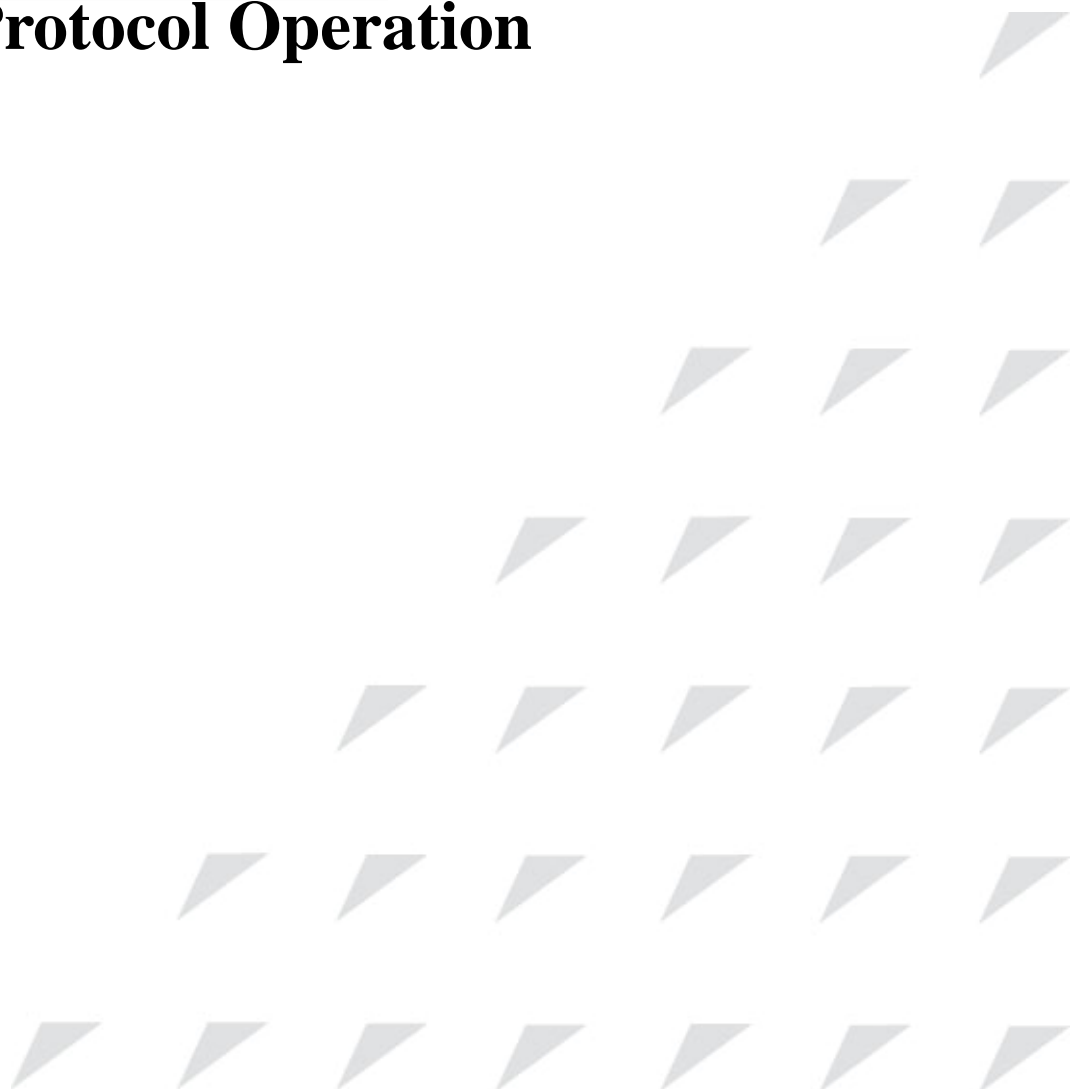


www.raisecom.com

Multicast Protocol Operation



Legal Notices

Raisecom Technology Co., Ltd makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. **Raisecom Technology Co., Ltd** shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Warranty.

A copy of the specific warranty terms applicable to your Raisecom product and replacement parts can be obtained from Service Office.

Restricted Rights Legend.

All rights are reserved. No part of this document may be photocopied, reproduced, or translated to another language without the prior written consent of **Raisecom Technology Co., Ltd.** The information contained in this document is subject to change without notice.

Copyright Notices.

Copyright ©2007 Raisecom. All rights reserved.

No part of this publication may be excerpted, reproduced, translated or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in Writing from **Raisecom Technology Co., Ltd.**

Trademark Notices

RAISECOM is the trademark of Raisecom Technology Co., Ltd.

Java™ is a U.S. trademark of Sun Microsystems, Inc.

Microsoft® is a U.S. registered trademark of Microsoft Corporation.

Windows NT® is a U.S. registered trademark of Microsoft Corporation.

Windows® 2000 is a U.S. registered trademark of Microsoft Corporation.

Windows® XP is a U.S. registered trademark of Microsoft Corporation.

Windows® and MS Windows® are U.S. registered trademarks of Microsoft Corporation.

Contact Information

Technical Assistance Center

The Raisecom TAC is available to all customers who need technical assistance with a Raisecom product, technology, or, solution. You can communicate with us through the following methods:

Address: 2nd Floor, South Building of Rainbow Plaza, No.11 Shangdi Information Road,
Haidian District, Beijing 100085

Tel: +86-10-82883305

Fax: +86-10-82883056

World Wide Web

You can access the most current Raisecom product information on the World Wide Web at the following URL:

<http://www.raisecom.com>

Feedback

Comments and questions about how the ... system software works are welcomed. Please review the FAQ in the related manual, and if your question is not covered, send email by using the following web page:

<http://www.raisecom.com/en/xcontactus/contactus.htm>.

If you have comments on the ... specification, instead of the web page above, please send comments to:

export@raisecom.com

We hope to hear from you!

CONTENTS

Chapter 1	System Overview	1
Overview		错误！未定义书签。
Function feature		错误！未定义书签。
Caption 2		错误！未定义书签。
Caption 3		错误！未定义书签。
Chapter 2	System Operation	错误！未定义书签。
Overview		错误！未定义书签。
System installation		错误！未定义书签。
System activation		错误！未定义书签。
Shutdown system		错误！未定义书签。
System Upgrade		错误！未定义书签。
System maintain		错误！未定义书签。
Chapter 3	System Security Management	错误！未定义书签。
Overview		错误！未定义书签。
User management		错误！未定义书签。
User group management		错误！未定义书签。
Management domain management		错误！未定义书签。
Operation log management		错误！未定义书签。
Influence on Device Configuratin Operations		错误！未定义书签。
Influence on operations		错误！未定义书签。
Chapter 4	System Overview	错误！未定义书签。
Appendix A	Abbreviation	错误！未定义书签。
Appendix B	FAQ	错误！未定义书签。
Index		错误！未定义书签。

Release Notes

Date of Release	Manual Version	Software Version	Revisions

Preface

About This Manual

This manual introduces primary functions of the configuration management software for RC series products.

Who Should Read This Manual

This manual is a valuable reference for sales and marketing staff, after service staff and telecommunication network designers. For those who want to have an overview of the features, applications, structure and specifications of ... device, this is also a recommended document.

Relevant Manuals

《Raisecom NView System User Manual》

《Raisecom Nview System Installation and Deployment Manual》

《... User Manual》

《... Commands Notebook》

Organization

This manual is an introduction of the main functions of ... EMS. To have a quick grasp of the using of the EMS of ... , please read this manual carefully. The manual is composed of the following chapters

Chapter 1 Overview

This chapter briefly introduces the basic function of ...

