AC configuration:

```
AC(config)#ip igmp snooping
AC(config)#ip igmp snooping vlan 4094
AC(config)#ip igmp snooping vlan 4094 l2-general-querier-version 3
AC(config)#ip igmp snooping vlan 4094 l2-general-querier-source 192.168.10.100
AC(config)#wireless
AC(config-wireless)#igmp snooping
AC(config-wireless)#network 2
AC(config-network)#vlan 10
AC(config-network)#igmp snooping m2u
AC(config-network)#exit
AC(config-wireless)#exit
AC(config)#exit
AC#wireless ap profile apply 1
All configurations will be sent to the aps associated with this profile. Are you sure you want to apply the profile configuration? [Y/N]y
```

1.4 AP IGMP Snooping Troubleshooting

When there are problems to use AP IGMP Snooping, please check is it is wrong with reasons as below:

- ☞ If configure IGMP Snooping and M2U function correctly and if issue the corresponding configuration to AP.
- ☞ If enable M2U function. It is multicast packet that client received, please check if clients number exceeds the threshold of enabling M2U.