www.raisecom.com

ISCOM5508 (A) Configuration Guide (Rel_03)

Raisecom Technology Co., Ltd. provides customers with comprehensive technical support and services. For any assistance, please contact our local office or company headquarters.

Website: http://www.raisecom.com

Tel: 8610-82883305

Fax: 8610-82883056

Email: export@raisecom.com

Address: Building 2, No. 28, Shangdi 6th Street, Haidian District, Beijing, P.R.China

Postal code: 100085

Notice

Preface

Objectives

This document introduces supported characters and related configurations of the ISCOM5508, including basic configuration, data service configuration, multicast service configuration, CATV service configuration, TDMoP service configuration, MAC address table configuration, VLAN configuration, Spanning Tree configuration, route configuration, DHCP configuration, QoS configuration, system security configuration, link security configuration, and system management configuration. In addition, this document provides related configuration examples. The appendixes of this document can help you understand termss and abbreviations involved in this document.

This guide helps you master basic principles and configurations of the ISCOM5508, as well as networking with the ISCOM5508.

Versions

The following table lists the product versions related to this document.

Product name	Hardware version	Software version
ISCOM5508	A.00 or later	V1.42 or later

Related manuals

The following table lists manuals and their contents related to the ISCOM6800.

Name	Description
ISCOM5508 Product Description	This guide includes product overview, networking applications, system structure, EPON feature, function and features, networking applications, management and maintenance, technical specifications, hardware installation, software installation and appendix.

Name	Description
ISCOM5508 Hardware Description	This guide mainly includes product overview, chassis, fan module, card overview, system management card, EPON interface card, Gigabit Ethernet card, 10 Gigabit Ethernet card, power card, cables, lookup table of interfaces and module specifications, and appendix.
ISCOM5508 Configuration Guide	This guide mainly includes basic configurations, data service configurations, multicast service configurations, VoIP service configurations, CATV service configurations, TDM service configurations, MAC address table configurations, VLAN configurations, Spanning Tree configurations, route configurations, DHCP configurations, QoS configurations, OAM configurations, system security configurations, link security configurations, and system management configurations.
ISCOM5508 Command Reference	This guide mainly includes commands used for configuring the following features: basic configuration, Ethernet, route, clock synchronization, network reliability, OAM, security, DHCP, QoS, multicast, and system management.
ISCOM5508 Maintenance Guide	This guide mainly includes safety introduction, routine maintenance, troubleshooting procedures, system trouble shooting, data troubleshooting, voice troubleshooting, and commonly-used maintenance commands table.
ISCOM5508 Installation Guide	This guide mainly includes safety introduction, installation preparation, installing the chassis, installing components, wiring cables, hardware installation check, power on check, and installation reference.
ISCOM5508 Quick Installation Guide	This guide mainly describes installation procedures, including installation tools, precaution, installation scenario, installation conditions, and installation steps.

Conventions

Symbol conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
	Indicates a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.
	Indicates a potentially hazardous situation that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.
	Provides additional information to emphasize or supplement important points of the main text.
	Indicates a tip that may help you solve a problem or save time.

General conventions

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Arial	Paragraphs in Warning, Caution, Notes, and Tip are in Arial.
Boldface	Names of files, directories, folders, and users are in **boldface**. For example, log in as user **root**.
Italic	Book titles are in *italics*.
`Lucida Console`	Terminal display is in `Lucida Console`.

Command conventions

Convention	Description
Boldface	The keywords of a command line are in **boldface**.
Italic	Command arguments are in *italics*.
[]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x | y | ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[x | y | ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x | y | ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[x | y | ...] *	The parameter before the & sign can be repeated 1 to n times.

Configuration mode prompt conventions

Convention	Description
/:*	ONU ID. The specified value of * varies on the actual value.
:	PON interface ID. The specified value of * varies on the actual value.
//*:*	ONU UNI interface ID. The specified value of * varies on the actual value.

Change history

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Issue 03 (2012-08-24)

The document is updated as follows:

- Modify known BUG.
- Add following configurations:
  - ONU call process voice parameters
  - ONU port rate limiting template
  - ONU VLAN configuration template
  - ONU IGMP Proxy
  - OSPF route
  - ARP Proxy
  - MVR dynamic multicast address learning
  - SIP DigitMap
- Optimize following configurations:
  - Statistics function on switching port
  - ONU MAC address statistic function
  - PON + LAN NMS configuration program
  - Card-based IGMP Snooping
  - ONU status display and status description of ONU dying gasp in CLI
  - 32-bit ONU POTS port telephone number

Issue 02 (2012-04-23)

The document is updated as follows:

- Modify known BUG.
- Add following configurations:
  - Hand-in-hand uplink port protection

  - ONU QoS template
- Optimize following configurations:
  - How to clear MACaddress table

Issue 01 (2011-11-30)

Initial commercial release

Contents

Figures

Tables

1 Basic configuration

The chapter introduces the basic configuration information and configuration process of ISCOM5508 device, and provides related configuration applications.

- Command line
- Accessing the device
- Configuring NM
- Configuring port management
- Configuring time management
- Configuring file management
- Load and upgrade
- Configuring task scheduling
- Configuring user permission and careful management
- Configuration examples

1.1 Command line

1.1.1 Overview of command line

Command line is a channel between users and devices to communicate with each other. Users can configure, monitor and manage the device by corresponding command lines.

Users can login the device by terminal device or running PC of terminal simulation program. It enters interface of command line if there is a prompt of command line.

There are some features of command line interface:

- Allow local configuration on console interface. Allow local or remote configuration by Telnet, SSHv2 (Secure Shell v2).Different levels of users can only execute the corresponding levels of commands. Different types of command lines belong to different command line modes, and users can execute some type of configuration only if it is in the corresponding command line mode.
- Users can use shortcut key to operate commands. Users can see or execute a history command by invoking history record (20 history commands at most).Users can enter "?" to get help online. It provides many intelligent analytic methods.

1.1.2 Level of command line

ISCOM5508 device takes cascade protection on command line, and command lines are divided as 16 levels.

- 0–4: visit class, users can execute tool command of network diagnoses (ping), clear statistics commands (clear), show history record commands (history) and so on.
- 5–10: monitor class, users can execute system maintenance commands (show).
- 11–14: configuration class, users can execute some configuration commands which are used to configure VLAN (Virtual Local Area Network), IP route and so on.
- 15: management class, it is used to execute basic commands in system.

1.1.3 Command line mode

Command line mode is interface environment which is used to execute command lines. All commands in system are registered in different command line modes, and commands can be executed only if it is in the corresponding mode.

We create a connection between terminal and ISCOM5508 device, if the device has default configuration, it will enter User EXEC:

```
Raisecom>
```

Input command **enable** and correct password and carriage return to enter Privileged EXEC.

```
Raisecom>enable
Password:
Raisecom#
```

In Privileged EXEC mode, input command **config** and enter global configuration mode.

```
Raisecom#config
Raisecom(config)#
```

In Privileged EXEC mode, input command **fttx** and enter global configuration mode of EPON system.

```
Raisecom#fttx
Raisecom(fttx)#
```

The command line prompt "Raisecom" is default host name of device, and users can modify name of host by command **hostname** *string* in Privileged EXEC mode. Some commands which are realized in global configuration mode can also be realized in other modes, but realized functions refer to command line modes.
In generally, the command **quite** or **exit** can be used to return to upper level of command line mode, but Privileged EXEC can return to User EXEC only by command **disable.**
All command line modes, except for User EXEC or Privileged EXEC mode, can return to Privileged EXEC mode by command **end**.

Mode	Access	Identifier
User EXEC	Log onto ISCOM5508 device and input user name and password.	`Raisecom>`
Privileged EXEC	Use the command **enable** and input password under User EXEC mode.	`Raisecom#`
Global configuration mode	Use the command **config** under Priviledged EXEC mode.	`Raisecom(config)#`
Interface port configuration mode	Use the command **interface port** *port-id* under Global configuration mode.	`Raisecom(config-port)#`
Interface range configuration mode	Use the command **interface range** *port-list* under Global configuration mode.	`Raisecom(config-range)#`
Interface IP configuration mode	Use the command **interface ip** *if-number* under Global configuration mode.	`Raisecom(config-ip)#`
VLAN configuration mode	Use the command **vlan** *vlan-id* under Global configuration mode.	`Raisecom(config-vlan)#`
Class Map configuration mode	Use the command **class-map** *class-map-name* [**match-all**|**match-any**] under Global configuration mode.	`Raisecom(config-cmap)#`
Policy Map configuration mode	Use the command **policy-map** *policy-map-name* under Global configuration mode.	`Raisecom(config-pmap)#`
Traffic classification configuration mode	Use the command **class-map** *class-name* under Policy Map configuration mode.	`Raisecom(config-pmap-c)#`
Access list configuration mode	Use the command **access-list-map** *access-list-map-number* {**permit**|**deny**} under Global configuration mode.	`Raisecom(config-aclmap)#`
EPON Global configuration mode	Input the command **fttx** in Priviliged EXEC mode.	`Raisecom(fttx)#`
SLOT configuration mode	Input the command **slot** *slot-id* in Global mode of EPON system.	`Raisecom(fttx-slot:slot-id )#`
OLT configuration mode	Input the command **interface olt** *slot-id/olt-id* in Global mode of EPON system.	`Raisecom(fttx-oltslot-id:olt-id)#`

Mode	Access	Identifier
OLT range configuration mode	Input the command **interface range olt** *slot-id*/*olt-list* in Global mode of EPON system.	`Raisecom(fttx-olt-range)#`
ONU configuration mode	Input the command **interface onu** *slot-id*/*olt-id*/*onu-id* in Global mode of EPON system.	`Raisecom(fttx-onu`*slot-id*`/`*olt-id*`:`*onu-id*`)#`
ONU range configuration mode	Input the command **interface range onu** *slot-id*/*olt-id*/*onu-list* in Global mode of EPON system.	`Raisecom(fttx-onu-range)#`
ONU UNI Ethernet port configuration mode	Input the command **uni ethernet** *uni-id* in ONU configuration mode.	`Raisecom(fttx-onu-uni` *slot-id*`/`*olt-id*`/`*onu-id*`:`*uni-id*`)#`
ONU UNI Ethernet port range configuration mode	Input the command **uni range ethernet** *uni-id-list* in ONU configuration mode.	`Raisecom(fttx-onu-uni-range)#`
ONU voice configuration mode	Input the command **voice** in ONU configuration mode.	`Raisecom(fttx-onu-voice` *slot-id*`/`*olt-id*`:`*onu-id*`)#`

1.1.4 Shortcut key of command line

Shortcut key	Description
up arrow (↑)	The previous command;
down arrow (↓)	The next command;
left arrow (←)	Move the cursor for one character toward left;
right arrow (→)	Move the cursor for one character toward right.
Backspace	delete the character before the cursor;
Tab	System will proceed partial help if users input incomplete key word and press **Tab** key: if matched key word isn't unique, system replace it by complete key word and leave a blank space between cursor and end of the last letter; if they are not matched or matched key word is not unique, we should see prefix firstly, and enter Tab key to translate words circularly, we don't leave a blank space between cursor and end of the last letter, enter spacebar to input next word.if a wrong key word is inputted, enter Tab key, line feeds and show wrong information and the key word doesn't change.
"Ctrl+A"	Move the cursor to the beginning of row.
"Ctrl+D" or "Delete"	Delete the character after the cursor.
"Ctrl+E"	Move the cursor to the end of row.

Shortcut key	Description
"Ctrl+K"	Delete all characters after the cursor (include the position of the cursor).
"Ctrl+X"	Delete all characters before the cursor (not include the position of the cursor).
"Ctrl+Z"	Return to Privileged EXEC mode from other modes (not include User EXEC mode).
"Space"or "y"	Continue to show information on next screen if command line of terminal print has exceeded.
"Enter"	Continue to show information on next row if command line of terminal print has exceeded.

1.1.5 Display of command line

Display attribute

Command line interface provides the following display attributes:

- We provide two voice display (Chinese and English) in help information and prompt information of command line interface.We provide pause function if display information is more than one screen, and users can choose the following function keys:

Table 1-1 Description for keys to display attribute

Function key	Description
Enter "Space" or "y"	Continue to show information in the next screen;
Enter "Enter"	Continue to show information in the next line;
Enter any character key (except for "y")	Stop display and execute commands;

Display information filtering

ISCOM5508 device provides a series of command lines which begin with "**show**" to show configuration, running status or diagnostic message of the device. Users can add filtering rules of information to remove unwanted information.

The command **show** supports three kinds of filtering ways:

- | **begin** *string*: show all lines starting from matched specific character string.
- | **exclude** *string*: show all lines which don't match specific character string.
- | **include** *string*: show all lines which only match specific character string.

Page break of display information

Device provides pause function if the display information is more than one screen, users can refer to Table 1-1.

Configuration	Description
Raisecom#**terminal page-break enable**	Enable Page break of display information.By default, Enable Page break of display information;

1.1.6 Viewing history command

ISCOM5508 device saves the latest 20 history commands in the buffer by default. Users can use command **history** to view or proceed history command record in any command mode.

Users are authorized to set history commands number saved in system by the command **terminal history** in User EXEC mode.

```
Raisecom>terminal history count
```

1.1.7 Getting help

Complete help

Users can get complete help in the following three situations:

- Users can press "?" key to get all command lines and description under the view in any command line mode.

```
Raisecom>?
```

Displayed information:

```
clear   Clear screen
clock   System time and date
config   Configuration from terminal interface
debug   Debugging functions
dir  Flash file system
disable  Turn off privileged mode command
download  Download system file from server
enable   Enable command information
erase   Erase configuration information
exit  Exit current mode and down to previous mode
fttx  FTTX configuration modeclear Clear screen
```

- Input a command, leave a blank space and input "?". If there is a key word, the screen will lists all key words and description.

```
Raisecom#clock ?
```

Displayed information:

```
mode   Clock mode
set   Set system time and date
summer-time Set summer time
timezone Set system timezone offsetpeer
```

- Input a command, leave a blank space and input "?". If there is a parameter, the screen will list range of the parameter and its effect.

```
Raisecom(config)#interface ip ?
```

Displayed information:

```
<0-14> IP interface number
```

Partial help

Users can get partial help in the following three situations:

- Input a string, leave a blank space and input "?". The device will show all key words which begin with the beginning of the string.

```
Raisecom(config)#c?
```

Displayed information:

```
clear  Clear screen
clock  System time and date
config Configuration from terminal interfaceclass-map  Set class map
```

- Input a command line, leave a blank space and input "?". The device will show all key words which begin with the string of the command line in current mode.

```
Raisecom(config)#show c?
```

Displayed information:

```
class-map  QoS class map information
clock  System date and time
cpu-utilization CPU utilization
ctrl-multicast  Controllable multicast
```

- Input the first letters of a key word in a command line, and press **Tab** and show a complete key word. It can be realized if the first letters stand for the key word uniquely, otherwise device will gives different key words circularly if users press **Tab** repeatedly, users can select required key word from them.

Description of wrong prompting message

The device will show the following wrong prompting message according to wrong types if users input wrong commands:

Wrong prompting message	Description
% " * " Incomplete command...	Command line is incomplete;
% Invalid input at '^' marked.	"^" stands for that the key word is illegal and nonexistent;
% Ambiguous input at '^' marked, follow keywords match it.	"^" stands for that the key word is ambiguous;
% Unconfirmed command.	Users don't input a unique command line;
% Unknown command.	The command line isn't existed;
% You Need higher priority!	Users can't execute the command line because they don't have the authority;

1.2 Accessing the device

1.2.1 Accessing the device through Console port

Console port is a common port which connects a network device with a PC running terminal simulation program. Users can configure and manage the local device by Console port. This management approach is the band (out-of-band) management. It does not need to communicate with the network, so even if the network is not running properly, it can control (console) port to configure and manage devices.

If users can't login a device by telnet, it can login and configure device by console port.

If users want to login a device through PC connecting with console port, firstly, users should connect console port of cable device with RS-232 of PC as figure 1-1; secondly, users should run terminal simulation program, such as "Hyper Terminal" program of windows XP operation system, and configure communication parameters as below table shows; finally, users can login the device.

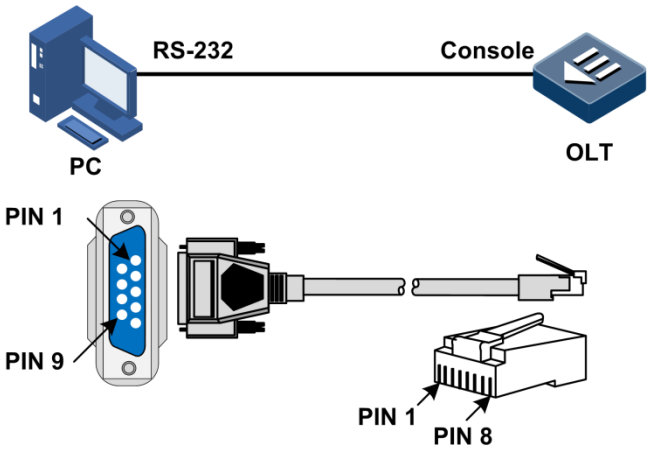

Figure 1-1 Logging in to the device from PC connected with Console port

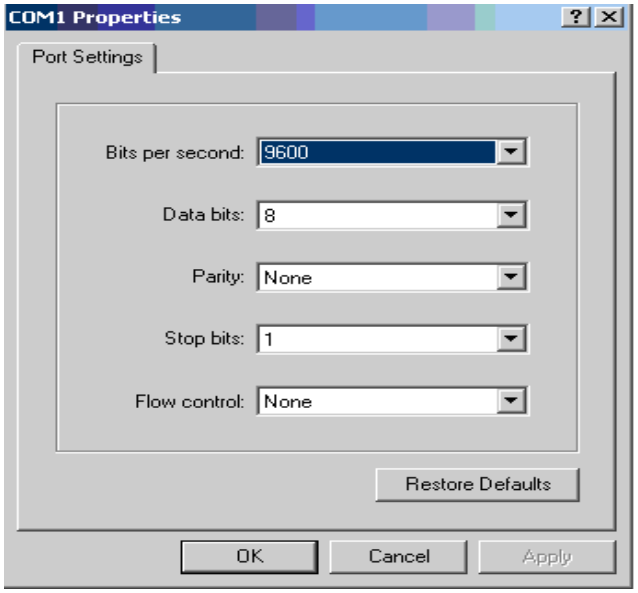

Figure 1-2 Communication parameters configuration in "HyperTerminal"

Note

Microsoft Company is not in support of hyper-terminal since Windows Vista system, users operate Windows Vista or Windows 7 system please download HyperTerminal program from internet. It is free to download HyperTerminal program.

1.2.2 Accessing the device through Telnet

Telnet provides an approach to login a device remotely. Users can login a network device by a PC, and then login other network devices in internet by Telnet approach, so they don't need to

connect the PC with all network devices. Users should ping and get response between devices and the PC before they login devices by telnet.

ISCOM5508 device provides the following services:

- Telnet Server: users run telnet client program to login device on PC, configure and manage the device as figure below.

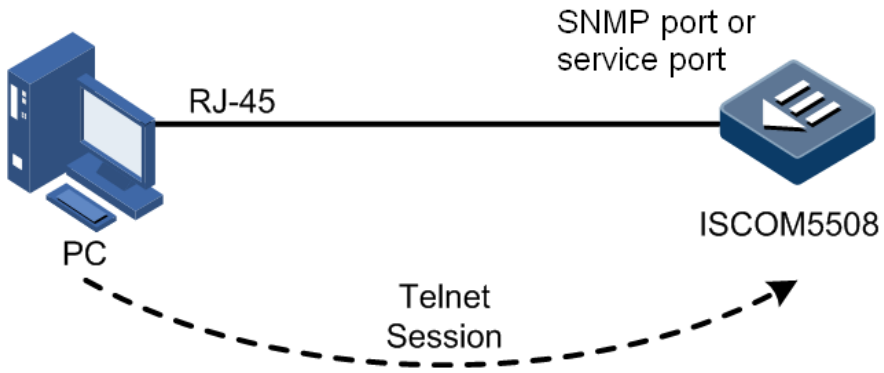

Figure 1-3 Telnet Server

Users should login device by console port and enable telnet service before they login device by telnet. Configure the device which needs to enable telnet service as below table:

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode;
2	`Raisecom(config)#interface ip` *if-number*	Enter layer-3 interface mode;
3	`Raisecom(config-ip)#ip address` *ip-address* [*ip-mask*] [*vlan-id*]	Configure IP address, mask and VLAN binding of specified IP, the VLAN can enable telnet service;
4	`Raisecom(config-ip)#exit`	Return to global configuration mode from layer-3 interface mode;
5	`Raisecom(config)#telnet-server accept port-list` *port-list*	Configure the port which can enable telnet service;
6	`Raisecom(config)#telnet-server max-session` *number*	(Optional) configure the maximum linking number of telnet;

- Telnet Client: users can connect to a device by simulation program of Hyper Terminal or telnet client program, and login other devices by command **telnet**, configure and manage the devices. ISCOM5508 device provides Telnet Client and Telnet Server as figure below.

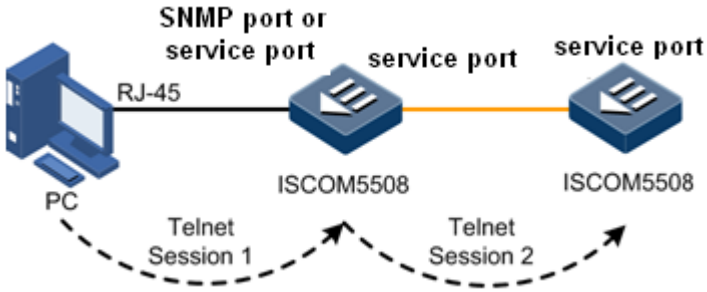

Figure 1-4 Telnet Client

Configuration	Description
`Raisecom#telnet` *ip-address* [`port` *port-id*]	Login other devices by telnet;

1.2.3 Accessing the device through SSHv2

It's dangerous to transmit data by telnet, because telnet doesn't have security certification and it uses TCP to transmit data. Telnet service leads to DoS (Denial of Service), IP address deceiving of host, route deceiving and so on.

Users don't accept to use traditional Telnet and FTP to transmit password and data. Sshv2 is a network security protocol, and prevents information leakage effectively in remote management process by encrypting network data.

SSHv2 can share data by TCP, and creates a safe channel on TCP. SSHv2 service supports port 22 and other service port to prevent illegal attacks.

Users login and enable SSHv2 service by console port.

Default configuration of sshv2 service on ISCOM5508 device:

Function	Default value
SSHv2 server status	Disable
RSA public key	None
Length of local SSHv2 key	512bit
Authentication	local user-password (use local user name and password to validate users)
SSHv2 server Authentication timeout period	600s
SSHv2 server to allow authentication failures	20 times
SSHv2 interception port number	22
SSHv2 session status	enable

Configure the device to enable sshv2 service:

Step	Configuration	Description
1	Raisecom#**config**	Enter the global configuration mode;
2	Raisecom(config)#**generate ssh-key**	Generate SSHv2 server key pair;
3	Raisecom(config)#**ssh2 server**	Start SSHv2 server;
4	Raisecom(config)#**ssh2 server authentication** { **password** | **rsa-key** | **public-key** }	Configure sshv2 authentication of device;
5	Raisecom(config)#**ssh2 server authentication-timeout** *timeout*	(Optional) configure timeout of sshv2 server authentication. Device will disconnect and stop authentication if time exceeds the upper limit;
6	Raisecom(config)#**ssh2 server authentication-retries** *count*	(Optional) configure the maximum number that allowing authentication failures. Device will disconnect and stop authentication if the times exceed the upper limit;
7	Raisecom(config)#**ssh2 server port** *port-id*	Configure sshv2 interception port number of device. **Note** New parameters won't take effect until restart sshv2 service.
8	Raisecom(config)#**ssh2 server session** *session-list* **enable**	Enable sshv2 session of device;

1.2.4 Managing login users

Users can connect PC with console port and input initial user name and password to login device and configure the device for the first time.

Note

At first, user name and password of device is Raisecom.

All remote users can login device by telnet or visit network by creating PPP (Point to Point Protocol) if SNMP (Simple Network Management Protocol) port or other service ports have configured IP address. It's dangerous for device and network. So we need to create user name and password for users and manage users.

Step	Configuration	Description
1	Raisecom#**user name** *username* **password** *password*	Create or modify user name and password;
2	Raisecom#**user name** *username* **privilege** *level*	Configure level and authority of users;

1.2.5 Checking configuration

No.	Item	Description
1	Raisecom#**show telnet-server**	Show port which supports Telnet and the maximum number of telnet connection.
2	Raisecom#**show ssh2 server**	Show SSHv2 server.
3	Raisecom#**show ssh2 session**	Show SSHv2 session.
4	Raisecom#**show ssh2 public-key authentication**	Show SSHv2 public-key authentication.
5	Raisecom#**show user** [**detail**]	Show user information.

1.3 Configuring NM

1.3.1 Default configuration of out-of-band/inner band NM

Function	Default value
Out-of-band NM	Default IP is 192.168.18.100.
Inner band NM	none

1.3.2 Configuring out-of-band NM

SNMP port is used in out-of-band NM on ISCOM5508. Users only need to configure IP address of SNMP port if users need to configure out-of-band NM.

Step	Configuration	Description
1	Raisecom#**config**	Enter the global configuration mode;
2	Raisecom(config)#**management-port ip address** *ip-address* [*netmask*]	Configure IP address of out-of-band management port; **Note** IP addresses will be classified according to default approach if users don't configure subnet mask.

1.3.3 Configuring inner band NM

User has to do below configuration as below on device to create layer-3 interface and configure IP address.

Step	Configuration	Description
1	Raisecom#**config**	Enter the global configuration mode;
2	Raisecom(config)#**create vlan** *vlan-id* **active**	Create and enable VLAN;
3	Raisecom(config)#**interface ip** *if-number*	Enter layer-3 interface mode;
4	Raisecom(config-ip)#**ip address** *ip-address* [*ip-mask*] *vlan-id*	Configure IP address of layer-3 interface and associate with static VLAN ID;

Ethernet port must belong to the associated static VLAN of layer-3 interface in order to perform inner band management. Refer to VLAN configuration for the VLAN detailed configuration.

When user has to make cross-network management for ISCOM5508, that is to say, when a message to be forwarding cannot be tranamitted to destination network routing, user can use the command of **ip default-gateway** to forward all messages to default gateway.

User has to do below configuration on device to configure default gateway.

Step	Configuration	Description
1	Raisecom#**config**	Enter the global configuration mode;
2	Raisecom(config)#**ip default-gateway** *ip-address*	Configure default gateway;

1.3.4 Checking configuration

No.	Item	Description
1	Raisecom#**show management-port ip**	Show IP information of out-of-band management port;
2	Raisecom#**show interface ip**	Show IP information of layer-3 interface;
3	Raisecom#**show ip route**	Show route table;

1.4 Configuring port management

1.4.1 Default configuration of port management

Default configuration of OLT port management

Default configuration of Ethernet electrical port on ISCOM5508 as following:

Function	Default value
State of port	enable
Rate of port	auto (auto-negotiation)
Duplex mode of port	auto (auto-negotiation)
Flow control	disable
Automatic recognition for crossover network cable and straight-through cable function	normal
MTU on port	1526 byte
Refresh frequency of dynamic statistics on port	2 s

Default configuration of ONU port management

Function	Default value
State of port	enable
Rate of port	auto (auto-negotiation)
Duplex mode of port	auto (auto-negotiation)
Flow control	disable
MTU on port	1596 byte
Refresh frequency of dynamic statistics on port	2 s

1.4.2 Configuring basic attribute of ports

Configuring basic attribute of OLT port

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**system mtu** *size*	Configure MTU (Maximum Transmission Unit) of all ports, namely the maximum number of bytes in message which are permitted to pass through port one time (no fragmentation). Device will discard a message if it exceeds the maximum number of bytes which are permitted to pass through port;
3	Raisecom(config)#**interface port** *port-id*	Enter physical layer port configuration mode;
4	Raisecom(config-port)#**speed** { **auto** | **10** | **100** | **1000** }	Configure rate of port, rate of optical port refers to specification of optical module;

Step	Configuration	Description
5	Raisecom(config-port)#**duplex** { **full** | **half** }	Configure duplex mode of port; Ethernet physical layer has two working mode: half-duplex and full-duplex mode; half-duplex can send or receive message at all time; full-duplex can send and receive messages at all time; self-negotiation means that devices on both end of a link select duplex mode according to interactive information, the devices use same duplex mode to transmit messages by negotiation;
6	Raisecom(config-port)#**mdi** { **auto** | **normal** | **across** }	Enter port MDIX mode;
7	Raisecom(config-port)#**description** *word*	Configure description of physical port;

Configuring basic attribute of ONU port

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system.
2	Raisecom(fttx)# **interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode.
3	Raisecom(fttx-onu*/*:*)#**system mtu** *size*	Configure MTU of all ports, namely the maximum number of bytes in message which are permitted to pass through port one time (no fragmentation). Device will discard a message if it exceeds the maximum number of bytes which are permitted to pass through port.
4	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter ONU UNI Ethernet port configuration mode;
5	Raisecom(fttx-onu-uni*/*/*:*)#**speed** { **auto** | **10** | **100** | **1000** } **duplex** { **half** | **full** }	Configure rate and duplex mode of ONU Ethernet port.
6	Raisecom(fttx-onu-uni*/*/*:*)#**uni name** *name*	Configure description of physical port.

1.4.3 Configuring statistical function of ports

Configuring statistics of OLT port

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**dynamic statistics time** *period*	Configure time interval of dynamic statistics on port. Range is 2s–300s.
3	Raisecom(config)#**clear port** *port-id* **statistics**	Clear statistics on port in the device.

Configuring statistics of ONU port

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system.
2	Raisecom(fttx)#**clear interface onu** *slot-id/olt-id/onu-id* **uni ethernet** *uni-id* **statistic**	Clear statistics on ONU Ethernet port.
3	Raisecom(fttx)#**clear interface onu** *slot-id/olt-id/onu-id* **uplink statistic**	Clear statistics on ONU PON port.

1.4.4 Configuring flow control of ports

Configuring flow control of OLT port

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer port configuration mode.
3	Raisecom(config-port)#**flowcontrol** { **receive** | **send** } { **on** | **off** }	Configure flow control of enabled/disabled physical port.

Configuring flow control of ONU port

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system.
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode.
3	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter ONU UNI Ethernet port configuration mode.
4	Raisecom(fttx-onu-uni*/*/*:*)# **flowcontrol** { **enable** | **disable** }	Configure flow control of enabled/disabled physical port.

1.4.5 Configuring switch of ports

Enabling/Disabling OLT port

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer port configuration mode.

Step	Configuration	Description
3	Raisecom(config-port)#**shutdown**	Disable current port. Use the command no shutdown to enable port if current port is disabled.

Enabling/Disabling ONU port

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system.
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode.
3	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter ONU UNI Ethernet port configuration mode.
4	Raisecom(fttx-onu-uni*/*/*:*)#**shutdown**	Disable current port. Use the command no shutdown to enable port if current port is disabled.

1.4.6 Checking configuration

Check ingconfiguration of OLT port

No.	Item	Description
1	Raisecom#**show interface port** *port-id*	Show OLT port state.
2	Raisecom#**show interface port** *port-id* **statistics dynamic** [**detail**]	Show dynamic statistics of port.
3	Raisecom#**show interface port** *port-id* **flowcontrol**	Show flow control information of port.
4	Raisecom#**show system mtu**	Show the maximum forwarding frame size of system.
5	Raisecom#**show interface ip** [*if-id*] **statistics**	Show system IP interface statistics.

Checking configuration of ONU port

No.	Item	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** *uni-id* **information**	Show ONU port state.

No.	Item	Description
2	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** *uni-id* **auto-negotiation ability**	Show auto-negotiation of ONU Ethernet port.
3	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** *uni-id* **name**	Show name of ONU Ethernet port.
4	Raisecom# **show interface onu** *slot-id/olt-id/onu-id* **system**	Show ONU MTU.
5	Raisecom# **show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** [*uni-id*] **statistic**	Show statistics of ONU Ethernet port.

1.5 Configuring time management

1.5.1 Default configuration of time

Function	Default value
Default time	2000-01-01 08:00:00.000
Default clock mode	system clock
Default time zone offset	+08:00
Default DST (Daylight Saving Time)	disable

1.5.2 Configuring time and time zone

Configuring time

Step	Configuration	Description
1	Raisecom#**clock mode** { **default** | **timestamp** }	Configure system time mode. • *default*: default mode. • *timestamp*: time stamp mode.
2	Raisecom#**clock set** *hour minute second year month day*	Configure system time.

Configuring time zone

Step	Configuration	Description
1	Raisecom#**clock timezone** { **+** | **-** } *hour minute*	Configure system time zone.
2	Raisecom#**clock set** *hour minute second year month day*	Configure system time.

1.5.3 Configuring DST

Step	Configuration	Description
1	Raisecom#**clock summer-time enable**	Enable DST of device.
2	Raisecom#**clock summer-time recurring** { *week* | **last** } { **fri** | **mon** | **sat** | **sun** | **thu** | **tue** | **wed** } { **month** | *month* } *hour minute* { *week* | **last** } { **fri** | **mon** | **sat** |**sun** | **thu** | **tue** | **wed** } { **month** | *month* } *hour minute offset-minutes*	Configure calculating period of system DST.

1.5.4 Configuring NTP

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ntp server** *ip-address* [**version** { **v1** | **v2** | **v3** }]	(Optional) configure address of NTP server.
3	Raisecom(config)#**ntp peer** *ip-address* [**version** { **v1** | **v2** | **v3** }]	(Optional) configure address of NTP peer.
4	Raisecom(config)#**ntp refclock-master** [*ip-address* | *stratum*]	(Optional) configure the device clock working as NTP reference clock source.

1.5.5 Configuring SNTP

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sntp server** *ip-address*	Configure address of time server.

1.5.6 Checking configuration

No.	Item	Description
1	Raisecom#**show clock**	Show configuration of system time and time zone.
2	Raisecom#**show clock summer-time-recurring**	Show DST and configuration of system.
3	Raisecom#**show sntp**	Show configuration of SNTP.

1.6 Configuring file management

1.6.1 Managing BootROM file

BootROM files are used to guide ISCOM5508 devices and complete initialization of the devices. Users can upgrade BootROM files by FTP (File Transfer Protocol). By default, file name of BootROM is bootrom or bootromfull.

If a device is electrified, firstly, the device runs BootROM file, press**Space** key to enter BootROM menu if screen shows "Press space into Bootrom menu...":

```
ram size:64M  testing...done

Init flash ...Done

Bootstrap_5.0.1.ISCOM5508.0.20100817, Raisecom Compiled Aug 17 2010,
16:53:54
Base Ethernet MAC address: 00:0e:5e:12:34:56

Press space into Bootstrap menu...
 0
 [Raisecom]:
```

The below operations are available under this menu:

Operation	Description
?	List all operations which can be executed.
b	Quickly execute system guide files.
h	List all operations which can be executed.
N	Set MAC (Medium Access Control) address of device.
R	Reboot device.
T	Download and replace system boot software by FTP.
V	Show version number of bootrom.
E	Format DOS file system.

1.6.2 Managing system files

Managing OLT system files

System files in ISCOM5508 device are divided as following:

- Bootrom: used for system startup, don't need to upgrade generally.
- system_boot.Z: system booting file, in support of online upgrade.

Step	Configuration	Description
1	Raisecom#**download bootrom** { **ftp** *ip-address username password filename* | **tftp** *ip-address filename* }	(Optional) Download system guide files by FTP or TFTP.
2	Raisecom#**download** { **onu-template** | **system-boot** } { **ftp** *ip-address username password filename* | **tftp** *ip-address filename* } [**schedule-list** *list-number*]	(Optional) Download ONU template files and system boot files by FTP or TFTP.
3	Raisecom#**upload system-boot** { **ftp** *ip-address username password filename* | **tftp** *ip-address filename* }	(Optional) Upload system boot files by FTP or TFTP.
4	Raisecom#**upload onu-template** { **ftp** *ip-address username password filename* | **tftp** *ip-address filename* } [**schedule-list** *list-number*]	(Optional) Upload ONU template files by FTP or TFTP.

Manage ONU template files

Step	Configuration	Description
1	Raisecom#**download onu-template** { **ftp** *ip-address username password filename* | **tftp** *ip-address filename* }	(Optional) Download ONU template files by FTP or TFTP.
2	Raisecom#**upload onu-template** { **ftp** *ip-address username password filename* | **tftp** *ip-address filename* } [**schedule-list** *list-number*]	(Optional) Upload ONU template files by FTP or TFTP.

1.6.3 Managing configuration files

Managing OLT configuration files

ISCOM5508 default configuration file is named as startup_config.conf. User can write the configuration file to the configuration file in flash file system by the command of **write**.

The memorized configuration information in startup_config.conf file will be uploaded by automation when user startup system next time.

Step	Configuration	Description
1	Raisecom#**download startup-config** { **ftp** *ip-address username password filename* | **tftp** *ip-address filename* }	(Optional) Download files which store device configuration data by FTP or TFTP.
2	Raisecom#**upload startup-config** { **ftp** *ip-address username password filename* | **tftp** *ip-address filename* } [**schedule-list** *list-number*]	(Optional) Upload files which store configuration data by FTP or TFTP.

Managing ONU configuration files

Configure the ONU configuration files as below.

Step	Configuration	Description
1	Raisecom#**download startup-config** { **ftp** *ip-address username password filename* | **tftp** *ip-address filename* } **onu** *slot-id/olt-id/onu-id*	Download files which store ONU configuration data by FTP or TFTP.
2	Raisecom#**upload startup-config** { **ftp** *ip-address username password filename* | **tftp** *ip-address filename* }**onu** *slot-id/olt-id/onu-id* [**schedule-list** *list-number*]	Upload files which store ONU configuration data by FTP or TFTP.
3	Raisecom#**fttx**	Enter global configuration mode of EPON system.
4	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode.
5	Raisecom(fttx-onu*/*:*)#**reload startup-config**	Reload saved configuration of ONU.
6	Raisecom(fttx-onu*/*:*)#**restore startup-config**	(Optional) restore ONU configuration as startup configuration.

1.6.4 Checking configuration

No.	Item	Description
1	Raisecom#**show startup-config**	Show loaded configuration after startup of device.
2	Raisecom#**show running-config**	Show current configuration of device.

1.7 Load and upgrade

1.7.1 Overview of load and upgrade

Users can upgrade device to add new features, optimize functions and solve BUG of current software version.

ISCOM5508 device can upgrade system software by FTP/TFTP.

1.7.2 Upgrading system software by FTP/TFTP

Users should build up FTP/TFTP environments before updating system software by FTP/TFTP updating way. PC works as FTP/TFTP server, ISCOM5508 device works as FTP/TFTP client and basic requirements as follows:

- ISCOM5508 connects with FTP/TFTP server;
- Configure FTP/TFTP server to ensure server is in a state of usefulness;
- Configure IP address of FTP/TFTP server, and ISCOM5508 can visit FTP/TFTP.

Step	Configuration	Description
1	Raisecom#**download system-boot** { **ftp** *ip-address username password filename* | **tftp** *ip-address filename* }	Download system boot software by FTP or TFTP;
2	Raisecom#**write**	Save current configuration into flash;
3	Raisecom#**reboot** [**now**]	Reboot device, device will load system configuration files which are saved on flash automatically;

1.7.3 ONU intellect load mode

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**auto-upgrade** { **enable** | **disable** }	Enable/disable intelligent upgrading;
3	Raisecom(fttx)#**auto-upgrade time** *start-time*	Configure start time of intelligent upgrading. Range is from 2:00 am to 5:00 am, default value is 4:00 am.
4	Raisecom(fttx)#**auto-upgrade add device-type** *onu-type* **ftp** *ip-address username password filename*	Add a intelligent upgrading plan (based on FTP);
	Raisecom(fttx)#**auto-upgrade add device-type** *onu-type* **tftp** *ip-address filename*	Add a intelligent upgrading plan (based on TFTP);
6	Raisecom(fttx)#**auto-upgrade delete device-type** *onu-type*	(Optional) delete a intelligent upgrading plan;
7	Raisecom(fttx)# **auto-upgrade device-type** *onu-type* **now**	Upgrade specified ONU model intelligently now; **Note** Device won't upgrade the version if the version has been upgraded in an hour or is same as the newest version;

1.7.4 Checking configuration

No.	Item	Description
1	Raisecom#**show auto-upgrade information**	Show intelligent upgrading configuration and running information;
2	Raisecom#**show version**	Show version information of system;

1.8 Configuring task scheduling

1.8.1 Configuring task scheduling

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**schedule-list** *number* **start** { **up-time** *days time* [**every** *days time* [**stop** *days time*]] | **date-time** *date time* [**every** { **day** | **week** | *days time* } [**stop** *date time*]] }	Add or modify schedule-list item, the command configure start time and end time of scheduling task, time interval between periods;
3	Raisecom(config)#*command-string* **schedule-list** *number*	Add command of schedule-list into scheduling list;

1.8.2 Checking configuration

No.	Item	Description
1	Raisecom#**show schedule-list**	Show configuration of schedule-list;

1.9 Configuring user permission and careful management

1.9.1 Configuring user permission and careful management

Step	Configuration	Description
1	Raisecom#**command-set** *comsetname*	Create command set and enter configuration mode of command set; use the command **no command-set** *comsetname* to delete command set. **Note** System prompts that command set is removed successfully if there is no command set; system prompts that command set is removed unsuccessfully if command set is being used by users;
2	Raisecom(command-set:*)#**command "** *comkeywords* **"**	Add commands in command set by key words in command line. Use the command **no command-set** {**all** | *comnum*} to delete commands in command set;

Step	Configuration	Description
3	Raisecom(command-set:*)#**exit** Raisecom#**user** *username* { **allow-exeset** | **disallow-exeset** } *comsetname*	Configure control privilege which enable/disable users to execute commands in command set. Use the command **no user** *username* {**allow-exeset** | **disallow-exeset**} *comsetname* to delete control configuration of command set.

Use **command "***comkeywords***"** to add commands in command sets, please note the following points:

- *comkeywords* is a key word of the commands, it doesn't include parameters in command line;
- *comkeyword* must put in "";
- If you just want to add a command, you must input the whole key word of the command. If you want to add commands in large scale, you can just input the same parts in the commands.

Example: To add command of **create vlan** *vlan-id* in command line pool as below:

```
Raisecom#command-set cmd1
Raisecom(command-set:cmd1)#command "creat vlan"
```

To add all commands related to ONU in command line pool as below:

```
Raisecom#command-set cmd1
Raisecom(command-set:cmd1)#command "onu"
```

1.9.2 Checking configuration

No.	Item	Description
1	Raisecom#**show command-set**	Show all command sets which include name of command set, the number of commands in the command set and status of command set;
2	Raisecom#**show command-set detail**	Show detailed information of all command sets which include name of command set, the number of commands in the command set and status of command set;
3	Raisecom#**show command-set detail** *comsetname*	Show detailed information of a specified command set which include name of command set, the number of commands in the command set and status of command set;

1.10 Configuration examples

1.10.1 Examples for configuring out-of-band NM

Networking requirements

As below figure, NView NNM NMS manages ISCOM5508 device by out-of-band and configure IP address of interface as 192.168.0.10.

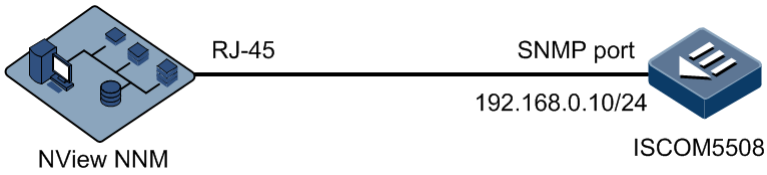

Figure 1-5 Configuring out-of-band NM

Configuration steps

Configure IP address of out-of-band management port.

```
Raisecom#config
Raisecom(config)#management-port ip address 192.168.0.10 255.255.255.0
```

Checking results

Show IP information of out-of-band management port.

```
Raisecom(config)#show management-port ip
IP address : 192.168.0.10
Subnet mask  : 255.255.255.0
```

1.10.2 Examples for configuring inner band NM

Networking requirements

NView NNM NMS manages ISCOM5508 device by inner band and configure IP address of interface as 192.168.0.1, configure mask as 255.255.255.0, VLAN ID as 10.