Chapter 2 Configuration Management

This chapter mainly introduces the central site configuration management function of the

Chapter 3 Performance Management

This chapter focuses on performance management function of

Chapter 4 Device Maintenance Management

This chapter introduces the device maintenance management function of

Appendix A Alarm Type

The alarm types supported by

Compliance

The RC series products developed by Raisecom are strictly complied with the following standards as well as ITU-T, IEEE, IETF and related standards from other international telecommunication standard organizations:

YD/T900-1997 SDH Equipment Technical Requirements - Clock

YD/T973-1998 SDH 155Mb/s and 622Mb/s Technical conditions of optical transmitter module and receiver module

YD/T1017-1999 Network node interface for the Synchronous Digital Hierarchy (SDH)

YD/T1022-1999 Requirement of synchronous digital hierarchy (SDH) equipment function

YD/T1078-2000 SDH Transmission Network Technique Requirements-Interworking of Network Protection Architectures

YD/T1111.1-2001 Technical Requirements of SDH Optical Transmitter/Optical Receiver Modules——2.488320 Gb/s Optical Receiver Modules

YD/T1111.2- 2001 Technical Requirements of SHD Optical Transmitter/Optical Receiver Modules——2.488320 Gb/s Optical Transmitter Modules

YD/T1179- 2002 Technical Specification of Ethernet over SDH

G.703 Physical/electrical characteristics of hierarchical digital interfaces

G.704 Synchronous frame structures used at 1544, 6312, 2048, 8448 and 44 736 kbit/s hierarchical levels

G.707 Network node interface for the synchronous digital hierarchy (SDH)

G.774 Synchronous digital hierarchy (SDH) - Management information model for the network element view

G.781 Synchronization layer functions

G.783 Characteristics of synchronous digital hierarchy (SDH) equipment functional blocks

G.784 Synchronous digital hierarchy (SDH) management

G.803 Architecture of transport networks based on the synchronous digital hierarchy (SDH)

G.813 Timing characteristics of SDH equipment slave clocks (SEC)

G.823 The control of jitter and wander within digital networks which are based on the 2048 kbit/s hierarchy

G.825 The control of jitter and wander within digital networks which are based on the synchronous digital hierarchy (SDH)

G.826 End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections

G.828 Error performance parameters and objectives for international, constant bit-rate synchronous digital paths

G.829 Error performance events for SDH multiplex and regenerator sections

G.831 Management capabilities of transport networks based on the synchronous digital hierarchy (SDH)

G.841 Types and characteristics of SDH network protection architectures

G.842 Interworking of SDH network protection architectures

G.957 Optical interfaces for equipments and systems relating to the synchronous digital hierarchy

G.691 Optical interfaces for single channel STM-64 and other SDH systems with optical amplifiers

G.664 Optical safety procedures and requirements for optical transport systems

I.731 ATM Types and general characteristics of ATM equipment

I.732 ATM Functional characteristics of ATM equipment

IEEE 802.1Q Virtual Local Area Networks (LANs)

IEEE 802.1p Traffic Class Expediting and Dynamic Multicast Filtering

IEEE 802.3 CSMA/CD Access Method and Physical Layer Instruction

Chapter 1 Multicast Overview

1.1 The confusion of unicast/broadcast

As Internet develops, on one side the interactive data, voice and video information in the network are becoming more and more, on the other side the rising services like electronic commerce, network meeting, network auction, video on demand and remote education are in gradual rise. These services have new request on information security and payment, which traditional unicast and broadcast can not meet well.

1.1.1 Information transmission in unicast

With unicast, the system will establish a single data transmission channel for the user who needs the information, and send a single copy to the user, as is shown below:

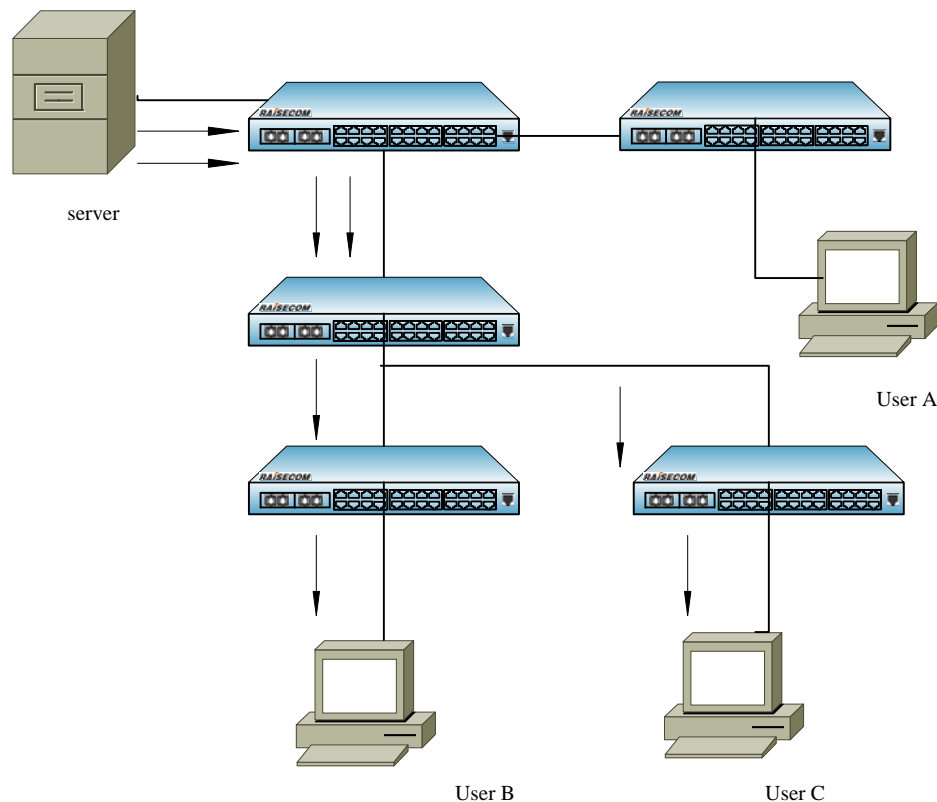


Fig 1-1 unicast transmission

Suppose user B and C need the information, the information source Server will establish transmission channel for user B and C respectively. Because the information capacity transmitted in the network is in proportion to the capacity of users who need the information, when the number of users who need the information is large, there will be several same information stream in the network. Then bandwidth will be a important bottleneck and unicast goes against sending information in large scale.

1.1.2 Transmitting information in broadcasting

Using broadcast, the system will send the information to all the network users, caring not if it is needed, any user can receive the information from broadcasting, as is shown below:

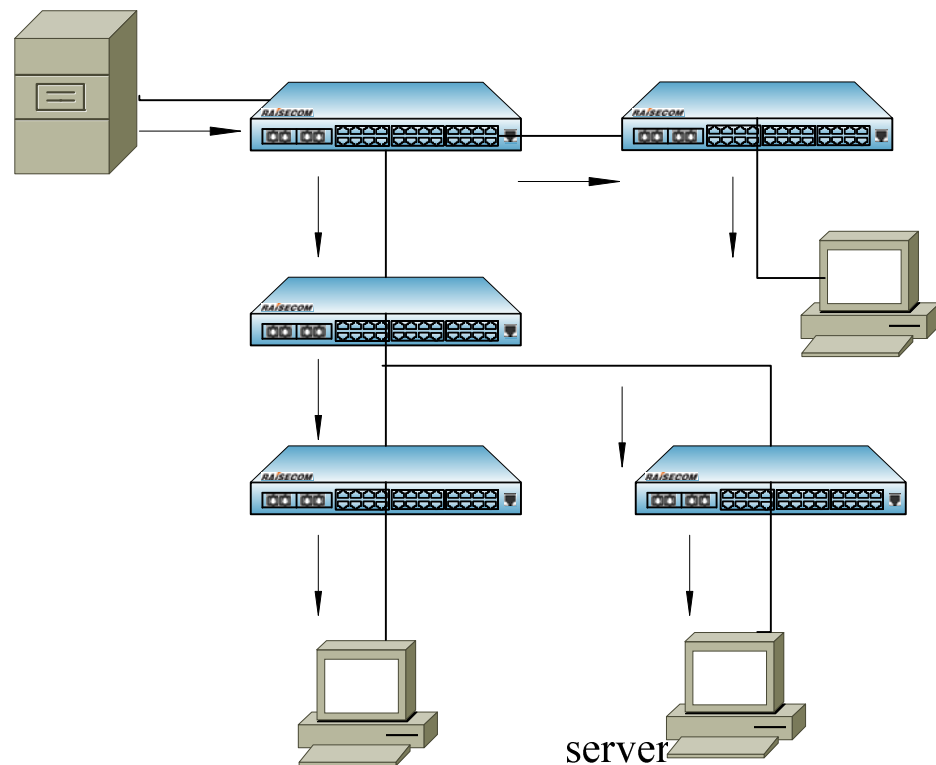


Fig 1-2 Information transmission in broadcast

Suppose user B and C need the information, then information source Server will broadcast the information by router, another network user A can also receive the information, which means information security and payment services can not be ensured. On the other side, when there is not so many users who need the information, network resource use ratio will be quite low, which is a great waste of the bandwidth. In summary, unicast suits the network with rare users, while broadcast suit the network with a lot of people. When the number of users who need the information is not so sure, unicast and broadcast are both low in efficiency.

1.2 The advantage of multicast

1.2.1 Information transmission in multicast

The appearance of multicast handles the problem in time. When some users in the network need specific information, multicast source send out information only once, and the information sent out will be copied and sent out in the crossing as far as possible, as is shown below:

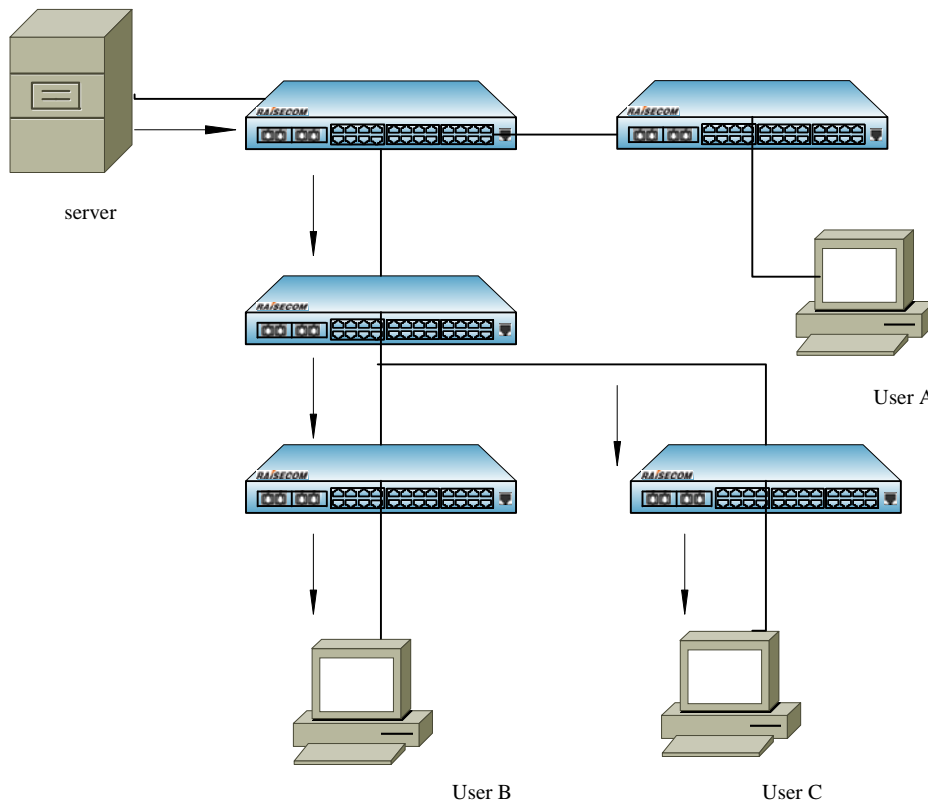


Fig 1-3 Information transmission in multicast

Suppose user B and C need the information, to send the information successfully to the user who really needs it, it is needed to form B, C into a receiver combination, then each switch in the network form its own multicast transmission table according to IGMP message, at last the information will be transmitted accurately to receiver B, C who need it really. In multicast information sender is called 'multicast source', but some information receiver call it the 'multicast group' of the information. The receiver member who joins the same multicast group can be located in any place in the network, that is to say, there is no domain limit with 'multicast group'. It should be noted that multicast source does not have to belong to multicast group, it send data to multicast group and don't have to be receiver itself. There can be several sources sending out messages to one multicast group.

1.2.2 Information transmission in multicast

The advantage of multicast is:

Increase the efficiency and decrease the network traffic, ease the load of the server and CPU;

Optimize the performance and decrease the redundant traffic;

Distributed application makes multi-point use possible.

Chapter 2 IGMP Snooping Configuration

This chapter is mainly about how to configure and maintain IGMP Snooping, including:

- ✧ About IGMP Snooping
- ✧ Configuration task list
- ✧ Monitoring and maintenance
- ✧ Typical application
- ✧ Trouble shooting

2.1 About IGMP Snooping protocol

IGMP Snooping, unlike ISO module, has no clear concept module, which takes the upper-layer protocol data information as the bottom-layer working consideration factor. In the transmission of multicast, IGMP Snooping confines data flooding to all the ports, but transmits information only to the multicast member ports, which helps saving the bandwidth.

IGMP snooping allows LAN switch to snoop on the IGMP transmissions between the host and the router and to keep track of multicast groups and member ports. When the switch receives an IGMP report from a host for a particular multicast group, the switch adds the host port number to the forwarding table entry; when it receives an IGMP Leave Group message from a host, it removes the host port from the table entry. It also periodically deletes entries if it does not receive IGMP membership reports from the multicast clients.

Layer 2 multicast groups learned through IGMP snooping are dynamic. However, you can statically configure MAC multicast groups by using the **ip igmp snooping static** command. If you specify group membership for a multicast group address statically, your setting supersedes any automatic manipulation by IGMP snooping. Multicast group membership lists can consist of both user-defined and IGMP snooping-learned settings. Raisecom series switches supports 1024 two-layer multicast transmission table item, and support IGMPv1 and IGMPv2 version.

2.2 IGMP snooping configuration

This part is about how to configure and maintain IGMP Snooping on switch, including:

- ✧ Enable and disable IGMP Snooping
- ✧ IGMP Snooping aging time
- ✧ Multicast Router port configuration
- ✧ Configuring immediate-leave function
- ✧ Manually configure multicast MAC address table.

2.2.1 Default IGMP Snooping configuration

Function	Default value
IGMP SNOOPING starting	On
IGMP SNOOPING out-time	300 秒

Configure the router time	Do not configure
MVR mode	Compatible
Quit immediately	Disabled
Multicast stable transmission table	Not configured

2.2.2 IGMP Snooping enable and disable

IGMP snooping is disabled on the switch by default. If IGMP snooping is globally enabled/disabled, all the VLAN will enable or disable IGMP snooping function. The following commands are used to enable IP IGMP Snooping:

Step	Command	Description
1	config	Enter global configuration mode
2	ip igmp snooping	Enable IGMP Snooping
3	exit	Exit to privilege mode
4	show ip igmp snooping	Show configuration situation

Use **no ip igmp-snooping** command to disable IP IGMP Snooping.

This command is used to globally disable IGMP snooping function. In order to disable IP IGMP snooping function on particular VLAN, use the following commands under VLAN configuration mode.

Step	Command	Description
1	config	Enter global configuration mode
2	vlan <i>vlan-id</i>	Enter VLAN configuration mode
3	no ip igmp snooping	Disable the IGMP snooping function for this VLAN.
4	exit	Exit to global configuration mode
5	exit	Exit to privileged EXEC mode

6	show ip igmp snooping vlan <i>vlan-id</i>	Show VLAN configuration information
----------	---	--

In order to enable IGMP snooping function on the VLAN, use **ip igmp snooping** in VLAN configuration mode.

If IGMP snooping is disabled globally, IGMP snooping function can not be enabled on particular VLAN.

If user needs to enable or disable IGMP Snooping function on several VLANs, use **ip igmp-snooping vlan** command in global configuration mode according to the following table:

Step	Command	Description
1	config	Enter global configuration mode
2	ip igmp snooping vlan 1-100	Enable IGMP snooping function on VLAN1-100
3	exit	Exit to privileged user mode
4	show ip igmp snooping	Show IGMP Snooping configuration information

Use **no ip igmp snooping vlan** command to disable IGMP snooping function on several VLAN at a time.

In order to check whether the configuration is correct or not, use show command:

```
Raisecom#show ip igmp snooping
```

```
IGMP snooping: Enable
```

```
IGMP snooping aging time: 300s
```

```
IGMP snooping active VLAN: 1,2
```

```
IGMP snooping immediate-leave active VLAN: --
```

```
Raisecom#show ip igmp snooping vlan 2
```

```
IGMP snooping: Enable
```

```
IGMP snooping aging time: 300s
```

```
IGMP snooping on VLAN 2: Enable.
```

```
IGMP snooping immediate-leave on VLAN 2: Disable.
```

2.2.3 IGMP snooping aging time configuration

If switch does detect IGMP Snooping Join or Query message within a period, the subscriber may have left already without sending any leaving message, so the switch needs to be deleted the multicast MAC address from the address table. The default aging time is 300 seconds. Configuration

steps are showed as follows:

Step	Command	Description
1	config	Enter global configuration mode.
2	ip igmp snooping timeout <i>timeout</i>	Set IGMP overtime.
3	exit	Exit to privilege EXEC mode
4	show ip igmp snooping	Show IGMP Snooping configuration information

The range of aging time is 30 seconds to 3600 seconds, in order to recover default value, use following command: **no ip igmp snooping timeout**

Example:

Raisecom#**config**

SCOM2826(config)# **ip igmp snooping timeout 1200**

ISCOM2826(config)#**exit**

Raisecom#show ip igmp snooping

GMP snooping: Enable

IGMP snooping aging time: 3000s

IGMP snooping active VLAN: 1, 2

IGMP snooping immediate-leave active VLAN: 1

2.2.4 Router port configuration

The Multicast Router port can be assigned by dynamically address learning (through IGMP request message), or manually configured (that is to say, multicast report and leave message of downlink hosts can be forwarded to multicast router port). The manual configuration steps of multicast router port are as follows:

Step	Command	Description
1	config	Enter global configuration mode
2	ip igmp snooping mrouter vlan <1-4094> port <1-26>	Configure router port
3	exit	Exit to privileged EXEC mode

4	show ip igmp snooping mrouter	Show Multicast Router port configuration information
----------	--	---

Use following command to delete configured Multicast Router port: no ip igmp snooping mrouter vlan 1 port 2

Configuration example:

```
ISCOM2826#config
```

```
ISCOM2826(config)#ip igmp snooping mrouter vlan 1 port 2
```

```
ISCOM2826(config)#exit
```

```
ISCOM2826#show ip igmp snooping mrouter
```

Ip Address	Port	Vlan	Age	Type

224.0.0.0/8	2	1	--	USER

2.2.5 Immediate-leave function configuration:

When you enable IGMP Immediate-Leave processing, the switch immediately removes a port when it detects an IGMP version 2 leave message on that port.