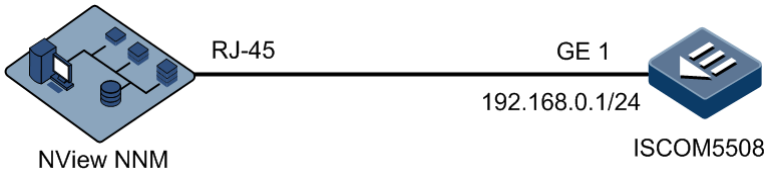

Figure 1-6 Configuring inner band NM

Configuration steps

Step 1 Create VLAN and configure attribute of port.

```
Raisecom#config
Raisecom(config)#create vlan 10 active
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 10
Raisecom(config-port)#exit
```

Step 2 Configure IP address of interface and associate with VLAN ID.

```
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address 192.168.0.1 255.255.255.0 10
```

Checking results

Show interface IP information.

```
Raisecom(config)#show interface ip
Index Ip Address    NetMask         Status      Vid
------------------------------------------------------------
1  192.168.0.1      255.255.255.0   active      10
```

1.10.3 Examples for configuring TFTP upgrading OLT

Networking requirements

As shown in below figure, TFTP server connects with ISCOM5508 device, and ISCOM5508 device has upgrading function to upgrade configuration files by TFTP server where IP address of TFTP server is 192.168.1.1.

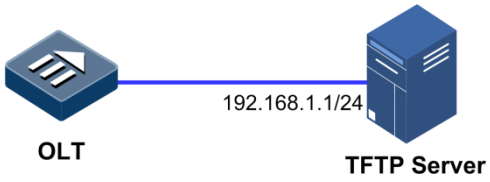

Figure 1-7 Upgrading configuration files by TFTP

Configuration steps

Step 1 Download system boot software by TFTP.

```
Raisecom#download system-boot tftp 192.168.1.1 systemboot.Z
```

Step 2 Write configured files to memory.

```
Raisecom#write
```

Step 3 Reboot device and the device will load new system boot files automatically.

```
Raisecom#reboot now
```

Checking results

Show OLT version information.

```
Raisecom#show version
Raisecom Operating System Software
Copyright (c) 2006-2009 Raisecom Technology Co., Ltd.
Product name: ISCOM5508
ROS Version: ISCOM5508_1.42.46.20120112.(Compiled Jan 12 2011, 14:39:49)
Bootrom Version: Bootrom_1.0.1.ISCOM5508.2.20100825
Hardware Version: Rev.A.0
System MacAddress is :000e.5e12.3456
  ISCOM5508 with
  64M bytes DRAM
  8 M bytes Flash Memory
Switch uptime is 0 days, 0 hours, 15 minutes
```

1.10.4 Examples for configuring intelligent upgrading ONU

Networking requirements

ONU can be upgraded by remote end termly as below figure.

Figure 1-8 Intelligent upgrading ONU

Configuration steps

Step 1 Configure IP address of TFTP server and add an intelligent upgrading configuration plan.

```
Raisecom#fttx
Raisecom(fttx)#auto-upgrade add device-type 5304 tftp 192.168.1.1
startup_config.conf
```

Step 2 Configure start time of intelligent upgrading is 2:00 am every day.

```
Raisecom(fttx)#auto-upgrade time 2
```

Step 3 Enable intelligent upgrading function.

```
Raisecom(fttx)#auto-upgrade enable
```

Checking results

Show intelligent upgrading and running information.

```
Raisecom#show auto-upgrade information
Auto-upgrade  : enable
Execution time everyday: 2:00AM
```

1.10.5 Examples for configuring user authority and careful management

Networking requirements

If users want to configure user authority and careful management on ISCOM5508, they need to create a command set cmd1 which includes 15 level command **create vlan** *vlan-id*, and create a 10 level user user1 which allows the user to proceed commands in command set.

Configuration steps

Step 1 Create command set cmd1 and add related commands.

```
Raisecom#command-set cmd1
Raisecom(command-set:cmd1)#command "creat vlan"
Raisecom(command-set:cmd1)#exit
```

Step 2 Create a user user1 and specify level of the user as level 10.

```
Raisecom#user name user1 password 123
Raisecom#user name user1 pri 10
```

Step 3 Configure authority of user1 in the command set.

```
Raisecom#user user1 allow-exeset cmd1
```

Checking results

Show user permission refinement management and running information.

```
Raisecom#show user detail
Username: user1
Priority: 10
Server:  Local
User command control config:
Type     Command set name
-----------------------------------
allow        cmd1
```

2 Configuring EPON service

This chapter contains the following information:

- Quick configuration of EPON service
- Configuring OLT
- Configuring ONU
- Maintenance
- Configuration examples

2.1 Quick configuration of EPON service

2.1.1 Configuring data service of EPON Ethernet

Networking requirements

As below figure, PC A is connected with UNI 1 of ONU, VLAN of user is 100. PON interface 1/1 of ISCOM5508 suspends ONU, GE 1 uplink IP network. Enable data service in the network topology.

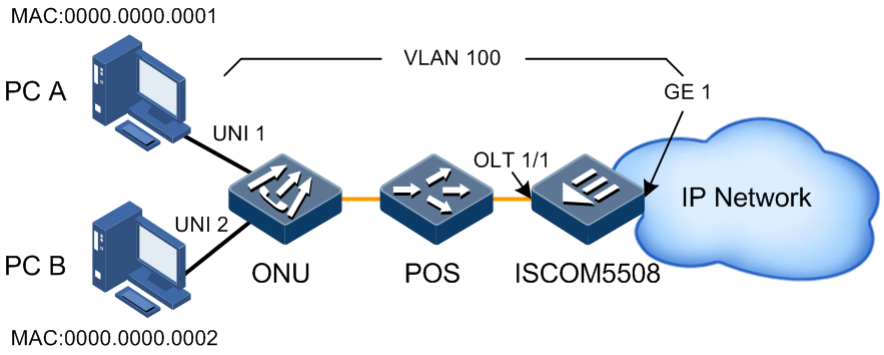

Figure 2-1 Data service

Configuration steps

- Configure OLT

Step 1 Create VLAN and configure port VLAN mode.

```
Raisecom#config
Raisecom(config)#create vlan 100 active
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 100
Raisecom(config-port)#exit
Raisecom(config)#interface port 7
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 100
Raisecom(config-port)#end
```

Step 2 Configure ONU authentication mode as "automatic registration".

```
Raisecom#fttx
Raisecom(fttx)#interface olt 1/1
Raisecom(fttx-olt1/1)#authorization mode none
Raisecom(fttx-olt1/1)#exit
```

- Configure ONU

Step 3 Configure user data VLAN.

```
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#uni ethernet 1
Raisecom(fttx-onu-uni1/1/1:1)#vlan mode tagged
Raisecom(fttx-onu-uni1/1/1:1)#native vlan 100
Raisecom(fttx-onu-uni1/1/1:1)#end
```

Checking results

Show VLAN configuration of OLT GE interface.

```
Raisecom#show interface port 1 switchport
Port: 1
Administrative Mode: trunk
Operational Mode: trunk
Access Mode VLAN: 1
Administrative Access Egress VLANs: 1
Operational Access Egress VLANs: n/a
Trunk Native Mode VLAN: 1
Administrative Trunk Allowed VLANs: 100
Operational Trunk Allowed VLANs: 1,100
Administrative Trunk Untagged VLANs: n/a
```

```
Operational Trunk Untagged VLANs: 1
```

Show VLAN configuration of OLT PON interface 1/1.

```
Raisecom#show interface port 7 switchport
Port: 7
Administrative Mode: trunk
Operational Mode: trunk
Access Mode VLAN: 1
Administrative Access Egress VLANs: 1
Operational Access Egress VLANs: n/a
Trunk Native Mode VLAN: 1
Administrative Trunk Allowed VLANs: 100
Operational Trunk Allowed VLANs: 1,100
Administrative Trunk Untagged VLANs: n/a
Operational Trunk Untagged VLANs: 1
```

Show registered ONU information.

```
Raisecom#show interface onu creation-information
ONU ID MAC Address  Mode  Creation Date Device Type State Mng-mode
description
------------------------------------------------------------------------
1/1/1  000e.5e0a.7a0e  auto  2000-01-01,08:00  ISCOM5104(C) active  oam  -
```

Show UNI VLAN configuration of ONU.

```
Raisecom#show interface onu 1/1/1 uni ethernet 1 vlan
Port ID: 1/1/1/1
   VLAN mode       : Tagged
   Native VLAN     : 100(CoS 0)
   Trans-rule list  : n/a
   Trunk allowed VLAN: n/a
```

2.1.2 Typical networking application for configuring PON+LAN (data service + NMS)

Networking requirements

As shown in Figure 2-2, the ISCOM5508 adopts the IP address pool to configure management parameters of ONUs in batch. The requirements are shown as below:

- The OLT must be configured with ONU IP address pool and the SNMP template. The ONU gains management parameters in batch through the IP address pool and the SNMP template.
- Table 2-1 lists requirements on parameters of the IP address pool.

Table 2-1 Parameters of ONU IP address pool

Parameter	Value
IP address pool ID	Automatically assigned by the system
IP address pool name	raisecom-ippool
Initial IP address of the IP address pool	192.168.1.11
End IP address of the IP address pool	192.168.1.254
Subnet mask of the IP address pool	255.255.255.0
Default gateway of the IP address pool	192.168.1.1
CVLAN of IP address pool management data	10
SVLAN of IP address pool management data	0 (Packets do not carry any VLAN.)
Priority of IP address pool management data	6 (Management packets need a higher priority.)

- Table 2-2 lists configuration requirements on the NView NNM system.

Table 2-2 Parameters of ONU SNMP template

Parameter	Value
SNMP template ID	Automatically assigned by the system
SNMP template name	raisecom-template
SNMP version	SNMP v2
IP address of the SNMP Trap host	10.1.1.1
Trap port	161
UDP port ID	162
SNMP community name	public
Name of the read SNMP community	public
Name of the write SNMP community	private

- VLAN of ONU data service channel is set to 20.

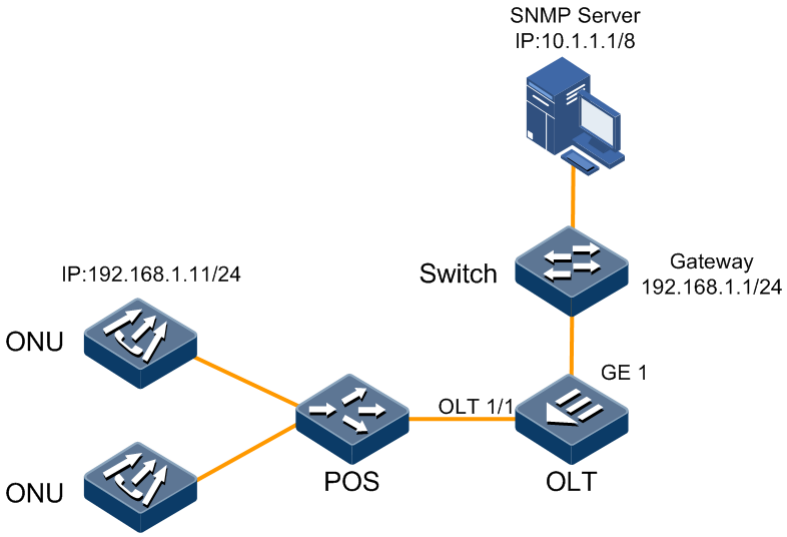

Figure 2-2 Configuring ONU independent network management (based on the IP address pool)

Configuration steps

Step 1 Create the ONU IP address pool.

```
Raisecom#fttx
Raisecom(fttx)#ip-pool 1 raisecom-ippool begin 192.168.1.11 end
192.168.1.254 255.255.255.0 default-gw 192.168.1.1 vlan 0 10 6
```

Step 2 Bind IP address pool to the PON interface.

```
Raisecom(fttx)#interface olt 1/1
Raisecom(fttx-olt1/1)#ip-pool 1
Raisecom(fttx-olt1/1)#exit
```

Step 3 Create the ONU SNMP template. For parameter requirements, see Table 2-2.

```
Raisecom(fttx)#snmp-template 1 raisecom-template snmp-server 10.1.1.1
version v2 trap-port 161 udp-port 162 security public community ro public
rw private
```

Step 4 Configure ONU management IP configuration mode and bind the SNMP template in batch.

```
Raisecom(fttx)#interface onu 1/1/1-64
Raisecom(fttx-onu-range)#ip-config auto overlay-local-ip
Raisecom(fttx-onu-range)#snmp-template 1
```

Step 5 Configure ONU management mode.

```
Raisecom(fttx-onu-range)#mng-mode snmp
Raisecom(fttx-onu-range)#end
```

Step 6 Configure Trunk mode on switching interface related to the PON interface, allowing VLAN 10 to pass.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)#switch mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 10 confirm
```

Step 7 Configure VLAN properties of data service interface on the OLT.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)#switch mode trunk
Raisecom(config-port)#switchport trunk native vlan 20
Raisecom(config-port)#exit
Raisecom(config)#interface port 7
Raisecom(config-port)#switch mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 20 confirm
```

Note

To learn the mapping relationship between device interfaces and switching interfaces, please see section 17 Appendix or use the **show port-mapping** command in privileged EXEC mode.

Checking results

Show information about ONU IP address pool bound to the OLT PON interface.

```
Raisecom#show interface olt 1/1 ip-pool information
ONU IP Pool: 1
   Pool Name      : raisecom-ippool
   Begin IP Address: 192.168.1.11
   End IP Address  : 192.168.1.254
   IP Mask        : 255.255.255.0
   Default Gateway : 192.168.1.1
   SVLAN          : 0
   CVLAN          : 0
   CoS            : 0
```

Show ONU management information, including ONU management modes, IP address configurations and SNMP template information.

```
Raisecom#show interface onu 1/1/1 mng-information
ONU ID   Mng-mode  IP Config Mode  SNMP Template ID  SNMP Template Name
------------------------------------------------------------------------
1/1/1       SNMP         auto           1             raisecom-template
```

2.2 Configuring OLT

2.2.1 Default configuration

Default configuration of EPON service:

Function	Default value
ONU authentication mode	Mac (authentication mode based on MAC address)
ONU status	active
Data encryption mode	tri-churning
Data encryption	disable
Data encryption direction	downstream
Timeout of triple stir key request-response	300 (unit is 0.1s)
Renewing cycle of triple stir key	100s
Downlink broadcast speed limit of flow	rate is 0kbit/s, burst is 4095 Bytes
Downlink unicast speed limit of flow	rate is 0kbit/s, burst is 4095 Bytes
ONU uplink fixed rate (FIR)	0kbit/s
ONU uplink Guarantee speed (CIR)	64kbit/s
ONU uplink peak rate (PIR)	30720kbit/s
ONU uplink service priority	0
Fec function	disable
The maximum round trip time	14000TQ (1TQ=16ns)
OLT layer-2 isolation	enable, that is, ONU in the same OLT PON isolate from each other, and they can't communicate on layer-2;
ONU layer-2 isolation	enable, that is, UNI in the same ONU PON isolate from each other;

Function	Default value
Detect VLAN which belongs to links	1
Detect testing frame size of links	1000 Bytes
Detect the number of testing frame of links	50

2.2.2 Configuring ONU authentication mode

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface olt** *slot-id/olt-id*	Enter OLT configuration mode;
3	Raisecom(fttx-olt*/*)#**authorization mode** { **mac** | **none** | **password** | **sn** | **sn-password** }	(Optional) Configuration ONU register mode. **Note** None mode is automatical register mode of ONU; in the mode, ONU can just connect with PON port of OLT by corresponding physical link to finish register;
4	Raisecom(fttx-olt*/*)#**create onu** [*onu-id*] **mac** *mac-address* [**device-type** *type-name*] [**description** *name*][**suspend**]	(Optional) Create ONU based on MAC address. If ONU uses register mode based on MAC, ONU can be created manually on OLT by the command. **Note** In the command, **mac** *mac-address* filed is PON MAC of ONU device; for not supporting type D protection group ONU, where PON MAC and ONU device MAC are the same; for ONU which supports type D protection group, where PON MAC is ONU device MAC;
	Raisecom(fttx-olt*/*)#**create onu** [*onu-id*] **sn** *sn* [**device-type** *type-name*] [**description** *name*] [**suspend**]	(Optional) Create ONU registered based on SN. If ONU uses register mode based on SN, ONU can be created manually on OLT by the command.;
	Raisecom(fttx-olt*/*)#**create onu** [*onu-id*] **password** *password* [**device-type** *type-name*] [**description** *name*] [**suspend**]	(Optional) Create ONU registered based on PASSWORD. If ONU uses register mode based on PASSWORD, ONU can be created manually on OLT by the command;

Step	Configuration	Description
	Raisecom(fttx-olt*/*)#**create onu** [*onu-id*] **sn** *sn* **password** *password* [**device-type** *type-name*] [**description** *name*] [**suspend**]	(Optional) Create ONU registered based on SN+PASSWORD. If ONU uses register mode based on SN+PASSWORD, ONU can be created manually on OLT by the command;
5	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
6	Raisecom(fttx-onu*/*:*)#**creation-type automatic-to-manual**	(Optional) change creation type from automatic to manual creation;
7	Raisecom(fttx-onu*/*:*)#**password** *string*	(Optional) modify saved ONU PASSWORD information in OLT device;

2.2.3 Rebinding ONU

Configure the device to re-binding ONU MAC address as below.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**rebind mac** *mac-address*	Rebind MAC address of ONU;

2.2.4 Activating/Suspending ONU

Configure as below to activate ONU on device.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**state** { **active** | **suspend** }	Active/suspend ONU;

2.2.5 Configuring ONU deregister

Configure as below to de-register ONU from device.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**deregister**	Configure ONU deregister;

2.2.6 Configuring ONU IP address pool

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**ip-pool** *pool-id pool-name* **begin** *ip-address* **end** *ip-address mask* **default-gw** *ip-address* **vlan** *svlan-id cvlan-id priority*	Configure IP address pool. Use **no ip-pool** *pool-id* command to delete address pool; *svlan-id* can't be configured, default value is 0;
3	Raisecom(fttx)#**ip-pool** *pool-id* **bind slot** *slot-id*	(Optional) bind the IP address pool with all PON interfaces based on the same slots in batch.
4	Raisecom(fttx)#**ip-pool** *pool-id* **bind all**	(Optional) bind the IP address pool with all PON interfaces in batch.
5	Raisecom(fttx)#**interface olt** *slot-id/olt-id*	Enter OLT configuration mode;
6	Raisecom(fttx-olt*/*)#**ip-pool** *pool-id*	(Optional) configure binding IP address pool of a single PON port. **Note** Many PON interfaces bind a ONU IP address pool is allowed; each PON interface can only bind a ONU IP address pool;
7	Raisecom(fttx-olt*/*)#**exit** Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
8	Raisecom(fttx-onu*/*:*)#**ip config** { **static** | **auto** [**overlay-local-ip**]}	Configure ONU management IP allocation mode. **Note** • static: static mode, management IP of ONU can be configured manually by users. • auto: automatical mode, ONU can get IP address from bound ONU IP address pool on corresponding PON interface; where *overlay-local-ip* means that automatically obtained IP address will overlay IP address configured by ONU;

2.2.7 Configuring data encryption

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface olt** *slot-id/olt-id*	Enter OLT configuration mode;
3	Raisecom(fttx-olt*/*)#**encryption mode** { **aes-128** | **triple-churning** }	Configure data encryption mode;
5	Raisecom(fttx)#**encryption triple-churning key-response-timeout** *period*	(Optional) Configure triple churning key response overtime. The response overtime must be smaller than key updating period.
6	Raisecom(fttx)#**encryption tiple-churning key-update-period** *period*	(Optional) Configure triple churning key updating period.
7	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
8	Raisecom(fttx-onu*/*:*)#**encryption** { **enable** | **disable** }	Configure enable/disable data encryption;
9	Raisecom(fttx-onu*/*:*)#**encryption direction** { **down** | **down-up** }	Configure data encryption direction.

Note

- Only triple-churning mode is in support now, AES-128 encapsulation mode is configurable but ineffective.
- Only in support of data encapsulation at downstream direction.
- Triple-churning timer is global configuration of single card, that is to say, it is effective for all ONU under PON port of single card.
- Generally, the triple-churning timer uses default configuration, no need to configure again.

2.2.8 Configuring speed limit of downstream

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface olt** *slot-id/olt-id*	Enter OLT configuration mode;
3	Raisecom(fttx-olt*/*)#**policing downstream broadcast rate** *rate burst*	Configuration OLT downlink broadcast data speed limit of flow; Use **no policing downstream broadcast rate** to return to default Configuration;
4	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
5	Raisecom(fttx-onu*/*:*)#**policing downstream rate** *rate burst*	Configuration ONU downlink unicast data speed limit of flow; Use **no policing downstream rate** to return to default Configuration;

2.2.9 Configuring DBA of upstream

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**sla fir** *fir*	Configure uplink fixed rate;
4	Raisecom(fttx-onu*/*:*)#**sla cir** *cir*	Configure uplink Guarantee speed;
5	Raisecom(fttx-onu*/*:*)#**sla pir** *pir*	Configure uplink peak rate;
6	Raisecom(fttx-onu*/*:*)#**sla priority** *priority-value*	Configuration service priority. use **no sla** {**cir** | **pir** | **fir** | **priority**} to return to default configuration;
7	Raisecom(fttx-onu*/*:*)#**dba sla** { **enable** | **disable** }	Configuration enable/disable ONU SLA;
8	Raisecom(fttx-onu*/*:*)#**dba sla queue** *queue-id* **fir** *fir* **cir** *cir* **pir** *pir* [**fix-pkt** *size*]	Configuration ONU SLA queue parameter;
9	Raisecom(fttx-onu*/*:*)#**dba sla queue-weight** *weight0 weight1 weight2 weight3 weight4 weight5 weight6 weight7*	Configuration ONU SLA queue schedule weight value.
10	Raisecom(fttx-onu*/*:*)#**dba sla queue-set** *queue-list*	Configuration ONU SLA scheduling queue;
11	Raisecom(fttx-onu*/*:*)#**dba sla best-effort-scheduling** { **sp** | **sp-wrr** | **wrr** }	Configuration schedule mode for best effort bandwidth.
12	Raisecom(fttx-onu*/*:*)#**dba sla high-priority-boundary** *priority-vlaue*	Configuration SP schedule priority boundary value under SP+WRR mode, the queue bigger or equal to this value will attend SP schedule, others attend WRR schedule.
13	Raisecom(fttx-onu*/*:*)#**dba queue-set** *number* **report-bit-map** *queue-list*	(Optional) Configure queue pool number in Report message transmitted by ONU and report bit map. User had better don't configure it by himself. Use **no dba queue-set** *number* **report-bit-map** to return to default configuration.
14	Raisecom(fttx-onu*/*:*)#**dba queue-set** *number* **report-threshold** *threshold0 threshold1 threshold2 threshold3 threshold4 threshold5 threshold6 threshold7*	(Optional) Configure queue pool number and threshold value of ONU transmitted frame. Use **no dba queue-set** *number* **report-threshold** to return to default configuration.
15	Raisecom(fttx-onu*/*:*)#**dba set queue-set** *list*	(Optional) Enable configured queue pool on ONU. Use **no dba set queue-set** to return to default configuration.

- Using the same value for ONU Priorities, can help DBA reach the best performance.
- When an ONU CIR is smaller than 1Mbit/s, the other ONU CIR is very big (nearly 980Mbit/s), and the actual transmitting flow is bigger than the biggest effective bandwidth 980Mbit/s, the ONU with smaller CIR will get de-register. So the actual transmitting flow of single ONU should not bigger than 980Mbit/s.

2.2.10 Configuring FEC

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system.
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode.
3	Raisecom(fttx-onu*/*:*)#**fec** { **enable** | **disable** }	Enable/disable FEC.

- In support of bi-directional FEC. FEC is fixed to be configured in auto-negotiation receiving mode (hybrid mode) at receiving direction of both OLT/ONU. That means, no matter transmitting direction enables FEC, the receiving direction can receive correct.
- At transmitting direction of OLT/ONU, it is in support of FEC enable/disable.
- It is in support of bi-directional FEC enable/disable at the same time.

2.2.11 Configuring round trip delay

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface olt** *slot-id/olt-id*	Enter OLT configuration mode;
3	Raisecom(fttx-olt*/*)#**rtt max** *rtt*	Configure the maximum round trip time;

By default, the max. rtt latency related to fiber distance is about 21km, usually, it doesn't need to modify the max. rtt latency.

2.2.12 Configuring port isolation

Configuring OLT switch port isolation

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer port configuration mode;
3	Raisecom(config-port)#**switchport protect**	Configure port isolation; use the command **no switchport protect** to recover it to default configuration;

Configuring P2P access control

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**p2p-access** { **add** | **remove** } *onu-list*	Configure ONU lists which can communicate with each other on the same PON interface;

Note

- The service may be shutdown for about 25ms when configuring P2P access control.
- The P2P function is only available to unicast service, but not unknown unicast, broadcast and multicast services.

Configuring ONU UNI port protection

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter ONU UNI Ethernet port configuration mode;
4	Raisecom(fttx-onu-uni*/*/*:*)#**switchport isolation** { **enable** | **disable** }	Enable/disable port isolation of UNI which is layer-2 isolation of ONU;

2.2.13 Configuring monitoring of logical links

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**link-test** [**vlan** *vlan-id*] [**size** *size*] [**count** *count*]	Detect packet loss and delay of link between OLT and ONU;

2.2.14 Configuring tracing and search of MAC address

Configure tracing of MAC address:

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**trace mac-address** *mac-address*	Configure MAC address tracing;

Configure search of MAC address:

Step	Configuration	Description
1	Raisecom#**search mac-address** *mac-address*	Search MAC address in OLT switching system;
2	Raisecom#**search interface olt** [*slot-id/olt-id*] **mac-address** *mac-address*	Search MAC address in OLT switching system;
3	Raisecom#**search interface onu** *slot-id/olt-id/onu-id* **mac-address** *mac-address*	Search MAC address in specified ONU;

2.2.15 Checking configuration

Step	Configuration	Description
1	Raisecom#**show interface olt** *slot-id/olt-id* **information**	Show authentication mode of ONU, data encryption mode and so on;
2	Raisecom#**show interface onu creation-information**	Show new ONU information, such as creation type, type of ONU, ONU status and so on;
3	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **information**	Show basic information of specified ONU, such as type of ONU, MAC address of ONU and so on;

Step	Configuration	Description
4	Raisecom#**show interface olt** [*slot-id/olt-id*] **ip-pool information**	Show bound ONU IP address pool information of OLT PON interface;
5	Raisecom#**show interface olt** *slot-id/olt-id* **illegal-onu**	Show illegal registered ONU information;
6	Raisecom#**show interface olt** *slot-id/olt-id* **policing downstream broadcast**	Show speed limit of flow configuration of OLT downstream broadcast data;
7	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **encryption**	Show encrypted function status and encryption direction of data;
8	Raisecom#**show encryption triple-churning timer**	Show configuration of triple stir timer;
9	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **dba sla**	Show SLA configuration information of ONU device;
10	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **dba queue-set**	Show configuration information of ONU DBA;
11	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **sla**	Show configuration information of CIR, PIR, FIR and service priority;
12	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **fec**	Show FEC status;
13	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **p2p-access**	Show access list among ONU;
14	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ehternet isolation**	Show layer-2 isolation status among UNI;
15	Raisecom#**show interface olt** *slot-id/olt-id* **ip-pool information**	Show information about the IP address pool on OLT interfaces.
16	Raisecom#**show snmp-template** [*template-id*] **information**	Show SNMP parameter template information.

2.3 Configuring ONU

2.3.1 Default configuration

Function	Default value
ONU device name	Raisecom
ONU management way	Oam
PON management IP of ONU	IP is 0.0.0.0, mask code is 0.0.0.0;
IP of ONU UNI port	IP is 192.168.1.254, mask code is 255.255.255.0
UNI name	Ehternet-uni-id

Function	Default value
Rate and duplex mode of UNI	Auto
Flow control of UNI	Disable
UNI Loss alarm	Disable
Enable or disable UNI	Enable
Flow control of ONU uplink interface	Disable
UNI data speed limit of flow	Disable
Speed limit of flow of UNI in the downstream direction	Guarantee speed is 4836kbit/s, peak rate is 0kbit/s;
Speed limit of flow of UNI in the upstream direction	Committed rate is 4836kbit/s, committed burst size is 64022Byte, excess burst size is 1514Byte;
Uplink interface limit rate of ONU	0kbit/s
ONU SLA	Disable
Scheduling way of ONU SLA queue	Sp
SLA scheduling queue	1,2
Parameter of SLA queue	FIR is 0kbit/s, CIR is 256kbit/s, PIR is 256kbit/s, fixpkt is 0Byte;
Port mirroring	Disable
Monitoring port	Uni 1
DLF message forwarding	Enable
BPDU message transmission transparently	Disable
Discovery function of ONU partner device	Disable
Management IP of partner device of ONU	IP is 0.0.0.0, mask code is 0.0.0.0
Management IP address type of partner device of ONU	Manual
Power supply management mode of PSE subcard	Auto
Usage threshold percentage of PSE power	99%
Report function status of ONU PSE related Trap	Enable
PSE function status of UNI	Enable
The maximum output power of UNI power supply	15400mw
Power supply priority of port	Low
Enable/disable service to pass through when UNI doesn't connect with PSE device	Disable

The common features and default configuration is only for reference since Raisecom has a lot of ONU device types and the different ONU model possesses different feature and default configuration.

2.3.2 Configuring file management

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**write**	(Optional) save configuration data in local ONU;
4	Raisecom(fttx-onu*/*:*)#**reload startup-config**	(Optional) reload configuration file;
5	Raisecom(fttx-onu*/*:*)#**restore startup-config**	(Optional) return configuration to default value;

After configure telnet for ONU on ISCOM5508, user has to perform data saving operation in ONU configuration mode other wise the configuration will be lost after device reboot.

2.3.3 Configuring name of ONU device

Step	Configuration	Description
1	Raisecom#**fttx**	Enter EPON system global configuration mode;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**hostname** *string*	Configure ONU device name. Use **no hostname** to return to default configuration;

2.3.4 Configuring ONU management parameter

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**mng-mode** { **oam** | **snmp** }	Configure management way of ONU;

Step	Configuration	Description
4	Raisecom(fttx-onu*/*:*)#**mng-ip address** *ip-address mask* **default-gw** *default-gw* **vlan** *cvlan-id svlan-id priority*	(Optional) Configure management IP on PON of ONU, users can use the configuration to manage ONU by SNMP way; use **no mng-ip address** to return to default configuration;
5	Raisecom(fttx-onu*/*:*)#**mng-ipv6 address** *ip-address mask* **default-gw** *default-gw* **vlan** *cvlan-id svlan-id priority*	(Optional) configure the management IPv6 address of ONU PON interface. This configuration is available when you manage ONUs through SNMP. Use the **no mng-ipv6 address** command to return to default configurations.
6	Raisecom(fttx-onu*/*:*)#**lan-ip address** *ip-address mask*	(Optional) Configure IP of ONU UNI port, users can use the configuration when ONU only has independent NM; use **no lan-ip address** to return to default configuration;
7	Raisecom(fttx-onu*/*:*)#**telnet** { **enable** | **disable** }	(Optional) Enable/disable remote Telnet to login ONU;
8	Raisecom(fttx-onu*/*:*)#**ip-config** { **static** | **auto** } [**overlay-local-ip**] **snmp-template** *template-id*	(Optional) configure the IP management mode of ONU and bind the SNMP parameter template.

Note

- IP address managed by ONU device including PON port management IP and UNI management IP. After configuring PON port IP, user can telnet remote ONU through OLT uplink port to do device management.
- The ONU PON port IP and UNI management IP address must be in different network segment, for different ONU PON port IP address, user must ensure IP address don't conflict.

2.3.5 'Configuring ONU SNMP template

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system.
2	Raisecom(fttx)#**snmp-template** *template-id template-name* **snmp-server** *ip-address* **version** { **v1** | **v2** } **trap-port** *port-id* **udp-port** *port-id* **security** *name* **community ro** *name* **rw** *name*	Create the ONU SNMP template. Use the no **snmp-template** *template-id* command to delete the ONU template.
3	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode.

Step	Configuration	Description
4	Raisecom(fttx-onu*/*:*)#**snmp-template** *template-id*	Apply the ONU SNMP template to ONUS. Multiple ONUs can be bound with the same SNMP template.

2.3.6 Configuring ONU service template

ONU service configuratipn template can configure ONU service function in batch, which reduces the configuration amount of work and the load of configuration personnel effectively.

Creating and modifying template

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**create onu-svr-template** *template-id* **name** *template-name* **uni-eth-num** *number*	Enter service configuration template; use **create onu-svr-template** *template-id* to delete configuration template.
3	Raisecom(fttx)#**onu-svr-template** *template-id*	Enter service template configuration mode.
4	Raisecom(fttx-onu-svr-template:*)#**name** *template-name*	(Optional) Configure current template name.
5	Raisecom(fttx-onu-svr-template:*)#**uni-eth-number sensitive** { **enable** | **disable** }	(Optional) Configure to enable/disable Ethernet interface number consistency function in template.
6	Raisecom(fttx-onu-svr-template:*)#**uplink rate-limit** *value*	(Optional) Configure ONU uplink interface speed limit.
7	Raisecom(fttx-onu-svr-template:*)#**uni ethernet** *uni-list* **vlan mode** { **tag** | **transparent** | **trunk** }	(Optional) Configure ONU UNI interface VLAN mode.
8	Raisecom(fttx-onu-svr-template:*)#**uni ethernet** *uni-list* **native vlan** *vlan-id*	(Optional) Configure ONU UNI interface default VLAN ID.
9	Raisecom(fttx-onu-svr-template:*)#**uni ethernet** *uni-list* **vlan trunk allowed** *vlan-list*	(Optional) Configure ONU UNI interface Trunk mode permitted VLAN ID.
10	Raisecom(fttx-onu-svr-template:*)#**uni ethernet** *uni-list* **speed auto**	(Optional) Configure ONU UNI interface speed auto-negotiation.
11	Raisecom(fttx-onu-svr-template:*)#**uni ethernet** *uni-list* **speed** { **10** | **100** | **1000** } **duplex** { **half** | **full** }	(Optional) Configure ONU UNI interface speed and duplex mode.

Step	Configuration	Description
12	Raisecom(fttx-onu-svr-template:*)#**uni ethernet** *uni-list* **policing egress** { **enable** | **disable** }	(Optional) Configure to enable/disable ONU UNI interface downstream speed limit.
13	Raisecom(fttx-onu-svr-template:*)#**uni ethernet** *uni-list* **policing egress cir** *cir-value*	(Optional) Configure ONU UNI interface downstream speed limit bandwidth.
14	Raisecom(fttx-onu-svr-template:*)#**uni ethernet** *uni-list* **policing ingress** { **enable** | **disable** }	(Optional) Configure to enable/disable ONU UNI interface upstream speed limit.
15	Raisecom(fttx-onu-svr-template:*)#**uni ethernet** *uni-list* **policing ingress cir** *cir-value*	(Optional) Configure ONU UNI interface upstream speed limit bandwidth.
16	Raisecom(fttx-onu-svr-template:*)#**uni ethernet** *uni-list* **multicast vlan** *vlan-id*	(Optional) Configure ONU UNI interface multicast VLAN.
17	Raisecom(fttx-onu-svr-template:*)#**uni ethernet** *uni-list* **multicast vlan tag-strip** { **enable** | **disable** }	(Optional) Configure ONU UNI interface multicast vlan tag-strip.

Note

The template bound to ONU cannot be modified and deleted.

Binding template

ONU service template can be bound to ONU, permitting the following two binding modes:

- Batch binding mode over PON port
- Separate binding mode over ONU

Please configure to bind template in batch binding mode over PON on device as shown below.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface olt** *slot-id/olt-id*	Enter OLT configuration mode;
3	Raisecom(fttx-olt*:*)#**onu-svr-template** *template-id* **binded-onu-list** *onu-list*	Bind service template to ONU list in batch.
4	Raisecom(fttx-olt*:*)#**onu-svr-template** *template-id* **binded-onu-list add** *onu-list*	Add ONU to ONU service template bound ONU list.
5	Raisecom(fttx-olt*:*)#**onu-svr-template** *template-id* **binded-onu-list remove** *onu-list*	Delete ONU from ONU service template bound ONU list.

Please configure to bind template in separate binding mode over ONU on device as shown below.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/*onu*-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**onu-svr-template** *template-id*	Bind template to ONU; use **no onu-svr-template** to delete the binding relationship between template and ONU.

2.3.7 Configuring ONU QoS template

Note

ONU QoS configuratipn template can configure ONU QoS in batch, which reduces the configuration amount of work and the load of configuration personnel effectively.

Creating and modifying template

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**create onu-qos-template** *template-id* **name** *template-name*	Create QoS configuration template; use no **create onu-qos-template** *template-id* to delete configuration template.
3	Raisecom(fttx)#**onu-qos-template** *template-id*	Enter QoS template configuration mode.
4	Raisecom(fttx-onu-qos-template:*)#**name** *template-name*	(Optional) Configure current template name.
5	Raisecom(fttx-onu-qos-template:*)#**best-effort-scheduling-scheme** { **sp** | **wrr weight** *w1 w2 w3 w4* | **sp-wrr weight** *w1 w2 w3 w4* **high-priority-boundary** value }	(Optional) Configure queue scheduling mode and queue weight.
6	Raisecom(fttx-onu-qos-template:*)#**weight** *weight-values*	(Optional) Configure queue weight.
7	Raisecom(fttx-onu-qos-template:*)#**high-priority-boundary** value	(Optional) Configure queue priority boundary value in SP + WRR mode, the queue whose value is graeter than or equal to the boundary value will join in SP scheduling, others for WRR scheduling.
8	Raisecom(fttx-onu-qos-template:*)#**cycle-length** *value*	(Optional) Configure scheduling cycle-length.
9	Raisecom(fttx-onu-qos-template:*)#**queue** *queue-id* **type fixed fir** *fir-value* [**fix-pkt** *size*]	(Optional) Configure fixed bandwidth.

Step	Configuration	Description
10	Raisecom(fttx-onu-qos-template:*)#**queue** *queue-id* **type assured cir** *cir-value* [**fix-pkt** *size*]	(Optional) Configure assured bandwidth.
11	Raisecom(fttx-onu-qos-template:*)#**queue** *queue-id* **type besteffort pir** *pir-value* [**fix-pkt** *size*]	(Optional) Configure peek bandwidth.
12	Raisecom(fttx-onu-qos-template:*)#**queue** *queue-id* **type fixed-assured fir** *fir-value* **cir** *cir-value* [**fix-pkt** *size*]	(Optional) Configure fixed bandwidth + assured bandwidth.
13	Raisecom(fttx-onu-qos-template:*)#**queue** *queue-id* **type fixed-besteffort fir** *fir-value* **pir** *pir-value* [**fix-pkt** *size*]	(Optional) Configure fixed bandwidth + peek bandwidth.
14	Raisecom(fttx-onu-qos-template:*)#**queue** *queue-id* **type assured-besteffort fir** *fir-value* **pir** *pir-value* [**fix-pkt** *size*]	(Optional) Configure assured bandwidth + peek bandwidth.
15	Raisecom(fttx-onu-qos-template:*)#**queue** *queue-id* **type fix-assured-besteffort fir** *fir-value* **cir** *cir-value* **pir** *pir-value* [**fix-pkt** *size*]	(Optional) Configure fixed bandwidth + assured bandwidth + peek bandwidth.

Note

- The template bound to ONU cannot be modified and deleted
- The priority boundary only can be used in SP+WRR mode and cannont be modified in other modes.
- In WRR and SP+WRR scheduling, the sum of each queue weight shall be 100. All queues weights in WRR cannot be 0.
- Each queue FIR≦CIR≦PIR, and the sum of each queues bandwidth cannot more than the totle ONU upstream bandwidth.

Note

- The bandwidth type is only convenient for the user to configure FIR, CIR, and PIR parameters. When configured for "fixed bandwidth", the assured bandwidth and best-effort bandwidth will be 0 automatically; for FIR = fixed bandwidth, CIR = fixed bandwidth + assured bandwidth, PIR = fixed bandwidth + assured bandwidth + best-effort bandwidth, then it just needs to input FIR, the PIR and CIR will be equal to FIR automatically.
- Similarly, when configured for "fixed bandwidth + best-effort bandwidth" type, the fixed bandwidth will be 0 automatically; it just needs to configure FIR and PIR.
- The rest types can be done in the same manner. Users can always use "fixed-bandwidth + assured bandwidth + best-effort bandwidth" type to specify FIR, CIR, and PIR parameters.

Binding template

Please bind template on the device as below.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;

Step	Configuration	Description
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/*onu*-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**onu-qos-template** *template-id*	Bind template to ONU; use **no onu-qos-template** to delete the binding relationship between template and ONU.

- No longer allow to use separate configuration command to modify the relevant parameters after ONU binding QoS template.
- To delete the binding relationship just release the binding relationship between ONU and QoS template, so that users can use separate command to configure the relevant parameters, while the corresponding template reference count will be decreased gradually. However, the QoS parameters configured by ONU binding template cannot be changed, users could use the command of dba sla disable to disable this function.
- If to rebind the ONU with binding template, new template will be in effect, while old template will automatically unbind with the ONU.
- Only when the template reference count is 0, that is, the template has not bound to any ONU, the template can be deleted.

2.3.8 Configuring rate limiting template for ONU ports

ONU policing template can be used to configure rate limiting of ONU UNI interfaces in batch. It reduces the configuration work and the load of configuration personnel effectively.

Creating and modifying rate limiting template

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system.
2	Raisecom(fttx)#**create policing-template** *template-id* **name** *template-name*	Create a rate limiting template. Use the **no create o policing -template** command to delete the template.
3	Raisecom(fttx)#**policing-template** *template-id*	Enter rate limiting configuration mode.
4	Raisecom(fttx-policing-template:*)#**name** *template-name*	(Optional) configure a name for the current rate limiting template.
5	Raisecom(fttx-onu-qos-template:*)#**ingress cir** *cir* [**cbs** *cbs*] [**ebs** *ebs*]	(Optional) configure the uplink rate limiting parameter for the template.

Step	Configuration	Description
6	Raisecom(fttx-onu-qos-template:*)#**engress cir** *cir* [**pir** *pir*]	(Optional) configure the downlink rate limiting parameter for the template.

The templates which have been bound to ONU port cannot be modified or deleted.

Binding rate limiting template

There are two kinds of binding modes if rate limiting template is bound to UNI port:

- Mass binding mode based on UNI ports
- Along binding mode based on UNI ports

Please configure device of mass binding mode based on UNI ports.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system.
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id*/onu-*id*	Enter ONU configuration mode.
3	Raisecom(fttx-onu*/*:*)#**policing-template** *template-id* **uni** *uni-list*	Bind the rate limiting template to UNI port in batch. Use the **no policing-template uni** *uni-list* command to delete binding relation between template and UNI port.

- ONU ports have different rate limiting capability. When binding a rate limiting template to the ONU port, OLT will automatically verify that the rate limiting parameters of the template are in the allowed range of the ONU port. If not, the template cannot be bounded to the port and the system will geive a prompt.
- When mass binding the template to UNI ports, if there is no UNI port, the system will give a prompt and continue to bind the template to other ports.
- If an ONU UNI port is bound with a rate limiting template, the independent rate limiting configuration command is invalid for it. Therefore, when the command is used to configure the rate limiting for the ONU UNI port, the system will give a prompt.
- For an ONU port that is bounded with rate limiting template and service template, the rate limiting parameter cannot be changed when the rate limiting template is released.

Please configure device of alone binding mode based on UNI port.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system.
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id*/onu-*id*	Enter ONU configuration mode.
3	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter UNI port configuration mode.
4	Raisecom(fttx-onu-uni*/*/*:*)#**policing-template** *template-id*	Bind template to UNI port. Use the **no policing-template** command to delete binding relation between template and UNI port.

2.3.9 Configuring ONU VLAN template

Note

The ONU VLAN template is used to configure VLANs on ONU UNI ports in batch. It reduces the configuration work and the load of configuration personnel effectively.

- The ONU VLAN template supports mass configuring identical Native VLAN ID for ONU UNI ports. In addition, all configured UNI ports are in Tag mode.
- The ONU VLAN template supports mass configuring different Native VLAN IDs for different ONU UNI ports. However, Native VLAN IDs for all UNI ports on the same ONU are identical.

Creating and modifying ONU VLAN template

Please take following configuration on device that needs to create and modify the ONU VLAN template.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system.
2	Raisecom(fttx)#**create onu-config-template** *template-id* **name** *template-name*	Create ONU VLAN template. Use the **no create onu-config -template** command to delete the template. **Note** In a newly-configured ONU VLAN template, the port mode is set to Tag mode by default. The default Native VLAN ID is set to 1.
3	Raisecom(fttx)#**onu-config-template** *template-id*	Enter ONU VLAN template VLAN configuration mode.

Step	Configuration	Description
4	Raisecom(fttx-onu-config-template:*)#**native vlan** *vlan-id-begin vlan-id-end*	Configure the Native VLAN parameter for the template.
5	Raisecom(fttx-onu-config-template:*)#**name** *template-name*	(Optional) configure a name for the current ONU VLAN template.

The ONU VLAN template which has been bound to ONU port can not be modified or deleted.