The settings are as following:

Step	Command	Description
1	config	Enter global configuration mode
2	vlan 1	Enter VLAN configuration mode
3	ip igmp snooping immediate-leave	Set immediate-leave function on the VLAN.
4	exit	Exit to global configuration mode.
5	exit	Exit to privilege EXEC mode.
6	show ip igmp snooping	Show IGMP Snooping configuration information

In VLAN configuration mode, use **no ip igmp snooping immediate-leave** command to restore default setting:

Configuration example:


```

ISCOM2826#config
ISCOM2826 (config)#vlan 1
ISCOM2826 (config-vlan)# ip igmp snooping immediate-leave
ISCOM2826 (config-vlan)#exit
ISCOM2826 (config)#exit
ISCOM2826#show ip igmp snooping vlan 1
IGMP snooping: Enable
IGMP snooping aging time: 300s
IGMP snooping on VLAN 1: Enable.
IGMP snooping immediate-leave on VLAN 1: Enable.

```

In order to configure the immediate-leave function in multiple VLAN, use following commands:

Step	Command	Description
1	config	Enter global configuration mode.
2	ip igmp snooping vlan <i>vlanlist</i> immediate-leave	Set immediate-leave function on the VLAN.
3	exit	Exit to privileged EXEC mode.
4	show ip igmp snooping	Show IGMP Snooping configuration information

In order to restore default settings, use following command: **no ip igmp snooping vlan *vlanlist* immediate-leave**

Example:

```

iscom2016#config
iscom2016(config)# ip igmp snooping vlan 1-10 immediate-leave
iscom2016(config)#exit
iscom2016#show ip igmp snooping
igmp snooping is globally Enabled
igmp snooping aging time is 1200(s)
IGMP snooping active vlan: 1
IGMP snooping immediate-leave active vlan:1-10

```

2.2.6 Stable multicast transmission table configuration

Usually a port joins multicast router through the IGMP report message from the host. For maintenance, you can add a port to the multicast group manually.

Step	Command	Description
1	config	Enter global configuration mode
2	mac-address-table static multicast <i>mac-addr</i> vlan <i>vlanid</i> port-list <i>portlist</i>	Add the port to the multicast group
3	exit	Exit to privilege user mode
4	show mac-address-table multicast	Show multicast MAC address information

The MAC address is the multicast MAC address, and the format is HHHH.HHHH.HHHH. For example, multicast IP address 224.8.8.8 is mapped to multicast MAC address 0100.5e08.0808; the range of the port is from 1 to 26. In order to delete the port from multicast group manually, use command **no mac-address-table static multicast** *mac-addr* **vlan** *vlanid* **port-list** *portlist*.

Configuration example:

```
Raisecom#config
```

```
ISCOM2826(config)# mac-address-table static multicast 0100.5e08.0808 vlan 2 port-list 1-6
```

```
ISCOM2826(config)#exit
```

```
ISCOM2826# show mac-address-table multicast
```

Multicast filter mode: Forward-all

Vlan	Group Address	Ports[Static](Hardware)
------	---------------	-------------------------

2	0100.5E08.0808	1-61-6
---	----------------	---------------

2.3 Monitoring and maintenance

Use show command to check switch IGMP snooping running and configuration status:

Step	Command	Description
------	---------	-------------

1	show ip igmp snooping [vlan vlan-id]	Show IGMP snooping configuration information in all the VLAN or designated VLAN of the switch.
2	show ip igmp snooping multicast [vlan vlan-id]	Show multicast router port information (dynamically learned or manually configured) of all the VLAN or a designated VLAN.
3	show mac-address-table multicast [vlan vlan-id] [count]	Show all the multicast MAC address; <i>Count</i> : indicates the total number of multicast MAC address

Use **show ip igmp snooping** command to check configuration information, for example the timer, VLAN configuration information.

Show IGMP Snooping configuration information:

```
Raisecom# show ip igmp snooping
```

```
IGMP snooping: Enable
```

```
IGMP snooping aging time: 300s
```

```
IGMP snooping active VLAN: 1, 2
```

```
IGMP snooping immediate-leave active VLAN: 1
```

Use **show ip igmp snooping vlan vlanid** command to show the IGMP snooping information in a particular VLAN. If you do not specify VLAN, all the VLAN information will be displayed, that is all the existent and active VLAN.

Show igmp-snooping multicast router information:

```
Raisecom# show ip igmp snooping mrouter
```

Ip Address	Port	Vlan	Age	Type

224.0.0.0/8	4	3	--	USER

```
Raisecom#show mac-address-table multicast
```

Multicast filter mode: Forward-all

Vlan	Group Address	Ports[Static](Hardware)

2	0100.5E08.0808	1-61-6

2.4 Typical configuration example

1) Configuration instruction:

To realize the switch IGMP Snooping function, it is needed to start IGMP Snooping on the switch (by default it's on). The router port (physical port 1) on the switch connects to the router, while other not-router ports connect to users' PC.

2) Typical network structure figure

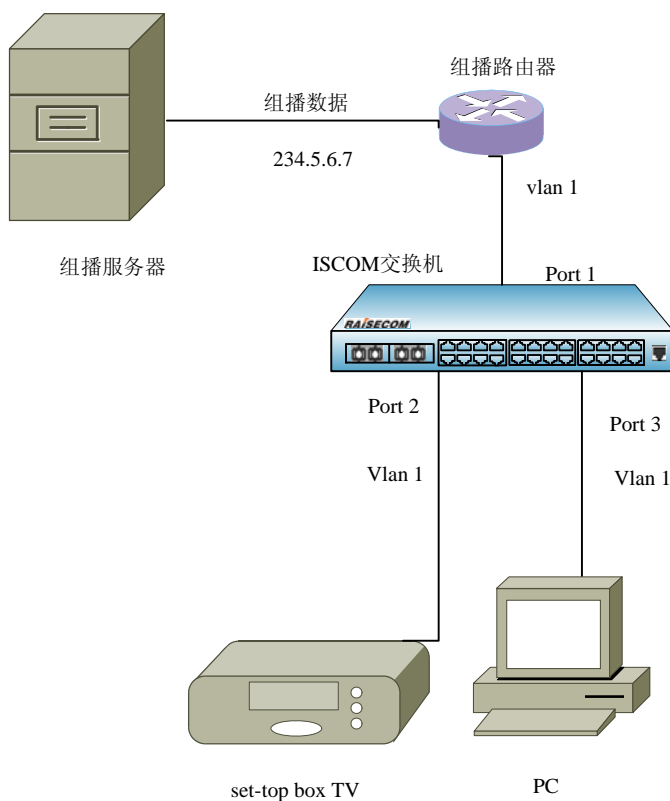


Fig 2-1 typical IGMP Snooping network structure

3) Configuration command

By default IGMP Snooping function is on, and it will be started to the existed VLAN port. For fig 2-1, use **ip igmp snooping mrouter vlan 1 port 1** to configure the router port on the switch.

2.5 IGMP snooping trouble shooting

1. If multicast router port has not been specified, all the IGMP reports will be transmitted to the port directly connected to the router;
2. If it is failed to add port to a multicast group manually, the reason may be incorrect multicast

MAC address format or the maximum layer 2 multicast router table (255) has been achieved;

3. If it is failed to delete the port from multicast group manually, the possible reason may be incorrect multicast MAC address format or MAC address/VLAN/port are not existent in multicast router.