Binding ONU VLAN template

Perform following configuration on device that needs to be bounded with ONU VLAN template.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system.
2	Raisecom(fttx)#**interface olt** *slot-id/olt-id*	Enter OLT configuration mode.
3	Raisecom(fttx-olt*:*)#**onu-config-template** *template-id* **apply-onu-list** *onu-list*	Apply the template to ONU.
4	Raisecom(fttx-olt*:*)#**onu-config-template** *template-id* **binded-onu-list** *onu-list*	Bind the template to ONU.

- ONU VLAN template and ONU service template are exclusive. Therefore, you cannot bind the ONU VLAN template and ONU service template to the same ONU.
- ONU VLAN template is only applied to a created ONU. If an ONU is online, the template will directly apply parameters to the ONU. If not, the ONU will apply parameters to the ONU as soon as the ONU is online.
- ONU VLAN template is only bounded to a non-created ONU. It cannot be bounded to a created ONU. When an ONU is created (ether munually or automatically), the template will apply paraters to the ONU.
- No matter whether the template is applied or bounded to an ONU, it is required the number for ONUs should be identical to the number for VLAN IDs. For example, when VLANs 1–5 are applied/bounded to ONUs 1–3, ONU 5 and ONUs 7–10, ONU 5 will be assigned with VLAN 4.
- You can still use command to modify the VLAN mode and Native VLAN ID for a ONU, which is mass bounded or applied with template.
- You cannot delete a template until it is not bounded to any ONU.

2.3.10 Configuring ONU serial port server

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**serial-com** [**range**] **port** *port-id*	Enter ONU serial port configuration mode;
4	Raisecom(fttx-onu-serial*/*/*:*)#**baud-rate** *value*	(Optional) Configure ONU serial port baud-rate.
5	Raisecom(fttx-onu-serial*/*/*:*)#**data-bits** *value*	(Optional) Configure ONU serial port data-bits.
6	Raisecom(fttx-onu-serial*/*/*:*)#**stop-bits** *value*	(Optional) Configure ONU serial portstop-bits
7	Raisecom(fttx-onu-serial*/*/*:*)#**parity** { **none** | **odd** | **even** | **mark** | **space** }	(Optional) Configure ONU serial port data parity mode.
8	Raisecom(fttx-onu-serial*/*/*:*)#**flow-control** { **none** | **xon-xoff** | **hardware** }	(Optional) Configure ONU serial port flow control mode
9	Raisecom(fttx-onu-serial*/*/*:*)#**serial-portocol** { **rs232** | **rs485** }	(Optional) Configure ONU serial port protocol type
10	Raisecom(fttx-onu-serial*/*/*:*)#**loop-back** *port-id*	(Optional) Configure ONU serial port loopback.
11	Raisecom(fttx-onu-serial*/*/*:*)#**shutdown**	(Optional) Configure to shut down ONU serial port.
12	Raisecom(fttx-onu-serial*/*/*:*)#**alarm** { **enable** | **disable** }	(Optional) Configure to enable/disable ONU serial port alarm.
13	Raisecom(fttx-onu-serial*/*/*:*)#**work-mode** { **tcp-realport** | **tcp-client** | **tcp-server** | **udp** }	(Optional) Configure ONU serial port work mode.
14	Raisecom(fttx-onu-serial*/*/*:*)#**server-port** *port-id*	(Optional) Configure ONU serial port communication server interface.
15	Raisecom(fttx-onu-serial*/*/*:*)#**peer ip-address** *ip-address*	(Optional) Configure ONU serial port communication peer IP address.
16	Raisecom(fttx-onu-serial*/*/*:*)#**peer server-port** *port-id*	(Optional) Configure ONU serial port communication peer service interface.
17	Raisecom(fttx-onu-serial*/*/*:*)#**connect-condition** { **always** | **char** | **dcd-on** | **dsr-on** }	(Optional) Configure ONU serial port communication connect-condition.

Step	Configuration	Description
18	Raisecom(fttx-onu-serial*/*/*:*)#**break-condition** { **none** | **dcd-off** | **dsr-off** }	(Optional) Configure ONU serial port communication break-condition.
29	Raisecom(fttx-onu-serial*/*/*:*)#**session-write-right** { **first** | **all** }	(Optional) Configure ONU serial port communication write-right.
20	Raisecom(fttx-onu-serial*/*/*:*)#**serial-com-max-session-num** *number*	(Optional) Configure ONU serial port communication maximum connection number.

2.3.11 Configuring UNI

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id*/onu-*id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter ONU UNI Ethernet port configuration mode;
4	Raisecom(fttx-onu-uni*/*/*:*)#**uni name** *string*	(Optional) Configure UNI name; use **no uni name** to return to default configuration;
5	Raisecom(fttx-onu-uni*/*/*:*)#**speed auto**	(Optional) Configure rate and duplex mode of UNI to start auto-negotiation;
6	Raisecom(fttx-onu-uni*/*/*:*)#**speed** { **10** | **100** | **1000** } **duplex** { **full** | **half** }	(Optional) Configure rate and duplex mode of UNI;
7	Raisecom(fttx-onu-uni*/*/*:*)#**flowcontrol** { **enable** | **disable** }	(Optional) Enable/disable flow control of UNI;
8	Raisecom(fttx-onu-uni*/*/*:*)#**auto-negotiation restart**	(Optional) force UNI to restart auto-negotiation;
9	Raisecom(fttx-onu-uni*/*/*:*)#**alarm loss**	(Optional) enable Loss alarm function of UNI; use **no alarm loss** to disable Loss alarm function of UNI;
10	Raisecom(fttx-onu-uni*/*/*:*)#**shutdown**	(Optional) disable UNI port; use **no shutdown** to enable UNI;

2.3.12 Configuring flow control of uplink interface

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id*/onu-*id*	Enter ONU configuration mode;

3	Raisecom(fttx-onu*/*:*)#**uplink**	Enter ONU UPLINK port configuration mode;
4	Raisecom(fttx-onu-uplink*/*/*)#**uplink flowcontrol** { **enable** | **disable** }	Enable/disable flow control of ONU uplink interface;

2.3.13 Configuring speed limit of flow

Configuring speed limit of flow on uplink interface

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**uplink**	Enter ONU UPLINK port configuration mode;
4	Raisecom(fttx-onu-uplink*/*/*)#**uplink rate-limit** *rate*	Configure speed limit of flow of ONU uplink interface; use **no uplink rate-limit** to return to default configuration;

Configuring speed limit of UNI flow

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter ONU UNI Ethernet port configuration mode;
4	Raisecom(fttx-onu-uni*/*/*:*)#**policing** { **all** | **egress** | **ingress** } { **enable** | **disable** }	Enable/disable data speed limit of flow of UNI port;
5	Raisecom(fttx-onu-uni*/*/*:*)#**policing egress cir** *cir* [**pir** *pir*]	Configure data speed limit of flow of UNI in the downstream direction; use **no policing egress cir** to return to default configuration;
6	Raisecom(fttx-onu-uni*/*/*:*)#**policing ingress cir** *cir* [**cbs** *cbs*] [**ebs** *ebs*]	Configure data speed limit of flow of UNI in the upstream direction; use **no policing ingress cir** to return to default configuration;

2.3.14 Configuring mirroring of UNI port

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id*/onu-*id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**mirror** { **enable** | **disable** }	Enable/disable mirroring of UNI port;
4	Raisecom(fttx-onu*/*:*)#**mirror monitor-port** *uni-id*	Configure monitoring port; use **no mirror monitor-port** to return to default configuration;
5	Raisecom(fttx-onu*/*:*)#**mirror source-port-list** { **both** | **egress** | **ingress** } *uni-id* [**uplink**]	Configure source port and monitoring way; use **no mirror source-port-list** {**both** | **egress** | **ingress**} to return to default configuration;

2.3.15 Configuring DLF and BPDU forwarding

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**dlf-pkt forwarding** { **enable** | **disable** }	Enable/disable forwarding DLF message;
4	Raisecom(fttx-onu*/*:*)#**relay bpdu** { **enable** | **disable** }	Configure transmission transparently/end of BPDU message;

2.3.16 Configuring partner discovery

ONU can discover the downlink Raisecom devices by the private partner discovery protocol. Then to configure IP, VLAN, etc. information through OLT to manage the partner devices.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id*/onu-*id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**partner discovery** { **enable** | **disable** }	Enable/disable partner device discovery function of ONU;
4	Raisecom(fttx-onu*/*:*)#**partner** *partner-id* **mng-ip address** *ip-address* **mask** *mask* **default-gw** *default-gw* **vlan** *cvlan-id svlan-id priority*	(Optional) Configure management IP of partner device of ONU; use **no partner** *partner-id* **mng-ip** to return to default configuration;

Step	Configuration	Description
5	Raisecom(fttx-onu*/*:*)#**partner** *partner-id* **mng-ip address-type** { **dynamic** | **manual** }	(Optional) Configure management IP address type of partner device of ONU; use **no partner** *partner-id* **mng-ip address-type** to return to default configuration;
6	Raisecom(fttx-onu*/*:*)#**partner** *partner-id* **outband default-gw** *default-gw*	(Optional) Configure default gateway of out-of-band NM of ONU partner device; use **no partner** *partner-id* **outband default-gw** to cancel the configuration;
7	Raisecom(fttx-onu*/*:*)#**partner** *partner-id* **outband ip-address** *ip-address mask*	(Optional) Configure IP address and mask code of out-of-band management of ONU partner device; use **no partner** *partner-id* **outband ip-address** to cancel the configuration;
8	Raisecom(fttx-onu*/*:*)#**partner** *partner-id* **snmp-server host** *ip-address*	(Optional) Configure IP address of SNMP target host of ONU partner device; use **no partner** *partner-id* **snmp-server host** to return to default configuration;
9	Raisecom(fttx-onu*/*:*)#**partner** *partner-id* **snmp-server security** *name*	(Optional) Configure SNMP message name of ONU partner device; use **no partner** *partner-id* **snmp-server security** to return to default configuration
10	Raisecom(fttx-onu*/*:*)#**partner** *partner-id* **snmp-server community** *name* { **ro** | **rw** }	(Optional) Configure SNMP community name of ONU partner device; use **no partner** *partner-id* **snmp-server community** {**ro** | **rw**} to return to default configuration

2.3.17 Configuring PPPoE Agent

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/*onu-*id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**pppoe-agent** { **enable** | **disable** }	Enable/disable PPPoE Agent;
4	Raisecom(fttx-onu*/*:*)#**pppoe-agent user-define suboption** { **enable** | **disable** }	Enable/disable user-define function of PPPoE Agent option;
5	Raisecom(fttx-onu*/*:*)#**pppoe-agent circuit-id attach-string** *string*	Configure attach-atring filed of Circuit_ID option of PPPoE Agent; use command **no pppoe-agent circuit-id attach-string** to return attach-atring filed as default value;

Step	Configuration	Description
6	Raisecom(fttx-onu*/*:*)#**pppoe-agent remote-id mode** { **onumac-binary** | **clientmac-binary** | **onumac-ascii** | **clientmac-ascii** | **user-define** }	Configure filling mode of Remote_ID option of PPPoE Agent. Use command **no pppoe-agent remote-id mode** to return Remote_ID option as default value;
7	Raisecom(fttx-onu*/*:*)#**pppoe-agent remote-id string** *string*	Configure defined value by users of Remote_ID option of PPPoE Agent;
8	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter configuration mode of UNI port;
9	Raisecom(fttx-onu-uni*/*/*:*)#**pppoe-agent circuit-id string** *string*	Configure Circuit_ID option port defined value of PPPoE Agent; use command **no pppoe-agent circuit-id** to return port defined value as default value;
10	Raisecom(fttx-onu-uni*/*/*:*)#**pppoe-agent policy { keep** | **replace }**	Configure processing policy of PPPoE message with Circuit_ID or Remote_ID option by PPPoE Agent. Use command **no pppoe-agent policy** to return message processing policy as default value;

2.3.18 Configuring PoE (Power Over Ethernet)

Only partial models of ONU support PD (Powered Device) or PSE (Power-sourcing Equipment).

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id*/onu-*id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**poe pse power-management** { **auto** | **manual** }	Configure power supply management mode of PSE. Use **no poe pse power-management** to return to default configuration;
4	Raisecom(fttx-onu*/*:*)#**poe pse power-threshold** *value*	(Optional) Configure percentage of threshold of PSE power. Use **no poe pse power-threshold** to return to default configuration;
5	Raisecom(fttx-onu*/*:*)#**poe pse temperature-protection** { **enable** | **disable** }	(Optional) Enable/disable over-temperature protection of PSE module;
6	Raisecom(fttx-onu*/*:*)#**poe pse trap** { **enable** | **disable** }	(Optional) Enable/disable ONU PSE related Trap report;
7	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter ONU UNI Ethernet port configuration mode;
8	Raisecom(fttx-onu-uni*/*/*:*)#**poe pse** { **enable** | **disable** }	Enable/disable PSE of UNI port;
9	Raisecom(fttx-onu-uni*/*/*:*)#**poe pse max-power** *vaule*	(Optional) Configure the maximum output power of UNI power supply. Use **no poe pse max-power** to return to the default configuration;

Step	Configuration	Description
10	Raisecom(fttx-onu-uni*/*/*:*)#**poe pse power-priority** { **critical** | **high** | **low** }	(Optional) Configure power supply priority of port. Use **no poe pse power-priority** to return to default configuration;
11	Raisecom(fttx-onu-uni*/*/*:*)#**poe pse-off service** { **enable** | **disable** }	(Optional) enable/disable services to pass through when ONU UNI port doesn't connect with PSE device;

2.3.19 Checking configuration

Step	Configuration	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **information**	Show ONU basic information, including ONU name and so on;
2	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **detail-information**	Show ONU detailed information, including ONU device model and MAC address.
3	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **creation-information**	Show creation information of ONU, including management way and so on;
4	Raisecom# **show interface onu** *slot-id/olt-id/onu-id* **mng-information**	Show ONU management information.
5	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **mng-ip**	Show management IP configuration of ONU PON interface;
6	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **mng-information**	Show ONU management information; including ONU management mode, IP address configuration and binding SNMP parameter template information;
7	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **lan-ip**	Show IP configuration of ONU UNI port;
8	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **telnet**	Show ONU Telnet status;
9	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** *uni-id* **name**	Show name of UNI;
10	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** *uni-id* **information**	Show rate, duplex mode, flow control, port connection status of UNI and so on;
11	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** *uni-id* **isolation**	Show port isolation status of UNI;
12	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** *uni-id* **alarm**	Show Loss alarm function status of UNI;
13	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uplink**	Show status and configuration information of ONU uplink interface;
14	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **policing downstream**	Show speed limit of flow configuration of ONU downstream unicast data;

Step	Configuration	Description
15	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet policing**	Show UNI speed limit of flow Configure;
16	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uplink**	Show ONU uplink interface speed limit of flow configuration;
17	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **mirror**	Show port mirroring configuration of ONU;
18	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **system**	Show ONU system configuration, including transmission transparently BPDU message and forwarding configuration of DLF message;
19	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **partner** [**discovery**]	Show discovery function status and configuration information of ONU partner device;
20	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **pppoe-agent**	Show PPPoE configuration information of ONU device;
21	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** [uni-id] **pppoe-agent**	Show PPPoE function configuration information of ONU device port;
22	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** [uni-id] **pppoe-agent statistics**	Show PPPoE statistics information of ONU device port;
23	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **poe pse information**	Show ONU power supply information;
24	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** *uni-id* **poe pse information**	Show configuration information of PSE port in ONU UNI port;
25	Raisecom#**show onu-qos-template** *template-id*	Show ONU QoS template information
26	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **onu-qos-template**	Show QoS template information bound with ONU.
27	Raisecom#**show policing-template**	Show ONU policing template configurations.
28	Raisecom#**show interface onu** *slot-id/olt-id/onu-list* **uni eth** [*uni-id*] **policing-template**	Show information about the policing template bound to ONU UNI interface.

2.4 Maintenance

Command	Description
Raisecom(fttx-olt*/*)#**clear illegal-onu**	Clear illegal ONU information;
Raisecom(fttx-olt*/*)#**clear interface olt-onu** *slot-id/olt-list* **statistics**	Clear all PON statistics of OLT and ONU;

Command	Description
Raisecom(fttx-onu*/*:*)#clear interface onu *slot-id/olt-id/onu-id* **uni ethernet** *uni-id* **{statistic | spanning-tree statistic}**	Clear statistics of ONU UNI port;
Raisecom(fttx-onu*/*:*)#**clear interface onu** *slot-id/olt-id/onu-id* **uplink statistic**	Clear statistics of ONU uplink interface;
Raisecom(fttx-onu*/*:*)#**clear interface onu** *slot-id/olt-id/onu-id* **pon statistic**	Clear statistics of ONU PON interface;
Raisecom(fttx-onu*/*:*)#**clear interface onu** *slot-id/olt-id/onu-id* **statistics {fec | mpcp | omp-emulation | basic | link-quality}**	Clear PON content statistics of ONU;
Raisecom(fttx-onu*/*:*)#**clear interface onu** *slot-id/olt-id/onu-id* **uni ethernet** [*uni-id*] **pppoe-agent statistics**	Clear PPPoE message statistics information of ONU port;

2.5 Configuration examples

2.5.1 Examples for configuring ONU automatic registration

Networking requirements

As shown in below figure, enable and configure ONU authentication mode on OLT 1/1 port as none, and ONU can be put into OLT by automatic registration.

Figure 2-3 ONU automatic registration

Configuration steps

Step 1 Configure ONU authentication mode as none.

```
Raisecom#fttx
Raisecom(fttx)#interface olt 1/1
Raisecom(fttx-olt1:1)#authorization mode none
```

Checking results

Show ONU authentication mode:

```
Raisecom#show interface olt 1/1 information
       MaxRTT   Encryption    Authorization      Registered
OLT ID  (TQ)     Mode          Mode              ONUs       SFP
-------------------------------------------------------------------
1/1     14000    tri-churning   none              1          ok
```

Show ONU information registered in OLT:

```
Raisecom#show interface onu creation-information
ONU ID     MAC Address Mode  Creation Date   Device Type   State  Mng-mode
description
-------------------------------------------------------------------------
1/1/1   000e.5e0a.7a0e auto  2000-01-01,08:00 ISCOM5104(C) active   oam
```

Show indicators of device:

LINK indicators of the PON interface normally on if ONU is registered successfully.

2.5.2 Examples for configuring ONU registration based on MAC address authentication mode

Networking requirements

As shown in below figure, enable MAC address authentication mode on OLT 1/1 port to register ONU, where ONU model which ready for registration is 5104c, MAC address is 0000.0000.0001.

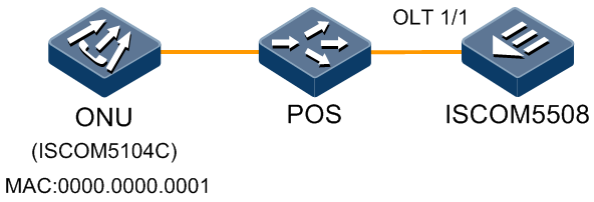

Figure 2-4 ONU registration based on MAC address authentication mode

Configuration steps

Step 1 Configure ONU authentication mode as MAC address authentication mode.

```
Raisecom#fttx
Raisecom(fttx)#interface olt 1/1
Raisecom(fttx-olt1:1)#authorization mode mac
```

Step 2 Create ONU based on MAC authorization entries.

```
Raisecom(fttx-olt1:1)#create onu 1 mac 0000.0000.0001 device-type 5104c
```

Checking results

Show ONU authentication mode.

```
Raisecom#show interface olt 1/1 information
OLT ID  (TQ)    Mode          Authorization  ONUs      ONUs      SFP
-------------------------------------------------------------------------
----
1/1    14000   tri-churning    none          1         0         ok
```

Show ONU information registered in OLT.

```
Raisecom#show interface onu creation-information
ONU ID  MAC Address   Mode  Creation Date  Device Type  State   Mng-mode
Description
-------------------------------------------------------------------------
1/1/1  0000.0000.0001  mac  2000-01-01,08:00 ISCOM5104(C) active   oam  --
```

Show indicators of device. LINK indicators of the PON interface normally on if ONU is registered successfully.

2.5.3 Examples for configuring ONU port mirroring

Networking requirements

As shown in below figure, PC A connects with UNI 1 of ONU, PC B connects with UNI 2 of ONU, and ONU links with OLT 1/1 port. PC B works as monitoring device to monitor data in UNI 1 of ONU and entry direction of uplink interface.

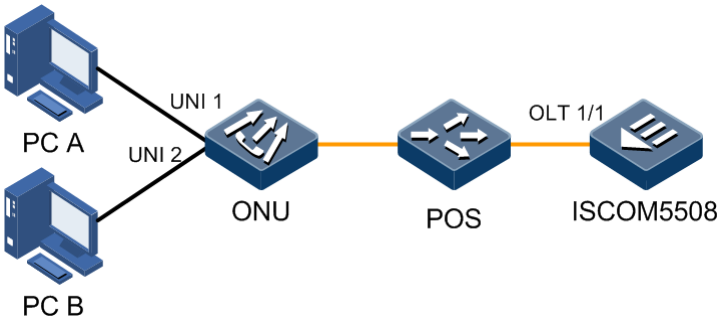

Figure 2-5 ONU port mirroring

Configuration steps

Step 1 Configure monitoring port.

```
Raisecom#fttx
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#mirror monitor-port 2
```

Step 2 Configure source port and monitoring way.

```
Raisecom(fttx-onu1/1:1)#mirror source-port-list ingress 1 uplink
```

Step 3 Enable port monitoring.

```
Raisecom(fttx-onu1/1:1)#mirror enable
```

Checking results

Show monitoring configuration of ONU port.

```
Raisecom#show interface onu 1/1/1 mirror
ONU ID:1/1/1
   Status      :Enable
   Monitor Port :2
   Ingress Ports:1,uplink
   Egress  Ports:n/a
```

2.5.4 Examples for configuring speed limit of flow

Networking requirements

As shown in below figure, PC A connects with UNI 1 and ONU links with OLT 1/1 port to realize the following speed limit of flow:

- Rate of ISCOM5508 downlink unicast is 40960kbit/s, burst is 40960Byte.
- Uplink DBA rate of ONU: FIR is 0 kbit/s, CIR is 512 kbit/s, PIR is 4096 kbit/s.
- Downlink guarantee speed of UNI 1 is 1024 kbit/s, peak rate is 2048 kbit/s.
- Uplink guarantee speed of UNI 1 is 512 kbit/s.

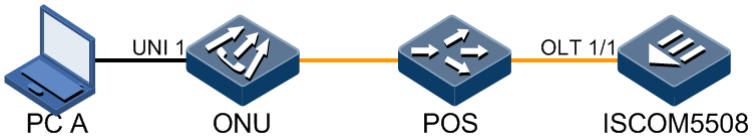

Figure 2-6 Speed limit of flow

Configuration steps

Step 1 Configure OLT downlink unicast speed limit of flow.

```
Raisecom#fttx
Raisecom(fttx)#interface olt 1/1
Raisecom(fttx-olt1:1)#policing downstream rate 40960 40960
Raisecom(fttx-olt1:1)#exit
```

Step 2 Configure ONU uplink DBA rate and enable it.

```
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#sla fir 0
Raisecom(fttx-onu1/1:1)#sla cir 512
Raisecom(fttx-onu1/1:1)#sla pir 4096
```

Step 3 Configure speed limit on downlink of ONU UNI port.

```
Raisecom(fttx-onu1/1:1)#uni ethernet 1
Raisecom(fttx-onu-uni1/1/1:1)#policing egress cir 1024 pir 2048
```

Step 4 Configure speed limit on uplink of ONU UNI port.

```
Raisecom(fttx-onu-uni1/1/1:1)#policing ingress cir 512
```

Step 5 Enable speed limit of UNI flow.

```
Raisecom(fttx-onu-uni1/1/1:1)#policing all enable
```

Checking results

Show OLT downlink unicast speed limit of flow:

```
Raisecom#show interface onu 1/1/1 policing downstream
ONU ID   Rate(Kbps)     Burst(Bytes)
-------------------------------------
1/1/1    40960          40960
```

Show ONU uplink DBA configuration:

```
Raisecom#fttx
Raisecom(fttx)#show interface onu 1/1/1 sla
FIR: Fixed information rate
CIR: Commited information rate
PIR: Peak information rate
ONU ID   FIR (Kbps)     CIR(Kbps)      PIR(Kbps)      Priority
-----------------------------------------------------------------
1/1/1    0              512            4096           0
```

Show speed limit configuration of flow on uplink/downlink of ONU UNI port:

```
Raisecom#show interface onu 1/1/1 uni ethernet 1 policing
Port ID: 1/1/1/1
   Ingress policing   : enable
   Ingress policing CIR: 512(512) Kbps
   Ingress policing CBS: 64022 Bytes
   Ingress policing EBS: 1514 Bytes
   Egress policing    : enable
   Egress policing CIR : 1024(1024) Kbps
   Egress policing PIR : 2048 Kbps
```

3 Configuring multicast service

The chapter introduces configuration information and configuration procedure of multicast service of ISCOM5508 device, and introduces configuration applications.

- Quick configuration of multicast service
- Configuring IGMP Snooping
- Configuring IGMP Proxy
- Configuring MVR
- Configuring MVR Proxy
- Configuring IGMP filter and the maximum number of multicast groups
- Configuring dynamic and controllable multicast
- Maintenance

3.1 Quick configuration of multicast service

3.1.1 Quick configuration of IGMP Snooping

Networking requirements

As shown in below figure, uplink port GE 1 of ISCOM5508 device connects with multicast route, PON port OLT 1/1 connects with ONU, two Ethernet ports UN1 and UN2 on ONU connects with two users separately, and all multicast users belong to one VLAN 101. Users can receive multicast data if we configure IGMP Snooping and immediate-leave on ISCOM5508 device and ONU device.

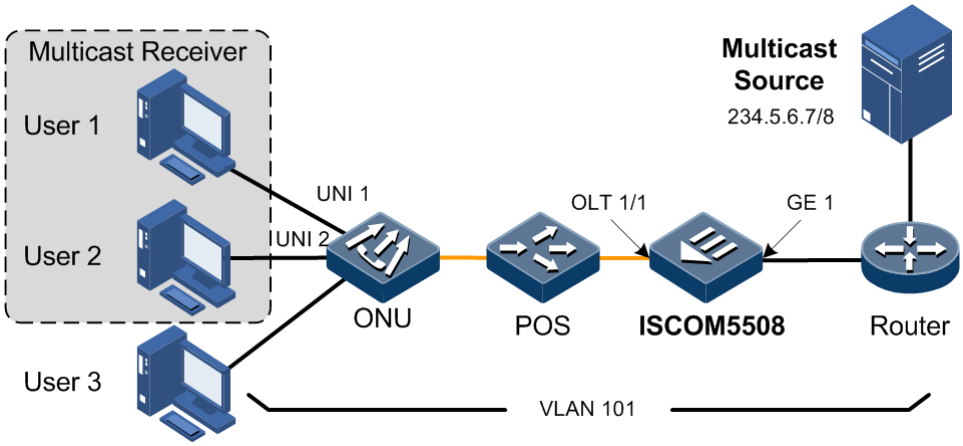

Figure 3-1 IGMP Snooping networking application

Configuration steps

- Configure OLT

Step 1 Create multicast VLAN and configure port attribute.

```
Raisecom#config
Raisecom(config)#create vlan 101 active
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 101
Raisecom(config-port)#exit
Raisecom(config)#interface port 7
Raisecom(config-port)# switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 101
Raisecom(config-port)#exit
```

Step 2 Enable IGMP Snooping and configure immediate-leave and port of multicast routing.

```
Raisecom#config
Raisecom(config)#vlan 101
Raisecom(config-vlan)#ip igmp snooping
Raisecom(config-vlan)#ip igmp snooping immediate-leave
Raisecom(config-vlan)#exit
Raisecom(config)#ip igmp snooping mrouter vlan 101 port 1
```

Step 3 Enable IGMP Snooping globally.

```
Raisecom(config)#ip igmp snooping
```

Step 4 Create multicast VLAN and configure port attribute.

```
Raisecom#fttx
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#uni ethernet 1
Raisecom(fttx-onu-uni1/1/1:1)#vlan mode tagged
Raisecom(fttx-onu-uni1/1/1:1)#multicast vlan 101
Raisecom(fttx-onu-uni1/1/1:1)#multicat vlan tag-strip enable
Raisecom(fttx-onu-uni1/1/1:1)#exit
Raisecom(fttx-onu1/1:1)#uni ethernet 2
Raisecom(fttx-onu-uni1/1/1:2)#vlan mode tagged
Raisecom(fttx-onu-uni1/1/1:2)#multicast vlan 101
Raisecom(fttx-onu-uni1/1/1:2)#multicat vlan tag-strip enable
Raisecom(fttx-onu-uni1/1/1:2)#exit
Raisecom(fttx-onu1/1:1)#uplink
Raisecom(fttx-onu-uplink1/1/1)#vlan mode trunk
Raisecom(fttx-onu-uplink1/1/1)#vlan trunk allowed 101
Raisecom(fttx-onu-uplink1/1/1)#exit
```

Step 5 Enable IGMP Snooping and configure immediate-leave.

```
Raisecom(fttx-onu1/1:1)#ip igmp mode snooping
Raisecom(fttx-onu1/1:1)#ip igmp immediate-leave
```

Step 6 Configure forwarding mode of multicast traffic flow.

```
Raisecom(fttx-onu1/1:1)#ip igmp vlan-aware enable
```

Checking results

- Check OLT configuration.

Check whether configuration of IGMP Snooping on OLT is correct.

```
Raisecom#show ip igmp snooping
IGMP snooping: Enable
IGMP querier:Disable
IGMP snooping aging time: 300s
IGMP snooping active VLAN: 1-4094
IGMP snooping immediate-leave active VLAN: 101
```

Check whether multicast routing information of IGMP Snooping is correct.

```
Raisecom#show ip igmp snooping mrouter
Ip Address      Port   Vlan   Age      Type
-------------------------------------------------
234.0.0.0/8       1     101    --       USER
```

- Check ONU configuration.

Check whether configuration of IGMP Snooping on OLT is correct.

```
Raisecom#show interface onu 1/1/1 ip igmp
ONU ID: 1/1/1
   IGMP Mode                      : snooping
   Last Member Query Count        : 2
   Last Member Query Interval     : 2s
   Aging Time                     : 300s
   VLAN Aware                     : enable
   Immediate-leave Administrative : enable
```

3.1.2 Quick configuration of MVR

Networking requirements

As shown in below figure, port GE 1 of ISCOM5508 device connects with multicast router, port OLT 1/1 connects with users by ONU, and users can receive multicast data of multicast 234.5.6.7 and 225.1.1.1.

If we specify VLAN 3 as multicast VLAN to configure MVR, multicast data doesn't need to be copied in every VLAN, but only copy multicast data one time in multicast VLAN, saving bandwidth.

If we enable MVR Proxy on ISCOM5508 device, it reduces communication between host and multicast router, and doesn't affect realization of multicast function.

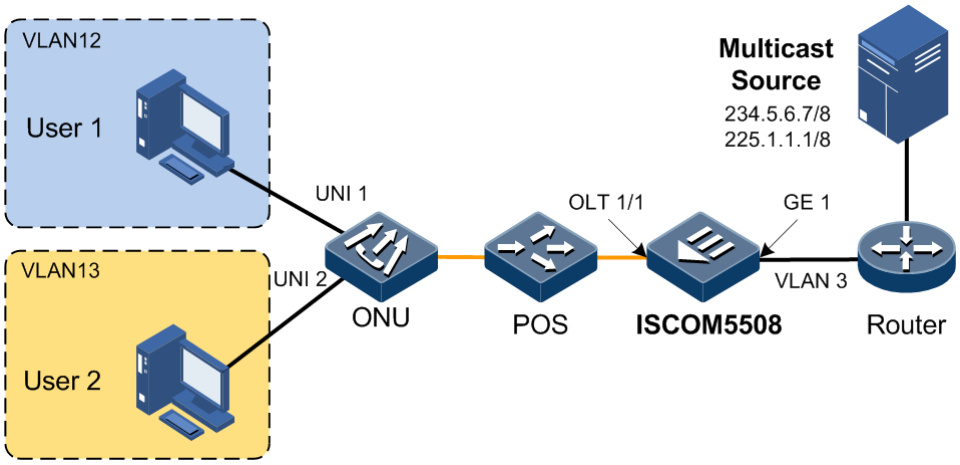

Figure 3-2 MVR networking application

Configuration steps

- Configure OLT.

Step 1 Enable MVR and MVR Proxy, and specify multicast VLAN and group address.

```
Raisecom#config
Raisecom(config)#creat vlan 3,12,13 active
Raisecom(config)#mvr enable
Raisecom(config)#mvr mode dynamic
Raisecom(config)#mvr proxy
Raisecom(config)#mvr vlan 3
Raisecom(config)#mvr vlan 3 group 234.5.6.7
Raisecom(config)#mvr vlan 3 group 225.1.1.1
```

Step 2 Configure source port information.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#mvr type source
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk native vlan 3
Raisecom(config-port)#switchport trunk untagged vlan 12,13
Raisecom(config-port)#exit
```

Step 3 Configure PON port information.

```
Raisecom(config)#interface port 7
Raisecom(config-port)#mvr type receiver
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 3,12,13
Raisecom(config-port)#end
```

- Configure ONU.

Step 4 Configure ONU port information.

```
Raisecom#fttx
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#uni ethernet 1
Raisecom(fttx-onu-uni1/1/1:1)#vlan mode tagged
Raisecom(fttx-onu-uni1/1/1:1)#native vlan 12
Raisecom(fttx-onu-uni1/1/1:1)#multicat vlan tag-strip enable
Raisecom(fttx-onu-uni1/1/1:1)#exit
Raisecom(fttx-onu1/1:1)#uni ethernet 2
Raisecom(fttx-onu-uni1/1/1:2)#vlan mode tagged
Raisecom(fttx-onu-uni1/1/1:2)#native vlan 13
Raisecom(fttx-onu-uni1/1/1:2)#multicat vlan tag-strip enable
Raisecom(fttx-onu-uni1/1/1:2)#exit
Raisecom(fttx-onu-uni1/1:1)#uplink
Raisecom(fttx-onu-uplink1/1/1)#vlan mode trunk
Raisecom(fttx-onu-uplink1/1/1)#vlan trunk allowed 3,12,13
Raisecom(fttx-onu-uplink1/1/1)#exit
```

Step 5 Configure treatment of IGMP message by ONU.

```
Raisecom(fttx-onu1/1:1)#ip igmp mode snooping
```

Checking results

- Check OLT configuration.

Check whether configuration of MVR Proxy is correct.

```
Raisecom#show mvr proxy
Mvr Proxy Suppression Status:enable
Ip Igmp Querier Status :enable
Mvr Proxy Source Ip :192.168.18.2
Mvr Proxy Version :V2
Ip Igmp Query Interval(s):60
Query Response Interval(s):10
Last Member Query Interval(s):1
Next IGMP General Query(s):5
```

Check whether configuration of MVR is correct.

```
Raisecom#show mvr
MVR Running: Enable
MVR Multicast VLAN(ref):3(2)
```

```
MVR Max Multicast Groups: 1024
MVR Current Multicast Groups: 2
MVR Timeout: 600 (second)
```

- MVR Mode: Dynamic checks ONU configuration.

Check treatment of ONU IGMP message.

```
Raisecom# show interface onu 1/1/1 ip igmp
ONU ID: 0/5/1
   IGMP Mode                   : snooping
   Last Member Query Count       : 2
   Last Member Query Interval    : 2s
   Aging Time                  : 300s
   VLAN Aware                  : enable
   Immediate-leave Administrative : disable
```

3.1.3 Quick configuration of IGMP filter and the maximum number of multicast groups

Networking requirements

As shown in below figure, port GE 1 of ISCOM5508 device connects with multicast router, port OLT 1/1 connects with users by ONU. User 1 and User 2 can have different multicast authorization control by configuring IGMP filter and the maximum number of multicast groups.

- User 1: allow 234.5.6.7–234.5.6.11 multicast group at most.
- User 2: allow 234.5.6.7–234.5.6.10 multicast group at most, if users add a new multicast group, a multicast group before the new one will be dropped out.

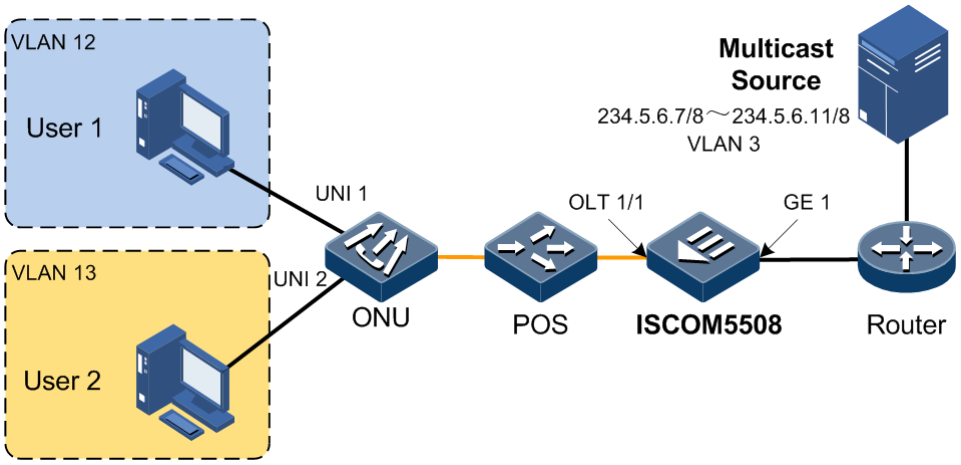

Figure 3-3 Networking application of IGMP filter and the maximum number of multicast groups

Configuration steps

- Configure OLT.

Step 1 Enable MVR.

```
Raisecom#config
Raisecom(config)#creat vlan 3,12,13 active
Raisecom(config)#mvr enable
Raisecom(config)#mvr proxy
Raisecom(config)#mvr vlan 3
Raisecom(config)#mvr vlan 3 group 234.5.6.7 5
Raisecom(config)#interface port 1
Raisecom(config-port)#mvr type source
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk native vlan 3
Raisecom(config-port)#switchport trunk untagged vlan 12,13
Raisecom(config-port)#exit
Raisecom(config)#interface port 7
Raisecom(config-port)#mvr type receiver
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 3,12,13
Raisecom(config-port)#exit
```

Step 2 Configure IGMP filter rules.

```
Raisecom(config)#ip igmp profile 1
Raisecom(config-igmp-profile)#range 234.5.6.7 234.5.6.10
Raisecom(config-igmp-profile)#permit
Raisecom(config-igmp-profile)#exit
```

Step 3 Apply filter rules on VLAN 13.

```
Raisecom(config)#ip igmp filter 1 vlan 13
Raisecom(config)#ip igmp max-group 1 vlan 13
Raisecom(config)#ip igmp max-group action replace vlan 13
```

- Configure ONU.

Step 4 Configure ONU port information.

```
Raisecom#fttx
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#uni ethernet 1
Raisecom(fttx-onu-uni1/1/1:1)#vlan mode tagged
Raisecom(fttx-onu-uni1/1/1:1)#native vlan 12
Raisecom(fttx-onu-uni1/1/1:1)#multicat vlan tag-strip enable
Raisecom(fttx-onu-uni1/1/1:1)#exit
Raisecom(fttx-onu1/1:1)#uni ethernet 2
Raisecom(fttx-onu-uni1/1/1:2)#vlan mode tagged
Raisecom(fttx-onu-uni1/1/1:2)#native vlan 13
Raisecom(fttx-onu-uni1/1/1:2)#multicat vlan tag-strip enable
Raisecom(fttx-onu-uni1/1/1:2)#exit
Raisecom(fttx-onu1/1:1)#uplink
Raisecom(fttx-onu-uplink1/1/1)#vlan mode trunk
Raisecom(fttx-onu-uplink1/1/1)# vlan trunk allowed 3,12,13
Raisecom(fttx-onu-uplink1/1/1)#exit
```

Step 5 Configure treatment of IGMP message by ONU.

```
Raisecom(fttx-onu1/1:1)#ip igmp mode snooping
```

Step 6 Configure forwarding mode of multicast traffic flow.

```
Raisecom(fttx-onu1/1:1)#ip igmp vlan-aware enable
```

Checking results

- Check OLT configuration.

Show global configuration of IGMP filtering.

```
Raisecom#show ip igmp filter
IGMP filter: Enable
```

Show IGMP filter configuration.

```
Raisecom#show ip igmp profile
IGMP profile 1
    permit
    range 234.5.6.7    234.5.6.10
```

Check whether IGMP filter configuration of VLAN 13 is correct.

```
Raisecom#show igmp filter vlan 13
VLAN    Filter    Max Groups    Current Groups  Action
------------------------------------------------------
13      1         1             0               Replace
```

- Check ONU configuration.

Show treatment mode of ONU IGMP message.

```
Raisecom# show interface onu 1/1/1 ip igmp
ONU ID: 1/1/1
   IGMP Mode                    : transparent
   Last Member Query Count       : 2
   Last Member Query Interval    : 2s
   Aging Time                   : 300s
   Immediate-leave Administrative : disable
```

Show VLAN configuration of ONU port.

```
Raisecom#show interface onu 1/1/1 uni ethernet vlan
Port ID: 1/1/1/1
   VLAN mode        : Transparent
   Native VLAN      : 12(CoS 0)
   Trans-rule list   : n/a
   Trunk allowed VLAN: n/a
Port ID: 1/1/1/2
   VLAN mode        : Transparent
   Native VLAN      : 13(CoS 0)
   Trans-rule list   : n/a
   Trunk allowed VLAN: n/a
Raisecom#show interface onu 1/1/1 uplink vlan
Port ID: 1/1/1 uplink
   VLAN mode        : Trunk
   Trunk allowed VLAN: 1-100
```

3.1.4 Quick configuration of dynamic and controllable multicast

Networking requirements

As shown in below figure, port GE 1 of ISCOM5508 device connects with multicast router, port OLT 1/1 of PON connects with users by ONU. User 1 and User 2 have different access right on channel 1 (234.5.6.7) and channel 2 (225.1.1.1) by configuring dynamic and controllable multicast.

- User 1: allow to watch channel 1, and have preview permission on channel 2 for 2 minutes.
- User 2: don't allow watching channel 1, but allow watching channel 2.

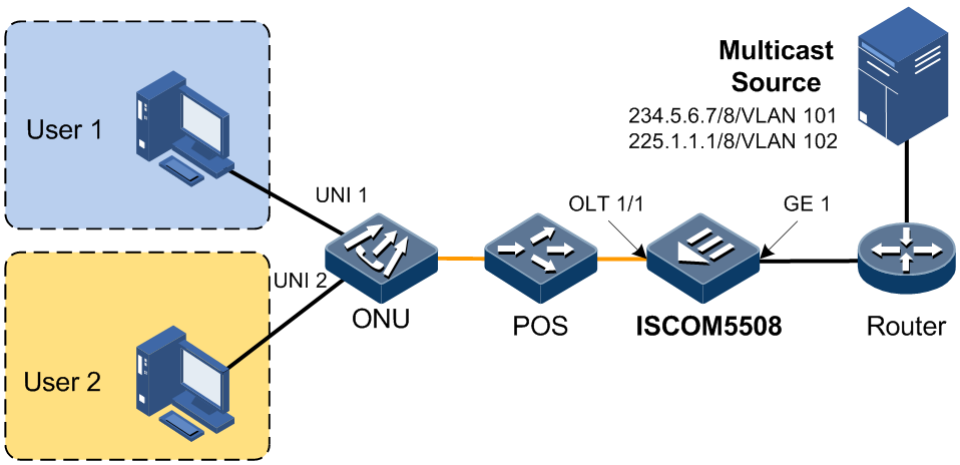

Figure 3-4 Networking application of dynamic and controllable multicast

Configuration steps

- Configure OLT.

Step 1 Create multicast VLAN, multicast channel and enable global dynamic and controllable multicast.

```
Raisecom#config
Raisecom(config)#creat vlan 101,102 active
Raisecom(config)#exit
```

Step 2 Enable IGMP Proxy.

```
Raisecom#fttx
Raisecom(fttx)#interface olt 1/1
Raisecom(fttx-olt1:1)#ip igmp proxy enable
Raisecom(fttx-olt1:1)#exit
```

Step 3 Create multicast channel and enable global dynamic and controllable multicast.

```
Raisecom(fttx)#ctrl-multicast creat channel 234.5.6.7 vlan-id 101
Raisecom(fttx)#ctrl-multicast creat channel 225.1.1.1 vlan-id 102
Raisecom(fttx)#ctrl-multicast enable
```

Step 4 Create dynamic and controllable multicast.

```
Raisecom(fttx)#ctrl-multicast creat user 1 onu 1/1/1 uni 1
Raisecom(fttx)#ctrl-multicast creat user 2 onu 1/1/1 uni 2
```

Step 5 Configure preview rules of dynamic and controllable multicast.