Chapter 3 MVR Configuration

This chapter is mainly about how to configure and maintain MVR and IGMP filtration on the switch, including:

- ✧ MVR overview
- ✧ MVR proxy principle introduction
- ✧ IGMP filtration overview
- ✧ MVR configuration
- ✧ MVR monitoring and maintenance
- ✧ MVR proxy configuration
- ✧ MVR proxy monitoring and maintenance
- ✧ IGMP filtration configuration
- ✧ IGMP filtration monitoring and maintenance
- ✧ Typical configuration example
- ✧ MVR and IGMP filtration trouble shooting

3.1 MVR principle

Multicast VLAN registration is applied as traffic multicast in the network of service provider, such as TV programme ordering. MVR allows subscriber on the port to order or cancel the multicast traffic in VLAN, allows data traffic sharing for different VLANs. There are two MVR aims:

1. By using simple configurations, use can transmit multicast among different VLANs safely and effectively;
2. Support multicast group joining and leaving dynamically;

The operation manner of MVR is similar to that of IGMP snooping. These two functions can be enabled simultaneously. MVR only processes the joining and leaving of configured multicast groups, the other multicast groups are managed by IGMP snooping. The difference between these two is that: with IGMP snooping, the multicast traffic can be transmitted within only one VLAN, while with MVR the multicast traffic can be transmitted within different VLANs.

There are two operation modes:

1. Compatible mode: all multicast data received at the source port (port connected with multicast router) will be forwarded to the other ports, no matter whether these source ports have members to join in or not. Simultaneously, multicast data are only forwarded to those receiving ports (ports connected with subscribers) which are specified to have already joined in the MVR group, the joining can be in the form of IGMP report or MVR static configuration. IGMP report will not be forwarded to the source port of switch. Therefore, the switch does not support source port joining dynamically. Under this mode, multicast router should be configured as forwarding all multicast data to the source port, since switch will not send IGMP joining information to the router.
2. Dynamic mode: Received multicast data are only forwarded to those ports which have member

to join (source port or receiving port), the joining can be in the form of IGMP report information or MVR static configurations. All received IGMP information is forwarded to the source port of the switch. This method could save much bandwidth.

MVR are operative only on Layer-2. It dose not work on Layer-3. One switch can configure only one multicast VLAN, support 256 multicast groups at most.

3.2 MVR proxy principle

MVR proxy provides a complete solution for the multicast operation of two-layer equipments through proxy mechanism. The two-layer network equipments that support MVR proxy take the role of Server on user side, and query user information periodically, and it take the role of Client on the web side, sending the current user's information to the network when needed. This will not only stop the two-layer multicast from flooding, but also help acquiring and controlling user information, at the same time it can help reduce the web side protocol messages and the network load. MVR proxy establish multicast table by holding up the IGMP messages between user and router, the up-link port of Proxy equipment takes the role of host, while down-link port takes the role of router.

3.3 IGMP filtration introduction

Administrator needs to limit the multicast users under some circumstances, such as to allow which ports to receive multicast on a switch, which ports to reject multicast data. Use can realize this kind of control on the port by configuring IGMP profile. One IGMP profile includes one or multiple multicast groups, and permit/deny items to access these groups. If one "deny" type IGMP profile is applied to the port, when the port receives IGMP joining information of this group, it will drop and do not allow receiving multicast data from this group. IGMP profile can be applied to dynamic multicast group, not suitable for static group.

In addition, the maximum multicast group can be configured on port.

3.4 MVR configuration

This part is about how to configure MVR on the switch, including:

- ✧ Default MVR configuration
- ✧ Global MVR configuration
- ✧ Configure MVR port information

3.4.1 Default MVR configuration

Attributes	Default configuration
MVR enable/disable	disabled
Multicast address	Not configured
MVR timeout	600 seconds
Multicast VLAN	1
MVR mode	compatible
Port MVR enable/disable	disabled

Port default configuration	Non MVR (neither source port, nor receiving port)
Intermediate leave	disabled

The steps below should be followed:

1. Receiving port can be only ACCESS port, but cannot be TRUNK port. Receiving port can belong to different VLANs, but cannot belong to multicast VLAN;
2. The maximum MVR multicast address is 256;
3. Since ISCOM28 series switches support Layer-2 multicast, which means multiple IP multicast addresses correspond to one MAC multicast address, MVR multicast address is not allowed using repetitive names during configuration.
4. MVR and IGMP snooping can coexist;
5. Source port should be in the multicast VLAN;

3.4.2 Global MVR configuration

Under the default situation, MVR is disabled. User can carry out the commands below to enable MVR under global configuration mode. Multicast VLAN, multicast address, operation modes can be configured as well. If MVR has not been enabled yet, it is allowed to configure MVR. Once MVR is enabled, these configurations will take effect at once.

Step	Command	Description
1	config	Enter global configuration mode
2	mvr enable	Enable MVR
3	mvr group ip -address [count]	Configure IP multicast address, if the parameter count is specified, you can configure a consecutive MVR group addresses (the range for count is from 1 to 256, 1 by default)
4	mvr timeout timeout	optional, MVR multicast entity timeout, unit is second, range is from 60 to 36000, 600 seconds by default.
5	mvr vlan vlanid	optional, to specify the VLANs for receiving multicast, all source ports should belong to this VLAN. Range is from 1 to 5094. 1 by default.

6	mvr mode { dynamic compatible }	optional, MVR operation modes: Dynamic——Dynamic mode Compatible——Compatible mode
7	exit	Back to privileged EXEC mode
8	show mvr	Show MVR configuration
9	show mvr members	Show MVR group address

To disable MVR, carry out command **mvr disable** under global configuration mode. To set the other configurations back to default status, you can use the command **no mvr {mode | group ip-address | timeout | vlan}**.

Command **mvr group ip-address** indicates which multicast traffic can be received. If this parameter is not specified, all traffics will be received.

The example below shows how to enable MVR, how to configure multicast address, timeout and multicast vlan:

```
raisecom(config)# mvr enable
```

```
raisecom (config)# mvr group 234.5.6.7
```

```
raisecom (config)# mvr timeout 180
```

```
raisecom (config)# mvr vlan 22
```

```
raisecom (config)# mvr mode dynamic
```

To check if the configurations are correct, use command **show**:

```
Raisecom#show mvr
```

```
MVR Running: Enable
```

```
MVR Multicast VLAN: 22
```

```
MVR Max Multicast Groups: 256
```

```
MVR Current Multicast Groups: 1
```

```
MVR Timeout: 180 (second)
```

```
MVR Mode: dynamic
```

To view MVR group address configurations:

```
Raisecom#show mvr members
```

```
MVR Group IP      Status      Members
```

```
-----
234.5.6.7         Inactive    none
```

3.4.3 MVR port information configuration

Under default situation, ports on switch are neither receiving port, nor source ports. User can

configure them under interface configuration mode:

Step	Command	Description
1	config	Enter global configuration mode
2	mvr	enable MVR
3	interface port 3	Enter interface configuration mode
4	mvr	Enable interface MVR
5	mvr type { source receiver }	<p>Mvr type configuration:</p> <p>Source——uplink port can be configured as source port for receiving multicast data, this port cannot be connect directly to subscribers, all source ports should belong to multicast VLAN.</p> <p>Receiver——configured as to connect subscribers straightforward, cannot belong to multicast VLAN.</p>
6	mvr vlan <i>vlanid</i> group <i>ip-address</i>	Optional, set the port to join multicast group statically. Under compatible mode, this command can applied to receiving port, and can be applied to source port or receiving port dynamically.
7	mvr immediate	Enable automatic leaving function on this port, this command can be only applied on receiving port
8	exit	Back to global configuration mode
9	exit	Back to privileged EXEC mode
10	show mvr	Show MVR configuration status
11	show mvr port [<i>portid</i>]	Show port mvr configuration

show mvr members	show MVR group information
show mvr port [portid]	show MVR port configuration information
show mvr port portid members	Show MVR static or dynamic group information

Show MVR global configuration information

Raisecom#show mvr

MVR Running: Enable

MVR Multicast VLAN: 1

MVR Max Multicast Groups: 256

MVR Current Multicast Groups: 0

MVR Timeout: 600 (second)

MVR Mode: Compatible

Show MVR group information

Raisecom#show mvr members

MVR Group IP	Status	Members
--------------	--------	---------

234.5.6.7	Active	1
234.5.6.8	Active	1
234.5.6.9	Inactive	None
234.5.6.10	Inactive	None

show MVR port configuration information

Raisecom#show mvr port

Port	Running	Type	Status	Immediate Leave
------	---------	------	--------	-----------------

1	Enable	Receiver	Inactive/down	Enable
2	Disable	Non-MVR	Inactive/down	Disable
3	Disable	Non-MVR	Inactive/down	Disable
4	Disable	Non-MVR	Inactive/down	Disable
5	Disable	Non-MVR	Inactive/down	Disable
6	Disable	Non-MVR	Inactive/down	Disable
7	Disable	Non-MVR	Inactive/Up	Disable

.....