```
Raisecom(fttx)#ctrl-multicast creat preview-rule 9
Raisecom(fttx)#ctrl-multicast preview-rule 9 time 10
```

Step 6 Configure dynamic and controllable multicast permission of User 1.

```
Raisecom(fttx)#ctrl-multicast creat right user 1 channel 234.5.6.7
Raisecom(fttx)#ctrl-multicast creat right user 1 channel 225.1.1.1
Raisecom(fttx)#ctrl-multicast right user 1 channel 234.5.6.7 permit
Raisecom(fttx)#ctrl-multicast right user 1 channel 225.1.1.1 preview
Raisecom(fttx)#ctrl-multicast right user 1 channel 225.1.1.1 preview-rule
9
```

Step 7 Configure dynamic and controllable multicast permission of User 2.

```
Raisecom(fttx)#ctrl-multicast creat right user 2 channel 234.5.6.7
Raisecom(fttx)#ctrl-multicast creat right user 2 channel 225.1.1.1
Raisecom(fttx)#ctrl-multicast right user 2 channel 234.5.6.7 deny
Raisecom(fttx)#ctrl-multicast right user 2 channel 225.1.1.1 permit
Raisecom(fttx)#end
```

Step 8 Disable IGMP Snooping globally.

```
Raisecom(config)#no ip igmp snooping
```

Step 9 Enable IGMP Snooping in multicast VLAN.

```
Raisecom#config
Raisecom(config)#vlan 101
```

```
Raisecom(config-vlan)#ip igmp snooping
Raisecom(config-vlan)#exit
Raisecom(config)#vlan 102
Raisecom(config-vlan)#ip igmp snooping
Raisecom(config-vlan)#exit
Raisecom(config)#ip igmp snooping mrouter vlan 101 port 1
Raisecom(config)#ip igmp snooping mrouter vlan 102 port 1
```

Step 10 Configure OLT port information.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 101,102
Raisecom(config-vlan)#exit
Raisecom(config)#interface port 7
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 101,102
Raisecom(config-port)#end
```

- Configure ONU.

Step 11 Configure multicast mode of ONU as dynamic and controllable multicast mode.

```
Raisecom#fttx
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#ip igmp mode ctrl-multicast
```

Step 12 Configure ONU port information.

```
Raisecom(fttx-onu1/1:1)#uplink
Raisecom(fttx-onu-uplink1/1/1)#vlan mode trunk
Raisecom(fttx-onu-uplink1/1/1)#vlan trunk allowed 101,102
Raisecom(fttx-onu-uplink1/1/1)#exit
Raisecom(fttx-onu1/1:1)#uni ethernet 1
Raisecom(fttx-onu-uni1/1/1:1)#vlan mode tagged
Raisecom(fttx-onu-uni1/1/1:1)#multicast vlan 101
Raisecom(fttx-onu-uni1/1/1:1)#multicat vlan tag-strip enable
Raisecom(fttx-onu-uni1/1/1:1)#exit
Raisecom(fttx-onu1/1:1)#uni ethernet 2
Raisecom(fttx-onu-uni1/1/1:2)#vlan mode tagged
Raisecom(fttx-onu-uni1/1/1:2)#multicast vlan 102
Raisecom(fttx-onu-uni1/1/1:2)#multicat vlan tag-strip enable
Raisecom(fttx-onu-uni1/1/1:2)#exit
```

Step 13 Configure forwarding mode and immediate-leaving of multicast traffic flow.

```
Raisecom(fttx-onu1/1:1)#ip igmp vlan-aware enable
Raisecom(fttx-onu1/1:1)#ip igmp immediate-leave
```

Checking results

- Check OLT configuration.

Show global configuration parameter of dynamic and controllable multicast.

```
Raisecom#show ctrl-multicast
Controllable multicast state   : Enable
Unregistered users right      : Deny
Unauthorized channel right    : Deny
Preview resetting period      : Daily
Preview time recorded threshold: 1 min
CDR state                   : Disable
CDR synchronization period    : 60 min
CDR time recorded threshold   : 1 min
Max No-Igmp-Report Duration   : 5 min
```

Show channel configuration of dynamic and controllable multicast.

```
Raisecom#show ctrl-multicast channel
Channel Address   Name            State    Online User Num  VID
-------------------------------------------------------------------
225.1.1.1       RaisecomCh       enable   0              102
234.5.6.7       RaisecomCh       enable   0              101
```

Show configuration of users.

```
Raisecom#show ctrl-multicast user
Total user number: 2
User ID: 1
   UNI                    : 1/1/1/1
   User name              : 1/1/1/1
   Current state          : Enable
   Online channel permitted: 16
   IP address             : 0.0.0.0
   Online channel list    :
User ID: 2
   UNI                     : 1/1/1/2
   User name              : 1/1/1/2
   Current state          : Enable
   Online channel permitted: 16
   IP address             : 0.0.0.0
   Online channel list    :
```

Show right configuration of users.

```
Raisecom#show ctrl-multicast right
                                                    Preview   Preview
User ID   Channel Address  Right    Rule ID    Count    Time(min)   State
-------------------------------------------------------------------------
1          234.5.6.7       permit     1          0          0       offline
1          225.1.1.1       preview    9          0          0       offline
2          234.5.6.7       deny       1          0          0       offline
1          225.1.1.1       permit     1          0          0       offline
```

- Check ONU configuration.

Show treatment mode of ONU IGMP message.

```
Raisecom# show interface onu 1/1/1 ip igmp
ONU ID: 1/1/1
   IGMP Mode                  : ctrl-multicast
   Last Member Query Count       : 2
   Last Member Query Interval    : 2s
   Aging Time                 : 300s
   Immediate-leave Administrative : enable
```

3.2 Configuring IGMP Snooping

3.2.1 Preparing for configuration

Networking situation

If many users want to receive data sent from source multicast on ONU, the device can run IGMP Snooping on ISCOM5508 device and ONU respectively, and create and maintain 2 pieces of multicast forwarding table by monitoring multicast message between router and host, to realize multicast over the link layer.

Create multicast forwarding table which multicast message and port PON on ISCOM5508 to realize distribution of multicast information based on port PON.Create multicast forwarding table which multicast message and port UNI on ONU to realize distribution of multicast information based on port UNI.

Precondition

The following tasks should be completed before configuring IGMP Snooping:

- Create and configure corresponding VLAN.
- Disable global MVP.

3.2.2 Default configuration of IGMP Snooping

Default configuration of IGMP Snooping on ISCOM5508 device:

Function	Default value
Global IGMP Snooping	disable
IGMP Snooping on VLAN	disable
IGMP query	disable
Aging time of multicast routing entries	300s
Ports of multicast router	N/A
immediate-leave	disable
Static multicast routing table	N/A

Default configuration of IGMP Snooping on Raisecom ONU device:

Function	Default value
IGMP mode	IGMP Snooping
Timeout times of the last member inquiring message	2 times
Interval of the last member sending IGMP query message	2s
Aging time of multicast routing entries	300s
Forwarding mode of multicast traffic flow	VLAN+MAC forwarding mode
immediate-leave	disable

Devices don't configure forwarding mode of multicast traffic flow in single port series ONU of Raisecom, and don't identify VLAN. By default, devices support forwarding according to MAC addresses.

3.2.3 Configuring IGMP Snooping

Configuring IGMP Snooping on OLT

- Configure global IGMP Snooping.

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode;

Step	Configuration	Description
2	Raisecom(config)#**ip igmp snooping**	Enable global IGMP Snooping;
3	Raisecom(config)#**ip igmp querier** { **enable** | **disable** }	(Optional) enable/disable IGMP query;
4	Raisecom(config)#**ip igmp querier query-interval** *period*	(Optional) configure time interval of IGMP query;

- Configure IGMP Snooping of many VLAN.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip igmp snooping vlan-list** *vlan-list*	Enable IGMP Snooping of many VLANs;
3	Raisecom(config)#**no ip igmp snooping vlan-list** *vlan-list*	(Optional) disable IGMP Snooping of many VLANs;

- Configure IGMP Snooping of single VLAN.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**vlan** *vlan-id*	Enter VLAN configuration mode;
3	Raisecom(config-vlan)#**ip igmp snooping**	Enable IGMP Snooping of single VLAN;
4	Raisecom(config-vlan)#**no ip igmp snooping**	(Optional)disable IGMP Snooping of single VLAN;

Note

- If users enable global IGMP Snooping, IGMP Snooping on all VLAN will be enabled. So users can disable IGMP Snooping of some VLAN in VLAN configuration mode or global configuration mode before enabling global IGMP Snooping.
- If users disable global IGMP Snooping, IGMP Snooping on VLAN will be disabled.

Configuring IGMP Snooping on ONU

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**ip igmp mode** { **snooping** | **ctrl-multicast** | **transparent** }	Configure treatment mode of IGMP message by ONU.

Step	Configuration	Description
4	Raisecom(fttx-onu*/*:*)#**ip igmp vlan-aware** { **enable** | **disable** }	(Optional)configure forwarding mode of multicast traffic flow;
5	Raisecom(fttx-onu*/*:*)#**ip igmp last-member-query-count** *count*	(Optional)timeout times of last-member query message triggered by leave-message;
6	Raisecom(fttx-onu*/*:*)#**ip igmp last-member-query-interval** *second*	(Optional)time-out period of query responding of last-member query message triggered by leave-message;

3.2.4 (Optional) configuring aging time of multicast routing entries

In IGMP Snooping, when a device cannot receive IGMP message of some layer-2 multicast routing, it may be caused by relevant host or router has left multicast group, but without transmitting leaving message. User can set aging time for multicast routing entry. Then the related entries will be deleted from multicast routing table once reaching aging time.

Configuring aging time of OLT multicast routing entries

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip igmp snooping timeout** { *period* | **infinite** }	Enter aging time of multicast routing entries;

Configuring aging time of ONU multicast routing entries

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**ip igmp aging-time** *period*	Enter aging time of multicast routing entries;

3.2.5 (Optional) configuring ports of multicast router

In ISCOM5508, multicast routing port is configured based on VLAN. Each VLAN can configure multiple router ports and the router port is available to all multicast group addresses.

- Configure global multicast router ports.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;

Step	Configuration	Description
2	Raisecom(config)#**ip igmp snooping mrouter vlan** *vlan-id* **port** *port-id*	Configure multicast router ports of specific VLAN;

- Configure card-based multicast router ports.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system.
2	Raisecom(fttx)#**slot** *slot-id*	Enter slot configuration mode.
3	Raisecom(fttx-slot:*)#**ip igmp snooping router learning** { **enable** | **disable** }	Configure card-based multicast router port learning.
4	Raisecom(fttx-slot:*)#**ip igmp snooping router static port-list** {**all** | *port-list* }	Configure card-based static router ports.

3.2.6 (Optional) configuring immediate-leave

When user host transmitting IGMP leaving message, device won't delete multicast routing by automation, it will wait some time before deletion. When there are a lot of users at downstream, and it is frequently operated in adding and leaving, immediate-leave can be used. The multicast routing can be deleted by automation when user hosts transmit IGMP leaving message.

This function is only available to IGMPv2/v3 version.

Configuring immediate-leave of OLT

- Configure immediate-leave of many VLANs on OLT.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip igmp snooping vlan** *vlan-list* **immediate-leave**	Enable immediate-leave based on many VLAN;

- Configure immediate-leave of single VLAN on OLT

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**vlan** *vlan-id*	Enter VLAN configuration mode;
3	Raisecom(config-vlan)#**ip igmp snooping immediate-leave**	Enable immediate-leave of single VLAN;

- Configure card-based immediate-leave.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system.
2	Raisecom(fttx)#**slot** *slot-id*	Enter slot configuration mode.
3	Raisecom(fttx-slot:*)#**ip igmp snooping immediate-leave port-list** {**all** | *port-list* }	Enable card-based immediate-leave.

Configuring immediate-leave of ONU

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**ip igmp immediate-leave**	Configure IGMP immediate-leave on ONU;

3.2.7 (Optional) configuring forwarding table of static multicast

The device usually add member ports into multicast routing table through auto-sensing user host, user can also configure device by manual to add member port into multicast routing table.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**mac-address-table static multicast** *mac-address* **vlan** *vlan-id* **port** *port-id*	Configure static multicast forwarding table, and add ports into multicast group;

3.2.8 (Optional) configuring multicast multi-VLAN VoD

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip igmp snooping multicast-vlan** *vlan-id* **protocol-vlanlist** { **add** | **remove** }*vlan-list*	Configure multicast multi-VLAN Voice on Demand (VoD).

3.2.9 (Optional) configuring multicast VLAN CoS priority

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip igmp cos** { **up-link** | **down-link** } *cos-value*	Configure multicast VLAN CoS priority.

3.2.10 Checking configuration

Checking OLT configuration

No.	Items	Description
1	Raisecom#**show ip igmp snooping** [**vlan** *vlan-id*]	Check whether configuration of IGMP Snooping is correct;
2	Raisecom#**show ip igmp snooping mrouter** [**vlan** *vlan-id*]	Check whether multicast routing information of IGMP Snooping is correct;
3	Raisecom#**show mac-address-table multicast** [**vlan** *vlan-id*] [**count**]	Check whether configuration of multicast over the link layer is correct;

Checking ONU configuration

No.	Items	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **ip igmp**	Check whether configuration of IGMP Snooping is correct;

3.3 Configuring IGMP Proxy

3.3.1 Preparing for configuration

Networking situation

In a big size network that uses multicast routing protocol, there are several hosts or client sub-net for receiving multicast information. To set IGMP Proxy on the device that connecting host and multicast router, block IGMP message between host and router to reduce network flow.

Configure IGMP Proxy can reduce configuration nand management for client sub-net from multicast router and meanwhile realize multicast connection among client sub-net.

IGMP Proxy is usually used to combine with IGMP Snooping, MVR or dynamic controllable multicast function.

Precondition

Create VLAN and add related port into VLAN before configuring IGMP Proxy.

3.3.2 Default configuration of IGMP Proxy

Function	Default value
IGMP Proxy status	disable
IGMP version	v2
Interval of IGMP query time	125s
The maximum responding time of sending Query message	10s
Query interval of the last member	1s
Query times of the last member	2
IGMP user and source IP address of IGMP Proxy sending message	0.0.0.0
VLAN ID of frame which is sent to IGMP server	Untagged
Neglect router-alert option carried by IGMP message	enable

3.3.3 Configuring IGMP Proxy

Configuring OLT IGMP Proxy

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface olt** *slot-id/olt-id*	Enter OLT configuration mode;
3	Raisecom(fttx-olt*:*)#**ip igmp proxy** { **enable** | **disable** }	Enable/Disable IGMP Proxy;
3	Raisecom(fttx-olt*:*)#**ip igmp proxy query-interval** *seconds*	(Optional) Configure time interval of IGMP query;
4	Raisecom(fttx-olt*:*)#**ip igmp proxy query-response-interval** *seconds*	(Optional) Configure responding interval of IGMP query;
5	Raisecom(fttx-olt*:*)#**ip igmp proxy last-member-query-interval** *seconds*	(Optional) Configure query interval of the last member in multicast group;
6	Raisecom(fttx-olt*:*)#**ip igmp proxy last-member-query-count** *count*	(Optional) Configure query times of the last member in multicast group;

Step	Configuration	Description
7	Raisecom(fttx-olt*:*)#**ip igmp proxy source-ip-address** *ip-address*	(Optional) Configure source IP address of source IP address sent by IGMP user;
8	Raisecom(fttx-olt*:*)#**ip igmp proxy vlan** { *vlan-id* | **untagged** }	(Optional) Configure VLAN Tag of frame sent to IGMP server;
9	Raisecom(fttx-olt*:*)#**ip igmp proxy version** { **v1** | **v2** | **v3** }	(Optional) Configure IGMP version;
10	Raisecom(fttx-olt*:*)#**ip igmp proxy router-alert-ignore** { **enable** | **disable** }	(Optional) neglect router-alert option carried by IGMP message;

Note

It is allowed to configure IGMP Proxy when IGMP Proxy has not been enabled: set source IP, query time interval, max. responding time for transmitting Query message, transmitting Query interval of the last member. Once startup IGMP Proxy, the configuration becomes effective.

Configuring ONU IGMP Proxy

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system.
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode.
3	Raisecom(fttx-onu*/*:*)#**ip igmp proxy vlan** *vlan-id*	Configure the VLAN of the IGMP Proxy.
4	Raisecom(fttx-onu*/*:*)# **ip igmp proxy ip-address** *ip-address*	Configure the IP address of the IGMP Proxy.

3.3.4 Checking configuration

No.	Items	Description
1	Raisecom#**show interface olt** *slot-id/olt-id* **ip igmp proxy**	Show configuration information of IGMP Proxy;

3.4 Configuring MVR

3.4.1 Preparing for configuration

Networking situation

When several hosts need to receive data from multi-sources, and the different hosts, multicast router and hosts are belonged to different VLAN, user can configure MVR on ISCOM5508 that connect host and multicast router. Then realize users from different VLAN receive identical multicast message and reduce bandwidth.

Precondition

Finish below tasks before configuring MVR:

- Create VLAN and add physical port into VLAN.
- Disable global IGMP Snooping in device.

3.4.2 Default configuration of MVR

Function	Default value
Global MVR	disable
Port MVR	disable
Multicast address	N/A
Aging time of MVR multicast entity	600s
Multicast VLAN	N/A
Multicast group addresses of multicast VLAN	N/A
MVR mode	Compatible (compatibility mode)
MVR port mode	N/A
Immediate-leave	disable

3.4.3 Configuring basic function of MVR

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode;
2	`Raisecom(config)#mvr { enable | disable }`	Enable/disable global MVR;
3	`Raisecom(config)#mvr timeout` *period*	(Optional) Configure aging time of MVR multicast entity;
4	`Raisecom(config)#mvr vlan` *vlan-id*	Configure MVR multicast VLAN;

Step	Configuration	Description
5	Raisecom(config)#**mvr vlan** *vlan-id* [**group** *ip-address* | **any** [*count*]]	Configure the multicast source IP address set related to the MVR multicast VLAN. **Note** • The *any* parameter is used to specify any address in the IP address set of a VLAN. • The *count* parameter is used to specify a continuous range of multicast addresses.
6	Raisecom(config)#**mvr mode** { **dynamic** | **compatible** }	Configure MVR mode;

3.4.4 Configuring port function of MVR

Caution

- Configure uplink port as source port for receiving multicast data, user cannot direct connect with source port, all source ports must in multicast VLAN. Configure the port that direct connects to user as receiving port, it should not belong to multicast VLAN.
- When using **mvr immediate** command to configure auto-leave, it can be used on the switch port that direct connects to user. Including PON port and GE ort. ISCOM5508 physical port and switch port relationship please refer to the port relationship table.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode of physical layer;
3	Raisecom(config-port)#**mvr**	Enable port MVR;
4	Raisecom(config-port)#**mvr type** { **source** | **receiver** }	Configure type of port MVR;
5	Raisecom(config-port)#**mvr immediate**	Configure immediate-leave of port;

3.4.5 Checking configuration

No.	Items	Description
1	Raisecom#**show mvr**	Check whether configuration of MVR is correct;
2	Raisecom#**show mvr members** [*ip-address*]	Check whether configuration of MVR multicast group is correct;

No.	Items	Description
3	Raisecom#**show mvr vlan group** [**vlan** *vlan-id*]	Check whether configuration of IP address in VLAN and MVR multicast VLAN is correct;
4	Raisecom#**show mvr port** [*port-id*]	Check MVR configuration information based on port is correct;
5	Raisecom#**show mvr port** [*port-id*] **members**	Show MVR multicast group member information based on port;

3.5 Configuring MVR Proxy

3.5.1 Preparing for configuration

Networking situation

In a big size network using multicast protocol, there are maybe several hosts and multiple user sub-net. To reduce multicast router configuration on user hosts or sub-net, and meanwhile to realize multicast connection of client sub-net. Configure MVR Proxy on ISCOM5508 that connects to sub-net, user hosts and multicast router. To create multicast forwarding table by block IGMP message between users and routers.

Precondition

Finish below tasks before configuring MVR Proxy:

- Configure basic function for MVR.
- Configure multicast VLAN and group address pool.
- Configure router ports and member ports and add them into related VLAN.

3.5.2 Default configuration of MVR Proxy

Function	Default value
global MVR Proxy	disable
compression function of IGMP message	disable
IGMP query	disable
Source address of message sent by MVR Proxy	IP 0
Interval of IGMP query time	60s
The maximum responding time of IGMP query message	10s
Time interval of IGMP query message by the last member	1s

3.5.3 Configuring MVR Proxy

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**mvr proxy**	Enable MVR Proxy. After enable MVR Proxy, IGMP report compression function and IGMP query function will be enabled at the same time.
3	Raisecom(config)#**mvr proxy suppression**	(Optional) Enable IGMP report compression function;
4	Raisecom(config)#**ip igmp querier enable**	(Optional) Enable IGMP query Function;
5	Raisecom(config)#**mvr proxy source-ip** *ip-address*	(Optional) Configure MVR Proxy transmitting message source IP.
6	Raisecom(config)#**ip igmp querier query-interval** *period*	(Optional) Configure IGMP query time interval.
7	Raisecom(config)#**mvr proxy query-max-response-time** *period*	(Optional) Configure IGMP query message max. response time.
8	Raisecom(config)#**mvr proxy last-member-query** *period*	(Optional) Configure IGMP query message timer interval transmitted from the last member.

Note

Other optional configuration may be ineffective if user hasn't enable MVR Proxy function in the device.

3.5.4 Checking configuration

No.	Items	Description
1	Raisecom#**show mvr proxy**	Check configuration information of MVR Proxy is correct;
2	Raisecom#**show mvr port** [*port-id*] [**statistics**]	Show MVR statistics information based on port;
3	Raisecom#**show ip igmp querier vlan**	Show VLAN information of user port;

3.6 Configuring IGMP filter and the maximum number of multicast groups

3.6.1 Preparing for configuration

Networking situation

ISCOM5508 is in support of IGMP filter based on member ports or VLAN and multicast group number limitation.

Raisecom ONU is in support of multicast group number limit based on member ports.

Precondition

Configure global IGMP Snooping function enable or MVR basic function before configuring IGMP filter.

3.6.2 Default configuration of IGMP filter and the maximum number of multicast groups

Function	Default value
Enable IGMP filtering globally	enable
IGMP port application	N/A
The maximum number of IGMP groups	N/A
Limitation of the maximum number of IGMP groups	disable
IGMP Profile	N/A
IGMP Profile	disable

3.6.3 Configuring IGMP filter template

Configure IGMP filter template and then binding the template with port or VLAN before configuring IGMP filter.

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode;
2	`Raisecom(config)#ip igmp profile` *profile-number*	Create IGMP filtering template and enter configuration mode of IGMP filtering template;
3	`Raisecom(config-igmp-profile)#permit | deny`	(Optional) Configure treatment mode of message by IGMP filtering template;
4	`Raisecom(config-igmp-profile)#range` *start-ip-address* [*end-ip-address*]	Configure range of multicast IP address of the IGMP filtering template;

3.6.4 Configuring IGMP filter based on ports and the maximum number of multicast groups

Configuring OLT based on IGMP filter based on ports and the maximum number of multicast groups of port

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip igmp filter**	Enable IGMP filtering globally;
3	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
4	Raisecom(config-port)#**ip igmp filter** *profile-number*	Configure IGMP filtering based on member port.A filtering template can be applied on many member ports, each member port can only be applied on a filtering template;
5	Raisecom(config-port)#**ip igmp max-groups** *group-number*	Configure member port and the maximum number of multicast groups;
6	Raisecom(config-port)#**ip igmp max-groups action** { **deny** | **replace** }	Specify the operations when the number of multicast groups specified by member port exceeds the maximum number;

Configuring ONU based on the maximum number of multicast groups of port

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter ONU UNI Ethernet port configuration mode;
4	Raisecom(fttx-onu-uni*/*/*:*)#**multicast max-group-num** *group-number*	Configure the maximum number of multicast groups of ONU Ethernet ports;
5	Raisecom(fttx-onu-uni*/*/*:*)#**multicast vlan tag-strip** { **enable** | **disable** }	(Optional) Configure UNI to strip VLAN Tag of multicast service message;

3.6.5 Configuring IGMP filter based on VLAN and the maximum number of multicast groups

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip igmp filter**	Enable IGMP filtering globally;
3	Raisecom(config)#**ip igmp filter** *profile-number* **vlan** *vlan-id*	Configure IGMP filtering based on VLAN;
4	Raisecom(config)#**ip igmp max-group** *group-number* **vlan** *vlan-id*	Configure the maximum number of multicast groups in VLAN;
5	Raisecom(config)#**igmp filter max-group action** { **deny** | **replace** } **vlan** *vlan-list*	Specify the action if the number of multicast groups exceeds the max.

3.6.6 Checking configuration

No.	Items	Description
1	Raisecom#**show ip igmp filter**	Show global configuration information of IGMP filtering;
2	Raisecom#**show ip igmp profile** [*profile-number*]	Check whether configuration of IGMP filtering is correct;
3	Raisecom#**show ip igmp filter port** [*port-id*]	Check whether configuration of IGMP filtering on specific port is correct;
4	Raisecom#**show igmp filter vlan** [*vlan-id*]	Check whether configuration of IGMP filtering on specific VLAN is correct;

3.7 Configuring dynamic and controllable multicast

3.7.1 Preparing for configuration

Networking situation

To realize multicast service operation in IP network, user must manage multicast source and receivers to control direction and range of multicast data. Otherwise, to operate multicast service will not only affect current IP network but also cannot get respected service quality fro receivers.

Precondition

User must configure dynamic controllable multicast function on both OLT and ONU in order to realize dynamic controllable multicast function in EPON system.

3.7.2 Default configuration of dynamic and controllable multicast

Default configuration of global parameters of dynamic and controllable multicast

Function	Default value
dynamic and controllable multicast function	disable
Unknown user right	disable
Access right of unauthorized channels for legal users	disable
Reset cycle of preview right	daily
Threshold of preview time record	1 minute
CDR function	disable
Synchronization time interval of CDR information	60 minutes
Time threshold of CDR record	1 minute
The maximum time of multicast service on port ONU if there isn't a IGMP control message	5 minutes

Default configuration of preview rules of dynamic and controllable multicast

ISCOM5508 supports at most 64 pieces of preview rules. By default the system provides 8 pieces of preview template at the initial, these templates can be modified but cannot be deleted.

Here is the 8 pieces of default preview rules provided by ISCOM5508.

No.	The maximum preview time each time (minute)	Interval of preview time (minute)	The maximum times of preview	The maximum of total preview time (minute)	The times that rules were quoted
1	2	2	500	1000	0
2	4	2	500	2000	0
3	6	4	1000	6000	0
4	8	4	1000	8000	0
5	10	8	1500	15000	0
6	12	8	1500	18000	0
7	14	16	2000	28000	0
8	16	16	2000	32000	0

3.7.3 Configuring global parameters of dynamic and controllable multicast

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**ctrl-multicast** { **enable** | **disable** }	Enable/disable dynamic and controllable multicast Function;
3	Raisecom(fttx)#**ctrl-multicast right unregistered-user** { **permit** | **deny** }	(Optional) Configure right of unknown user;
4	Raisecom(fttx)#**ctrl-multicast right unauthorized-channel** { **permit** | **deny** }	(Optional) Configure access right of unauthorized channels for legal users;
5	Raisecom(fttx)#**ctrl-multicast preview resetting-period** { **daily** | **weekly** | **monthly** | **yearly** }	(Optional) Configure reset cycle of preview right;
6	Raisecom(fttx)#**ctrl-multicast preview time-recorded-thresold** *minute*	(Optional) Configure time record threshold of preview;
7	Raisecom(fttx)#**ctrl-multicast max-non-igmp-report-duration** *minute*	(Optional) Configure the maximum effective time of ONU port multicast service if there isn't a IGMP control message;

3.7.4 Configuring user management

ISCOM5508 provides user management function taking ONU UNI port as identifier.

Configure device for dynamic controllable multicast user management as below:

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**ctrl-multicast creat user** *user-id* **onu** *slot-id/olt-id/onu-id* **uni** *uni-id* **[name** *name* **]**	Create dynamic and controllable multicast users.A UNI can only create a user;
3	Raisecom(fttx)#**ctrl-multicast user** *user-id* { **enable** | **disable** }	Configure user status;
4	Raisecom(fttx)#**ctrl-multicast user name** *name* **user-id** *user-id*	(Optional) Configure multicast user name;
5	Raisecom(fttx)#**ctrl-multicast user** *user-id* **max-online-channel** *channel-number*	(Optional) Configure the maximum number of online channels;
6	Raisecom(fttx)#**ctrl-multicast user ip-address** *ip-address* **user-id** *user-id*	(Optional) Configure IP addresses of users.  It is only supported by IGMP v3;

3.7.5 Configuring management of channel multicasting

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**ctrl-multicast creat channel** *ip-address* [**vlan-id** *vlan-id*] [**name** *name*]	Create multicast channels;
3	Raisecom(fttx)#**ctrl-multicast channel** *ip-address* **name** *name*	(Optional) Configure name of multicast channel;
4	Raisecom(fttx)#**ctrl-multicast channel** *ip-address* **vlan** *vlan-id*	(Optional) Configure VLAN ID of multicast channel;

3.7.6 Configuring management of preview rule

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**ctrl-multicast creat preview-rule** [*rule-id*] [**time** *minute*] [**interval** *interval*] [**total-count** *total-count*] [**total-time** *minute*]	Configure preview rules of dynamic and controllable multicast;
3	Raisecom(fttx)#**ctrl-multicast preview-rule** *rule-id* **interval** *interval*	(Optional) Configure preview interval of dynamic and controllable multicast;
4	Raisecom(fttx)#**ctrl-multicast preview-rule** *rule-id* **total-count** *total-count*	(Optional) Configure the maximum times of previewing dynamic and controllable multicast;
5	Raisecom(fttx)#**ctrl-multicast preview-rule** *rule-id* **time** *minute*	(Optional) Configure the maximum time of dynamic and controllable multicast for one time;
6	Raisecom(fttx)#**ctrl-multicast preview-rule** *rule-id* **total-time** *minute*	(Optional) Configure the maximum total time of previewing dynamic and controllable multicast;

3.7.7 Configuring management of user channel authority

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**ctrl-multicast creat right user** *user-id* **channel** *ip-address* [**preview-rule** *rule-id*]	Configure right table of user channel;

Step	Configuration	Description
3	Raisecom(fttx)#**ctrl-multicast right user** *user-id* **channel** *ip-address* { **permit** | **deny** | **preview** }	(Optional) Configure user channel right;
4	Raisecom(fttx)#**ctrl-multicast right user** *user-id* **channel** *ip-address* **preview-rule** *rule-id*	(Optional) Configure preview rules of right table;
5	Raisecom(fttx)#**ctrl-multicast right user** *user-id* **channel** *ip-address* **preview-stats-resetting**	(Optional) Configure resetting of preview counter;

3.7.8 Configuring management of CDR record

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**ctrl-multicast cdr**{ **enable** | **disable** }	Enable/Disable CDR record management function;
3	Raisecom(fttx)#**ctrl-multicast cdr synch-period** *second*	(Optional) Configure interval of CDR information sync to management system;
4	Raisecom(fttx)#**ctrl-multicast cdr time-recorded-threshold**	(Optional) Configure time threshold of CDR record;

3.7.9 Checking configuration

No.	Items	Description
1	Raisecom#**show ctrl-multicast**	Show global configuration information of dynamic and controllable multicast;
2	Raisecom#**show ctrl-multicast user onu** *slot-id/olt-id/onu-id*	Show multicast user information on a ONU;
3	Raisecom#**show ctrl-multicast user** [*user-list*]	Show user configuration information;
4	Raisecom#**show ctrl-multicast online-unregistered-user**	Show online and unregistered user information;
5	Raisecom#**show ctrl-multicast channel** [*ip-address*]	Show channel information;
6	Raisecom#**show ctrl-multicast channel** [*ip-address*] **online-user**	Show legal user information of channel;
7	Raisecom#**show ctrl-multicast online-unauthorized-channel**	Show online user information of unauthorized channel;
8	Raisecom#**show ctrl-multicast channel vlan-id** *vlan-id*	Show multicast channel information in VLAN;

No.	Items	Description
9	Raisecom#**show ctrl-multicast preview-rule** [*rule-list*]	Show configuration information of preview information;
10	Raisecom#**show ctrl-multicast right** { **preview** *rule-list* | **preview-rule** *rule-list* | **permit** | **deny** | **user** *user-list* | **channel** *ip-address* }	Show user channel right information;
11	Raisecom#**show ctrl-multicast cdr** { **history** | **current** | **all** }	Show CDR record information;

3.8 Maintenance

Command	Description
Raisecom(fttx)#**ctrl-multicast cdr clear history-record**	Clear CDR historical record information;

4 Configuring VoIP service

The chapter introduces VoIP service configuration and procedure of ISCOM5508, and provides related configuration applications.

- Quick configuration of VoIP service
- Configuring VoIP protocol
- Configuring POTS port
- Configuring SIP
- Configuring H.248
- Configuring second dial-up service
- Configuring fax service
- Configuring call emulation test
- Maintenance

4.1 Quick configuration of VoIP service

Here we provide a typical configuration instance to help users to enable VoIP service quickly.

4.1.1 Examples for configuring SIP voice service (Proxy calling)

Networking requirements

Configure SIP voice service (Proxy calling) on OLT as below figure:

- Related data service configuration refers to 2.2 Quick configuration of EPON service;
- VLAN of voice service is 3999;
- Configure two telephone numbers: telephone number of POTS1 is 1001, telephone number of POTS2 is 1002;

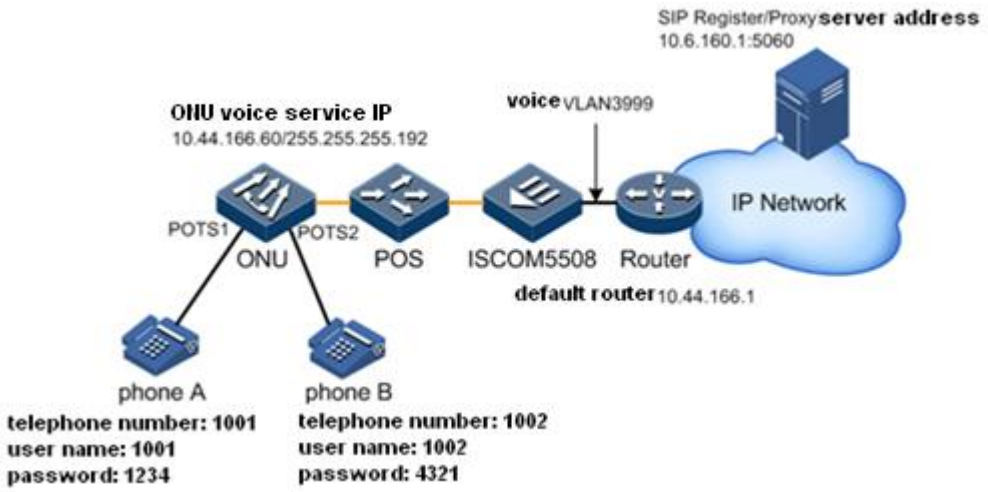

Figure 4-1 Instance of SIP voice service (Proxy calling)

Configuration steps

Step 1 Configure VoIP signaling protocol.

```
Raisecom#fttx
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#voice
Raisecom(fttx-onu-voice-1/1:1)#voip-protocol sip
Raisecom(fttx-onu-voice-1/1:1)#exit
Raisecom(fttx-onu1/1:1)#write
Raisecom(fttx-onu1/1:1)#reboot now
```

Caution

OLT needs time to send configuration to ONU if it uses command **write** to save configuration. So we reboot ONU by command **Reboot Now** in ten seconds, otherwise it fails to send configuration.

Step 2 Configure voice VLAN.

```
Raisecom#fttx
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#voice
Raisecom(fttx-onu-voice-1/1:1)#vlan mode tagged
Raisecom(fttx-onu-voice-1/1:1)#vlan 3999 cos 6
```

Step 3 Configure IP of voice service.

```
Raisecom(fttx-onu-voice-1/1:1)#ip address 10.44.166.60 255.255.255.192
```

```
Raisecom(fttx-onu-voice-1/1:1)#ip route default 10.44.166.1
```

Step 4 Configure POTS telephone number.

```
Raisecom(fttx-onu-voice-1/1:1)#pots phone-number 1001 1
Raisecom(fttx-onu-voice-1/1:1)#pots phone-number 1002 2
```

Step 5 Configure proxy and register server (two servers exist in the same IP address).

```
Raisecom(fttx-onu-voice-1/1:1)#sip primary proxy-server ip 10.6.160.1
Raisecom(fttx-onu-voice-1/1:1)#sip primary register-server ip 10.6.160.1
```

Step 6 (optional, only if we need to certify SIP server) configure authentication information of users.

```
Raisecom(fttx-onu-voice-1/1:1)#sip pots authentication 1001 password 1234
1
Raisecom(fttx-onu-voice-1/1:1)#sip pots authentication 1002 password 4321
2
```

Checking results

Check whether the connection between ONU voice node and soft switch exists. Configure in-band management IP address and default gateway of OLT.

```
Raisecom#config
Raisecom(config)#ip default-gateway 10.44.166.1
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address 10.44.166.61 255.255.255.192 3999
Raisecom(config-ip)#end
Raisecom#ping 10.6.160.1
Type CTRL+C to abort.
Sending 5, 72-byte ICMP Echos to 10.6.160.1 , timeout is 1 seconds:
!!!!!
Success rate is 100 percent(5/5)
round-trip (ms)  min/avg/max = 0/3/16
```

Show POTS telephone number.

```
Raisecom#fttx
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#voice
```

```
Raisecom(fttx-onu-voice-1/1:1)#show interface onu 1/1/1 voice pots
Pots ID    Admin Status   Port Status     Service Status  CodecType
-------------------------------------------------------------------
1/1/1/1    enable       register failed  normal        G.711A
1/1/1/2    enable       register failed  normal        G.711A
```

Show POTS register information.

```
Raisecom(fttx-onu-voice-1/1:1)#show interface onu 1/1/1 voice sip pots 1
service
Port ID: 1/1/1:1
   Register state     : registerSucceed
   Call state        : hookon
   Caller ID state    : enable
   Call wait state    : disable
   Three way conference: disable

Raisecom(fttx-onu-voice-1/1:1)#show interface onu 1/1/1 voice sip pots 2
service
Port ID: 1/1/1:2
   Register state     : registerSucceed
   Call state        : hookon
   Caller ID state    : enable
   Call wait state    : disable
   Three way conference: disable
```

Show IP information of voice server.

```
Raisecom(fttx-onu-voice-1/1:1)#show interface onu 1/1/1 voice ip
ONU ID: 1/1/1
   IP mode           : static
   IP address        : 10.44.166.60
   Subnet mask       : 255.255.255.192
   Default route     : 10.44.166.1
   DNS server IP address: 0.0.0.0
   Vlan mode         : tagged
   VID              : 3999
   Cos              : 6
   Outter VID        : 0
   MAC address       : 000e.5e07.7ac0
   IP QoS trust policy  : None
   QoS default-dscp    : 0
   QoS default-tos     : 0
   QoS default-priority : 0
```

Show addresses of SIP Proxy/Register server.

```
Raisecom(fttx-onu-voice-1/1:1)#show interface onu 1/1/1 voice sip primary
proxy-server
ONU ID   Proxy IP        Udp Port   Tcp Port   Transport
------------------------------------------------------------
1/1/1    10.6.160.1      5060       5060       udp
Raisecom(fttx-onu-voice-1/1:1)#show interface onu 1/1/1 voice sip primary
register-server
ONU ID   Server IP       Udp Port   Tcp Port   Transport   Fresh Period(s)
------------------------------------------------------------------------
1/1/1    10.6.160.1      5060       5060       udp         3600
```

Show authentication information of users.

```
Raisecom(fttx-onu-voice-1/1:1)#show interface onu 1/1/1 voice sip pots
authentication
Pots ID     Authentication Name      Authentication Password
------------------------------------------------------------
1/1/1:1     1001                     1234
1/1/1:2     1002                     4321
1/1/1:3     N/A                      *
1/1/1:4     N/A                      *
1/1/1:5     N/A                      *
1/1/1:6     N/A                      *
1/1/1:7     N/A                      *
1/1/1:8     N/A                      *
1/1/1:9     N/A                      *
1/1/1:10    N/A                      *
1/1/1:11    N/A                      *
1/1/1:12    N/A                      *
1/1/1:13    N/A                      *
1/1/1:14    N/A                      *
1/1/1:15    N/A                      *
1/1/1:16    N/A                      *
```

They can communicate with each other on ONU if SIP register is successfully:

- A caller off-hook and hears the dial tone;
- A caller dials the number of called party, ringing, and the caller hears ring back tone;
- The caller communicates with the called normally;
- The caller hears busy tone if the called on-hook;

4.1.2 Examples for configuring SIP voice service (Direct calling)

Networking requirements

Configure SIP voice service (Direct calling) on OLT as below figure:

- Headquarter, R&D 1, R&D 2, production department and outside nodes can communicate with each other normally by IP, and there is no VLAN in network;

- An extension number of headquarter is 3xxx, IP of IAD SIP voice device is 192.168.20.100;
- An extension number of R&D 1 is 86xx, IP of ONU A voice device is 192.168.10.100;
- An extension number of R&D 2 is 85xx, IP of ONU B voice device is 192.168.10.101;
- An extension number of production department is 5xxx or 6xxx, IP of IAD SIP voice device is 192.168.30.100;
- IP of outside node is 192.168.40.100, the first number is 0, and the last number is #;
- We take R&D1 as an example, and dial rule configuration of all devices is the same;
- SIP router table:

1 86xx	192.168.10.100
2 85xx	192.168.10.101
3 3xxx	192.168.20.100
4 [5-6]xxx	192.168.30.100
5 0x.#	192.168.40.100

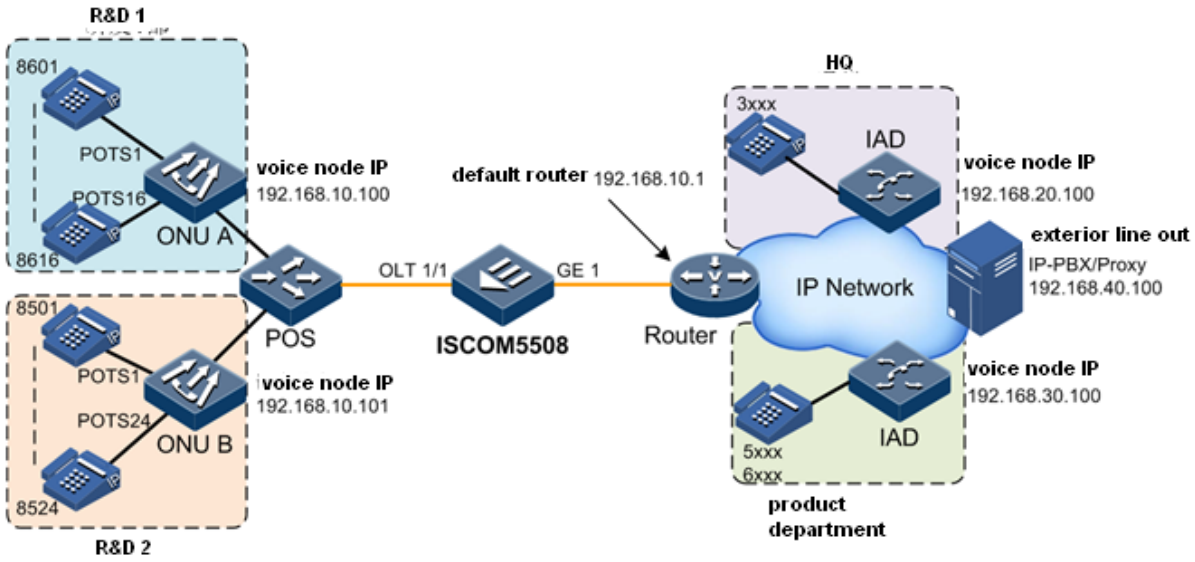

Figure 4-2 SIP voice service (Direct calling)

Configuration steps

Step 1 Configure VoIP signaling protocol.

```
Raisecom#fttx
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#voice
```

```
Raisecom(fttx-onu-voice-1/1:1)#voip-protocol sip
Raisecom(fttx-onu-voice-1/1:1)#exit
Raisecom(fttx-onu1/1:1)#write
Raisecom(fttx-onu1/1:1)#reboot now
```

Caution

OLT needs time to send configuration to ONU if it uses command **write** to save configuration. So we reboot ONU by command **Reboot Now** in ten seconds, otherwise it fails to send configuration.