25	Disable	Non-MVR	Inactive/down Disable
26	Disable	Non-MVR	Inactive/down Disable

To show designated port information:

Raisecom#show mvr port 1

Running: Enable

Type: Receiver

Status: Inactive/down

Immediate Leave: Enable

Show MVR port group information

Raisecom#show mvr port 1 members

MVR Group IP	Type	Status

234.5.6.7	static	Inactive
234.5.6.8	static	Inactive

3.6 Configure MVR Proxy

This part is about how to configure MVR proxy on the switch, including:

- ✧ Default MVR proxy configuration
- ✧ Configure MVR proxy
- ✧ MVR proxy monitoring and maintaining

3.6.1 Default MVR proxy configuration

Feature	State
Message compress function	disable
Querier function	disable
MVR proxy source IP address	Use the IP address of IP port 0, if IP port 0 is not configured, use 0.0.0.0
Query time interval	60s
The maximum responding time of sending query message	10s

The last member sending query interval	1s
---	----

3.6.2 MVR Proxy configuration

By default, MVR proxy is off on the switch. In global configuration mode use the following commands to activate MVR proxy configuration. You can also set source IP address, query time interval, the maximum responding time of sending query message, the last member sending query interval. If MVR proxy is not started, configuring MVR proxy is allowed, and once MVR proxy is started, these configurations will take effect immediately.

Step	Command	Description
1	config	Enter global configuration mode
2	mvr proxy	Start MVR proxy function. When it is started, MVR message compress function and MVR querier function will be started at the same time.
3	mvr proxy suppression	Start message compress function
4	mvr proxy querier	Start querier function
5	mvr proxy source-ip <i>A.B.C.D</i>	Optical, the given MVR proxy packet source IP address. If not configured use the IP address of IP port 0, if IP port 0 is not configured, use 0.0.0.0
6	mvr proxy query-interval <i>seconds</i>	Optical, set the querier query time interval. Default value is 60s, range is 10-65535
7	mvr proxy query-max-response-time <i>seconds</i>	Optical, set the maximum responding time of query message. Default value is 10s, range is 1-25
8	mvr proxy last-member-query <i>seconds</i>	Optical, configure the last member sending query interval, default value is 1s, range is 1-25

To stop MVR proxy, in global configuration mode run command **no mvr proxy** to disable message compress and querier function. In global configuration mode use **no mvr proxy suppression** and **no mvr proxy querier** to disable message compress and querier function respectively. To restore other configurations to default value, use **no mvr proxy {source-ip | query-interval |**

query-max-response-time | mvr proxy last-member-query}.

The following example shows how to start MVR proxy, set the source IP to 192.168.0.1, query interval 100s, query message maximum responding time 20s, the last member sending query interval 5s.

```
Raisecom (config)# mvr proxy
```

```
Raisecom (config)# mvr proxy source-ip 192.168.0.1
```

```
Raisecom (config)# mvr proxy query-interval 100
```

```
Raisecom (config)# mvr proxy query-max-response-time 20
```

```
Raisecom (config)# mvr proxy last-member-query 5
```

Use command **show** to examine if the configuration is correct:

```
Raisecom # show mvr proxy
```

```
Mvr proxy suppression status:          enable
Mvr proxy querier status:              enable
Mvr proxy source ip:                  192.168.0.1
Mvr proxy version:                    V2
Mvr query interval(s):                 100
Query Response Interval(s):            20
Last Member Query Interval(s):         5
Next IGMP general query(s):            5
```

3.7 MVR Proxy monitoring and maintenance

Use the commands below to show MVR proxy configuration and port MVR static.

Command	Description
show mvr proxy	Show MVR proxy configuration
show mvr port [portid] statistics	Show port MVR static
clear mvr port [portid] statistics	Clear port static information

Show MVR proxy configuration:

```
Raisecom # show mvr proxy
```

```
Mvr proxy suppression status:          enable
Mvr proxy querier status:              enable
Mvr proxy source ip:                  192.168.0.1
Mvr proxy version:                    V2
Mvr query interval(s):                 100
Query Response Interval(s):            20
```

Last Member Query Interval(s): 5

Next IGMP general query(s): 5

Show port MVR static

Raisecom # show mvr port statistics

Port 1:

Received query packets: 10

Received report packets: 10

Received leave packets: 10

Drop query packets: 10

Drop report packets: 10

Drop leave packets: 10

Last replace new multicast address: 224.1.1.1

Last replace old multicast address: 224.2.2.2

Total replace count: 5

Port 2:

Received query packets: 10

Received report packets: 10

Received leave packets: 10

Drop query packets: 10

Drop report packets: 10

Drop leave packets: 10

Last replace new multicast address: 224.1.1.1

Last replace old multicast address: 224.2.2.2

Total replace count: 5

.....

3.8 IGMP filter configuration

This part is about how to configure IGMP filter on the switch, including:

- ✧ Default IGMP filter configuration
- ✧ IGMP profile configuration
- ✧ Use IGMP profile

3.8.1 Default IGMP filter configuration

Feature	state
IGMP filter enable/disable	Enabled
Port application	No application
Maximum group	No limit
Maximum group action	Reject
IGMP profile	Not defined
IGMP profile action	reject

3.8.2 IGMP profile configuration

Use command **ip igmp profile** under global configuration mode, you can create IGMP profile and enter profile configuration mode. Parameters such as range, actions and etc. can be configured under this mode.

Step	Command	Description
1	config	Enter global configuration mode
2	ip igmp profile <i>profile-number</i>	Create profile and enter profile configuration mode, series number of profile is from 1 to 65535.
3	permit deny	Optional, actions configuration including permit or deny multicast group access, the default status is deny.
4	range <i>start-ip</i> [<i>end-ip</i>]	IP multicast address or address range configurations. If inputting address range, the starting address, blanks and ending address should be within the group address.
5	exit	Back to global configuration mode
6	exit	Back to privileged EXEC mode
8	show ip igmp profile [<i>profile-number</i>]	Show IGMP profile configuration information

To delete profile, carry out **no ip igmp profile** under global configuration mode. To delete a multicast address of profile, use command **no range start-ip**.

The example below shows how to create profile 1 and configure single multicast address:

```
raisecom(config)# ip igmp profile 1
raisecom (config-profile)# range 234.5.6.7
raisecom (config-profile)# range 234.5.6.9
raisecom (config-profile)# permit
raisecom (config-profile)#exit
raisecom (config)#exit
```

To check if the configurations are correct, use command show:

```
Raisecom#show ip igmp profile 1
IGMP profile 1
    permit
    range 234.5.6.7
    range 234.5.6.9
```

3.8.3 Applying IGMP filter under interface

Use command **ip igmp filter** under interface configuration mode to apply the created IGMP profile on a specified port. One IGMP profile can be applied to multiple ports, but one port can have only one IGMP profile.

Step	Command	Description
1	config	Enter global configuration mode
2	interface port 1	Enter interface mode
3	ip igmp filter <i>profile-number</i>	Apply IGMP profile on the port
4	ip igmp max-groups <i>group-number</i>	Set the maximum number of the groups that is allowed for entry
5	ip igmp max-groups action { deny replace }	The action taken when the group number on the port exceeds the maximum group number
6	exit	Return to global configuration mode
7	exit	Return to privileged EXEC mode
8	show ip igmp filter port	Show the IGMP profile applied

[*portid*]

on the port

To cancel applying IGMP profile, use command **no ip igmp filter** under interface configuration mode. If no IGMP profile is applied to port, no result will be shown.

The example below shows how to apply IGMP profile 1:

```
raisecom(config)# interface port 1
```

```
raisecom (config-port)# ip igmp filter 1
```

```
raisecom (config-port)#exit
```

```
raisecom (config)#exit
```

To check if the configurations are correct, use command **show**:

```
Raisecom#show ip igmp filter port
```

Port	Filter	Max Groups	Current Groups	Action

1	1	20	0	Deny
2	0	20	0	Deny
3	0	0	0	Deny
.....				
25	0	0	0	Deny
26	0	0	0	Deny

To view port 1 information:

```
Raisecom#show ip igmp filter port 1
```

```
IGMP Filter: 1
```

```
Max Groups: 20
```

```
Current groups: 0
```

```
Action: Deny
```

3.8.4 Applying IGMP filter under VLAN

By default, there is no IGMP filter applying rules under VLAN, no maximum group limit, the maximum group action is deny. Follow the steps below in global configuration mode to configure the applied filter rules under VLAN, maximum group limit and maximum action.