Step 2 Configure IP of voice service.

```
Raisecom#fttx
Raisecom#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#voice
Raisecom(fttx-onu-voice-1/1:1)#ip address 192.168.10.100
Raisecom(fttx-onu-voice-1/1:1)#ip route default 192.168.10.1
```

Step 3 Configure POTS telephone number.

```
Raisecom(fttx-onu-voice-1/1:1)#pots phone-number 8601 1
Raisecom(fttx-onu-voice-1/1:1)#pots phone-number 8602 2
Raisecom(fttx-onu-voice-1/1:1)#pots phone-number 8603 3
Raisecom(fttx-onu-voice-1/1:1)#pots phone-number 8604 4
Raisecom(fttx-onu-voice-1/1:1)#pots phone-number 8605 5
Raisecom(fttx-onu-voice-1/1:1)#pots phone-number 8606 6
Raisecom(fttx-onu-voice-1/1:1)#pots phone-number 8607 7
Raisecom(fttx-onu-voice-1/1:1)#pots phone-number 8608 8
Raisecom(fttx-onu-voice-1/1:1)#pots phone-number 8609 9
Raisecom(fttx-onu-voice-1/1:1)#pots phone-number 8610 10
Raisecom(fttx-onu-voice-1/1:1)#pots phone-number 8611 11
Raisecom(fttx-onu-voice-1/1:1)#pots phone-number 8612 12
Raisecom(fttx-onu-voice-1/1:1)#pots phone-number 8613 13
Raisecom(fttx-onu-voice-1/1:1)#pots phone-number 8614 14
Raisecom(fttx-onu-voice-1/1:1)#pots phone-number 8615 15
Raisecom(fttx-onu-voice-1/1:1)#pots phone-number 8616 16
```

Step 4 Configure SIP No. mapped rule.

```
Raisecom(fttx-onu-voice-1/1:1)#sip dial-map-rule 1 86xx 192.168.10.100
Raisecom(fttx-onu-voice-1/1:1)#sip dial-map-rule 2 85xx 192.168.10.101
Raisecom(fttx-onu-voice-1/1:1)#sip dial-map-rule 3 3xxx 192.168.20.100
Raisecom(fttx-onu-voice-1/1:1)#sip dial-map-rule 4 [5-6]xxx
192.168.30.100
Raisecom(fttx-onu-voice-1/1:1)#sip dial-map-rule 5 0x.# 192.168.40.100
```

Checking results

Show dial rule configuration.

```
Raisecom#fttx
Raisecom#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#voice
Raisecom(fttx-onu-voice-1/1:1)#show int onu 1/1/1 voice sip dial-map-rule
ONU ID: 1/1/1
   Rule ID  Phone Number               SIP URI
   ---------------------------------------------
   1        86xx                      192.168.10.100
   2        85xx                      192.168.10.101
   3        3xxx                      192.168.20.100
   4        [5-6]xxx                   192.168.30.100
   5        0x.#                      192.168.40.100
```

Show current configuration files of ONU.

```
Raisecom(fttx-onu-voice-1/1:1)#show running-config
!Voice current configuration:
sip dial-map-rule 1 86xx 192.168.10.100
sip dial-map-rule 2 85xx 192.168.10.101
sip dial-map-rule 3 3xxx 192.168.20.100
sip dial-map-rule 4 [5-6]xxx 192.168.30.100
sip dial-map-rule 5 0x.# 192.168.40.100
pots phone-number 8601 1
pots phone-number 8602 2
pots phone-number 8603 3
pots phone-number 8604 4
pots phone-number 8605 5
pots phone-number 8606 6
pots phone-number 8607 7
pots phone-number 8608 8
pots phone-number 8609 9
pots phone-number 8610 10
pots phone-number 8611 11
pots phone-number 8612 12
pots phone-number 8613 13
pots phone-number 8614 14
pots phone-number 8615 15
pots phone-number 8616 16
ip address 192.168.10.100 255.255.255.0
ip route default 192.168.10.1
!
```

Check whether the connection between voice node and gateway exists. Configure in-band management IP address and default gateway of OLT firstly.

```
Raisecom(fttx-onu-voice-1/1:1)#end
Raisecom#config
Raisecom(config)#interface ip 0
Raisecom(config)#ip default-gateway 192.168.10.1
Raisecom(config-ip)#ip address 192.168.10.253 255.255.255.0 1
Raisecom(config-ip)#end
Raisecom#ping 192.168.10.1
Sending 5, 72-byte ICMP Echos to 192.168.10.1 , timeout is 1 seconds:
!!!!!
Success rate is 100 percent(5/5)
round-trip (ms)  min/avg/max = 0/24/110
```

We can dial a number by a telephone of R&D 1 to test if configuration of all devices in network has been configured successfully.

- A caller off-hook and hears the dial tone;
- A caller dials the four numbers which begin with 86, 85, 3, 5, 6, or long numbers (more than two bit) which begin with 0, ringing, and the caller hears ring back tone;
- The caller can communicate with the called normally;
- The caller hears busy tone if the called on-hook;

4.1.3 Examples for configuring H.248 voice service

Networking requirements

Configure H.248 voice service and two voice communications in ONU can be realized as below figure. The instance helps to explain quick configuration of voice service, users can refer to 4.6 Configure H.248 if they need to see more function configurations.

Please configure the values as the set value which is provided in actual situation.

Items	Set value
IP address and mask code of ONU voice node	IP is 10.44.166.60 Mask is 255.255.255.192
Router gateway of voice node	10.44.166.1
Voice VLAN and priority of service	Voice VLAN is 3999, priority of service is 6;
MG registration way	domain-name
MG name(registration of ip and mac doesn't need registration name)	raisecom
Transmission port number of MG	2944
Signaling coding method of H.248 protocol	text
IP address of MGC server	10.6.160.1
Generation way of POTS TID of MG	line

Items	Set value
Name of POTS TID of MG	TID name of POTS1 is EPON001; TID name of POTS2 is EPON002;
RTP TID prefix and length of digital of MG	Prefix is RTP, length of digital is 5;
Telephone number	Users need to configure POTS TID, not telephone number. The telephone number is generated from MGC of official department;

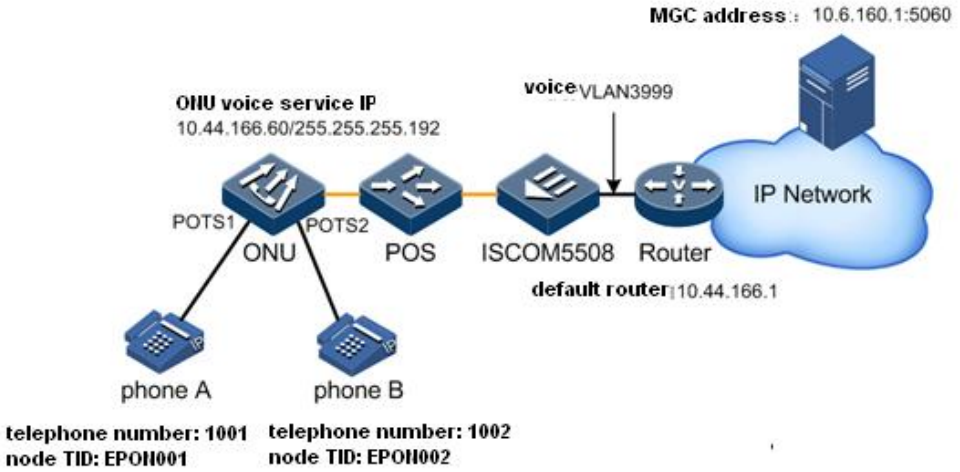

Figure 4-3 H.248 voice service

Configuration steps

Step 1 Choose type of VoIP signaling protocol.

```
Raisecom#fttx
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#voice
Raisecom(fttx-onu-voice-1/1:1)#voip-protocol h248
Raisecom(fttx-onu-voice-1/1:1)#exit
Raisecom(fttx-onu1/1:1)#write
Raisecom(fttx-onu1/1:1)#reboot now
```

Caution

OLT needs time to send configuration to ONU if it uses command **write** to save configuration. So we reboot ONU by command **Reboot Now** in ten seconds, otherwise it fails to send configuration.

Step 2 Configure voice VLAN.

```
Raisecom(fttx-onu-voice-1/1:1)#vlan mode tagged
Raisecom(fttx-onu-voice-1/1:1)#vlan 3999 cos 6
```

Step 3 Configure IP of ONU voice service.

```
Raisecom(fttx-onu-voice-1/1:1)#ip address 10.44.166.60 255.255.255.192
Raisecom(fttx-onu-voice-1/1:1)#ip route default 10.44.166.1
```

Step 4 Configure MG information.

```
Raisecom(fttx-onu-voice-1/1:1)#h248 mg register-mode domain-name
Raisecom(fttx-onu-voice-1/1:1)#h248 mg name raisecom
Raisecom(fttx-onu-voice-1/1:1)#h248 mg encode text
Raisecom(fttx-onu-voice-1/1:1)#h248 mg transport port 2944
```

Step 5 Configure port TID and RTP TID of POTS.

```
Raisecom(fttx-onu-voice-1/1:1)#h248 mg tid mode line
Raisecom(fttx-onu-voice-1/1:1)#h248 pots tid name EPON001 1
Raisecom(fttx-onu-voice-1/1:1)#h248 pots tid name EPON002 2
Raisecom(fttx-onu-voice-1/1:1)#h248 mg tid rtp prefix RTP length 5
```

Step 6 Configure MGC server.

```
Raisecom(fttx-onu-voice-1/1:1)#h248 primary mgc ip 10.6.160.1 port 2944
Raisecom(fttx-onu-voice-1/1:1)#no h248 primary mgc authentication
```

Step 7 Save configuration.

```
Raisecom(fttx-onu-voice-1/1:1)#exit
Raisecom(fttx-onu1/1:1)#write
Raisecom(fttx-onu1/1:1)#end
```

Checking results

Check whether the connection between ONU voice node and MGC exists. Configure in-band management IP address and default gateway of OLT firstly.

```
Raisecom#config
Raisecom(config)#ip default-gateway 10.44.166.1
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address 10.44.166.61 255.255.255.192 3999
Raisecom(config-ip)#end
Raisecom#ping 10.6.160.1
Type CTRL+C to abort.
Sending 5, 72-byte ICMP Echos to 10.6.160.1 , timeout is 1 seconds:
!!!!!
Success rate is 100 percent(5/5)
round-trip (ms)  min/avg/max = 0/3/16
```

Show MG registration status.

```
Raisecom#fttx
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#voice
Raisecom(fttx-onu-voice-1/1:1)#show interface onu 1/1/1 voice h248 mg
ONU ID: 1/1/1
   Transport Port      : 2944
   Encode Mode         : text
   Register Mode       : IP
   Name                : raisecom
   Long Timer          : 20s
   Short Timer         : 5s
   Start Timer         : 10s
   State               : registered
   Maximum waiting delay: 180s
```

Show registration status of POTS port.

```
Raisecom(fttx-onu-voice-1/1:1)# show interface onu 1/1/1 voice h248 pots
Pots ID    TID Name                          Status
-----------------------------------------------------------
1/1/1/1    EPON001                           inservice
1/1/1/2    EPON002                           inservice
```

Users can communicate with each other in ONU if H.248 has been registered successfully.

- A caller off-hook and hears the dial tone;
- A caller dials telephone number of the called (search the number from MGC configuration), ringing, and the caller hears ring back tone;
- The caller can communicate with the called normally;
- The caller hears busy tone if the called on-hook;

4.2 Configuring VoIP protocol

4.2.1 Preparing for configuration

Networking situation

Configure VoIP signaling protocol firstly and choose transmission way of voice signaling to realize voice calling procedure.

4.2.2 Default configuration of VoIP protocol

Function	Default value
Type of VoIP protocol	H.248
IP of ONU voice service	IP address is 0.0.0.0, mask code is 0.0.0.0
Default router of ONU voice service	0.0.0.0
DHCP Client of ONU voice service	disable
DHCP Client host name of ONU voice service	raisecomFTTx
VLAN mode of ONU voice service	transparent
VLAN of signalling streaming and media streaming of ONU voice service	0
CoS of signalling streaming and media streaming of ONU voice service	6

4.2.3 Configuring type of VoIP protocol

Step	Configuration	Description
1	`Raisecom#fttx`	Enter global configuration mode of EPON system;
2	`Raisecom(fttx)#interface onu` *`slot-id/olt-id/onu-id`*	Enter ONU configuration mode;
3	`Raisecom(fttx-onu*/*:*)#voice`	Enter configuration mode of ONU voice;
4	`Raisecom(fttx-onu-voice-*/*:*)#voip-protocol { sip | h248 }`	Configure type of VoIP protocol;
5	`Raisecom(fttx-onu-voice-*/*:*)#exit` `Raisecom(fttx-onu*/*:*)#write`	Save configuration;
6	`Raisecom(fttx-onu*/*:*)#reboot`	Reboot device;

Users need to save configuration after choosing different VoIP protocols, and then use reboot or reload operations to reload ONU configuration files. (The later configuration of protocol and service can be done based on selected VoIP protocol).

OLT needs time to send configuration to ONU if it uses command **write** to save configuration. So we reboot ONU by command **Reboot Now** in ten seconds, otherwise it fails to send configuration.

4.2.4 Configuring VoIP network parameter

IP address of ONU voice service can configure static IP address manually, or enable DHCP Client to get dynamic IP address.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter configuration mode of ONU voice;
4	Raisecom(fttx-onu-voice-*/*:*)#**ip address** *ip-address* [*mask*]	Configure IP address and mask of ONU voice service;
5	Raisecom(fttx-onu-voice-*/*:*)#**ip route default** *ip-address*	Configure default router of ONU voice service;
6	Raisecom(fttx-onu-voice-*/*:*)#**ip dhcp client**	(Optional) Start DHCP client service of ONU voice.
7	Raisecom(fttx-onu-voice-*/*:*)#**ip dhcp client hostname** *string*	(Optional) Configure DHCP Client host name of ONU voice.
8	Raisecom(fttx-onu-voice-*/*:*)#**vlan mode** { **transparent** | **tagged** | **stacking** }	Configure VLAN mode of ONU voice.
9	Raisecom(fttx-onu-voice-*/*:*)#**ip dhcp client class-id** *class-id*	(Optional) Configure ClassID of DHCP Client of ONU voice.
10	Raisecom(fttx-onu-voice-*/*:*)#**ip dhcp client client-id** *client-id*	(Optional) Configure ClientID of DHCP Client of ONU voice.
11	Raisecom(fttx-onu-voice-*/*:*)#**vlan** *vlan-id* [**cos** *cos-value*]	Configure VLAN ID, CoS priority of ONU voice signaling streaming; users can configure higher priority to ensure voice message can be scheduled firstly;
12	Raisecom(fttx-onu-voice-*/*:*)#**ip qos trust** { **dscp** | **priority** | **tos** | **none** }	Configure QoS trust policy of ONU voice.
13	Raisecom(fttx-onu-voice-*/*:*)#**ip qos default-dscp** *dscp-value*	Configure value of QoS trust DSCP of ONU voice;
14	Raisecom(fttx-onu-voice-*/*:*)#**ip qos default-priority** *priority-value*	Configure value of QoS trust IP priority of ONU voice;

Step	Configuration	Description
15	Raisecom(fttx-onu-voice-*/*:*)#**ip qos default-tos** *tos-value*	Configure value of QoS trust ToS of ONU voice;

4.2.5 Configuring network parameter of media streaming

Usually, when voice signaling and media flows are in the same network property, users only need to configure above parameters, not need to individually configure VLAN and IP address of media streams. In actual network topology, if it's necessary to set VLAN aimed at voice signaling and media, separate configuring media VLAN and IP would be needed.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter configuration mode of ONU voice;
4	Raisecom(fttx-onu-voice-*/*:*)#**media vlan** *vlan-id* [**cos** *cos-value*]	Configure media streaming VLAN ID and CoS priority of ONU voice service; VLAN of media streaming and signaling streaming is inconsistent; configure VLAN firstly, and then configure IP;
5	Raisecom(fttx-onu-voice-*/*:*)#**media ip address** *ip-address* [*mask*]	Configure IP address and mask code of media streaming in ONU voice service;
6	Raisecom(fttx-onu-voice-*/*:*)#**media ip route default** *ip-address*	Configure default router of media streaming in ONU voice service;
7	Raisecom(fttx-onu-voice-*/*:*)#**media ip qos trust** { **dscp** | **priority** | **tos** }	Configure QoS trust way of media streaming in ONU voice service;
8	Raisecom(fttx-onu-voice-*/*:*)#**media ip qos default-dscp** *dscp-value*	Configure value of QoS trust DSCP of media streaming in ONU voice service;
9	Raisecom(fttx-onu-voice-*/*:*)#**media ip qos default-priority** *priority-value*	Configure value of QoS trust IP priority of media streaming in ONU voice service;
10	Raisecom(fttx-onu-voice-*/*:*)#**media ip qos default-tos** *tos-value*	Configure value of QoS trust ToS priority of media streaming in ONU voice service;

4.2.6 Configuring parameters for call process voice

Please configure parameters for call process voice.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system.

Step	Configuration	Description
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode.
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode.
4	Raisecom(fttx-onu-voice-*/*:*)#**call-progress-tone** { **busy** | **congestion** | **dial** | **ringback** | **waiting** } { **high-frequency** | **low-frequency** } *frequency*	Configure the low-frequency and high-frenquency of ONU call process voice.
5	Raisecom(fttx-onu-voice-*/*:*)#**call-progress-tone** { **busy** | **congestion** | **dial** | **ringback** | **waiting** } { **high-frequency** | **low-frequency** } **volume** *volume*	Configure the low-frequency volume gain and high-frequency volume gain of ONU call process voice.
6	Raisecom(fttx-onu-voice-*/*:*)#**call-progress-tone** { **busy** | **congestion** | **dial** | **ringback** | **waiting** } { **first-sigal** | **second-sigal** } **on-time** *value* **off-time** *value*	Configure the starting time and the ending time for the first and second signals of ONU call process voice.

Note

After modifying parameters of call process voice, you need to save configurations and reset the ONU. Otherwise, new configuration will not take effect.

4.2.7 Checking configuration

Step	Configuration	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **voice voip-protocol**	Show current type of VoIP protocol in ONU;
2	Raisecom#**show interface onu voice ip**	Show VoIP network parameter configuration of ONU;
3	Raisecom#**show interface onu voice ip dhcp client**	Show DHCP Client configuration of ONU voice service;
4	Raisecom#**show interface onu voice media ip**	Show network parameter configuration of ONU voice service media streaming;
5	Raisecom# **show interface onu** *slot-id/olt-id/onu-list* **voice call-progress-tone** [**busy** | **congestion** | **dial** | **ringback** | **waiting**] **information**	Show ONU call process voice parameter configurations.

4.3 Configuring POTS port

4.3.1 Preparing for configuration

Networking situation

POTS is used for voice calling, when using SIP protocol to transmit VoIP signaling, users need to configure POTS port phone number. After connecting POTS port, users will have their own phone number and they can dial to achieve voice calling function

Precondition

Users need to plan their own phone numbers. POTS port phone number must be unique in the entire VoIP network. ONU cannot check whether it conflicts with the POTS port phone numbers on other ONU, so users need to ensure the uniqueness of POTS port phone number in the process of configuration.

4.3.2 Default configuration of POTS port

Function	Default value
Telephone number of ONU POTS port	N/A
User name of ONU POTS port	pots-uni-line number
State of ONU POTS port	enable
Echo cancellation of ONU POTS port	enable
Silence compression of ONU POTS port	disable
Comfortable noise function of ONU POTS port	enable
Preferred type of coding of ONU line	G711A

4.3.3 Configuring POTS port

Step	Configuration	Description
1	`Raisecom#fttx`	Enter global configuration mode of EPON system;
2	`Raisecom(fttx)#interface onu` *`slot-id/olt-id/onu-id`*	Enter ONU configuration mode;
3	`Raisecom(fttx-onu*/*:*)#voice`	Enter ONU voice configuration mode;

Step	Configuration	Description
4	Raisecom(fttx-onu-voice-*/*:*)#**pots phone-number** *number pots-id*	Configure telephone number of ONU POTS port, between 0 and 9, and the maximum number of the telephone number is 32; **Note** The telephone number is required field in configuration of SIP protocol; the telephone number is optional field in configuration of H.248 protocol;
5	Raisecom(fttx-onu-voice-*/*:*)#**pots name** *string pots-id*	Configure user name of ONU POTS port;
6	Raisecom(fttx-onu-voice-*/*:*)#**pots** { **enable** | **disable** } *pots-list*	Enable/disable POTS port; If POTS port is disabled, current communication will be broke, the port can't start a call or receive a new call;
7	Raisecom(fttx-onu-voice-*/*:*)#**pots echo-cancellation** { **enable** | **disable** } *pots-list*	Enable/disable echo cancellation of POTS port;
8	Raisecom(fttx-onu-voice-*/*:*)#**pots silence-compression** { **enable** | **disable** } *pots-list*	Enable/disable silence compression of POTS port;
9	Raisecom(fttx-onu-voice-*/*:*)#**pots cng** { **enable** | **disable** } *pots-list*	Enable/disable comfortable noise function of POTS port;
10	Raisecom(fttx-onu-voice-*/*:*)#**pots prefer-codec** { **g711a** | **g729** | **g711u** | **g723** | **g726** } *pots-list*	Configure preferred type of coding of ONU line ONU
11	Raisecom(fttx-onu-voice-*/*:*)#**pots circuit-test** *pots-id*	Configure POTS port to execute circuit test;
12	Raisecom(fttx-onu-voice-*/*:*)#**pots loop-line-test** *pots-id*	Configure POTS port to execute loop line test;

4.3.4 Checking configuration

Step	Configuration	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **voice pots**	Show management state of ONU POTS port;
2	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **voice pots service**	Show service information of ONU POTS port, including telephone number, name and preferred codec;

4.4 Configuring SIP

4.4.1 Preparing for configuration

When VoIP uses SIP as the signaling transmission protocol, users can take the following configuration to achieve ONU SIP voice services as well as configure a variety of service features, such as caller ID, call waiting, three-way calling, etc.

SIP (Session Initiation Protocol) is one of the VoIP signaling protocols, proposed by IETF. It is used to create, modify and terminate interactive user session, such as video, voice, instant communication, etc. which contains multimedia elements. It will push service and control to terminal so as to achieve terminal intellectualization.

4.4.2 Default configuration of SIP protocol

Function	Default value
Monitor port of SIP transmission protocol	5060
TCP transmission function	disable
IP address of primary/secondary SIP Proxy server of ONU register	0.0.0.0
Monitor port of protocol and message of primary/secondary SIP Proxy server of ONU register	5060
Transmission protocol type of primary/secondary SIP Proxy server of ONU register	UDP
IP address of primary/secondary SIP Register server of ONU register	0.0.0.0
Monitor port of protocol and message of primary/secondary SIP Register server of ONU register	5060
Transmission protocol type of primary/secondary SIP Register server of ONU register	UDP
Time interval in which ONU sends registered message to SIP Register server	3600s
SIP primary/secondary agent swap function	enable
Period of heartbeat of ONU SIP protocol	60s
Timeout times of heartbeat of ONU SIP protocol	3
Detection mode of heartbeat of ONU SIP protocol	send-option
Switch of heartbeat of ONU SIP protocol	off
Caller ID display function of ONU POTS	enable
Encapsulation pattern of caller ID message on ONU POTS port	BELLCORE
Call waiting service	disable
Three party service	disable

Function	Default value
Transparent transmission service of SIP Modem	enable
Reverse polarity service	enable
Hot line service	disable
SIP number matching rule	min

4.4.3 Configuring SIP transmission protocol

Please pay attention to SIP monitoring protocol and port configuration parameters:

- Keep consistent with opposite Proxy/Register servers, and do not modify randomly.
- By default, use UDP protocol, port number for 5060 and no modification in the practical application.
- RTP/RTCP media streams of ONU equipment will use UDP protocol, with port starting from 60000. Note that the configuration of SIP protocol monitoring port do not conflict, otherwise, SIP protocol will not work normally.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**sip transport** { **udp** | **tcp** } **port** *port-number*	Configure monitor port of ONU SIP transmission protocol;
5	Raisecom(fttx-onu-voice-*/*:*)#**sip transport tcp** { **enable** | **disable** }	Enable/Disable TCP transmission;

4.4.4 Configuring SIP Proxy/Register server

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**sip** { **primary** | **secondary** } **proxy-server ip** *ip-address* [{ **udp** | **tcp** } **port** *port-number*]	Configure IP address and monitor port of primary/secondary SIP Proxy server of ONU register;
5	Raisecom(fttx-onu-voice-*/*:*)#**proxy-server transport** { **udp** | **tcp** }	Configure transmission protocol type of primary/secondary SIP Proxy server of ONU register;

Step	Configuration	Description
6	Raisecom(fttx-onu-voice-*/*:*)#**sip** { **primary** | **secondary** } **register-server ip** *ip-address* [{ **udp** | **tcp** } **port** *port-number*]	Configure IP address and monitor port of primary/secondary SIP Register server of ONU register;
7	Raisecom(fttx-onu-voice-*/*:*)#**sip** { **primary** | **secondary** } **register-server transport** { **udp** | **tcp** }	Configure transmission protocol type of primary/secondary SIP Register server of ONU register;
8	Raisecom(fttx-onu-voice-*/*:*)#**sip proxy-swap** { **enable** | **disable** }	Enable SIP primary/secondary agent swap function;
9	Raisecom(fttx-onu-voice-*/*:*)#**sip register fresh-period** *period*	Configure time interval in which ONU sends registered message to SIP Register server, and the minimum interval is 60s;
10	Raisecom(fttx-onu-voice-*/*:*)#**sip realm** *string*	Configure SIP domain name, it is used with out-bond Proxy server;
11	Raisecom(fttx-onu-voice-*/*:*)#**sip outbound proxy-server ip** *ip-address* [**udp port** *port-number*]	Configure IP and monitor port of out-bond Proxy server;

Note

- It is recommended that user can configure registration message refresh interval over 300 seconds in order to avoid multiple POTS phone users on multiple ONU transmit SIP Register message frequently to SIP Register server which may cause SIP Register server burden.
- If SIP Proxy or Register server uses TCP transmission protocol, the device must enable TCP transmission protocol.

4.4.5 Registering and deregistering phone user

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**sip pots** { **register** | **deregister** } *pots-list*	Deregister or register users again; they are mainly used in tests; use operation deregister to delete register information from register server; use operation register to register users again;

4.4.6 Configuring SIP heartbeat

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**sip heartbeat cycle** *period*	(Optional) Configure period of heartbeat of ONU SIP protocol;
5	Raisecom(fttx-onu-voice-*/*:*)#**sip heartbeat timeout count** *number*	(Optional) Configure timeout times of heartbeat of ONU SIP protocol;
6	Raisecom(fttx-onu-voice-*/*:*)#**sip heartbeat mode** { **send-option** | **receive-option** | **send-info** | **receive-info** }	(Optional) Configure detection mode of heartbeat of ONU SIP protocol;
7	Raisecom(fttx-onu-voice-*/*:*)#**sip heartbeat** { **on** | **off** }	(Optional) Configure switch of heartbeat of ONU SIP protocol;

Note

To detect the connection among ONU, registration, and proxy server, the server will regularly send SIP information to ONU or ONU sends information to server regularly.

Note

- It is recommended that the heartbeat cycle should be not less than 60s; otherwise, it will affect ONU and server performance.
- The heartbeat way and cycle requirement should cooperate with server. If the server does not support heartbeat, user needs to turn off heartbeat detection.

4.4.7 Configuring SIP user authentication

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**sip pots authentication** *name* [**password** *password*] *pots-list*	Configure SIP authentication information of ONU POTS;

4.4.8 Configuring SIP DigitMap

Please configure SIP DigiMap.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system.
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode.
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode.
4	Raisecom(fttx-onu-voice-*/*:*)#**sip digitmap** *string*	Configure SIP DigitMap.
5	Raisecom(fttx-onu-voice-*/*:*)#**sip digitmap timer** { **long** | **short** | **start** } *time*	(Optional) configure SIP timer.

Note

- To prevent unauthorized users from access, under normal circumstances, SIP Proxy/Register server or SIP opposite device allow access after authentication.
- ONU with voice function is in support of two authentication modes: authentication with user name and authentication with user name and password.

4.4.9 Showing caller's number

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**sip pots caller-id** { **enable** | **disable** } *pots-list*	Enable/disable caller ID display of ONU POTS;
5	Raisecom(fttx-onu-voice-*/*:*)#**pots caller-id mode** { **bellcore** | **etsi** | **ntt** } *pots-list*	Configure encapsulation pattern of caller ID message on ONU POTS port;

4.4.10 Configuring call waiting

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**sip pots call-wait** { **enable** | **disable** } *pots-list*	Enable/disable ONU call waiting function;

If it is soft switch in local side and needs to configure call waiting service, user should firstly enable call waiting service on soft switch.

4.4.11 Configuring third-part call service

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**sip pots 3-way-conference** { **enable** | **disable** } *pots-list*	Enable/disable ONU three party service function;

If it is soft switch in local side and needs to configure call waiting service, user should firstly enable three-way calling service on soft switch.

4.4.12 Configuring Modem transparent transmitting service

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**sip modem** { **enable** | **disable** }	Enable/disable SIP modem function;

4.4.13 Configuring antipolarity service

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**sip pots polarity-reverse** { **enable** | **disable** } *pots-list*	Enable reverse polarity of ONU POTS port;

4.4.14 Configuring hot-line service

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**sip pots hot-line** { **disable** | **instant** | **delay** } *pots-list*	Configure hot line of ONU POTS port;
5	Raisecom(fttx-onu-voice-*/*:*)#**sip pots hot-line phone-number** *number pots-id*	Configure telephone number of hot line on ONU POTS port;

4.4.15 Configuring mapping rule of SIP number

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**sip dial-map-rule** *rule-id phone-number sipuri*	Add mapping of called telephone number;
5	Raisecom(fttx-onu-voice-*/*:*)#**digitmap match-mode** { **min** | **max** }	Configure matching mode of number;

Note

- ONU with voice function is in support of add, delete and query operations of SIP number mapping rules. SIP number mapping rules shows how the called phone number mapped to corresponding SIP URI address format of "sip: user @ host IP". This section contains two parts:
- Collect No.: ONU equipment collects numbers from the calling user and initiates the call after getting the complete number string.
- Number mapping: after collecting number, according to number mapping rule, the first part of matching results begin to match, then choose corresponding SIP URL to call.
- The called phone number is in support of 'x','.','#','*','[]','-' and numbers 0 to 9. Therein, 'x' indicates one digit number; '.' indicates to repeat the previous character for zero or more times; '-' indicates a section of continuous value, such as "[2-8]" indicates the phone number is in support of any character from 2 to 8, including 2 and 8.
- Support supplementary services required'#','*' characters.
- Dial mapping rules cannot start with '.'.

- The called phone number of different dial-up mapping rules cannot be the same.

Configuration applications:

- [2-8]xxxxxxx indicates 8-bit local calls number starting from "2" to "8", such as 2128892, 50158293
- 13xxxxxxxxx indicates 13-bit mobile phone number starting with "13", such as 13810292839
- 0xxxxxxxxxxxxxx indicates 15-bit long-distance number starting with "0", such as 057 182 882 492
- 9xxxx indicates 5-bit special service number starting with "9", such as 95555
- x. # indicates to match the number ending with '#'
- 1 [0124-9] x indicates the 3-bit phone number starting with "1" and the middle bit is not "3", such as: 110,114,120, etc.
- [0-9 * #]. indicates to match all phone number, including '*' and '#'
- x. indicates to match all phone number, excluding '*' '#'
- SIP URI supports the IP: PORT format. IP must be the calling destination IPv4 format address; if the IP is not configured, the default call will switch to SIP Proxy (already configured); the system will use 5060 by default without configuring PORT.

4.4.16 Checking configuration

Step	Configuration	Description
1	Raisecom#**show interface onu voice sip transport**	Show transmission protocol information of ONU SIP;
2	Raisecom#**show interface onu voice sip** { **primary** | **secondary** } **proxy-server**	Show primary/secondary SIP Proxy server configuration information of ONU SIP;
3	Raisecom#**show interface onu voice sip** { **primary** | **secondary** } **register-server**	Show primary/secondary SIP Register server configuration information of ONU SIP;
4	Raisecom#**show interface onu voice sip active proxy-server**	Show type of current primary/secondary server of ONU SIP protocol;
5	Raisecom#**show interface onu voice sip proxy-swap**	Show primary/secondary swap configuration of ONU SIP proxy;
6	Raisecom#**show interface onu voice sip realm**	Show domain name information of ONU SIP;
7	Raisecom#**show interface onu voice sip outbound proxy-server**	Show configuration information of ONU Outbound Proxy server;
8	Raisecom#**show interface onu voice sip pot service**	Show service information of SIP protocol on ONU POTS port;
9	Raisecom#**show interfac onu voice sip heartbeat**	Show heartbeat configuration of SIP protocol on ONU POTS port;
10	Raisecom#**show interface onu voice sip pots authentication**	Show authentication information of ONU POTS;
11	Raisecom#**show interface onu voice pots service**	Show feature information of ONU POTS port;
12	Raisecom#**show interface onu voice sip dial-map-rule**	Show mapping table of numbers on ONU SIP;
13	Raisecom#**show interface onu** *slot-id*/olt-*id*/*onu-list* **voice sip digitmap timer**	Show ONU SIP timer configuration.

4.5 Configuring H.248

4.5.1 Preparing for configuration

Networking situation

H.248 is one of VoIP signaling protocols, used between MG and MGC. Through MGC coordination control, the MG users can achieve voice call and conversation.

H.248 is one of VoIP signaling protocols supported by RAISECOM ONU; if users choose H.248 as signaling protocol, they can achieve voice service through the following configuration.

4.5.2 Default configuration of H.248 protocol

Function	Default value
Register way of MG	ip
Transmission port number of MG	2944
Signalling coding method of H.248 protocol	text
IP address of primary/secondary MGC server	0.0.0.0
Transmission port number of primary/secondary MGC server	2944
Generation mode of MG TID	line
Prefix of RTP	RTP
Length of digitals in RTP	1
Origination TID of RTP	0
Total resource of RTP	2×the number of POTS ports
The maximum waiting delay of MG	180s
The period of MG heartbeat	60s
MG heartbeat mode	ITO
Timeout times of MG breakdown judgment	3
Matching mode of H.248 DigitMap	min
Long timer in H.248 DigitMap	20s
Short timer in H.248 DigitMap	5s
Start timer in H.248 DigitMap	10s
MGC type of H.248 protocol authentication	national
Parameters of H.248 protocol authentication	G is 2, p is N/A, ki is N/A

4.5.3 Configuring MG

MG is H.248 media gateway unit. All ONU with voice function can achieve a MG object.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**h248 mg register-mode** { **ip** | **domain-name** | **device-name** | **mac** | **mid** }	(Optional) Configure register way of MG; Users can configure the item if official department give a registration mode, otherwise they don't configure the item;
5	Raisecom(fttx-onu-voice-*/*:*)#**h248 mg name** *name*	(Optional) Configure MG name; Users must configure the item if registration mode is domain-name, device-name or mid, and MG name refers to specified name which is given by official department;
6	Raisecom(fttx-onu-voice-*/*:*)#**h248 mg max-waiting-delay** *time*	(Optional) Configure the maximum waiting delay;
7	Raisecom(fttx-onu-voice-*/*:*)#**h248 mg transport port** *port-number*	(Optional) Configure transmission port number of MG;
8	Raisecom(fttx-onu-voice-*/*:*)#**h248 mg encode** { **text** | **compact-text** | **bin** }	(Optional) Configure signalling coding method of H.248 protocol;

Note

- The basic MG parameters must be consistent with the opposite MGC server, does not allow arbitrary modification.
- ONU equipment RTP/RTCP media streams will use UDP protocol with port starting from 60000. Note that don't make MG transmission port numbers conflict, otherwise, H.248 protocol will not work normally.
- If not setting MG name, the system will register according to "local IP address: port number" by default.

4.5.4 Configuring MGC

MGC is H.248 media gateway controller unit, which can be achieved in soft switch.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;

Step	Configuration	Description
4	Raisecom(fttx-onu-voice-*/*:*)#**h248** { **primary** | **secondary** } **mgc ip** *ip-address* [**port** *port-number*]	Configure IP address and transmission port number of ONU's primary/secondary MGC server;
5	Raisecom(fttx-onu-voice-*/*:*)#**h248** { **primary** | **secondary** } **mgc name** *string*	(Optional) Configure name of ONU's primary/secondary MGC server; **Note** Name of primary and secondary MGC server may be different;
6	Raisecom(fttx-onu-voice-*/*:*)#**h248** { **primary** | **secondary** } **mgc authentication** *auth-id*	(Optional) Configure authentication information of ONU's primary/secondary MGC server;
7	Raisecom(fttx-onu-voice-*/*:*)#**h248 mgc-swap** { **enable** | **disable** }	(Optional) enable/disable swap of ONU's primary/secondary MGC server;

Note

- When configuring basic H.248 service, user must configure basic MGC attributes on ONU, including IP address, port number and MGC name. These parameters must correspond with MGC configuration.
- When configuring primary and secondary MGC, user needs to enable heartbeat detection for primary and secondary MGC switching.

4.5.5 Configuring TID

H.248 indicates MG user endpoint through TID, TID can be divided into POTS TID and RTP TID. POTS TID is the only MG port identification on MGC, while POTS TID can be bound with specific phone number on MGC.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**h248 mg tid mode** { **auto** | **line** | **multilayer** }	Configure TID generation mode of POTS port;
5	Raisecom(fttx-onu-voice-*/*:*)#**h248 mg tid prefix** *prefix* **name** *name*	(Optional) Configure prefix and name of POTS TID; Users can configure the item only if mode of POTS TID is auto;
	Raisecom(fttx-onu-voice-*/*:*)#**h248 mg tid name** *name pots-id*	(Optional) Configure end user name of POTS port; Users can configure the item only if mode of POTS TID is line;

Step	Configuration	Description
6	Raisecom(fttx-onu-voice-*/*:*)#**h248 mg tid rtp prefix** *prefix* **length** *length*	(Optional) Configure prefix and length of digitals of RTP TID; If official department specify name of RTP, and it is different with default value, users can configure the item; otherwise they can't configure the item;
7	Raisecom(fttx-onu-voice-*/*:*)#**h248 mg tid rtp begin** *value*	Configure start TID of RTP;
8	Raisecom(fttx-onu-voice-*/*:*)#**h248 mg tid rtp number** *value*	Configure total resources of RTP;

Note

- RTP TID prefix configuration cannot be empty.
- If there is no limit to the number of RTP resource on MGC, it is better to configure as twice of the port number (default value).
- The unused user port needn't to configure TID.
- The configured TID value in different user port cannot be the same.

4.5.6 Configuring MG heartbeat

To detect the link connectivity between MG and MGC, MG and MGC may send information to each other to verify operation situation.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**h248 mg heartbeat cycle** *period*	Configure heartbeat period of voice gateway;
5	Raisecom(fttx-onu-voice-*/*:*)#**h248 mg heartbeat mode** { **disable** | **svc** | **ito** | **audit** }	Configure heartbeat mode of voice gateway;
6	Raisecom(fttx-onu-voice-*/*:*)#**h248 mg heartbeat timeout count** *number*	Configure timeout times of breakdown judgment of voice gateway;

Note

- It is recommended that the MG heartbeat timeout is less than MGC heartbeat timeout.
- The heartbeat way and cycle need to coordinate with server; if the server is not in support of heartbeat, user needs to disable heartbeat detection.

4.5.7 Configuring H.248 DigitMap

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**h248 digitmap** *dm-id name string*	Configure H.248 DigitMap;
5	Raisecom(fttx-onu-voice-*/*:*)#**digitmap match-mode** { **min** | **max** }	Configure matching mode of DigitMap;
6	Raisecom(fttx-onu-voice-*/*:*)#**h248 mg digitmap long-timer** *longtime*	Configure long timer in ONU H.248 media gateway DigitMap;
7	Raisecom(fttx-onu-voice-*/*:*)#**h248 mg digitmap short-timer** *shorttime*	Configure short timer in ONU H.248 media gateway DigitMap;
8	Raisecom(fttx-onu-voice-*/*:*)#**h248 mg digitmap start-timer** *starttime*	Configure start timer in ONU H.248 media gateway DigitMap;

Caution

At present, user needs not to configure DigitMap but uses MGC issued DigitMap in prior.

4.5.8 Configuring H.248 authentication

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**h248 create authentication** *auth-id* **type** *mgc-type*	Add MGC type in voice gateway authentication information of H.248 protocol; Use **no h248 create authentication** {*auth-id* | **all**} to delete voice gateway authentication parameters of H.248 protocol;
5	Raisecom(fttx-onu-voice-*/*:*)#**h248 create authentication** *auth-id* **g** *g* **p** *p* **ki** *ki* **mginfo** *mg-info*	Add parameter G in voice gateway authentication information of H.248 protocol; Use **no h248 create authentication** {*auth-id* | **all**} to delete voice gateway authentication parameters of H.248 protocol;

Step	Configuration	Description
6	Raisecom(fttx-onu-voice-*/*:*)#**h248 authentication** *auth-id* **type** *mgc-type*	Modify MGC type in voice gateway authentication information of H.248 protocol;
7	Raisecom(fttx-onu-voice-*/*:*)#**h248 authentication** *auth-id* **g** *g* **p** *p* **ki** *ki* **mginfo** *mg-info*	Modify parameters in voice gateway authentication information of H.248 protocol;

Caution

When connecting device and MGC, user needs to configure voice gateway authentication information if MGC requires authenticating voice gateway.

4.5.9 Configuring H.248 service management

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**h248 mg forced-deregister**	Force to deregister voice gateway;
5	Raisecom(fttx-onu-voice-*/*:*)#**h248 mg register**	Register voice gateway;
6	Raisecom(fttx-onu-voice-*/*:*)#**h248 mg delay-deregister** *delay-time*	Delay to deregister voice gateway;
7	Raisecom(fttx-onu-voice-*/*:*)#**h248 pots forced-deregister** *pots-list*	Force to deregister pots;
8	Raisecom(fttx-onu-voice-*/*:*)#**h248 pots register** *pots-list*	Register pots;
9	Raisecom(fttx-onu-voice-*/*:*)#**h248 pots delay-deregister** *delay-time pots-list*	Delay to deregister pots;

4.5.10 Checking configuration

Step	Configuration	Description
1	Raisecom#**show interface onu voice h248 mg**	Query voice gateway parameter of H.248 protocol;
2	Raisecom#**show interface onu voice h248 mg heartbeat**	Query heartbeat information of voice gateway;
3	Raisecom#**show interface onu voice h248 pots**	Show TID information of POTS;
4	Raisecom#**show interface onu voice h248** { **primary** | **secondary** } **mgc**	Show primary/secondary MGC server configuration information of ONU H248 protocol;

Step	Configuration	Description
5	Raisecom#**show interface onu voice h248 mgc-swap**	Show primary/secondary MGC server swap information of ONU;
6	Raisecom#**show interface onu voice h248 active mgc**	Show current H.248 MGC of ONU;
7	Raisecom#**show interface onu voice digitmap**	Show matching mode of DigitMap;
8	Raisecom#**show interface onu voice h248 digitmap**	Show H.248 DigitMap;
9	Raisecom#**show interface onu voice h248 authentication**	Show authentication information of ONU H.248;
10	Raisecom#**show interface onu voice h248 mg**	Show state information of gateway;
11	Raisecom#**show interface onu voice h248 pots**	Show state information of port;

4.6 Configuring second dial-up service

4.6.1 Preparing for configuration

Networking situation

Second dial-up refers to dial again after getting through, such as dial an extension, enter card password, etc.

Second dial-up function supports four transmission modes to transmit dial-up information:

- Voice transparent transmission (Transparent) mode
- RFC 2833 mode
- RFC 2833 redundancy mode (using RFC 2198 protocol)
- SIP-INFO mode

Actual equipment uses DTMF mode, subject to SDP protocol negotiation result; if the SDP protocol is without DTMF mode, use local configuration mode.

SIP-INFO mode is only valid when using SIP protocol and cannot be configured for H.248 protocol.

Precondition

The second dial-up transmission type should be consistent with butting device.

4.6.2 Default configuration of second dial-up service

Function	Default value
transmission information of second dial-up function	transparent

4.6.3 Configuring second dial-up service

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**dtmf** { **rfc2833-relay** | **rfc2833-redundancy** | **sip-info** | **transparent** }	Configure transmission information of second dial-up function on ONU;

4.6.4 Checking configuration

Step	Configuration	Description
1	Raisecom#**show interface onu voice dtmf**	Show transmission information of second dial-up function on ONU;

4.7 Configuring fax service

4.7.1 Preparing for configuration

Networking situation

ONU supports two fax transmission modes: voice transparent transmission (Transparent) and T38 protocol. When using T38 protocol, user can choose two error correction modes: forward error correction (FEC) and redundant transmission (Redundancy).