Step	Command	Description
1	config	Enter global configuration mode
2	ip igmp filter <i>profile</i> vlan <i>vlanlist</i>	Specify the defined filter rules on VLAN. The applied filter rule

		number should have been created, or the configuration fails. <i>Vlanlist</i> range is 1-4094.
3	<code>ip igmp max-group max-group vlan <i>vlanlist</i></code>	Set the maximum group number on specified VLAN. The configured maximum group number must be no larger than the maximum group number that the equipment supports
4	<code>ip igmp max-group action {deny replace} vlan <i>vlanlist</i></code>	Configure the maximum group action the specified VLAN, default value is 'deny'.
5	<code>exit</code>	Return to privileged EXEC mode
6	<code>show ip igmp filter vlan [<i>vlanid</i>]</code>	Show the configured filter information under VLAN.
7	<code>config</code>	Enter global configuration mode
8	<code>ip igmp filter <i>profile</i> vlan <i>vlanlist</i></code>	Specify the defined filter rules on VLAN. The applied filter rule number should have been created, or the configuration fails. <i>Vlanlist</i> range is 1-4094.

Use **no ip igmp filter vlan *vlanlist*** to delete the configured filter rules under VLAN, use **no ip igmp max-group vlan *vlanlist*** to delete the configured maximum group limit under VLAN.

The following example shows how to apply filter rules under VLAN and configure the maximum group limit and maximum group action:

```
Raisecom (config)# ip igmp filter 1 vlan 1
```

```
Raisecom (config)# ip igmp max-group 10 vlan 1
```

```
Raisecom (config)# ip igmp max-group action replace vlan 1
```

Use the command **show** to examine if the configuration is correct

```
Raisecom # show ip igmp filter vlan 1
```

VLAN	Filter	Max Groups	Current Groups	Action
1	1	10	0	Replace

3.9 IGMP filter monitoring and maintenance

Use some **show** commands to show the switch IGMP filter running state and configuration state for monitoring and maintenance. Use the following **show** commands to do IGMP filter monitoring and maintenance:

Command	Description
show ip igmp filter	Show IGMP filter global configuration information
show ip igmp profile [<i>profile-number</i>]	Show IGMP profile information
show ip igmp filter port [<i>portid</i>]	Show IGMP filter port configuration information
show ip igmp filter vlan [<i>vlanid</i>]	Show the IGMP filter rules configuration under specified VLAN. When <i>vlanid</i> is not specified, show the configuration state of VLAN that have been configured filter rules.

3.10 Typical configuration example

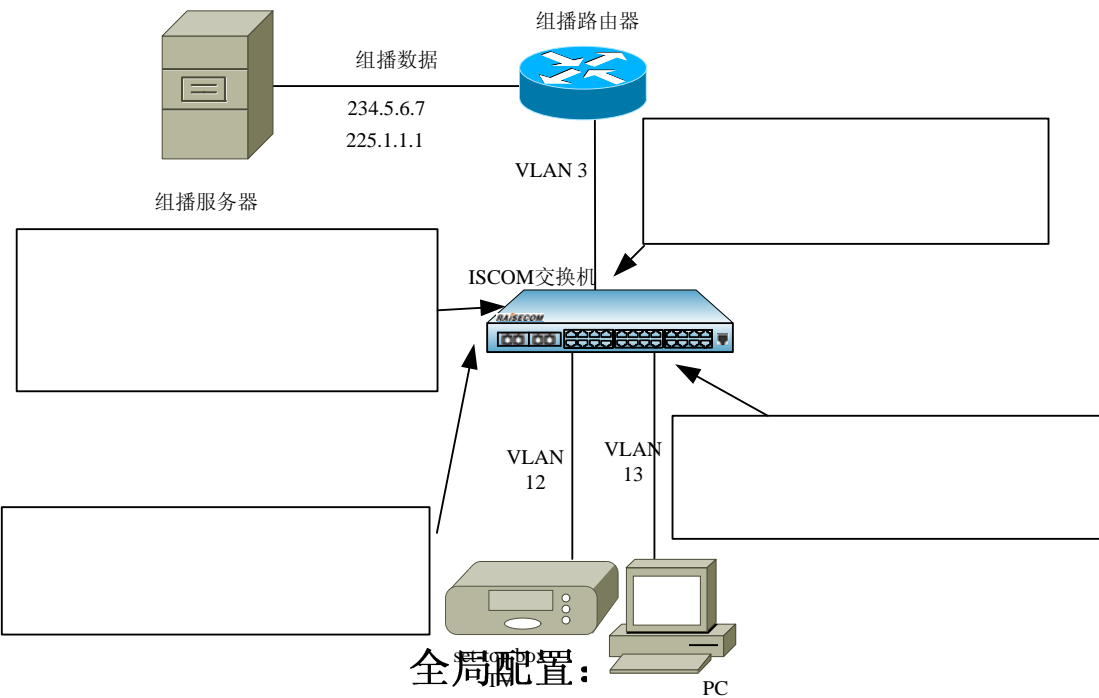
3.10.1 MVR typical configuration example

PC or TV set-top box can receive multicast traffics, one or multiple PC or televisions can connect to a receiving port called subscriber. When selecting scheduled programs, set-top or PC sends IGMP report information to join a group. If IGMP report matches to the configured multicast addresses on the switch, the CPU on the switch will modify the multicast switch table in the hardware, and add this port to the multicast VLAN group. When the source port receives the multicast traffic, it will send the traffic to the receiving ports according to the multicast forwarding table in the hardware.

When switching channels or shutting down the TV, the set-top box or PC will send IGMP leaving information, then the switch will forward this information to the multicast router, the router will send IGMP query information, if there is no other member in this group, the switch will delete this port from the group.

If enabling immediate leaving function on the receiving port, port will leave the group faster. If the immediate leaving function is not enabled yet, when the receiving port receives IGMP leaving information, the switch will forward router's IGMP query information and wait IGMP member report. If no report is received within the maximum query time, the member will be deleted from the group. If enabling the immediate leaving function, port member will be deleted as soon as it receives IGMP leaving information. This feature is normally used in the situation that one port is connected to only one user.

Multicast traffic will not be transmitted in all VLANs, but only need to be transmitted in multicast VLAN. Use can save much bandwidth in this way.



全局配置:

```
raisecom(config)#mvr enable
raisecom(config)#mvr mode dynamic
raisecom(config)#mvr vlan 3
raisecom(config)#mvr group 234.5.6.7
raisecom(config)#mvr group 225.1.1.1
```

Fig 3-1 MVR application topology

3.10.2 MVR proxy typical configuration example

Enable MVR proxy on ISCOM switch. Configure port 1 to source port, port 2 and 3 to receive port. In the figure below, when PC and set-top box for the same multicast group, the switch will receive two IGMP report messages, and send only one IGMP report message to the multicast router. The IGMP query message sent from multicast router will no longer transmit to downstream, but send IGMP query message by the switch periodically.