Configuring as T38 protocol does not mean using these configuration data for voice fax switching; whether to use T38 protocol and T38 fax specific parameters are based on the actual negotiation result of SDP protocol. If T38 protocol switching fails, it will automatically switch to voice transparent transmission mode to fax.

4.7.2 Default configuration of fax service

Function	Default value
Configure transmission type of ONU fax	transparent
Configure error correction mode of ONU T38 fax	redundancy
Configure fax rate of POTS port T38	14400bit/s

4.7.3 Configuring fax service

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**fax transport** { **transparent** | **t38** }	Configure transmission type of ONU fax ;
5	Raisecom(fttx-onu-voice-*/*:*)#**fax error-correction-mode** { **redundancy** | **fec** }	Configure error correction mode of ONU T38 fax ;
6	Raisecom(fttx-onu-voice-*/*:*)#**pots fax relay rate** { **2400** | **4800** | **7200** | **9600** | **12000** | **144000** } *pots-list*	Configure fax rate of POTS port T38;

4.7.4 Checking configuration

Step	Configuration	Description
1	Raisecom#**show interface onu voice fax**	Show ONU fax configuration information;
2	Raisecom#**show interface onu voice pots fax**	Show ONU POTS fax service information;

4.8 Configuring call emulation test

4.8.1 Preparing for configuration

Networking situation

Call emulation is an important means of VoIP equipment network troubleshooting, does not require user involvement, but complete the call through the process simulation of user dialing/calling operation and events.

Call emulation contains incoming emulation and outgoing emulation; incoming emulation is used to locate voice calling failure; outgoing emulation is used to locate the voice dialing fault. User can use query command to get the current port state, detect emulation testing process. The command of test disable can stop the port hang up test and get test result; if the test fails, user will get fault reasons.

Precondition

Use ISCOM52xx, DLCOM2096 and other ONU equipments with voice function, other ONU equipments does not support this function.

4.8.2 Configuring call emulation test

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**voice**	Enter ONU voice configuration mode;
4	Raisecom(fttx-onu-voice-*/*:*)#**pots call-test start** *pots-id* **caller** [**timeout** *timeout*] **media** { **tone** | **loopback** } **phone-number** *number*	Start calling out of emulation test;
5	Raisecom(fttx-onu-voice-*/*:*)#**pots call-test start** *pots-id* **callee** [**timeout** *timeout*] **media** { **tone** | **loopback** } **phone-number** *number*	Start calling in emulation test;
6	Raisecom(fttx-onu-voice-*/*:*)#**pots call-test stop** *pots-id*	Stop call emulation test;
7	Raisecom(fttx-onu-voice-*/*:*)#**pots call-test query** { **all** | *pots-list* }	Query call emulation test;

Note

User cannot take port call emulation with voice service or being tested. All ONU equipment can take a line test and be exclusive with internal and external lines test, which cannot be taken simultaneously.

4.9 Maintenance

Command	Description
Raisecom(fttx-onu-voice-*/*:*)#**clear interface onu slot-id/olt-id/onu-id voice statistics sip**	Clear message statistics of ONU SIP protocol;
Raisecom(fttx-onu-voice-*/*:*)#**clear interface onu slot-id/olt-id/onu-id voice statistics h248**	Clear performance statistics of ONU H.248 protocol;
Raisecom(fttx-onu-voice-*/*:*)#**clear interface onu slot-id/olt-id/onu-id voice statistics rtp**	Clear media packet statistics of ONU RTP;
Raisecom(fttx-onu-voice-*/*:*)#**clear interface onu slot-id/olt-id/onu-id voice statistics call pots {all | pots-id}**	Clear calling statistics of ONU POTS port;
Raisecom(fttx-onu-voice-*/*:*)#**clear interface onu slot-id/olt-id/onu-id voice statistics error-code**	Clear error code statistics of ONU protocol;

Command	Description
Raisecom(fttx-onu-voice-*/*:*)#**clear interface onu slot-id/olt-id/onu-id voice statistics sdp**	Clear performance statistics of ONU SDP;

5 Configuring CATV service

The chapter introduces configuration information and procedure of CATV service in ISCOM5508 device, and provides related configuration applications.

- Quick configuration of CATV service
- Preparing for configuration
- Configuring CATV service
- Checking configuration

5.1 Quick configuration of CATV service

5.1.1 Networking requirements

As shown in below figure, PON port OLT 1/1 of ISCOM5508 connects with ONU, a RF port on ONU connects with a user. Users can configure CATV function on ONU device to receive TV signals.

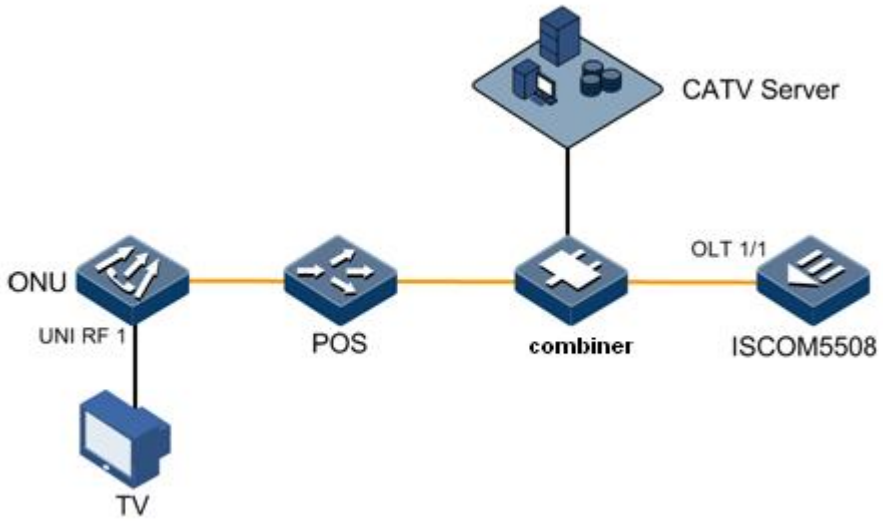

Figure 5-1 CATV service networking

5.1.2 Configuration steps

Enable CATV function on RF port.

```
Raisecom#fttx
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#uni rf 1 enable
```

5.1.3 Checking results

Check whether configuration of CATV service on ONU is correct.

```
Raisecom#show interface onu 1/1/1 uni rf information
RF UNI ID  Admin State
----------------------
1/1/1/1    enable
```

5.2 Preparing for configuration

Networking situation

As shown in below figure, we need to configure CATV service on ONU in typical triple-play, in order to send CATV service by ODN network.

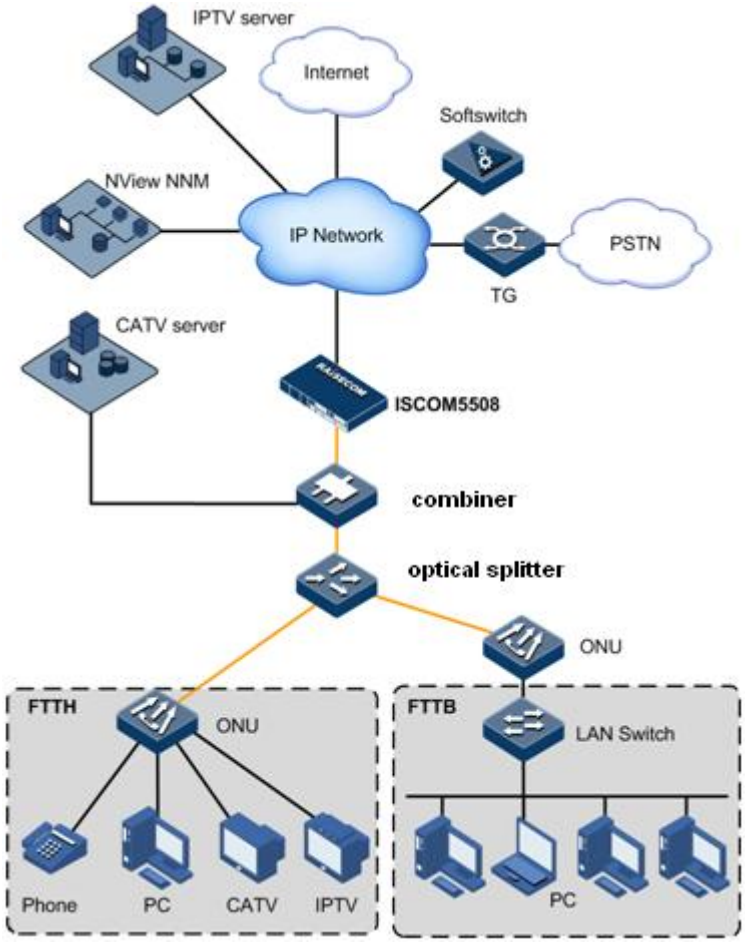

Figure 5-2 Typical triple-play

Precondition

Please users confirm whether ONU supports CATV service before configuring CATV service.

5.3 Configuring CATV service

Step	Configuration	Description
1	`Raisecom#fttx`	Enter global configuration mode of EPON system;
2	`Raisecom(fttx)#interface onu` *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	`Raisecom(fttx-onu*/*:*)#uni rf` *uni-id* `{ enable | disable }`	Enable/disable CATV service;

5.4 Checking configuration

No.	Item	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni rf** [*uni-id*] **information**	Show port information of ONU RF user;
2	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **nni catv** [*nni-id*] **information**	Show port information of ONU CATV network;

6 Configuring TDMoP service

The chapter introduces TDMoP service configuration information and configuration process, and provides related configuration application.

- Quick configuration of TDMoP service
- Preparing for configuration
- Configuring global parameters of TDMoP service
- Configuring port mode of TDMoP service
- Configuring system clock of TDMoP service
- Configuring Bundle
- (Optional) configuring TDM loopback
- (Optional) configuring TDM port alarm
- Checking configuration
- Maintenance

6.1 Quick configuration of TDMoP service

6.1.1 Networking requirements

As shown in below figure, uplink port GE 1 connects with router of IP network in ISCOM5508, PON port OLT 1/1 connects with ONU, port TDM-UNI 1, TDM-UNI 2, TDM-UNI 3 and TDM-UNI 4 on ONU connect with TDM device. Users need to configure TDMoP on ONU device to realize transparent transmission of TDM service on PSN network.

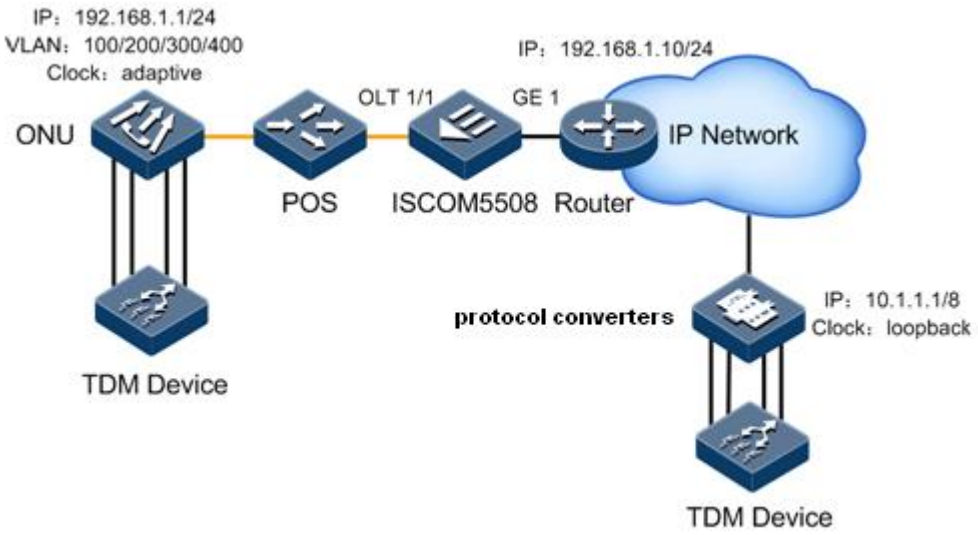

Figure 6-1 Networking of TDMoP

Parameter	Value
source IP address of TDM	192.168.1.1/255.255.255.0
Clock level	stratum-3
TDM-1	• E1 • unframed • clock: adaptive (self-adaptive) • Bundle: 1
TDM-2	• E1 • framed • clock: adaptive (self-adaptive) • Bundle: 2 • Enable E1-CRC
TDM-3	• E1 • framed-cas (multiframe) • clock: adaptive (self-adaptive) • Bundle: 3 • Enable E1-CRC
TDM-4	• E1 • unframed • clock: adaptive (self-adaptive) • Bundle: 6

Parameter	Value
Bundle-1	• Type of payload: SAToP • PSN type: UDPIP • E1 port number: TDM-UNI 1 • time slot configuration: N/A • source Bundle ID: 1001 • destination Bundle ID: 1001 • VLAN: 100 • CoS: 6 • destination IP address: 10.1.1.1 • next-hop type: IP • next-hop IP address: 192.168.1.10 • loading time of message: 125us • Jitterbuffer: 3ms
Bundle-2	• Type of payload: CESoP • PSN type: UDPIP • E1 port number: TDM-UNI 2 • time slot configuration: 1-15 • source Bundle ID: 1002 • destination Bundle ID: 1002 • VLAN: 100 • CoS: 6 • destination IP address: 10.1.1.1 • next-hop type: IP • next-hop IP address: 192.168.1.10 • loading time of message: 125us • Jitterbuffer: 3ms
Bundle-3	• Type of payload: AAL1 • PSN type: UDPIP • E1 port number: TDM-UNI 2 • time slot configuration: 16-31 • source Bundle ID: 1003 • destination Bundle ID: 1003 • VLAN: 200 • CoS: 6 • destination IP address: 10.1.1.1 • next-hop type: IP • next-hop IP address: 192.168.1.10 • loading time of message: 125us • Jitterbuffer: 3ms

Parameter	Value
Bundle-4	• Type of payload: CESoP • PSN type: MPLS • E1 port number: TDM-UNI 3 • time slot configuration: 1-5 • source Bundle ID: 1004 • destination Bundle ID: 1004 • VLAN: 300 • CoS: 6 • next-hop type: IP • next-hop IP address: 192.168.1.10 • the number of MPLS label: 2 • outer MPLS label: 14 • inner MPLS label: 104 • loading time of message: 125us • Jitterbuffer: 3ms
Bundle-5	• Type of payload: AAL1 • PSN type: UDPIP • E1 port number: TDM-UNI 3 • time slot configuration: 6-15,17-31 • source Bundle ID: 1005 • destination Bundle ID: 1005 • VLAN: 300 • CoS: 6 • destination IP address: 10.1.1.1 • next-hop type: IP • next-hop IP address: 192.168.1.10 • loading time of message: 125us • Jitterbuffer: 3ms
Bundle-6	• Type of payload: AAL1 • PSN type: MPLS • E1 port number: TDM-UNI 4 • time slot configuration: 0-31 • source Bundle ID: 1006 • destination Bundle ID: 1006 • VLAN: 400 • CoS: 6 • next-hop type: IP • next-hop IP address: 192.168.1.10 • the number of MPLS label: 2 • outer MPLS label: 16 • inner MPLS label: 106 • loading time of message: 125us • Jitterbuffer: 3ms

6.1.2 Configuration steps

Step 1 Configure global parameters.

```
Raisecom#fttx
Raisecom(fttx)#interface onu 1/1/1
```

```
Raisecom(fttx-onu1/1:1)#tdm
Raisecom(fttx-onu-tdm-1/1:1)#ip-address 192.168.1.1 255.255.255.0
Raisecom(fttx-onu-tdm-1/1:1)#source-clock-quality stratum-3
```

Step 2 Enable TDM port.

```
Raisecom(fttx-onu-tdm-1/1:1)#e1t1 rage 1-4
Raisecom(fttx-onu-e1t1-range)#port-admin enable
```

Step 3 Configure parameters of TDM port.

- Configure TDM-1.

```
Raisecom(fttx-onu-tdm-1/1:1)#e1t1 1
Raisecom(fttx-onu-e1t11/1/1:1)#service-type e1
Raisecom(fttx-onu-e1t11/1/1:1)#e1-frame-mode unframed
Raisecom(fttx-onu-e1t11/1/1:1)#tx-clock-src arc
Raisecom(fttx-onu-e1t11/1/1:1)#adaptive-bundleid 1
```

- Configure TDM-2.

```
Raisecom(fttx-onu-tdm-1/1:1)#e1t1 2
Raisecom(fttx-onu-e1t11/1/1:2)#service-type e1
Raisecom(fttx-onu-e1t11/1/1:2)#e1-frame-mode framed
Raisecom(fttx-onu-e1t11/1/1:2)#e1-crc enable
Raisecom(fttx-onu-e1t11/1/1:2)#tx-clock-src arc
Raisecom(fttx-onu-e1t11/1/1:2)#adaptive-bundleid 2
```

- Configure TDM-3.

```
Raisecom(fttx-onu-tdm-1/1:1)#e1t1 range 3
Raisecom(fttx-onu-e1t11/1/1:3)#service-type e1
Raisecom(fttx-onu-e1t11/1/1:3)#e1-frame-mode framed-cas
Raisecom(fttx-onu-e1t11/1/1:3)#e1-crc enable
Raisecom(fttx-onu-e1t11/1/1:3)#tx-clock-src arc
Raisecom(fttx-onu-e1t11/1/1:3)#adaptive-bundleid 3
```

- Configure TDM-4.

```
Raisecom(fttx-onu-tdm-1/1:1)#e1t1 range 4
Raisecom(fttx-onu-e1t11/1/1:4)#service-type e1
Raisecom(fttx-onu-e1t11/1/1:4)#e1-frame-mode unframed
```

```
Raisecom(fttx-onu-e1t11/1/1:4)#tx-clock-src arc
Raisecom(fttx-onu-e1t11/1/1:4)#adaptive-bundleid 6
```

Step 4 Configure Bundle parameters.

- Configure Bundle-1.

```
Raisecom(fttx-onu-tdm1/1:1)#create bundle 1 payload-type satop psn-type
udpip dest-bundle 1001 src-bundle 1001 port 1 time-slot 0-31
Raisecom(fttx-onu-tdm1/1:1)#bundle range 1
Raisecom(fttx-onu-bundle1/1/1:1)#vlan mode tag
Raisecom(fttx-onu-bundle1/1/1:1)#vlan inner-vlanid 100
Raisecom(fttx-onu-bundle1/1/1:1)#vlan inner-cos 6
Raisecom(fttx-onu-bundle1/1/1:1)#udp dest-ip 10.1.1.1
Raisecom(fttx-onu-bundle1/1/1:1)#udp nexthop-address-type ip
Raisecom(fttx-onu-bundle1/1/1:1)#udp ip-address-nexthop 192.168.1.10
Raisecom(fttx-onu-bundle1/1/1:1)#packet-load-time 125
Raisecom(fttx-onu-bundle1/1/1:1)#jitter-buffer 30
```

- Configure Bundle-2.

```
Raisecom(fttx-onu-tdm1/1:1)#create bundle 2 payload-type cesop psn-type
udpip dest-bundle 1002 src-bundle 1002 port 2 time-slot 1-15
Raisecom(fttx-onu-tdm1/1:1)#bundle range 2
Raisecom(fttx-onu-bundle1/1/1:2)#vlan mode tag
Raisecom(fttx-onu-bundle1/1/1:2)#vlan inner-vlanid 100
Raisecom(fttx-onu-bundle1/1/1:2)#vlan inner-cos 6
Raisecom(fttx-onu-bundle1/1/1:2)#udp dest-ip 10.1.1.1
Raisecom(fttx-onu-bundle1/1/1:2)#udp nexthop-address-type ip
Raisecom(fttx-onu-bundle1/1/1:2)#udp ip-address-nexthop 192.168.1.10
Raisecom(fttx-onu-bundle1/1/1:1)#packet-load-time 125
Raisecom(fttx-onu-bundle1/1/1:1)#jitter-buffer 30
```

- Configure Bundle-3.

```
Raisecom(fttx-onu-tdm1/1:1)#create bundle 3 payload-type aal1 psn-type
udpip dest-bundle 1003 src-bundle 1003 port 2 time-slot 16-31
Raisecom(fttx-onu-tdm1/1:1)#bundle range 3
Raisecom(fttx-onu-bundle1/1/1:3)#vlan mode tag
Raisecom(fttx-onu-bundle1/1/1:3)#vlan inner-vlanid 200
Raisecom(fttx-onu-bundle1/1/1:3)#vlan inner-cos 6
Raisecom(fttx-onu-bundle1/1/1:3)#udp dest-ip 10.1.1.1
Raisecom(fttx-onu-bundle1/1/1:3)#udp nexthop-address-type ip
Raisecom(fttx-onu-bundle1/1/1:3)#udp ip-address-nexthop 192.168.1.10
Raisecom(fttx-onu-bundle1/1/1:1)#packet-load-time 125
Raisecom(fttx-onu-bundle1/1/1:1)#jitter-buffer 30
```

- Configure Bundle-4.

```
Raisecom(fttx-onu-tdm1/1:1)#create bundle 4 payload-type cesop psn-type
mpls dest-bundle 1004 src-bundle 1004 port 3 time-slot 1-5
Raisecom(fttx-onu-tdm1/1:1)#bundle range 4
Raisecom(fttx-onu-bundle1/1/1:4)#vlan mode tag
Raisecom(fttx-onu-bundle1/1/1:4)#vlan inner-vlanid 200
Raisecom(fttx-onu-bundle1/1/1:4)#vlan inner-cos 6
Raisecom(fttx-onu-bundle1/1/1:4)#mpls label-num 2
Raisecom(fttx-onu-bundle1/1/1:4)#mpls outer1-label 14
Raisecom(fttx-onu-bundle1/1/1:4)#mpls outer2-label 104
Raisecom(fttx-onu-bundle1/1/1:4)#udp nexthop-address-type ip
Raisecom(fttx-onu-bundle1/1/1:4)#udp ip-address-nexthop 192.168.1.10
Raisecom(fttx-onu-bundle1/1/1:1)#packet-load-time 125
Raisecom(fttx-onu-bundle1/1/1:1)#jitter-buffer 30
```

- Configure Bundle-5.

```
Raisecom(fttx-onu-tdm1/1:1)#create bundle 5 payload-type aal1 psn-type
udpip dest-bundle 1005 src-bundle 1005 port 3 time-slot 6-15,17-31
Raisecom(fttx-onu-tdm1/1:1)#bundle range 5
Raisecom(fttx-onu-bundle1/1/1:5)#vlan mode tag
Raisecom(fttx-onu-bundle1/1/1:5)#vlan inner-vlanid 300
Raisecom(fttx-onu-bundle1/1/1:5)#vlan inner-cos 6
Raisecom(fttx-onu-bundle1/1/1:5)#udp dest-ip 10.1.1.1
Raisecom(fttx-onu-bundle1/1/1:5)#udp nexthop-address-type ip
Raisecom(fttx-onu-bundle-1/1/1:5)#udp ip-address-nexthop 192.168.1.10
Raisecom(fttx-onu-bundle1/1/1:1)#packet-load-time 125
Raisecom(fttx-onu-bundle1/1/1:1)#jitter-buffer 30
```

- Configure Bundle-6.

```
Raisecom(fttx-onu-tdm1/1:1)#create bundle 6 payload-type aal1 psn-type
mpls dest-bundle 1006 src-bundle 1006 port 4 time-slot 0-31
Raisecom(fttx-onu-tdm1/1:1)#bundle range 6
Raisecom(fttx-onu-bundle1/1/1:6)#vlan mode tag
Raisecom(fttx-onu-bundle1/1/1:6)#vlan inner-vlanid 400
Raisecom(fttx-onu-bundle1/1/1:6)#vlan inner-cos 6
Raisecom(fttx-onu-bundle1/1/1:6)#mpls label-num 2
Raisecom(fttx-onu-bundle1/1/1:6)#mpls outer1-label 16
Raisecom(fttx-onu-bundle1/1/1:6)#mpls outer2-label 106
Raisecom(fttx-onu-bundle1/1/1:6)#udp nexthop-address-type ip
Raisecom(fttx-onu-bundle1/1/1:6)#udp ip-address-nexthop 192.168.1.10
Raisecom(fttx-onu-bundle1/1/1:1)#packet-load-time 125
Raisecom(fttx-onu-bundle1/1/1:1)#jitter-buffer 30
```

Step 5 Enable Bundle.

```
Raisecom(fttx-onu-tdm1/1:1)#bundle range 1-6
Raisecom(fttx-onu-bundle-range)#bundle enable
```

6.1.3 Checking results

Check whether global configuration of TDM is correct.

```
Raisecom#show interface onu 1/1/1 tdm information
ONU ID: 1/1/1
   IP Address         : 192.168.1.1
   Subnet Mask        : 255.255.255.0
   MAC Address        : 000c.d562.1545
   Outer TPID         : 0x9100
   UDP Multiplex Method : src-port
   OAM Frame ID       : 16383
   OOS Code          : 0x7f
   OOS Signalling     : 5
   Source Clock Quality : stratum3
```

Configure configuration of TDM port on device is correct.

```
Raisecom#show interface onu 1/1/1 tdm port information
Port ID : 1/1/1/1
   Description       : tdm-uni-1
   Service-type      : E1
   Port-state       : Enable
   E1-frame-mode     : Unframed
   T1-frame-mode     : Unframed
   E1-crc           : Disable
   T1-signal-mode    : --
   Ts-idle-code      : 0xFF
   Signal-idle-code  : 0x5
   Loopback-mode     : None
   Tx-clock-source   : Adaptive recovery clock
   Adaptive-bundle-id : 1
   LOS              : Yes
   LOF              : No
   AIS              : No
   LCV              : No
   RAI              : No
   CRC Error        : No
LOMF      :No
Port ID : 1/1/1/2
   Description       : tdm-uni-2
   Service-type      : E1
   Port-state       : Enable
   E1-frame-mode     : Framed
   T1-frame-mode     : --
   E1-crc           : Enable
```

```
    T1-signal-mode    : --
    Ts-idle-code      : 0xFF
    Signal-idle-code   : 0x5
    Loopback-mode     : None
    Tx-clock-source   : Adaptive recovery clock
    Adaptive-bundle-id : 2
    LOS             : Yes
    LOF             : Yes
    AIS             : No
    LCV             : No
    RAI             : No
    CRC Error        : No
LOMF       :No
Port ID : 1/1/1/3
    Description       : tdm-uni-3
    Service-type      : E1
    Port-state        : Enable
    E1-frame-mode     : CAS multi-frame
    T1-frame-mode     : --
    E1-crc           : Enable
    T1-signal-mode    : --
    Ts-idle-code      : 0xFF
    Signal-idle-code   : 0x5
    Loopback-mode     : None
    Tx-clock-source   : Adaptive recovery clock
    Adaptive-bundle-id : 4
    E1 Service        : Disable
    LOS             : Yes
    LOF             : Yes
    AIS             : No
    LCV             : No
    RAI             : No
    CRC Error        : No
LOMF       :No
Port ID : 1/1/1/4
    Description       : tdm-uni-4
    Service-type      : E1
    Port-state        : Enable
    E1-frame-mode     : Unframed
    T1-frame-mode     : Unframed
    E1-crc           : Disable
    T1-signal-mode    : --
    Ts-idle-code      : 0xFF
    Signal-idle-code   : 0x5
    Loopback-mode     : None
    Tx-clock-source   : Adaptive recovery clock
    Adaptive-bundle-id : 6
    E1 Service        : Disable
    LOS             : No
    LOF             : No
    AIS             : No
    LCV             : No
    RAI             : No
    CRC Error        : No
    LOMF       : No
```

Check whether Bundle configuration is correct.

```
Raisecom#show interface onu 1/1/1 tdm bundle
PSN:Packet Switch Network
Bundle ID   Payload  PSN    Destination  Source  Port  Timeslot
          Type     Type   Bundle       Bundle
------------------------------------------------------------------
1/1/1/1     satop    udpip  1001         1001    1     0-31
1/1/1/2     cesop    udpip  1002         1002    2     1-15
1/1/1/3     aal1     udpip  1003         1003    2     17
1/1/1/4     cesop    mpls   1004         1004    3     1-5
1/1/1/5     aal1     udpip  1005         1005    3     6-15,17-31
1/1/1/6     aal1     mpls   1006         1006    4     0-31
```

6.2 Preparing for configuration

As shown in below figure, ONU provides TDM service for many users. TDMoP service will be configured on ONU which connects with ISCOM5508, and TDM service will be transmitted by IP network.

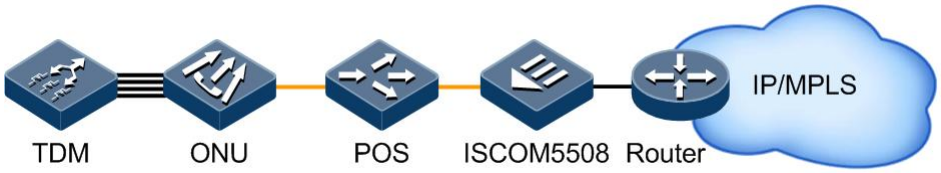

Figure 6-2 Networking of TDMoP application

6.3 Configuring global parameters of TDMoP service

Note

TDMoP feature is realized on ONU in Raisecom EPON system; please confirm whether ONU which connects with ISCOM5508 supports TDMoP service.

Step	Configuration	Description
1	`Raisecom#fttx`	Enter global configuration mode of EPON system;
2	`Raisecom(fttx)#interface onu` *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	`Raisecom(fttx-onu*/*:*)#tdm`	Enter TDM configuration mode;
4	`Raisecom(fttx-onu-tdm-*/*:*)#ip-address` *ip-address* [*ip-mask*]	Configure source IP address of TDM service;

Step	Configuration	Description
5	Raisecom(fttx-onu-tdm-*/*:*)#**source-clock-quality** { **stratum-1** | **stratum-2** | **stratum-3** | **stratum-3e** | **stratum-4** }	Configure level of system clock source;
6	Raisecom(fttx-onu-tdm-*/*:*)#**oam frame-id** *frame-id*	Configure ID of frame which transmits OAM messages;
7	Raisecom(fttx-onu-tdm-*/*:*)#**udp-multiplex-method** { **src-port** | **dest-port**}	Configure location of destination Bundle ID sending UDP message on local side;
8	Raisecom(fttx-onu-tdm-*/*:*)#**double-tagging tpid** *tp-id*	Configure outer TPID of Bundle;
9	Raisecom(fttx-onu-tdm-*/*:*)#**oss-code** *code-value*	Configure OSS data code;
10	Raisecom(fttx-onu-tdm-*/*:*)#**oss-signaling** *code-value*	Configure OSS signaling code;

6.4 Configuring port mode of TDMoP service

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**tdm**	Enter TDM configuration mode;
4	Raisecom(fttx-onu-tdm-*/*:*)#**e1t1** *port-id*	Enter configuration mode of TDM port;
5	Raisecom(fttx-onu-e1t1*/*/*:*)#**port-admin** { **enable** | **disable** }	Enable TDM function of port;
6	Raisecom(fttx-onu-e1t1*/*/*:*)#**service-type** { **e1** | **t1** }	Configure service type of TDM port;
7	Raisecom(fttx-onu-e1t1*/*/*:*)#**e1-frame-mode** { **unframed** | **framed** | **framed-cas** }	Configure framing type of E1 port;
8	Raisecom(fttx-onu-e1t1*/*/*:*)#**t1-frame-mode** { **unframed** | **sf** | **esf** }	Configure framing type of T1 port;
9	Raisecom(fttx-onu-e1t1*/*/*:*)#**e1-crc** { **enable** | **disable** }	Configure E1 CRC functon;
10	Raisecom(fttx-onu-e1t1*/*/*:*)#**t1-signal-mode** { **none** | **robbed-bit** }	Configure T1 signaling mode;
11	Raisecom(fttx-onu-e1t1-*/*/*:*)#**ts-idle-code** *code-value*	Configure time slot Idle code;
12	Raisecom(fttx-onu-e1t1*/*/*:*)#**signal-idle-code** *code-value*	Configure signaling Idle code;
13	Raisecom(fttx-onu-e1t1*/*/*:*)#**description** *description*	(Optional) Configure description of TDM port;

6.5 Configuring system clock of TDMoP service

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**tdm**	Enter TDM configuration mode;
4	Raisecom(fttx-onu-tdm-*/*:*)#**e1t1** *port-id*	Enter configuration mode of TDM port;
5	Raisecom(fttx-onu-e1t1*/*/*:*)#**tx-clock-src** { **arc** | **drc** | **loopback** | **system** }	Configure TX clock source;
6	Raisecom(fttx-onu-e1t1*/*/*:*)#**adaptive-bundleid** *id*	Configure clock recovery Bundle ID ;

6.6 Configuring Bundle

6.6.1 Creating and enabling Bundle

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**tdm**	Enter TDM configuration mode;
4	Raisecom(fttx-onu-tdm-*/*:*)#**creat bundle** *bundle-id* **payload-type** { **aal1** | **aal2** | **cesop** | **staop** | **hdlc** } **psn-type** { **udpip** | **mpls** | **l2tp** | **mef** } **dest-bundle** *dest-bundle-id* **src-bundle** *src-bundle-id* **port** *port-id* **timeslot** *timeslot*	Create Bundle management table;
5	Raisecom(fttx-onu-tdm-*/*:*)#**bundle** *bundle-id*	Enter configuration mode of Bundle port;
6	Raisecom(fttx-onu-bundle*/*/*:*)#**bundle** { **enable** | **disable** }	Enable/disable Bundle;

6.6.2 Configuring basic parameters of Bundle

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;

Step	Configuration	Description
3	Raisecom(fttx-onu*/*:*)#**tdm**	Enter TDM configuration mode;
4	Raisecom(fttx-onu-tdm-*/*:*)#**bundle** *bundle-id*	Enter configuration mode of Bundle port;
5	Raisecom(fttx-onu-bundle*/*/*:*)#**desription** *desription*	(Optional) Configure description of Bundle port;
6	Raisecom(fttx-onu-bundle*/*/*:*)#**payload-type** { **aal1** | **aal2** | **cesop** | **satop** | **hdlc** }	(Optional) Configure payload type of Bundle;
7	Raisecom(fttx-onu-bundle*/*/*:*)#**psn-type** { **udpip** | **mpls** | **l2tp** | **mef** }	(Optional) Configure PSN type;
8	Raisecom(fttx-onu-bundle*/*/*:*)#**dest-bundle** *dest-bundle-id*	(Optional) Configure port number of destination Bundle;
9	Raisecom(fttx-onu-bundle*/*/*:*)#**src-bundle** *src-bundle-id*	(Optional) Configure port number of source Bundle;
10	Raisecom(fttx-onu-bundle*/*/*:*)#**oss-status** { **lbit** | **txoff** }	(Optional) Configure OSS mode;
11	Raisecom(fttx-onu-bundle*/*/*:*)#**protocol-port** *port-id*	(Optional) Configure the port number which doesn't fill in Bundble ID in UDP message;
12	Raisecom(fttx-onu-bundle*/*/*:*)#**oam-connectivity** { **enable** | **disable** }	(Optional) Enable/disable OAM connectivity;

6.6.3 Configuring parameters of port E1/T1

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**tdm**	Enter TDM configuration mode;
4	Raisecom(fttx-onu-tdm-*/*:*)#**bundle** *bundle-id*	Enter configuration mode of Bundle port;
5	Raisecom(fttx-onu-bundle*/*/*:*)#**port** *port-id*	(Optional) Configure E1/T1 port for Bundle;
6	Raisecom(fttx-onu-bundle*/*/*:*)#**timeslot** *timeslot-list*	(Optional) Configure time slot for Bundle;

6.6.4 Configuring related information of PSN

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;

Step	Configuration	Description
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**tdm**	Enter TDM configuration mode;
4	Raisecom(fttx-onu-tdm-*/*:*)#**bundle** *bundle-id*	Enter Bundle configuration mode;
5	Raisecom(fttx-onu-bundle*/*/*:*)#**udp dest-ip** *ip-address*	(Optional) Configure destination IP address connecting with Bundle;
6	Raisecom(fttx-onu-bundle*/*/*:*)#**udp next-hop-address-type** { **ip** | **mac** }	(Optional) Configure Bundle next hop's address type;
7	Raisecom(fttx-onu-bundle*/*/*:*)#**udp ip-address-nexthop** *ip-address*	(Optional) Configure Bundle next hop's IP address;
8	Raisecom(fttx-onu-bundle*/*/*:*)#**udp mac-address-nexthop** *mac-address*	(Optional) Configure Bundle next hop's MAC address;
9	Raisecom(fttx-onu-bundle*/*/*:*)#**mpls label-num** *label-num*	(Optional) Configure the number of Bundle MPLS's outer label;
10	Raisecom(fttx-onu-bundle*/*/*:*)#**mpls outer1-label***label-val*	(Optional) Configure value of Bundle MPLS's outer label 1;
11	Raisecom(fttx-onu-bundle*/*/*:*)#**mpls outer2-label***label-val*	(Optional) Configure value of Bundle MPLS's outer label 2;
12	Raisecom(fttx-onu-bundle*/*/*:*)#**mpls exp** *exp-val*	(Optional) Configure EXP field of Bundle MPLS;
13	Raisecom(fttx-onu-bundle*/*/*:*)#**mpls ttl** *ttl-val*	(Optional) Configure TTL field of Bundle MPLS;
14	Raisecom(fttx-onu-bundle*/*/*:*)#**vlan mode** { **tag** | **double-tag** | **untag** }	(Optional) Configure mode of Bundle VLAN;
15	Raisecom(fttx-onu-bundle*/*/*:*)#**vlan inner-vlanid** *vlan-id*	(Optional) Configure Bundle's inner VLAN ID;
16	Raisecom(fttx-onu-bundle*/*/*:*)#**vlan outer-vlanid** *vlan-id*	(Optional) Configure Bundle's outer VLAN ID;
17	Raisecom(fttx-onu-bundle*/*/*:*)#**vlan inner-cos** *cos-val*	(Optional) Configure Bundle's inner VLAN priority;
18	Raisecom(fttx-onu-bundle*/*/*:*)#**vlan outer-cos** *cos-val*	(Optional) Configure Bundle's outer VLAN priority;
19	Raisecom(fttx-onu-bundle*/*/*:*)#**rip** { **enable** | **disable** }	(Optional) Enable RTP function of Bundle;

6.6.5 Configuring loading time of message and JitterBuffer

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**tdm**	Enter TDM configuration mode;
4	Raisecom(fttx-onu-tdm-*/*:*)#**bundle** *bundle-id*	Enter Bundle configuration mode;
5	Raisecom(fttx-onu-bundle*/*/*:*)#**packet-load-time** *time*	(Optional) Configure loading time of Bundle message;
6	Raisecom(fttx-onu-bundle*/*/*:*)#**jitter-buffer** *buffer-size*	(Optional) Configure size of Jitter Buffer;

6.6.6 Configuring statistics and alarm information

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**tdm**	Enter TDM configuration mode;
4	Raisecom(fttx-onu-tdm-*/*:*)#**bundle** *bundle-id*	Enter Bundle configuration mode;
5	Raisecom(fttx-onu-bundle*/*/*:*)#**alarm** { **overvlow** | **underflow** | **local-faiture** }	(Optional) Enable Bundle alarm;

6.7 (Optional) configuring TDM loopback

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**tdm**	Enter TDM configuration mode;
4	Raisecom(fttx-onu-tdm-*/*:*)#**e1t1**	Enter configuration mode of TDM port;
5	Raisecom(fttx-onu-e1t1*/*/*:*)#**loopback** { **none** | **internalloop** | **externalloop** | **bidirectional** }	Configure loopback type of ports;

6.8 (Optional) configuring TDM port alarm

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**tdm**	Enter TDM configuration mode;
4	Raisecom(fttx-onu-tdm-*/*:*)#**e1t1**	Enter configuration mode of TDM port;
5	Raisecom(fttx-onu-e1t1*/*/*:*)#**alarm** { **failture** | **time-unlock** | **los** | **lof** | **ais** | **crc-error** | **lomf** }	Enable port alarm;

6.9 Checking configuration

No.	Item	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **tdm information**	Show TDM system configuration;
2	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **tdm port** *port-list* **timeslot-assignment**	Show distribution of TDM port time slot;
3	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **tdm port** *port-list* **information**	Show configuration of TDM E1/T1 port;
4	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **tdm port** *port-list* **alarm**	Show TDM port alarm information;
5	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **tdm bundle** *bundle-list* **information**	Show TDM Bundle configuration;
6	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **tdm bundle** *bundle-list* **current-status**	Show running status of TDM Bundle;
7	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **tdm bundle** *bundle-list* **udp information**	Show management information of TDM Bundle UDP;
8	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **tdm bundle** *bundle-list* **mpls information**	Show management information of TDM Bundle MPLS;
9	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **tdm bundle** *bundle-list* **vlan information**	Show management information of TDM Bundle VLAN;
10	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **tdm bundle** *bundle-list* **alarm**	Show TDM Bundle alarm information;

6.10 Maintenance

Command	Description
Raisecom(config)#**clear interface onu** *slot-id/olt-id/onu-id* **tdm port** *port-list* **statistics**	Clear performance statistics of ONU TDM port;
Raisecom(config)#**clear interface onu** *slot-id/olt-id/onu-id* **tdm bundle** *bundle-list* **statistics**	Clear performance statistics of Bundle;

7 Configuring MAC address table

The chapter introduces basic principle and configuration procedure of MAC address table in ISCOM5508, and provides related configuration applications.

- Configuring aging time of MAC address
- Configuring learning of MAC address
- Configuring MAC address limit
- Clearing MAC address table
- Configuring acquisition and search of MAC address
- Configuring static unicast MAC address
- Configuring static multicast MAC address
- Configuring coping of MAC address
- Configuration examples

7.1 Configuring aging time of MAC address

7.1.1 Preparing for configuration

Networking situation

Aging time of dynamic MAC address forwarding table should be configured to prevent explosive increase of MAC address forwarding table. Time starts from the moment which a MAC address adds into MAC address forwarding table, if all port don't receive the frame whose source address is the MAC address in aging time, the MAC address will be deleted from dynamic MAC address forwarding table. Otherwise, timer of aging time will be updated.

7.1.2 Default configuration of aging time of MAC address

Default configuration of aging time of MAC address on ISCOM5508:

Function	default value
Aging time of MAC address	300s

Default configuration of aging time of MAC address on Raisecom ONU device:

Function	default value
Aging time of MAC address	300s

7.1.3 Configuring aging time of OLT MAC address

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**mac-address-table aging-time** { **0** | *period* }	Enter aging time of MAC address;

7.1.4 Configuring aging time of ONU MAC address

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**mac-address-table aging-time** { **0** | *period* }	Enter aging time of MAC address.0 means MAC address without aging;

7.1.5 Checking configuration

Checking OLT configuration

No.	Item	Description
1	Raisecom#**show mac aging-time**	Show OLT aging time of MAC address;

Checking ONU configuration

No.	Item	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **mac-address-table aging-time**	Show ONU aging time of MAC address;

7.2 Configuring learning of MAC address

7.2.1 Preparing for configuration

Networking situation

If scale of network is large or location of host in network is changed frequently, static MAC address will increase maintenance workload of work. So we need to configure MAC address learning to finish basic layer-2 forwarding function.

7.2.2 Default configuration of MAC address learning

Default configuration of MAC address learning on ISCOM5508 device:

Function	default value
MAC address learning	enable

Default configuration of MAC address learning on Raisecom ONU device:

Function	default value
MAC address learning	enable

7.2.3 Enabling/Disabling OLT MAC address learning

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**mac-address-table learning** { **enable** | **disable** } **port-list** { **all** | *port-list* }	Enable/disable MAC address learning on physical port;

7.2.4 Enabling/Disabling OLT MAC address learning

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter configuration mode of ONU UNI Ethernet port;
4	Raisecom(fttx-onu-uni*/*/*:*)#**mac-address-table learning** { **enable** | **disable** }	Enable/disable MAC address learning of ONU Ethernet port;

7.2.5 Checking configuration

Checking OLT configuration

No.	Item	Description
1	Raisecom#**show interface port** [*port-id*]	Show status of ports;

Checking ONU configuration

No.	Item	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** [*uni-id*] **mac-address-table**	Show configuration information of MAC address table on ONU Ethernet port;

7.3 Configuring MAC address limit

7.3.1 Preparing for configuration

Networking situation

Users should configure quantity limitation of learning dynamic MAC address forwarding table to prevent explosive increase of MAC address forwarding table.

7.3.2 Default configuration of MAC address limit

Function	default value
Quantity limitation of MAC addresses	unlimited

7.3.3 Configuring ONU MAC address limit

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter configuration mode of ONU UNI Ethernet port;
4	Raisecom(fttx-onu-uni*/*/*:*)#**mac-address-table threshold** { **unlimited** | *number* }	Configure the number of MAC addresses allowed to learn on ONU Ethernet port. *number*: a integer, and range is 1–128;

7.3.4 Checking configuration

No.	Item	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet mac-address-table**	Show the number of MAC addresses allowed to learn on ONU Ethernet port;

7.4 Clearing MAC address table

7.4.1 Preparing for configuration

Networking situation

ISCOM5508 device supports two layers MAC address table:

- Clear all MAC address lists.
- Clear dynamic learned MAC address lists.
- Clear static configured MAC address lists.

7.4.2 Clearing OLT MAC address

Clearing MAC address on PON port

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface olt** *slot-id/olt-id*	Enter OLT configuration mode;
3	Raisecom(config-olt*/*)#**clear interface olt** *slot-id/olt-id* **mac-address-table** { **all** | **dynamic** | **static** }	Clear specific types of MAC addresses on PON port in MAC address table;

Clearing MAC address of switching chip

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**clear mac-address-table** { **all** | **dynamic** | **static** } [**vlan** *vlan-id*] [**port** *port-id*]	Clear specific types of MAC addresses in MAC address table of switching chip;
3	Raisecom(config)#**no mac-address-table** *mac-address* [**vlan** *vlan-id*]	Clear specified MAC address in MAC address table of switching chip;
4	Raisecom(config)#**no mac-address-table static unicast** *mac-address* **vlan** *vlan-id*	Clear specified unicast MAC address in MAC address table of switching chip;

Step	Configuration	Description
5	Raisecom(config)#**no mac-address-table static multicast** *mac-address* **vlan** *vlan-id* **port-list** *port-list*	Clear specified multicast MAC address in MAC address table of switching chip;

7.4.3 Clearing ONU MAC address

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**clear interface onu** *slot-id/olt-id/onu-id* **mac-address-table** { **all** | **dynamic** | **static** }	Clear specific types of MAC addresses in MAC address table;

7.4.4 Checking configuration

Checking OLT configuration

No.	Item	Description
1	Raisecom#**show mac-address-table l2-address count**	Show the number of MAC addresses with specific types in MAC address table;

Checking ONU configuration

No.	Item	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **mac-address-table l2-address** { **all** | **dynamic** | **static** } [**count**]	Show all specific types of MAC addresses in MAC address table;

7.5 Configuring acquisition and search of MAC address

7.5.1 Preparing for configuration

Networking situation

Use MAC address acquisition command to show MAC address entries of OLT or ONU.Use MAC address search command to show whether there is related MAC address information in MAC address table of OLT or ONU.

7.5.2 Configuring acquisition and search of OLT MAC address

Step	Configuration	Description
1	Raisecom#**search mac-address** *mac-address*	Search and show specific MAC address information in MAC address table;

7.5.3 Configuring acquisition and search of ONU MAC address

Step	Configuration	Description
1	Raisecom#**search interface onu** *slot-id/olt-id/onu-id* **mac-address-table** *mac-address*	Search and show specific MAC address information in MAC address table;

7.5.4 Checking configuration

Checking OLT configuration

No.	Item	Description
1	Raisecom#**show mac-address-table l2-address port** *port-id*	Show MAC address on specific ports;
2	Raisecom#**show mac-address-table l2-address vlan** *vlan-id*	Show MAC address in VLAN;
3	Raisecom#**show mac-address-table l2-address count**	Show the number of dynamic MAC addresses, static MAC address, other MAC address and the total number of MAC address of device;
4	Raisecom#**show mac-address-table l2-address count port** *port-id*	Show the number of dynamic MAC addresses, static MAC address, other MAC address and the total number of MAC address on specific ports;
5	Raisecom#**show mac-address-table l2-address count vlan** *vlan-id*	Show the number of dynamic MAC addresses, static MAC address, other MAC address and the total number of MAC address in VLAN;
6	Raisecom#**show interface port** [*port-id*]	Show status of ports;

Checking ONU configuration

No.	Item	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **mac-address-table l2-address** { **all** | **dynamic** | **static** }	Show specific types of MAC addresses in MAC address table;

7.6 Configuring static unicast MAC address

7.6.1 Preparing for configuration

Networking situation

Users can configure static MAC address if they fix server, staff, in order to ensure all data streaming which goes to the MAC address forwarding on the port which refers to static MAC address.

7.6.2 Configuring OLT static unicast MAC address

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**mac-address-table static unicast** *mac-address* **vlan** *vlan-id* **port** *port-id*	Configure static unicast MAC address;

7.6.3 Configuring ONU static unicast MAC address

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**mac-address-table static unicast** *mac-address* **uni ethernet** *uni-id*	Configure ONU static unicast MAC address;

7.6.4 Checking configuration

Checking OLT configuration

No.	Item	Description
1	Raisecom#**show mac-address-table static** [**port** *port-id* | **vlan** *vlan-id*]	Show static address (of specific port or specific VLAN);

Checking ONU configuration

No.	Item	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **mac-address-table static** [**uni ethernet** *uni-id*]	Show static unicast MAC address configured by an or all Ethernet port of ONU;

7.7 Configuring static multicast MAC address

7.7.1 Preparing for configuration

Networking situation

Video conference on network, video on demand use multicast mode. Multicast can transfer data of all target nodes one time and transfer data for specific object, but unicast and broadcast can't realize the above aim.

7.7.2 Configuring OLT static multicast MAC address

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**mac-address-table static multicast** *mac-address* **vlan** *vlan-id* **port-list** *port-list*	Configure static multicast MAC address;

7.7.3 Configuring ONU static multicast MAC address

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**mac-address-table static multicast** *mac-address* **vlan** *vlan-id* **uni ethernet** *uni-list*	Configure ONU static multicast MAC address;

7.7.4 Checking configuration

Checking OLT configuration

No.	Item	Description
1	Raisecom#**show mac-address-table multicast** [**vlan** *vlan-id*][**count**]	Show static multicast MAC address;

Checking ONU configuration

No.	Item	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **mac-address-table static multicast** [**vlan** *vlan-id*]	Show MAC address of ONU specific VLAN or all static multicast;

7.8 Configuring coping of MAC address

7.8.1 Preparing for configuration

Networking situation

Coping of MAC addresses has three modes:

- N:1 mode: MAC addresses of many learned VLAN are copied in a VLAN.
- 1:N mode: MAC addresses of a learned VLAN are copied in many VLAN.
- 1:1 mode: MAC addresses of a learned VLAN are copied in a VLAN.

Where 1:1 mode is a specific application of N:1 or 1:N mode. Copied MAC address with static MAC address exists in destination VLAN.

7.8.2 Configuring coping of OLT MAC address

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter configuration mode of physical layer ports;
3	Raisecom(config-port)#**mac-address-table vlan-copy from vlan-list** *vlan-list* **to vlan-id** *vlan-id*	(Optional) Configure N:1 coping, and copy MAC address learned from *vlan-list* to *vlan-id*;

Step	Configuration	Description
4	Raisecom(config-port)#**mac-address-table vlan-copy from vlan-id** *vlan-id* **to vlan-list** *vlan-list*	(Optional) Configure N:1 coping, and copy MAC address learned from *vlan-id* to *vlan-list*;

Note

Use the command **no mac-address-table vlan-copy** *vlan-list* to cancel configured VLAN coping relation, where *vlan-list* is destination VLAN list. The above command is used to cancel coping MAC address of other VLAN to these destinations VLAN. Value of *vlan-list* must be consistent with destination VLAN.

7.8.3 Checking configuration

No.	Item	Description
1	Raisecom#**show mac-address-table l2-address port** *port-id*	Show MAC address table on ports;
2	Raisecom#**show mac-address-table static** [**port** *port-id* | **vlan** *vlan-id*]	Show static unicast MAC address;
3	Raisecom#**show mac-address-table multicast** [**vlan** *vlan-id* | **count**]	Show layer-2 multicast address;
4	Raisecom#**show mac-address-table vlan-copy** [**port-list** *portlist*]	Show coping configuration of MAC address of ports;

7.9 Configuration examples

7.9.1 Examples for configuring MAC address table

Networking requirements

As shown in below figure, location of PC A is fixed and important. Configure a static unicast MAC address for PC A between ONU A which connects with PC A and ISCOM5508, where MAC address of PC A is 0000.0000.0001, they belong to VLAN 10.

Configure dynamic MAC address learning on ONU B and ISCOM5508, and aging time of MAC address is 500s.

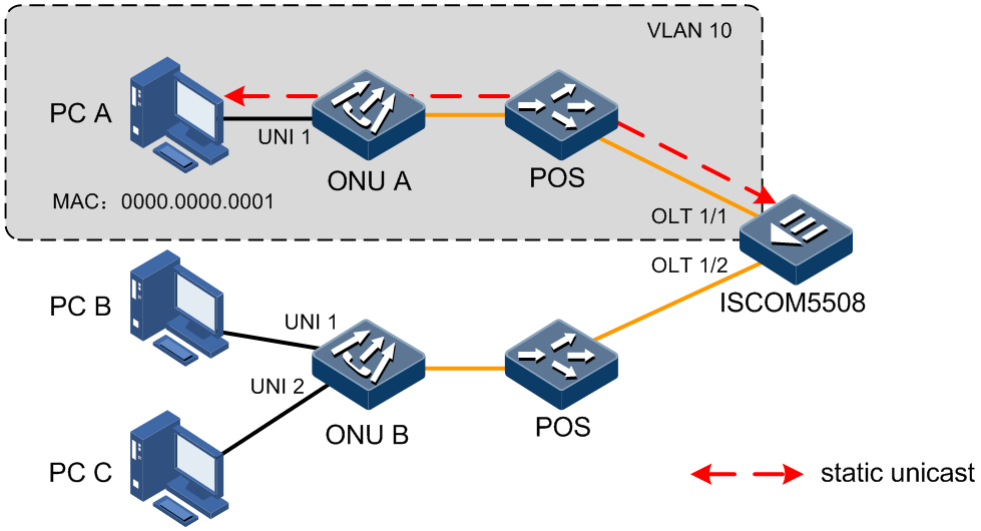

Figure 7-1 Configuring MAC address table

Configuration steps

- Configure static unicast MAC address of PC A.

Step 1 Create VLAN and configure port mode on ISCOM5508.

```
Raisecom#config
Raisecom(config)#create vlan 10 active
Raisecom(config)#interface port 7
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 10
Raisecom(config-port)#exit
```

Step 2 Configure static unicast MAC address on ISCOM5508.

```
Raisecom(config)#mac-address-table static unicast 0000.0000.0001 vlan 10
port 7
Raisecom(config)#end
```

Step 3 Create VLAN and configure port mode on ONU.

```
Raisecom#fttx
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#uni ethernet 1
Raisecom(fttx-onu-uni1/1/1:1)#vlan mode tagged
Raisecom(fttx-onu-uni1/1/1:1)#native vlan 10
Raisecom(fttx-onu-uni1/1/1:1)#exit
Raisecom(fttx-onu1/1:1)#uplink
```

```
Raisecom(fttx-onu-uplink1/1:1)#vlan mode transparent
Raisecom(fttx-onu-uplink1/1:1)#exit
```

Step 4 Configure static unicast MAC address on ONU.

```
Raisecom(fttx-onu1/1:1)#mac-address-table static unicast 0000.0000.0001
uni ethernet 1
Raisecom(fttx-onu1/1:1)#end
```

- Configure MAC address learning on ONU B and ISCOM5508.

Step 5 Configure dynamic MAC learning and aging time on ISCOM5508.

```
Raisecom#config
Raisecom(config)#mac-address-table learning enable port-list 8
Raisecom(config)#mac-address-table aging-time 500
Raisecom(config)#end
```

Step 6 Configure dynamic MAC learning and aging time on ONU.

```
Raisecom#fttx
Raisecom(fttx)#interface onu 1/2/1
Raisecom(fttx-onu1/2:1)#mac-address-table aging-time 500
Raisecom(fttx-onu1/2:1)#uni ethernet 1
Raisecom(fttx-onu1/2/1:1)#mac-address-table learning enable
Raisecom(fttx-onu1/2/1:1)#exit
Raisecom(fttx-onu1/2:1)#uni ethernet 2
Raisecom(fttx-onu1/2/1:2)#mac-address-table learning enable
```

Checking results

- Check OLT results.

Show aging time of MAC address.

```
Raisecom#show mac aging-time
Aging time:500 seconds
```

Show MAC address information in VLAN.

```
Raisecom#show mac-address-table l2-address vlan 10
Mac Address       Port   vp    Vlan    Flags
```

```
-------------------------------------------------
0000.0000.0001    7      0    10    Static
```

- Check ONU results.

Show aging time of MAC address.

```
Raisecom#show interface onu 1/2/1 mac-address-table aging-time
ONU ID   AgingTime(s)
-----------------------
1/2/1    500
```

Show static unicast MAC address configured by ONU.

```
Raisecom#show interface onu 1/1/1 mac-address-table static uni ethernet 1
Port ID     Static Mac Address
------------------------------
1/1/1/1     0000.0000.0001
```

8 Configuring VLAN

The chapter introduces basic principle and configuration procedure of ISCOM5508 device, and provides related configuration applications.

- Configuring VLAN
- Configuring QinQ
- Configuring VLAN translation
- Maintenance
- Configuration examples

8.1 Configuring VLAN

8.1.1 Preparing for configuration

The main function of VLAN is partition of logical network segment, and there are two kinds of typical application modes.

- In small-scale LAN, a two-layer device has many VLAN, hosts in a VLAN can communicate with each other, but hosts in different VLAN can't communicate with each other;
- In large-scale LAN or Enterprise network, there are many hosts; hosts in a department can communicate with each other. But hosts in different VLAN can't communicate with each other; if hosts in different VLAN want to communicate with each other, we need router.

8.1.2 Default configuration of VLAN

Default configuration of VLAN on ISCOM5508:

Function	Default value
TPID of PON port	0x8100
Filtering type of uplink data packet on PON port	All (all packets are allowed to pass)
VLAN processing mode of PON port	• uplink: Transparent • downstream: Transparent

Function	Default value
New priority used in VLAN Tag of data on PON port	• uplink: 0 • downstream: 0
Whether to use new priority on VLAN Tag of data on PON port	• uplink: Disable • downstream: Disable
VLAN ID used in VLAN Tag of data on PON port	• uplink: 1 • downstream: 1

Default configuration of VLAN on Raisecom ONU:

Function	Default value
VLAN processing mode of UNI	Transparent
default VLAN of UNI	1
default priority of UNI	0
VLAN processing mode of uplink port	Transparent

8.1.3 Configuring VLAN of OLT switching port

Creating VLAN

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode;
2	`Raisecom(config)#create vlan` *vlan-id* `{ active | suspend }`	Create VLAN;
3	`Raisecom(config)#vlan` *vlan-id*	(Optional) Create VLAN or enter VLAN configuration mode; Use this command to create VLAN as suspending state;
4	`Raisecom(config-vlan)#name` *name*	(Optional) Configure VLAN name;
5	`Raisecom(config-vlan)#state { active | suspend }`	(Optional) Configure VLAN activating or suspending state;

Note

- By default there are two VLAN in the system, that is default VLAN (VLAN1) and cluster VLAN (VLAN2), all the ports belongs to the default VLAN. Default VLAN is not allowed to be deleted. To learn more about cluster VLAN, ref. 19-cluster management function.
- By default, the default VLAN (VLAN1) name is 'Default', other static VLAN name is 'VLAN' added with 4 figure VLAN ID, for example the default name of VLAN 3is 'VLAN0003', the default name of VLAN 4094 is 'VLAN4094'.

- Only when a VLAN be activated in the system can it be active. When VLAN active status is suspend, user can configure the VLAN, like to delete/add port, configure VLAN priority, the system will keep the configuration, once the VLAN is activated, and the configuration will take effect in the system.

Configuring VLAN mode of OLT switching port

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-port)#**switchport mode** { **access** | **trunk** }	Configure mode of ports as Access or Trunk;

Configuring VLAN of access mode port

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-port)#**switchport mode access**	Configure VLAN mode of port as Access;
4	Raisecom(config-port)#**switchport access vlan** *vlan-id*	Configure Access VLAN;
5	Raisecom(config-port)#**switchport access egress-allowed vlan** { **all** | [**add** | **remove**] *vlan-list* } [confirm]	(Optional) Configure VLAN on Access port which is allowed to egress;

- By default, all the ports allow default VLAN (VLAN1) to pass, and all the data packets of the default VLAN transmitted from the ports do not take the corresponding VLAN TAG.
- In port Access mode, no matter how the VLAN list that is allowed to pass Access port is configured, the port allows the data packets of Access VLAN to pass, and the packets sent out do not take corresponding VLAN TAG.
- In port Access mode, when configuring Access VLAN, if the VLAN is not created and activated, the system will create and enable the VLAN automatically.
- In port Access mode, if Access VLAN is deleted or hanged up by user, the system will configure the port Access VLAN to default VLAN (VLAN1).

Configuring VLAN of trunk mode port

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;

Step	Configuration	Description
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-port)#**switchport mode trunk**	Configure mode of ports as Trunk;
4	Raisecom(config-port)#**switchport trunk native vlan** *vlan-id*	(Optional) Configure Native VLAN of port;
5	Raisecom(config-port)#**switchport trunk allowed vlan** { **all** | [**add** | **remove**] *vlan-list* } [confirm]	Configure VLAN which is allowed to pass on Trunk port; **Note** By default, all VLAN are allowed to pass on port with trunk mode if we don't configure this command;
6	Raisecom(config-port)#**switchport trunk untagged vlan** { **all** | [**add** | **remove**] *vlan-list* } [confirm]	(Optional) Configure untagged VLAN on Trunk egress port;

Note

- In port Trunk mode, no matter the configuration of the VLAN list that is able to pass Trunk port and Untagged VLAN list, the port allows the data packets of NATIVE VLAN to pass, and the transmitted data packets do not take corresponding VLAN TAG.
- In port Trunk mode, when configured Native VLAN, if the VLAN is not created or enabled, the system will create and enable the VLAN automatically.
- In port Trunk mode, if Native VLAN is deleted or blocked by user, the system will set the port Trunk Native VLAN to default VLAN (VLAN1) automatically.
- In port Trunk mode, if the configured Native VLAN is not default VLAN, while the VLAN list that allows passing Trunk port includes not default VLAN, then the port will not allow default VLAN data packets pass.
- Configuring Trunk allowed VLAN list and Trunk Untagged VLAN list is related. When configuring Trunk allowed VLAN list, the system will delete the not allowed VLAN in Trunk Untagged VLAN list; when configuring Trunk Untagged VLAN list, the system will add all Untagged VLAN to Trunk allowed VLAN.
- Access VLAN and Trunk Native VLAN cannot be configured to cluster VLAN.
- The VLAN list that is allowed to pass Access port, Trunk allowed VLAN list and Trunk Untagged VLAN list takes effect only to static VLAN, not to cluster VLAN, GVRP static VLAN.

Configuring interface

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface ip** *if-number*	Enter interface configuration mode;
3	Raisecom(config-ip)#**ip address** *ip-address* [*ip-mask*] *vlan-id*	Configure IP address of interface and associate with VLAN;

8.1.4 Configuring VLAN of OLT PON port

Configuring TPID of PON port

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface olt** *slot-id/olt-id*	Enter OLT configuration mode;
3	Raisecom(fttx-olt*/*)#**vlan tpid** *tpid*	Configure TPID of VLAN on PON port;

- PON port can identify a data packet as tagged packet if its TAG type is TPID (default value is 0x8100) or 0x9100 (Raisecom ONU), otherwise it is untagged packet;
- Use the TPID when adding VLAN tag or transfer VLAN Tag.

Configuring uplink VLAN of PON port

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface olt** *slot-id/olt-id*	Enter OLT configuration mode;
3	Raisecom(fttx-olt*/*)#**vlan upstream onu** *onu-list* **permit** { **all** | **untagged** | **tagged** **vlan-id** *vlan-id* }	Data packets coming from ONU are filtrated;
4	Raisecom(fttx-olt*/*)#**vlan upstream onu** *onu-list* **mode** { **stacking** | **tagged** | **translation** | **transparent** }	Configure processing mode of uplink VLAN;
5	Raisecom(fttx-olt*/*)#**vlan upstream onu** *onu-list* **new-tag priority** *priority*	(Optional) new VLAN priority is allowed to use if VLAN mode is non transparent and uplink data packet adds with VLAN Tag;
6	Raisecom(fttx-olt*/*)#**vlan upstream onu** *onu-list* **new-tag priority** { **enable** | **disable** }	(Optional) whether allow to use new VLAN priority if VLAN mode is non transparent and uplink data packet adds with VLAN Tag;
7	Raisecom(fttx-olt*/*)#**vlan upstream onu** *onu-list* **new-tag vlan-id** *vlan-id*	(Optional) new VLAN ID will replace with old VLAN ID if VLAN mode is non transparent and uplink data packet adds with VLAN Tag;

Note

- Data packet filtering: filtering match on data packet from ONU, and VLAN Tag processing, if it doesn't match, then discard it;
- VLAN Tag: matched data packets can be transferred and Tag operation according to configured VLAN mode.

Configuring downstream VLAN of PON port

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface olt** *slot-id/olt-id*	Enter OLT configuration mode;
3	Raisecom(fttx-olt*/*)#**vlan downstream tagged** *vlan-list* **mode** { **discard** | **removed** | **translation** | **transparent** }	Configure downstream VLAN data processing mode;
4	Raisecom(fttx-olt*/*)#**vlan downstream untagged forwarding** { **enable** | **disable** }	Enable/disable PON port to transform downstream untagged message;
5	Raisecom(fttx-olt*/*)#**vlan downstream tagged** *vlan-list* **new-tag priority** *priority*	(Optional) new VLAN priority is allowed to use if VLAN mode is non transparent and downstream data packet adds with VLAN Tag;
6	Raisecom(fttx-olt*/*)#**vlan downstream tagged** *vlan-list* **new-tag priority** { **enable** | **disable** }	(Optional) whether allow new VLAN priority to replace with old one if VLAN mode is non transparent and downstream data packet adds with VLAN Tag;
7	Raisecom(fttx-olt*/*)#**vlan downstream tagged** *vlan-id* **new-tag vlan-id** *vlan-id*	(Optional) whether allow new VLAN ID to replace with old one if VLAN mode is non transparent and downstream data packet adds with VLAN Tag;

8.1.5 Configuring VLAN of ONU UNI port

Configuring VLAN mode

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter OLT configuration mode;
3	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter configuration mode of UNI Ethernet port;
4	Raisecom(fttx-onu-uni*/*/*:*)#**vlan mode** { **tagged** | **translation** | **transparent** | **trunk** }	Configure VLAN mode of UNI;

Configuring VLAN switching rules

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**vlan translation-rule** *rule-id* **old** *vlan-id priority* **new** *vlan-id priority*	Create VLAN translation rules;
3	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
4	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter configuration mode of UNI Ethernet port;
5	Raisecom(fttx-onu-uni*/*/*:*)#**vlan translation-rule** *rule-list*	Use VLAN translation rules;

Note

- The rule number and content must be unique;
- Rules can't be modified, if users want to modify it, you can delete it and create it again;
- The rules cited by UNI can't be deleted; users can delete the citing relation and delete the rules.

Configuring default VLAN of UNI port

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter configuration mode of UNI Ethernet port;
4	Raisecom(fttx-onu-uni*/*/*:*)#**native vlan** *vlan-id* [*priority*]	Configure default VLAN and priority of UNI; the command is effective only if VLAN mode is tag, trunk and translation mode;

Configuring trunk VLAN

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter configuration mode of UNI Ethernet port;

Step	Configuration	Description
4	Raisecom(fttx-onu-uni*/*/*:*)#**vlan trunk allowed** *vlan-list*	Configure VLAN list of UNI which is allowed to pass in Trunk mode;

Configuring UNI TPID

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**vlan double-tagging tpid** *tpid*	Configure TPID of outer label in ONU double VLAN label;

8.1.6 Configuring VLAN of ONU uplink port

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**uplink**	Enter ONU uplink configuration mode;
4	Raisecom(fttx-onu-uplink*/*/*)#**vlan mode** { **transparent** | **trunk** }	Configure VLAN mode of uplink port;
5	Raisecom(fttx-onu-uplink*/*/*)#**vlan trunk allowed** *vlan-list*	Configure VLAN list of uplink port which is allowed to pass in Trunk mode;

8.1.7 Checking configuration

No.	Item	Description
1	Raisecom#**show vlan**	Show VLAN configuration;
2	Raisecom#**show interface port** *port-id* **switchport**	Show port VLAN configuration;
3	Raisecom#**show interface ip**	Show IP address configuration of interface;
4	Raisecom#**show interface olt** *slot-id/olt-list* **vlan tpid**	Show VLAN TPID configuration of PON port;
5	Raisecom#**show interface olt** *slot-id/olt-id* **vlan upstream onu** *onu-list*	Show VLAN configuration of uplink data on OLT PON port;
6	Raisecom#**show interface olt** *slot-id/olt-id* **vlan downstream**	Show VLAN configuration of downstream data on OLT PON port;

No.	Item	Description
7	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet vlan**	Show VLAN configuration of UNI;
8	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **vlan**	Show ONU VLAN Stacking configuration;
9	Raisecom#**show onu-remote vlan translation-rule**	Show existed VLAN translation rules of ONU;
10	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uplink vlan**	Show VLAN configuration of ONU uplink port;

8.2 Configuring QinQ

8.2.1 Preparing for configuration

Networking situation

- Basic QinQ

Basic QinQ is a kind of simple layer-two VPN channel technology, which makes message being able to go through the carriers' backbone network (public network) by encapsulating outer-layer VLAN Tag on the carrier access end for the private network messages. In public network, messages transmit according only to outer-layer VLAN Tag, while user private VLAN Tag can be transmitted as the data in the message. The technology helps relieving the public network VLAN ID resource that is becoming rare, while user can now his own private VLAN ID which wouldn't conflict with public network VLAN ID.

- Flexible QinQ

Flexible QinQ is an enhanced application of basic QinQ, which is based on the combination of port and VLAN. Except all the function of basic QinQ, flexible QinQ can take different action according to different VLAN Tags for the messages received from the same port, and adds different outer-layer VLAN ID for different inner-layer VLAN DI. With flexible QinQ, user can configure inner and outer layer Tag mapping rule, and encapsulate different outer-layer Tags for the messages with different inner-layer Tags according to the mapping rules. Flexible QinQ makes carriers network structure more elastic, and different terminal users can be sorted on the port that is connected with access devices according to VLAN Tag, while QoS strategy can be configured on public network according to outer-layer Tag, and configure the transmission priority flexibly, so that each user can acquire corresponding service.

Precondition

The following tasks should be completed before configuring QinQ:

- Connect with ports and configure physical parameters of ports, and physical layer state of ports is up;
- Create VLAN.

8.2.2 Default configuration of QinQ

Function	Default value
TPID of outer label	0x8100
QinQ function	disable

8.2.3 Configuring basic QinQ

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**mls double-tagging tpid** *tpid*	(Optional) Configure TPID of outer label;
3	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
4	Raisecom(config-port)#**switchport qinq dot1q-tunnel**	Enable basic QinQ function of port;
5	Raisecom(config-port)#**switchport mode access**	Configure mode of ports as access;
6	Raisecom(config-port)#**switchport access vlan** *vlan-id*	Configure access VLAN;

8.2.4 Configuring flexible QinQ

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**mls double-tagging tpid** *tpid*	(Optional) Configure TPID of outer label;
3	Raisecom(config)#**qinq vlan-mapping source-ip** *ip-address* [*mask*] **add-outer** *vlan-id*	Configure flexible QinQ based on source IP ;
	Raisecom(config)#**qinq vlan-mapping source-mac** *mac-address* [*mask*] **add-outer** *vlan-id*	Configure flexible QinQ based on source MAC;
4	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
5	Raisecom(config-port)#**switchport vlan-mapping ethertype** { **arp** | **eapol** | **flowcontrol** | **ip** | **ipv6** | **loopback** | **mpls** | **mpls-mcast** | **pppoe** | **pppoedisc** | **x25** | **x75** | **user-define** *protocol-num* } **add-outer** *vlan-id*	Configure flexible QinQ based on Ethernet frame type;
	Raisecom(config-port)#**switchport vlan-mapping cvlan** *vlan-list* **add-outer** *vlan-id*	Configure flexible QinQ based on inner VLAN;

Step	Configuration	Description
	Raisecom(config-port)#**switchport vlan-mapping acl** *acl-id* **add-outer** *vlan-id* [**cos** *cos-value*]	Configure flexible QinQ based on ACL;

8.2.5 Configuring output port as trunk mode

VLAN mode of egress port need to be configured when configuring QinQ, and messages with double-layer tag can pass through egress port normally.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-port)#**switchport mode trunk**	Configure Trunk mode of port to allow double tag message to pass;

8.2.6 Checking configuration

No.	Item	Description
1	Raisecom#**show switchport qinq**	Show basic QinQ configuration;
2	Raisecom#**show interface port** *port-id* **vlan-mapping add-outer**	Show flexible QinQ configuration;

8.3 Configuring VLAN translation

8.3.1 Preparing for configuration

Networking situation

VLAN translation is different from QinQ; VLAN conversion function needs not multi-layer VLAN Tag encapsulation, and let the messages transmit in the network planning of public network. The typical topology of VLAN conversion is similar with typical flexible QinQ topology.

- VLAN ID of user service is translated as VLAN ID of a operator;
- VLAN ID of many types of user services is translated as VLAN ID of a operator;

Precondition

The following tasks should be completed before configuring VLAN:

- Connect with ports and configure physical parameters of ports, and physical layer state of ports is up;

- Create VLAN.

8.3.2 Configuring 1:1 VLAN translation

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-port)#**switchport vlan-mapping** { **ingress** | **egress** } *vlan-list* **translate** *vlan-id*	Configure 1:1 VLAN translation rules based on ingress or egress of port;

8.3.3 Configuring N:1 VLAN translation

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-port)#**switchport vlan-mapping cvlan** *vlan-list* **translate** *vlan-id*	Configure N:1 VLAN translation rules;

8.3.4 Configuring VLAN translation based on ACL

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-port)#**switchport vlan-mapping acl** *acl-id* **translate** [**inner** *vlan-id*][**outer** *vlan-id*][**innercos** *cos-value*][**outercos** *cos-value*]	Configure VLAN translation rules based on ACL;

8.3.5 Checking configuration

No.	Item	Description
1	Raisecom#**show interface port** *port-id* **vlan-mapping** { **ingress** | **egress** | both } **translate**	Show configuration of VLAN switching;

8.4 Maintenance

Command	Description
`Raisecom(fttx)#clear interface onu slot-id/olt-id/onu-id uni ehternet uni-id statistic`	Clear statistics data of ONU UNI port;

8.5 Configuration examples

8.5.1 Examples for configuring VLAN

Networking requirements

As shown in below figure, users connect with UNI 1 of ONU, and VLAN of users is 100. ISCOM5508 uplinks IP network by GE port GE 1, and PON port OLT 1/1 downlinks ONU. Users enable data service in the following network topology.

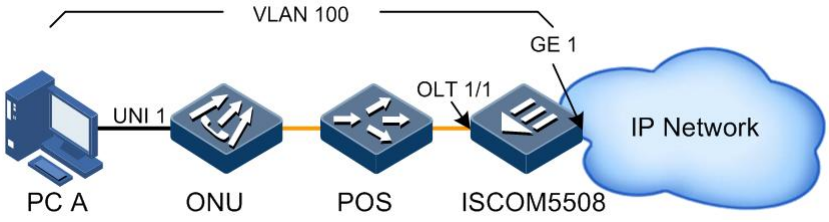

Figure 8-1 Configuring VLAN

Configuration steps

- Configure OLT.

Step 1 Create VLAN.

```
Raisecom#config
Raisecom(config)#create vlan 100 active
```

Step 2 Configure VLAN of GE port.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 100
Raisecom(config-port)#exit
```

Step 3 Configure VLAN of PON port.

```
Raisecom(config)#interface port 7
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 100
Raisecom(config-port)#end
```

Step 4 Configure ONU automatic registration.

```
Raisecom#fttx
Raisecom(fttx)#interface olt 1/1
Raisecom(fttx-olt1/1)#authorization mode none
Raisecom(fttx-olt1/1)#exit
```

- Configure ONU.

Step 5 Configure VLAN of user data.

```
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#uni ethernet 1
Raisecom(fttx-onu-uni1/1/1:1)#vlan mode tagged
Raisecom(fttx-onu-uni1/1/1:1)#native vlan 100
Raisecom(fttx-onu-uni1/1/1:1)#end
```

Checking results

Show VLAN configuration of OLT GE port and PON port respectively.

```
Raisecom#show interface port 1 switchport
Port: 1
Administrative Mode: trunk
Operational Mode: trunk
Access Mode VLAN: 1
Administrative Access Egress VLANs: 1
Operational Access Egress VLANs: n/a
Trunk Native Mode VLAN: 1
Administrative Trunk Allowed VLANs: 100
Operational Trunk Allowed VLANs: 1,100
Administrative Trunk Untagged VLANs: n/a
Operational Trunk Untagged VLANs: 1

Raisecom#show interface port 7 switchport
Port: 7
Administrative Mode: trunk
Operational Mode: trunk
Access Mode VLAN: 1
Administrative Access Egress VLANs: 1
Operational Access Egress VLANs: n/a
Trunk Native Mode VLAN: 1
```

```
Administrative Trunk Allowed VLANs: 100
Operational Trunk Allowed VLANs: 1,100
Administrative Trunk Untagged VLANs: n/a
Operational Trunk Untagged VLANs: 1
```

Show registered ONU.

```
Raisecom#show interface onu creation-information
ONU ID   MAC Address    Mode   Creation Date    Device Type       State
Mng-mode
--------------------------------------------------------------------------
1/1/1    000e.5e0a.7a0e  auto   2000-01-01,08:00  ISCOM5104(C)      active
oam
```

Show UNI VLAN configuration of ONU.

```
Raisecom#show interface onu 1/1/1 uni ethernet 1 vlan
Port ID: 1/1/1/1
   VLAN mode        : Tagged
   Native VLAN      : 100(CoS 0)
   Trans-rule list   : n/a
   Trunk allowed VLAN: n/a
```

8.5.2 Examples for configuring basic QinQ

Networking requirements

As shown in below figure, PC A accesses IP network by EPON, VLAN of the user is 1001, VLAN of operators is 601, and they can be realized by basic QinQ.

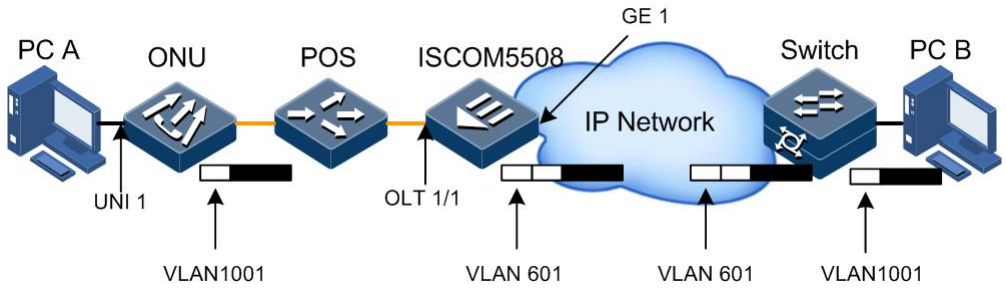

Figure 8-2 Basic QinQ

Configuration steps

The steps only refer to basic QinQ configuration of user PC A, namely configuration on ISCOM5508 device.

- Configure OLT.

Step 1 Create VLAN and modify TPID.

```
Raisecom#config
Raisecom(config)#create vlan 601,1001 active
Raisecom(config)#msl double-tagging tpid 8100
```

Step 2 Configure VLAN of GE uplink port.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport trunk allowed vlan 601
```

Step 3 Configure VLAN of PON port.

```
Raisecom(config-port)#exit
Raisecom(config)#interface port 7
Raisecom(config-port)#switchport access vlan 601
Raisecom(config-port)#switchport qinq dot1q-tunnel
```

- Configure ONU.

Step 4 Configure VLAN of UNI users.

```
Raisecom(config-port)#end
Raisecom#fttx
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#uni ethernet 1
Raisecom(fttx-onu-uni1/1/1:1)#vlan mode tagged
Raisecom(fttx-onu-uni1/1/1:1)#native vlan 1001
```

Checking results

Show QinQ configuration.

```
Raisecom#show switchport qinq
Outer TPID: 0x8100
  Port      QinQ Status
-----------------------------
  1             --
  2             --
  3             --
  4             --
```

```
5               --
6               --
7               Dot1q-tunnel
8               --
```

Show VLAN configuration of UNI.

```
Raisecom#show interface onu 1/1/1 uni ethernet 1 vlan
Port ID: 1/1/1
   VLAN mode        : Tagged
   Native VLAN      : 1001(CoS 0)
   Trans-rule list  : n/a
   Trunk allowed VLAN: n/a
```

Show VLAN configuration of GE port.

```
Raisecom#show interface port 1 switchport
Port: 1
Administrative Mode: access
Operational Mode: access
Access Mode VLAN: 1
Administrative Access Egress VLANs: 1
Operational Access Egress VLANs: 1
Trunk Native Mode VLAN: 1
Administrative Trunk Allowed VLANs: 601
Operational Trunk Allowed VLANs: n/a
Administrative Trunk Untagged VLANs: n/a
Operational Trunk Untagged VLANs: n/a
```

Show VLAN configuration of PON port.

```
Raisecom#show interface port 7 switchport
Port: 7
Administrative Mode: access
Operational Mode: access
Access Mode VLAN: 601
Administrative Access Egress VLANs: 1
Operational Access Egress VLANs: 1,601
Trunk Native Mode VLAN: 1
Administrative Trunk Allowed VLANs: 1-4094
Operational Trunk Allowed VLANs: n/a
Administrative Trunk Untagged VLANs: 1
Operational Trunk Untagged VLANs: n/a
```

8.5.3 Examples for configuring flexible QinQ

Networking requirements

PPPOE service of User A adds inner VLAN label 100, and transparently transmits to PON port of OLT by ONU, and then adds 2002 label according to type of Ethernet message, and enters BRAS by uplink port GE 1, ends outer label 2002.

IPOE service of User B adds inner VLAN label 200, and transparently transmits to PON port of OLT by ONU, and then adds 2001 label according to type of Ethernet message, and enters BUSR by uplink port GE 2, ends outer label 2001.

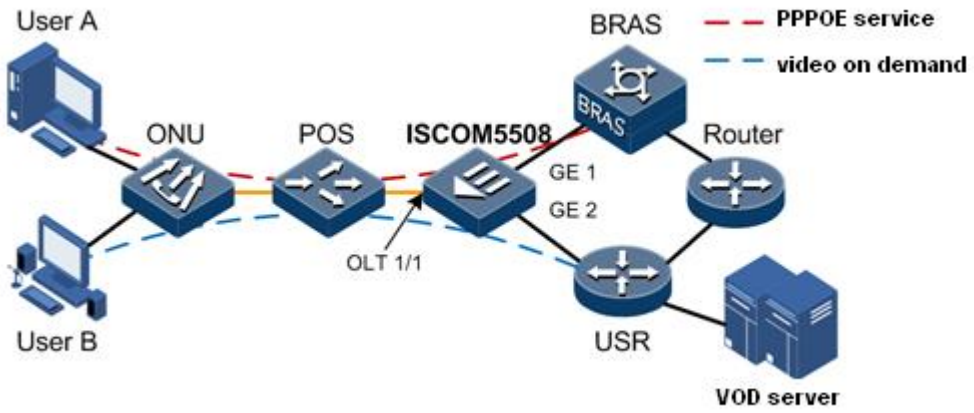

Figure 8-3 Flexible Qin

Configuration steps

- Configure OLT.

Step 1 Create VLAN and modify TPID.

```
Raisecom#config
Raisecom(config)#create vlan 100,200,2000,2001 active
Raisecom(config)#msl double-tagging tpid 8100
```

Step 2 Configure VLAN of GE uplink port 1/1.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 2002
Raisecom(config-port)#exit
```

Step 3 Configure VLAN of GE uplink port 1/2.

```
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 2001
Raisecom(config-port)#exit
```

Step 4 Configure VLAN of PON port.

```
Raisecom(config)#interface port 7
Raisecom(config-port)#switchport trunk allowed vlan 2000,2001
Raisecom(config-port)#switchport trunk untagged vlan 2000,2001
Raisecom(config-port)#switchport vlan-mapping ethertype pppoe add-outer
2001
Raisecom(config-port)#switchport vlan-mapping ethertype user-define 8800
add-outer 2002
Raisecom(config-port)#end
```

- Configure ONU.

Step 5 Configure UNI 1.

```
Raisecom#fttx
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#uni ethernet 1
Raisecom(fttx-onu-uni1/1/1:1)#vlan mode tagged
Raisecom(fttx-onu-uni1/1/1:1)#native vlan 100
```

Step 6 Configure UNI 2.

```
Raisecom(fttx-onu-uni1/1/1:1)#exit
Raisecom(fttx-onu1/1:1)#uni ethernet 2
Raisecom(fttx-onu-uni1/1/1:2)#vlan mode tagged
Raisecom(fttx-onu-uni1/1/1:2)#native vlan 200
```

Checking results

Show flexible QinQ configuration.

```
Raisecom#show interface port vlan-mapping add-outer

Inner VLAN based QinQ mapping rule:
Port   Outer VLAN    Inner VLAN List
------------------------------------------------

EtherType based QinQ mapping rule:
```

```
Port  EtherType      Add-outer VLAN
-------------------------------------------------
7     pppoe          2001
7     0x8800         2002
```

Show VLAN configuration of UNI.

```
Raisecom#show interface onu 1/1/1 uni ethernet vlan
Port ID: 1/1/1/1
   VLAN mode        : Tagged
   Native VLAN      : 100(CoS 0)
   Trans-rule list   : n/a
   Trunk allowed VLAN: n/a
Port ID: 1/1/1/2
   VLAN mode        : Tagged
   Native VLAN      : 200(CoS 0)
   Trans-rule list   : n/a
   Trunk allowed VLAN: n/a
```

8.5.4 Examples for configuring VLAN translation

Networking requirements

As shown in below figure, OLT 1/1 of ISCOM5508 A connects with A department which uses VLAN 100 and B department which uses VLAN 200, OLT 1/1 of ISCOM5508 B connects with C department which uses VLAN 100 and D department which uses VLAN 200. In operator network, A and C department are transformed by VLAN 1000, and B and D department are transformed by VLAN 2008.

ISCOM5508 A and B configure 1:1 VLAN transition to realize normal communication among PC users, terminal users and their server.

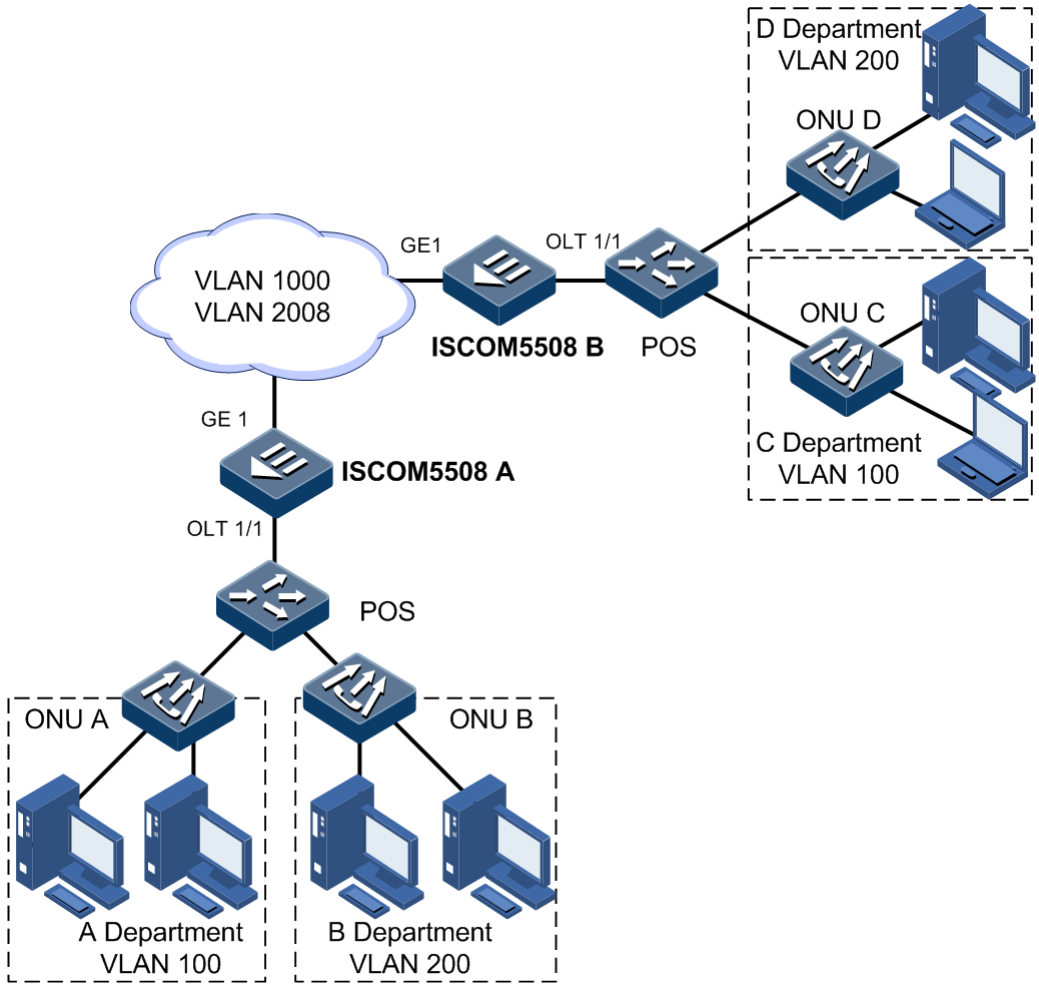

Figure 8-4 VLAN transition

Configuration steps

Configuration of ISCOM5508 A is the same as ISCOM5508 B, so we only describe configuration of ISCOM5508 A.

Step 1 Create VLAN and activate it.