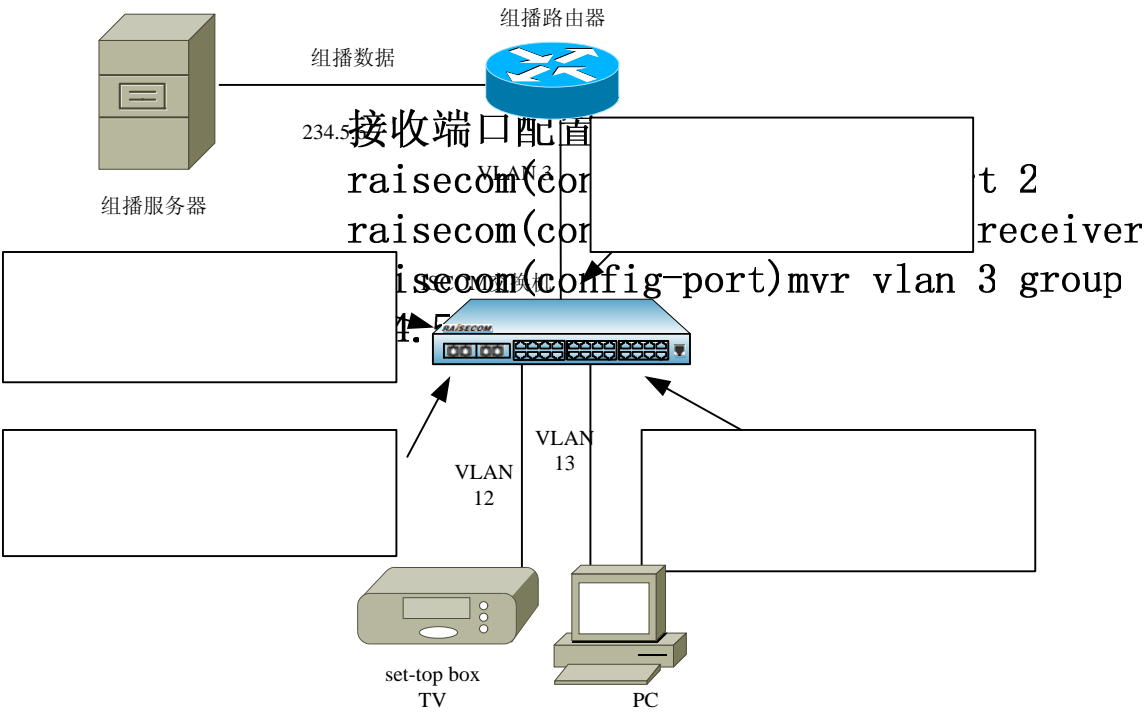


Fig 3-2 MVR proxy application topology

3.10.3 IGMP filter under VLAN typical configuration example

Enable IGMP filter on the switch, establish filter rule profile 1, and set address range from 234.5.6.7 to 234.5.6.10, the action is set to allow. According to the IGMP filter rule under VLAN 12, PC and set-top box can both enter the multicast group 234.5.6.7, PC can join the multicast group 234.5.6.11 while set-top box can not. According to the maximum group limit of VLAN 12, after set-top box enter 234.5.6.7, if it enter 234.5.6.8, it will quit from the multicast group 234.5.6.7 before.

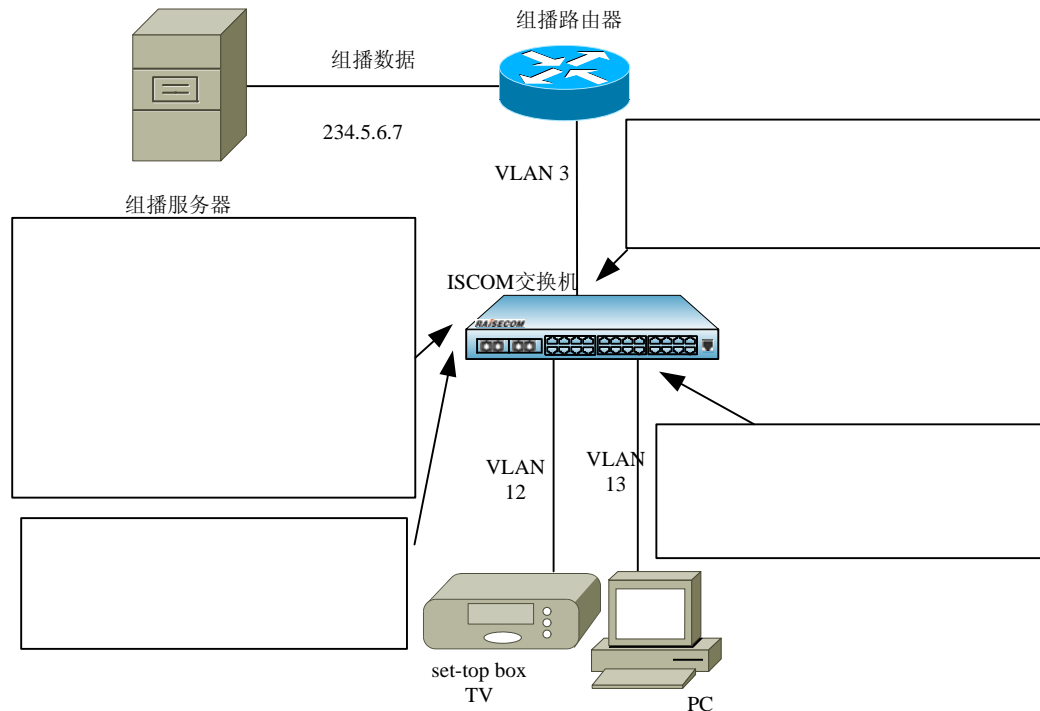


Fig 3-3 the IGMP filter application topology under VLAN

3.10.4 The IGMP filter under port typical configuration example

Enable IGMP filter on the switch, establish filter rule profile 1, and set address range from 234.5.6.7 to 234.5.6.10, the action is set to allow. According to the IGMP filter rule under port 2, PC and set-top box can both enter the multicast group 234.5.6.7, PC can join the multicast group 234.5.6.11 while set-top box can not. According to the maximum group limit of port 2, after set-top box enter 234.5.6.7, if it enter 234.5.6.8, it will quit from the multicast group 234.5.6.7 before.

全局配置

```
raisecom(config)#mvr enable
raisecom(config)#mvr mode dynamic
raisecom(config)#mvr vlan 3
raisecom(config)#mvr proxy
raisecom(config)#ip igmp filter 1
vlan 12
raisecom(config)#ip igmp max-group
1 vlan 12
raisecom(config)#ip igmp max-group
action replace vlan 12
```

接收端口配置:

```
raisecom(config)#interface port 2
raisecom(config-port)mvr type
receiver
raisecom(config-port)mvr
```

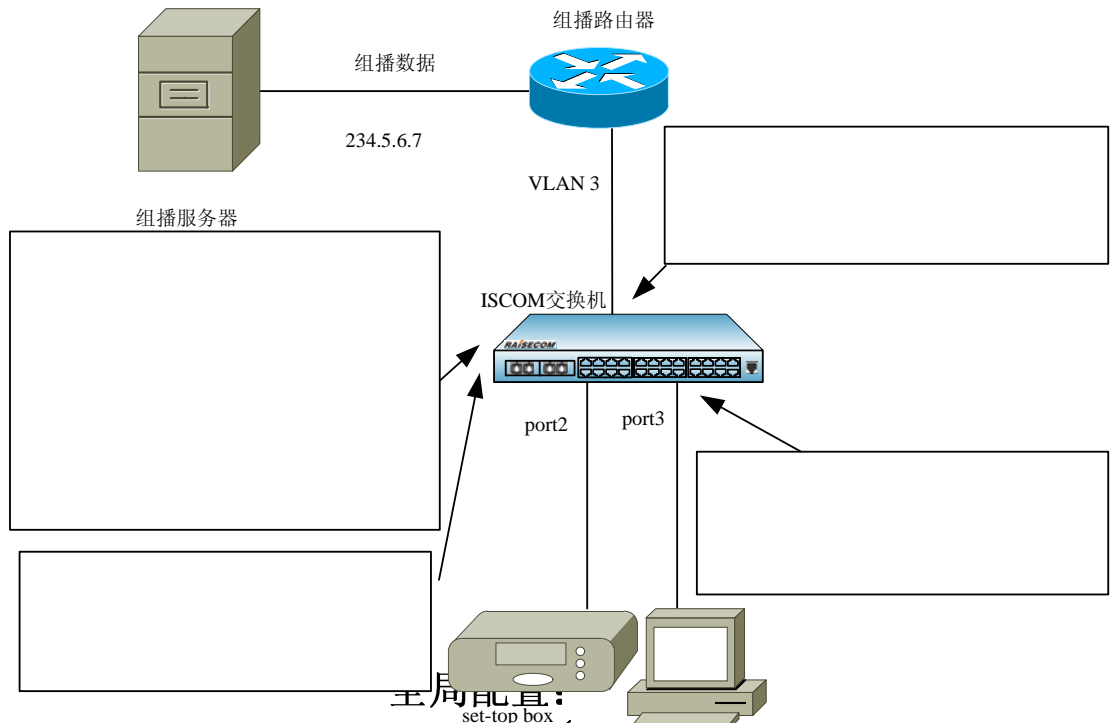


Fig 3-4 the IGMP filter application topology under port

3.11 MVR, MVR Proxy and IGMP filter trouble shooting

1. When configuring source port, it is not within multicast VLAN;
2. When configuring receive port, it is in multicast VLAN;
3. When configuring MVR group, the group addresses conflict because several IP multicast addresses suit one MAC multicast address;
4. When configuring stable group on the port, the address is not within MVR range;
5. In MVR compatible mode, configure stable multicast on source port.

接收端口配置:

```
raisecom(config)#interface port 2
raisecom(config-port)mvr type
receiver
raisecom(config-port)mvr
```




北京瑞斯康达科技发展有限公司
RAISECOM TECHNOLOGY CO.,LTD.

Address: 2nd Floor, South Building of Rainbow Plaza, No.11 Shangdi Information Road,
Haidian District, Beijing Postcode: 100085 Tel: +86-10-82883305 Fax: +86-10-82883056
Email: export@raisecom.com <http://www.raisecom.com>