```
Raisecom#config
Raisecom(config)#create vlan 100,200,1000,2008 active
```

Step 2 Configure uplink port GE 1 as trunk mode and it allows VLAN 1000 and VLAN 2008 to pass.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 1000,2008 confirm
Raisecom(config-port)#exit
```

Step 3 Configure interface OLT 1/1 as trunk mode, it allows VLAN 100, 200 to pass, and enable VLAN transforming function.

```
Raisecom(config)#interface port 7
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)# switchport trunk allowed vlan 100,200 confirm
Raisecom(config-port)#switchport vlan-mapping ingress 100 translate 1000
Raisecom(config-port)#switchport vlan-mapping egress 1000 translate 100
Raisecom(config-port)#switchport vlan-mapping ingress 200 translate 2008
Raisecom(config-port)#switchport vlan-mapping egress 2008 translate 200
Raisecom(config-port)#exit
```

Checking results

Use the command **show interface port** *port-id* **vlan-mapping** {**ingress** | **egress**} **translate** to show 1:1 VLAN transition configuration.

```
Raisecom#show interface port 7 vlan-mapping engress translate
Direction: Egress
Port  Outer VLAN  Customer VLAN List           Provider VLAN List
------------------------------------------------------------------------
7    100          n/a                                  1000
7    200          n/a                                  2008
Raisecom#show interface port 7 vlan-mapping engress translate
Direction: Ingress
Port  Outer VLAN  Customer VLAN List           Provider VLAN List
------------------------------------------------------------------------
7    1000         n/a                                   100
7    2008         n/a                                   200
```

9 Configuring STP

The chapter introduces STP (Spanning Tree Protocol) configuration information and procedure of ISCOM5508 device, and provides related configuration applications.

- Configuring STP
- Configuring MSTP
- Configuring RSTP of ONU
- Maintenance
- Configuration examples

9.1 Configuring STP

9.1.1 Preparing for configuration

Networking situation

The equipments that is running the protocol find loop in the network through exchanging message, and stop some ports selectively, then cut the loop network structure into tree network without any loop, which stop message breeding and looping endlessly, and avoid the host's message handling ability to decline because of receiving the same message.

Precondition

Users should configure physical parameters of ports before configuring VLAN, and physical layer state of port is up.

STP has the same function with port backup and Ethernet ring, so they can't be enabled at the same time. Disable port backup and Ethernet ring functions before configuring STP.

9.1.2 Default configuration of STP protocol

Function	Default value
global STP function	disable
port STP function	Enable

Function	Default value
system STP priority	32768
port STP priority	128
path cost of port	0

9.1.3 Enabling STP

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**spanning-tree mode stp**	Configure spanning tree mode as STP mode;
3	Raisecom(config)#**spanning-tree enable**	Enable global STP function;
4	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
5	Raisecom(config-port)#**spanning-tree** { **enable** | disable }	(Optional) Enable /disable port STP function; **Note** If we enable global STP function, interaction of STP message will occur on uplink GE interface and PON port; so users should disable STP function on PON port after we enable global STP function;

9.1.4 Configuring STP parameters

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**spanning-tree priority** *priority-value*	(Optional) Configure system priority;
3	Raisecom(config)#**spanning-tree root** { **primary** | **secondary** }	(Optional) Configure a device as primary or secondary root device;
4	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
5	Raisecom(config-port)#**spanning-tree priority** *priority-value*	(Optional) Configure priority of port;
6	Raisecom(config-port)#**spanning-tree inter-path-cost** *cost-value*	(Optional) Configure inner path cost of port;

Step	Configuration	Description
7	Raisecom(config-port)#**spanning-tree extern-path-cost** *cost-value*	(Optional) Configure outer path cost of port;

9.1.5 Checking configuration

No.	Item	Description
1	Raisecom#**show spanning-tree**	Show STP basic configuration;
2	Raisecom#**show spanning-tree port** *port-id*	Show spanning tree configuration on port;

9.2 Configuring MSTP

9.2.1 Preparing for configuration

Networking situation

In large-scale LAN or small domain convergence, there is a ring among convergence devices working as backup of line and sharing load of service. MSTP protocol can choose different and unique forwarding path for a VLAN or a group of VLANs.

Precondition

Users should configure physical parameters of ports before configuring MSTP, and physical layer state of port is up.

MSTP has the same function with port backup and Ethernet ring, so they can't be enabled at the same time. Disable port backup and Ethernet ring functions before configuring MSTP.

9.2.2 Default configuration of MSTP protocol

Function	Default value
global MSTP function	disable
port MSTP function	enable
The maximum number of hops in MST field	20
Priority of system	32768
Priority of port	128
path cost of port	0
The maximum number of sending messages in each hellotime	3

Function	Default value
max-age timer	20s
hello-time timer	2s
forward-delay timer	15s
Revision levels of MST field	0

9.2.3 Enabling MSTP

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode;
2	`Raisecom(config)#spanning-tree mode mstp`	Configure spanning tree mode as MSTP mode;
3	`Raisecom(config)#spanning-tree enable`	Enable global MSTP function;
4	`Raisecom(config)#interface port` *port-id*	Enter port configuration mode on physical layer;
5	`Raisecom(config-port)#spanning-tree { enable | disable }`	(Optional) Enable /disable port MSTP function; **Note** If we enable global MSTP function, interaction of MSTP message will occur on uplink GE interface and PON port; so users should disable MSTP function on PON port after we enable global MSTP function;

9.2.4 Configuring MST and the maximum number of hops in MST field

When the switch running in MSTP mode, the switch can be configured the region information where it belongs to. Which MST region a switch belongs to is determined by the region name, VLAN mapping table and MSTP modification configuration. By the following steps user can put the current switch into a special MST region

MST region maximum hop number confines the scope of MST region. Only when the configured switch is the region root, can the configured maximum hop number be taken as MST region maximum hop number, while other not-region root switches configuration is not valid on it. From the root switch of the spanning tree in the region, BPDU in the region hop number will decrease by 1 when transmitted by one switch, and the switch will drop the configuration information that receives 0 hop number. It will make the switch that is out of the max hop number not being able to take part in the spanning tree calculation, which confines the scope of MST region.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**spanning-tree region-configuration**	Enter configuration mode of MST field;
3	Raisecom(config-region)#**name** *name*	Configure name of MST field;
4	Raisecom(config-region)#**revision-level** *level-value*	Configure revision level of MST field;
5	Raisecom(config-region)#**instance** *instance-id* **vlan** *vlan-id*	Set mapping relationship from VLAN to instance of MST field;
6	Raisecom(config-region)#**exit**	Exit MST field ;
7	Raisecom(config)#**spanning-tree max-hops** *hops-value*	Configure the maximum number of hops in MST field of device;

Note

Configured max-hop works as max-hop of MST field only if configured field is region root.

9.2.5 Configuring primary and secondary root

MSTP can configure the switch priority, and then after a spanning tree calculation, to determine the root of the tree root switch to back up or exchange; On the other hand, the user can also specify the order directly. It should be noted that if the root switch designated direct way, then the whole network, users can not modify the proposed switch to any of the priority; Otherwise, the root cause designated switch or switch back up the root is invalid.

When the roots switch failure or shutdown, the switch can replace the backup root root switch into the corresponding instance of the root switch. However, at this time if the user has set up a new root switch, then switch back up the root will not be a root switch. If a user to configure a number of applications spanning tree root switch back up, when the root switch fails, MSTP will choose the smallest of the MAC address of the switch as a backup root switch.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**spanning-tree** [**instance** *instance-id*] **root** { **primary** | **secondary** }	Configure the device as primary or secondary root bridge for a STP instance;

Note

- Users can instance instance-id parameter to determine the root switch, or switch to back up the root of the entry into force of instance. If the instance-id value is 0, or omit parameters instance instance-id, the current switch will be designated as the root of the CIST or switch to back up the root switch.

- In the instance of the current switch in the type of root is independent of each other, that is, it can be used as an instance of the root switch or switch back up the root, at the same time as other applications of tree roots or switch to back up the root switch. But at the same instance of a tree, the same cannot switch it as a root switch and root as a backup switch.
- At the same time, the user can not be designated as an instance of spanning tree two or more root switch; On the contrary, the user can specify multiple spanning tree with a back-up roots. Under normal circumstances, the proposal for a user to specify a spanning tree roots and a number of back-up roots.

9.2.6 Configuring priority of system and port

Spanning tree protocol spanning tree calculation, the elections need to root port (root port) and designated ports (designated port), in the path of the port costs in line under the premise of the port-side ID of the smaller ports more vulnerable to root for the election or designated port. Users can set up port priority, to reduce port ID, and then there's the purpose of controlling spanning tree protocol to choose a specific port to become the root port or the designated port. With the same priority, the port that has smaller number has higher priority.

Bridge ID switch determines if the size of this switch can be selected as the root of the tree. Through the allocation of a smaller priority, the smaller switches Bridge ID can be got so that a certain switch can be the spanning tree root. Priority same, small MAC address for the small roots.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**spanning-tree** [**instance** *instance-id*] **priority** *priority-value*	Configure system priority of device for a STP instance; *priority-value*: a integer and range is 0–61440;
3	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
4	Raisecom(config-port)#**spanning-tree** [**instance** *instance-id*] **priority** *priority-value*	Configure port priority for a STP instance;

Value of priority must be a multiple of 4096, and default value is 32768.

9.2.7 Configuring network diameter of switching network

RSTP in the agreement, the network diameter refers to the number of switches in the network to exchange up to the path that, switch the number of nodes. MSTP in the agreement, the network diameter settings only effective CIST for example MSTI invalid. And in the same region, no matter how many nodes path, just as a computing node. This fact, the network should be defined as the diameter across the region up to that path, the number of regions. If the network has only one region, then running network diameter is 1.

MST with the region of the largest jump a few similar, if and only if the switch configuration for the CIST root switch, configure the entry into force.

Comparison of the MST's largest region is used to jump a few region characterization of the size of the network diameter is the characterization of the entire network of the size of a parameter. Network that the greater the diameter of a larger network.

When the user switches to configure the network parameters in diameter, MSTP through the switch will automatically calculate the Hello Time, Forward Delay, and Max Age three times to set the parameters for a better value.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**spanning-tree bridge-diameter** *bridge-diameter-value*	Set diameter of switching network;

9.2.8 Configuring inner path cost of port

When STP is computing the spanning tree, it is needed to vote root port and designated port, the less the port patch costs, the easier the port be voted as root port or designated port.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-port)#**spanning-tree** [**instance** *instance-id*] **inter-path-cost** *cost-value*	Configure inner path cost of port for a STP instance;

9.2.9 Configuring outer path cost of path

Outer path cost is path cost from devices to CIST total root, and outer path cost in a field ia the same.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-config)#**spanning-tree extern-path-cost** *cost-value*	Configure outer path cost of port;

9.2.10 Configuring the maximum sending rate of interface

Use the command to configure the maximum BPDU number that is allowed to be sent every Hello Time for MSTP. This parameter is a relative value, not units, the configuration parameters have been greater, each with Hello Time allowed to send the message, the more the number, but also will take up more resources to switch. With the same parameters of the time, only the root switch configuration comes into force.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**spanning-tree transit-limit** *value*	Configure the maximum sending rate of port;

9.2.11 Configuring MSTP timer

There are three time parameter: Forward Delay, Hello Time and Max Age:

- Hello Time: the time interval of the switch's sending BPDU, which is used to determine if there is fault in the link. Every Hello Time the switch will send hello message to the switches nearby to make sure if there is fault with the link. The default value is 2s, user can change the value according to the network state. If there is frequent change in network links, the value can be shortened in a certain degree to enhance STP stability. On the opposite, enlarging the value will decrease STP resource taken rate to the system CPU.
- Forward Delay: to make sure the time parameter of the switch state safe transformation. Link fault will bring in the re-computing of the spanning tree and the corresponding change of the network structure, but the new configuration information that is re-computed cannot spread all through the network. If the newly elected root port and designated port started immediately transmit the data, may cause a temporary path of the loop. To this end an agreement to adopt a state transfer mechanism: the root port and designated port will go through a betweenness before data re-transmission (state of learning), a state in the middle Forward Delay after delay of time before they can enter the state forward. The delay to ensure that the new configuration information has been spread throughout the network. Default value is 15 seconds, and the user can adjust the value of the actual situation, when the network topology changes frequently are not able to reduce the value, increasing the contrary.
- Max Age: the bridge configuration information that is used by the spanning tree protocol has life cycle to determine whether the configuration information is out of date. The switch will discard the configuration information out of date. When the bridge configuration information expired, spanning tree protocol will be re-spanning tree. Default is 20 seconds, the value is too small will lead to weight spanning tree calculation too often, too much will lead to spanning tree protocol in a timely manner cannot adapt to the network topology.

The entire network to exchange all of the switches used CIST root switch on the three parameters of the time, only in the root switch configuration on the entry into force. Specific configuration steps are as follows:

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**spanning-tree hello-time** *value*	Configure value of Hello Time;
	Raisecom(config)#**spanning-tree forward-delay** *value*	Configure value of Forward Delay;
	Raisecom(config)#**spanning-tree max-age** *value*	Configure value of Max Age;

Note

If users modify value of Hello Time, it leads to change of Forward Delay and Max Age. The formula as below:

- MaxAge=(4+network diameter/2) * HelloTime +network diameter- 1 - ((HelloTime + 1)/2)*((network diameter+ 1)/2), and MaxAge is less than 6, MaxAge =6; MaxAge is more than 40, MaxAge =40.
- If ((HelloTime + 1) * network diameter)/2 equals to 0, ForwardDelay= 2* HelloTime + ((HelloTime + 1) *network diameter)/2; otherwiseForwardDelay = 2* HelloTime + ((HelloTime + 1) *network diameter)/2 + 1; if ForwardDelay is less than 4, ForwardDelay=4; if ForwardDelay is more than 30, ForwardDelay=30.
- If configured value goes beyond range between 4 <= ForwardDelay <= 30 and ForwardDelay >= MaxAge/2 + 1, return fails, it prompts wrong information.

Value of Forward Delay will change if value of max-age changes, the formula:

- ForwardDelay = 4 if three quarters of MaxAge is less than 4;
- Otherwise, ForwardDelay = 30 if three quarters of MaxAge is more than 30;
- Otherwise, ForwardDelay= 3/4 * HelloTime
- If configured value goes beyond range between6 <= MaxAge <= 40 and MaxAge >= 2* HelloTime + 1, return fails, it prompts wrong information.

9.2.12 Configuring edge port

Edge port: the port that has no direct connection to the switch or indirect connection to any switch through the network.

Configure the edge port so that the port state can transform into transmission state rapidly, without waiting for; for Ethernet port that is has direct connection with user's terminal equipment, it is supposed to be set to edge port for rapid transformation to transmission state.

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode;
2	`Raisecom(config)#interface port` *port-id*	Enter port configuration mode on physical layer;
3	`Raisecom(config-port)#spanning-tree edged-port { auto | force-true | force-false }`	Configure edged port attribute of port;

9.2.13 Configuring types of links

By transmitting synchronal message the two ports that is connected by point to point link can move to transmission state rapidly, which reduces the unnecessary transmission delay. By default, MSTP set the link type of the port according to duplex state. Full duplex port is seen as point to point link, while half duplex port is seen as shared link.

Users can configure by hand to force the current Ethernet ports and point-to-point links connected, but the system will get into trouble if the link is not point to point link, usually it is supposed that this configuration is set to be auto so that the system will find out if the ports are connected with point to point link.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-port)#**spanning-tree link-type** { **point-to-point** | **shared** }	Configure link type of port;

9.2.14 Configuring rootguard

Reselect when the bridge received a packet in higher priority, but the new elections weak network connectivity, and consumes CPU resources. As for the network with MSTP enabled, if someone send higher-priority BPDU message to attack, networks would be instable caused by continual election. But generally speaking, each bridge priority has been configured in the network planning stage, the more edge, the lower priority. Therefore, down streaming port generally will not received the highest priority packet than that of the bridge, unless of malicious attacks. For these ports, users can open rootguard, and refused to deal with the packet with high priority than bridge. If received higher-priority packet, it will block ports for a period of time, to prevent more attacks against upper link.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-port)#**spanning-tree rootguard** { **enable** | **disable** }	Configure root port protection attribute of port;

9.2.15 Configuring port loopguard

Spanning tree has two main functions: prevent loop back and link backup. Loopback prevention requires a topological cut in a tree shape, and link backup needed when the topology has redundant links. Spanning tree is through the obstruction to prevent loopback, and when the link has the failure, enable redundant links for link backup function.

Spanning tree module would periodically exchanged messages, if in a certain time didn't receive a message that regard it as link failures. Then take the election, freeing the backup port. But in practical applications, it may not caused by link failures. In this case, if release the backup port , it will bring a loop back .

The loopguard will not selection when the port in a certain period of time does't receive a message, , keep original condition.

Note

The loopguard and link backup are opposite, i.e. they will not take effect at the same time.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-port)#**spanning-tree loopguard** { **enable** | **disable** }	Configure loopback protection attribute of port;

9.2.16 Executing mcheck operation

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-port)#**spanning-tree mcheck**	Proceed mcheck operation to return port to MSTP mode forcibly;

9.2.17 Checking configuration

No.	Item	Description
1	Raisecom#**show spanning-tree**	Show STP basic configuration;
2	Raisecom#**show spanning-tree** [**instance** *instance-id*] **port** *port-list* [**detail**]	Show spanning tree configuration on port;
3	Raisecom#**show spanning-tree region-configuration**	Show MST field configuration

9.3 Configuring RSTP of ONU

9.3.1 Preparing for configuration

Networking situation

Configure RSTP on ONU for preventing broadcast storm or network meltdown because of loop of network. UNI and user network form tree network topology to avoid loss.

Precondition

RSTP is mutually exclusive with loop detection and BPDU transmission transparently mode. So note the following preconditions before enabling RSTP:

- Disable loop detection of all ONU Ethernet port;
- Configure BPDU transmission transparently mode as end mode.

9.3.2 Default configuration of RSTP protocol

Function	Default value
ONU RSTP function	disable
Priority of RSTP system	32768
Priority of RSTP port	128
Whether UNI is edged port or not	yes
path cost	0

9.3.3 Configuring RSTP of ONU

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**spanning-tree enable**	Enable RSTP function;

9.3.4 Configuring RSTP parameters of ONU

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**spanning-tree priority** *priority-value*	Configure priority of RSTP system;
4	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter ONU UNI Ethernet port configuration mode;
5	Raisecom(fttx-onu-uni*/*/*:*)#**spanning-tree priority** *priority-value*	Configure priority of RSTP port of UNI;
6	Raisecom(fttx-onu-uni*/*/*:*)#**spanning-tree edged-port**	Configure UNI as edged port;
7	Raisecom(fttx-onu-uni*/*/*:*)#**spanning-tree path-cost** *value*	Configure path cost;

9.3.5 Checking configuration

No.	Item	Description
1	Raisecom(fttx)#**show interface onu** *slot-id/olt-id/onu-id* **spanning-tree**	Show spanning tree configuration of ONU;
2	Raisecom(fttx)#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** [*uni-id*] **spanning-tree** [**statistics**]	Show spanning tree configuration and statistics of UNI;

9.4 Maintenance

Command	Description
Raisecom(fttx)#**clear interface onu** *slot-id/olt-id/onu-id* **uni ethernet** *uni-id* **spanning-tree statistic**	Clear spanning tree statistics data of ONU UNI port;

9.5 Configuration examples

9.5.1 Examples for configuring STP

Networking requirements

As shown in below figure, three devices ISCOM5508 A, ISCOM5508 B and ISCOM5508 C are formed into a ring. Users need to solve loop problem in physical link, so they need enable STP on the three devices, set priority of ISCOM5508 A as 0, and set path cost from ISCOM5508 B to ISCOM5508 A as 10.

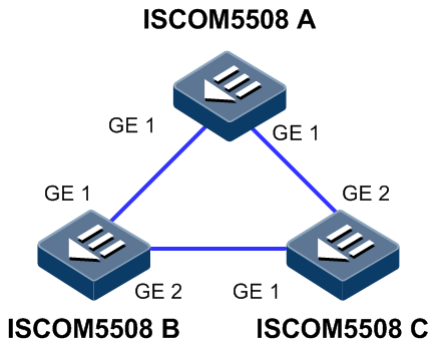

Figure 9-1 STP networking

Configuration steps

Step 1 Enable STP function on the three devices.

Configure ISCOM5508 A.

```
Raisecom#config
Raisecom(config)#spanning-tree enable
Raisecom(config)#spanning-tree mode stp
```

Configure ISCOM5508 B.

```
Raisecom#config
Raisecom(config)#spanning-tree enable
Raisecom(config)#spanning-tree mode stp
```

Configure ISCOM5508 C.

```
Raisecom#config
Raisecom(config)#spanning-tree enable
Raisecom(config)#spanning-tree mode stp
```

Step 2 configure port mode of the three devices.

Configure ISCOM5508 A.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
```

Configure ISCOM5508 B.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
```

Configure ISCOM5508 C.

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

```
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
```

Step 3 Configure priority of spanning tree and path cost of port.

Configure ISCOM5508 A.

```
Raisecom(config)#spanning-tree priority 0
Raisecom(config)#interface port 2
Raisecom(config-port)#spanning-tree extern-path-cost 10
Raisecom(config-port)#exit
```

Configure ISCOM5508 B.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#spanning-tree extern-path-cost 10
Raisecom(config-port)#exit
```

Checking results

Show bridge status.

- ISCOM5508 A

```
Raisecom#show spanning-tree
MSTP Admin State: Enable
Protocol Mode: STP
BridgeId:    Mac 000E.5E7B.C557  Priority 0
Root:       Mac 000E.5E7B.C557  Priority 0   RootCost 0
Operational:  HelloTime 2, ForwardDelay 15, MaxAge 20
Configured:   HelloTime 2, ForwardDelay 15, MaxAge 20 TransmitLimit 3
```

- ISCOM5508 B

```
Raisecom#show spanning-tree
MSTP Admin State: Enable
Protocol Mode: STP
BridgeId:    Mac 000E.5E83.ABD1  Priority 32768
Root:       Mac 000E.5E7B.C557  Priority 0   RootCost 10
Operational:  HelloTime 2, ForwardDelay 15, MaxAge 20
Configured:   HelloTime 2, ForwardDelay 15, MaxAge 20 TransmitLimit 3
```

- ISCOM5508 C

```
Raisecom#show spanning-tree
MSTP Admin State: Enable
Protocol Mode: STP
BridgeId:    Mac 000E.5E83.ABD5  Priority 32768
Root:       Mac 000E.5E7B.C557  Priority 0    RootCost 20000
Operational:  HelloTime 2, ForwardDelay 15, MaxAge 20
Configured:   HelloTime 2, ForwardDelay 15, MaxAge 20 TransmitLimit 3
```

Show port status.

- ISCOM5508 A

```
Raisecom#show spanning-tree port 1,2
Port ID:port 1
PortEnable: admin: enable       oper: enable
Rootguard:  disable
Loopguard:  disable
ExternPathCost:10
Partner MSTP Mode: stp
Bpdus send:   279  (TCN<0>   Config<279>  RST<0>  MST<0>)
Bpdus received:13  (TCN<13>   Config<0>  RST<0>  MST<0>)
State:forwarding  Role:designated     Priority:128   Cost: 20000
Root:       Mac 000E.5E7B.C557  Priority 0    RootCost 0
DesignatedBridge: Mac 000E.5E7B.C557  Priority 0    DesignatedPort 32777

Port ID:port 2
PortEnable: admin: enable       oper: enable
Rootguard:  disable
Loopguard:  disable
ExternPathCost:20000
Partner MSTP Mode: stp
Bpdus send:   279  (TCN<0>   Config<279>  RST<0>  MST<0>)
Bpdus received:6  (TCN<6>   Config<0>  RST<0>  MST<0>)
State:forwarding  Role:designated     Priority:128   Cost: 20000
Root:       Mac 000E.5E7B.C557  Priority 0    RootCost 0
DesignatedBridge: Mac 000E.5E7B.C557  Priority 0    DesignatedPort 32778
```

- ISCOM5508 B

```
Raisecom#show spanning-tree port 1,2
Port ID:port 1
PortEnable: admin: enable       oper: enable
Rootguard:  disable
Loopguard:  disable
ExternPathCost:10
Partner MSTP Mode: stp
Bpdus send:   357  (TCN<0>   Config<357>  RST<0>  MST<0>)
```

```
Bpdus received:13  (TCN<12>    Config<1>  RST<0>  MST<0>)
State:forwarding  Role:designated     Priority:128   Cost: 20000
Root:       Mac 000E.5E7B.C557  Priority 0    RootCost 10
DesignatedBridge: Mac 000E.5E7B.C557  Priority 0    DesignatedPort 32777
Port ID:port 2
PortEnable: admin: enable       oper: enable
Rootguard:  disable
Loopguard:  disable
ExternPathCost:20000
Partner MSTP Mode: stp
Bpdus send:    36  (TCN<13>    Config<23>  RST<0>  MST<0>)
Bpdus received:335  (TCN<0>    Config<335>  RST<0>  MST<0>)
State:forwarding  Role:root     Priority:128   Cost: 20000
Root:       Mac 000E.5E7B.C557  Priority 0    RootCost 20000
DesignatedBridge: Mac 000E.5E83.ABD1  Priority 32768    DesignatedPort
32777
```

- ISCOM5508 C

```
Raisecom#show spanning-tree port 1,2
Port ID:port 1
PortEnable: admin: enable       oper: enable
Rootguard:  disable
Loopguard:  disable
ExternPathCost:20000
Partner MSTP Mode: stp
Bpdus send:    22  (TCN<12>    Config<10>  RST<0>  MST<0>)
Bpdus received:390  (TCN<0>    Config<390>  RST<0>  MST<0>)
State:blocking  Role:non-designated     Priority:128   Cost: 20000
Root:       Mac 000E.5E7B.C557  Priority 0    RootCost 20000
DesignatedBridge: Mac 000E.5E83.ABD1  Priority 32768    DesignatedPort
32777

Port ID:port 2
PortEnable: admin: enable       oper: enable
Rootguard:  disable
Loopguard:  disable
ExternPathCost:20000
Partner MSTP Mode: stp
Bpdus send:    38  (TCN<6>    Config<32>  RST<0>  MST<0>)
Bpdus received:368  (TCN<0>    Config<368>  RST<0>  MST<0>)
State:forwarding  Role:root     Priority:128   Cost: 20000
Root:       Mac 000E.5E7B.C557  Priority 0    RootCost 0
DesignatedBridge: Mac 000E.5E7B.C557  Priority 0    DesignatedPort 32778
```

9.5.2 Examples for configuring MSTP

Networking requirements

As shown in below figure, three devices ISCOM5508 A, B, C are formed a ring and run MSTP protocol, field name is aaa. Where, ISCOM5508 B and ISCOM5508 C connect with two PC respectively which belong to VLAN 3 and VLAN 4 respectively. Instance 3 associate VLAN 3 and Instance 4 associate VLAN 4. Users should configure path cost of ISCOM5508 B in instance 3 to transform messages of two VLAN in two paths respectively, in order to realize load sharing and remove the loop.

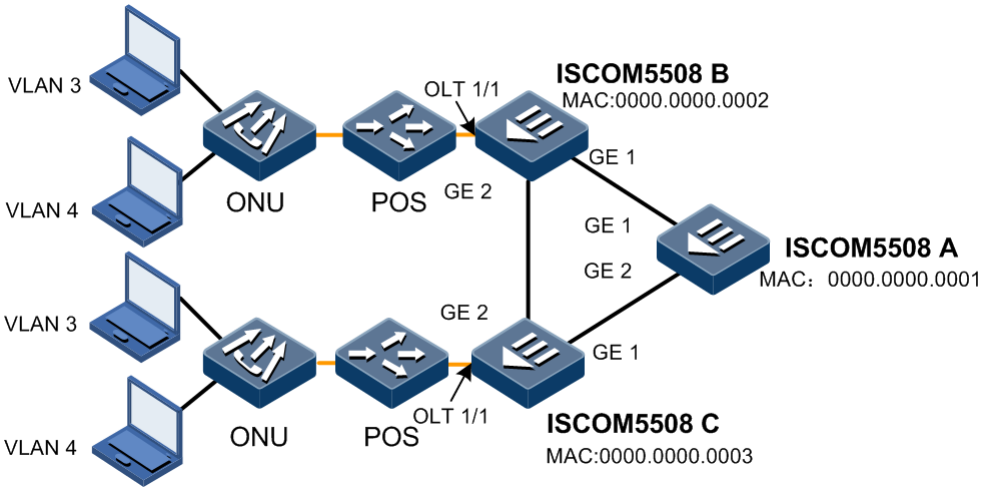

Figure 9-2 MSTP networking

Configuration steps

Step 1 Create and activate VLAN 3 and VLAN 4 on the three OLT respectively.

Configure ISCOM5508 A.

```
Raisecom#config
Raisecom(config)#create vlan 3-4 active
```

Configure ISCOM5508 B.

```
Raisecom#config
Raisecom(config)#create vlan 3-4 active
```

Configure ISCOM5508 C.

```
Raisecom#config
Raisecom(config)#create vlan 3-4 active
```

Step 2 Uplink port GE1, GE2 of ISCOM5508 A with trunk mode allow all VLAN to pass, uplink port GE1, GE2 of ISCOM5508 B with trunk mode allow all VLAN to pass, uplink port GE1, GE2 of ISCOM5508 C with trunk mode allow all VLAN to pass. Downlink PON port GE1 of ISCOM5508 B, ISCOM5508 C with trunk mode allow VLAN 3, VLAN 4 to pass.

Configure ISCOM5508 A.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
```

Configure ISCOM5508 B.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 7
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 3,4
Raisecom(config-port)#exit
```

Configure ISCOM5508 C.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 7
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 3,4
Raisecom(config-port)#exit
```

Step 3 ISCOM5508 A, ISCOM5508 B, ISCOM5508 C set spanning tree mode as MSTP, and enable STP. Enter MSTP configuration mode and set field name as aaa, revision version as 0, instance 3 associate VLAN 3, instance 4 associate VLAN 4.

Configure ISCOM5508 A.

```
Raisecom(config)#spanning-tree mode mstp
Raisecom(config)#spanning-tree enable
Raisecom(config)#spanning-tree region-configuration
Raisecom(config-region)#name aaa
Raisecom(config-region)#revision-level 0
Raisecom(config-region)#instance 3 vlan 3
Raisecom(config-region)#instance 4 vlan 4
Raisecom(config-region)#exit
```

Configure ISCOM5508 B.

```
Raisecom(config)#spanning-tree mode mstp
Raisecom(config)#spanning-tree enable
Raisecom(config)#spanning-tree region-configuration
Raisecom(config-region)#name aaa
Raisecom(config-region)#revision-level 0
Raisecom(config-region)#instance 3 vlan 3
Raisecom(config-region)#instance 4 vlan 4
Raisecom(config-region)#exit
```

Configure ISCOM5508 C.

```
Raisecom(config)#spanning-tree mode mstp
Raisecom(config)#spanning-tree enable
Raisecom(config)#spanning-tree region-configuration
Raisecom(config-region)#name aaa
Raisecom(config-region)#revision-level 0
Raisecom(config-region)#instance 3 vlan 3
Raisecom(config-region)#instance 4 vlan 4
Raisecom(config-region)#exit
```

Step 4 ISCOM5508 B modifies inner path cost of port GE 1 in spanning tree instance 3 as 500000.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#spanning-tree instance 3 inter-path-cost 500000
Raisecom(config-port)#exit
```

Checking results

Show configuration of MST field.

```
Raisecom#show spanning-tree region-operation
Operational:
-----------------------------------------------
```

```
Name: aaa
Revision level: 0       Instances running: 3
Digest: 0x024E1CF7E14D5DBBD9F8E059D2C683AA
Instance     Vlans Mapped
--------     ---------------------
0          1,2,5-4094
3          3
4          4
```

Show whether basic information of MSTP instance 3 is correct.

- ISCOM5508 A

```
Raisecom#show spanning-tree instance 3
MSTP Admin State: Enable
Protocol Mode: MSTP
MST ID: 3
------------------------------------------------------------
BridgeId:    Mac 0000.0000.0001  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost 0
PortId  PortState   PortRole   PathCost  PortPriority  LinkType   TrunkPort
------------------------------------------------------------------------
1      forwarding  designated 20000    128         point-to-point  no
2      forwarding  designated 20000    128         point-to-point  no
```

- ISCOM5508 B

```
Raisecom#show spanning-tree instance 3
MSTP Admin State: Enable
Protocol Mode: MSTP
MST ID: 3
------------------------------------------------------------
BridgeId:    Mac 0000.0000.0002  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost 40000
PortId  PortState   PortRole   PathCost  PortPriority  LinkType   TrunkPort
------------------------------------------------------------------------
1      discarding  alternate  500000    128          point-to-point  no
2      forwarding  root       20000    128         point-to-point  no
7      forwarding  designated 20000    128          point-to-point  no
```

- ISCOM5508 C

```
Raisecom#show spanning-tree instance 3
MSTP Admin State: Enable
Protocol Mode: MSTP
MST ID: 3
------------------------------------------------------------
```

```
BridgeId:    Mac 0000.0000.0003  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost 20000
PortId  PortState   PortRole   PathCost  PortPriority  LinkType   TrunkPort
--------------------------------------------------------------------------
1      forwarding  root       20000    128         point-to-point  no
2      forwarding  designated 20000    128          point-to-point  no
7      forwarding  designated 20000    128          point-to-point  no
```

Show whether basic information of MSTP instance 4 is correct.

- ISCOM5508 A

```
Raisecom#show spanning-tree instance 4
MSTP Admin State: Enable
Protocol Mode: MSTP
MST ID: 4
------------------------------------------------------------
BridgeId:    Mac 0000.0000.0001  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost 0
PortId  PortState   PortRole   PathCost  PortPriority  LinkType   TrunkPort
--------------------------------------------------------------------------
1      forwarding  designated 20000    128          point-to-point  no
2      forwarding  designated 20000    128          point-to-point  no
```

- ISCOM5508 B

```
Raisecom#show spanning-tree instance 4
MSTP Admin State: Enable
Protocol Mode: MSTP
MST ID: 4
------------------------------------------------------------
BridgeId:    Mac 0000.0000.0002  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost 20000
PortId  PortState   PortRole   PathCost  PortPriority  LinkType   TrunkPort
--------------------------------------------------------------------------
1      forwarding  root      200000    128          point-to-point  no
2      forwarding  designated 20000    128         point-to-point  no
7      forwarding  designated   20000    128          point-to-point  no
```

- ISCOM5508 C

```
Raisecom#show spanning-tree instance 4
MSTP Admin State: Enable
Protocol Mode: MSTP
MST ID: 4
------------------------------------------------------------
BridgeId:    Mac 0000.0000.0003  Priority 32768
```

```
RegionalRoot: Mac 0000.0000.0001  Priority 32768    InternalRootCost 20000
PortId  PortState   PortRole   PathCost  PortPriority  LinkType  TrunkPort
--------------------------------------------------------------------------
1       forwarding  root       20000    128          point-to-point  no
2       discarding  alternate  200000    128          point-to-point  no
7       forwarding  designated   20000    128          point-to-point  no
```

9.5.3 Examples for configuring ONU RSTP

Networking requirements

As shown in below figure, user PC connects with UNI 1, ONU suspend on OLT1/1. Enable RSTP function on ONU to prevent generation of broadcast storm, in order to prevent presence of loop in network.

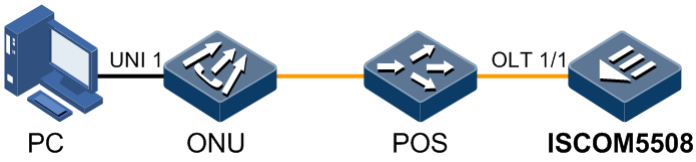

Figure 9-3 ONU RSTP application

Configuration steps

Step 1 Enable RSTP function of ONU.

```
Raisecom#fttx
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#spanning-tree enable
Raisecom(fttx-onu1/1:1)#exit
```

Checking results

Show RSTP configuration of ONU.

```
Raisecom(fttx)#show interface onu 1/1/1 spanning-tree
ONU ID: 1/1/1
    Admin state             : enable
    Mode                   : RSTP
    Priority               : 32768
    Max-age-time            : 0s
    Bridge max-age-time      : 20s
    Hello time             : 0s
    Bridge hello time        : 2s
    Hold time              : 0s
    Forward delay           : 0s
    Bridge forward delay     : 15s
```

```
Root bridge ID          : 000E.5E12.3456(priority-MAC)
Root port ID           : 0
Root cost              : 0
Default path cost  version: stp8021t2001
Max transmission limit    : 3(per hello time)
Protocol specification    : ieee8021d
Time since topology change: 0 days 0 hours 0 minutes
Topology change times     : 0
```

10 Configuring route

The chapter introduces function deployment and procedure of route in ISCOM5508 device, and provides related configuration applications.

- Configuring ARP
- Configuring ARP Proxy
- Configuring static route
- Configuring RIP
- Configuring OSPF
- Maintenance
- Configuration examples

10.1 Configuring ARP

10.1.1 Preparing for configuration

Networking situation

Mapping of IP address and MAC address is saved in mapping table of ARP address.

In general, entries of ARP address mapping are maintained by devices dynamically, and the devices search mapping relation between IP address and MAC address according to ARP protocol automatically. Users need to add entries of static ARP address mapping manually to prevent dynamic ARP learning bam.

10.1.2 Default configuration of ARP

Function	Default value
Static ARP entries	N/A
Aging time of dynamic ARP entries	1200s
Learning mode of dynamic ARP	learn-reply-only

10.1.3 Configuring static ARP entries

- IP address of ARP entries added statically must belong to IP segment which interface belongs to.
- Users need add and delete ARP entries manually.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**arp** *ip-address mac-address*	Configure static ARP entries ;

10.1.4 Configuring dynamic ARP entries

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**arp aging-time** { **0** | *second* }	(Optional) Configure aging time of dynamic ARP entries, the device will delete the ARP dynamic entries which exceed aging time; *0*: no aging;
3	Raisecom(config)#**arp mode** { **learn-all** | **learn-reply-only** }	(Optional) Configure learning mode of dynamic ARP entries;

ARP dynamic entries won't age if users configure aging time of ARP entries as 0s.

10.1.5 Checking configuration

No.	Item	Description
1	Raisecom#**show arp**	Show whether all entry information in ARP address mapping table is correct;
2	Raisecom#**show arp** *ip-address*	Show whether ARP entry information corresponding to specific IP address is correct;
3	Raisecom#**show arp ip** *if-number*	Show whether ARP entry information corresponding to three-layer interface is correct;
4	Raisecom#**show arp static**	Show whether static ARP entry information is correct;

10.2 Configuring ARP Proxy

10.2.1 Preparing for configuration

Scenario

Before configuring ARP Proxy, you need to confirm the following scenarios:

- When needing to transmit ARP request packets across network segment, you need to enable the common ARP Proxy.
- When needing to transmit ARP request packets across ONU, you need to enable the local ARP Proxy.

Prerequisite

Before configuring ARP Proxy, you need to finish the following operations:

- Configure the Internet layer properties of the port and make the network reachable.
- Enable Layer 3 interface and related VLAN.
- Enable the route.

10.2.2 Default configuration

Default configurations about the ARP Proxy on the ISCOM5508 are shown in the following table.

Default configurations about the ARP Proxy

Function	Default value
Common ARP Proxy	Disabled
Local ARP Proxy	Disabled

10.2.3 Configuring common ARP Proxy

Please configure the common ARP Proxy on device.

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface ip` *if-number*	Enter Layer 3 interface configuration mode.
3	`Raisecom(config-ip)#proxy-arp { enable | disable }`	Enable/Disable the common ARP Proxy.

10.2.4 Configuring local ARP Proxy

Please configure the local ARP Proxy on device.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
3	Raisecom(config-ip)#**local-proxy-arp** { **enable** | **disable** }	Enable/Disable the local ARP Proxy.

10.2.5 Checking configurations

Please perform the following operation to check configuration result.

No.	Item	Description
1	Raisecom#**show proxy-arp**	Show configuration and state information about ARP Proxy.

10.3 Configuring static route

10.3.1 Preparing for configuration

Networking situation

Configure static route for simple topology structure of network. Users need configure static route manually to create a communicating network.

Precondition

Please configure IP address of interface correctly.

10.3.2 Default configuration of routing

Function	Default value
Router function	disable
default gateway	N/A
default route	0.0.0.0
default management distance of static route	1

10.3.3 Configuring default gateway

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**no ip routing**	Disable route function;
3	Raisecom(config)#**ip default-gateway** *ip-address*	Configure IP address of default gateway; **Note** If a message which will be forwarded doesn't have corresponding route in a device, use the command **ip default-gateway** to configure default gateway. It helps to forward the message to default gateway. IP address of the default gateway should stay in the same network segment with local IP address of the device.

Note

Configuration of default gateway takes effect only if route disables.

10.3.4 Configuring static route

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip routing**	Enable route function;
3	Raisecom(config)#**ip route** *ip-address ip-mask next-hop* [**distance** *value*] [**description** *description*] [**tag** *tag-id*]	Configure static route; Use **no ip route** *ip-address* [*ip-mask*] to delete static route;
4	Raisecom(config)#**ip route static distance** *value*	(Optional) Configure default management distance of IPv4;

10.3.5 Checking configuration

No.	Item	Description
1	Raisecom#**show ip route** [detail]	Show details of IPv4 route;
2	Raisecom#**show ip route ip-access-list** *acl-number* [**detail**]	Show routing information after filtering of ACL rules;
3	Raisecom#**show ip route** *ip-address* [*ip-mask*] [**longer-prefixes**] [**detail**]	Show routing information between start and a specific IP address;

No.	Item	Description
4	Raisecom#**show ip route** *ip-address ip-mask ip-address ip-mask* [**detail**]	Show routing information between start and a range of addresses;
5	Raisecom#**show ip route protocol** { **static** | **direct** | **rip** | **ospf** | **isis** }	Show routing information of a protocol;
6	Raisecom#**show ip route statistics**	Show routing statistics;
7	Raisecom#**show ip route protocol statistics**	Show routing protocol statistics;
8	Raisecom#**show router id**	Show route ID;

10.4 Configuring RIP

10.4.1 Preparing for configuration

Networking situation

RIP is a simple inner gateway protocol, and mainly used in small-scale network.

10.4.2 Default configuration of RIP

Function	Default value
global RIP function	disable
global RIP version	Send RIP1, receive RIP1 or RIP2
RIP message detect source IP address	enable
Host router Rx function	enable
RIP Tx trap function	disable
RIP management distance	120
default additional measurement of RIP	1
additional measurement of sending RIP	0
RIP timer	• Updating timer (Update) is 30s; • Aging timer (Invalid) is 180s; • Clear timer (Flush) is 120s; • Suppression timer (Suppress) is 120s.
RIP2 authentication mode	none
Whether IP interface is passive interface	no passive interface
split horizon function	enable
poison reverse function	disable

10.4.3 Configuring basic function of RIP

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**router rip**	Enable RIP, and enter RIP configuration mode;
3	Raisecom(config-rip)#**network** *net-address*	Use RIP on specific network segment;
4	Raisecom(config-rip)#**version** { **1** | **2** }	Configure global RIP version;
5	Raisecom(config-rip)#**exit** Raisecom(config)#**interface ip** *if-number*	Enter three-layer interface configuration mode;
6	Raisecom(config-ip)#**rip receive version** { **1** | **2** | **both** }	Configure RIP version of IP interface in Rx;
7	Raisecom(config-ip)#**rip send version** { **1** | **2** }	Configure RIP version of IP interface in Tx;

10.4.4 Configuring router attribute of RIP

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**router rip**	Enable RIP, and enter RIP configuration mode;
3	Raisecom(config-rip)#**distance** *value*	Configure management distance of RIP protocol;
4	Raisecom(config-rip)#**exit** Raisecom(config)#**interface ip** *if-number*	Enter three-layer interface configuration mode;
5	Raisecom(config-ip)#**rip metric-offset in** *vlaue*	Configure additional measurement when IP interface receives RIP router;
6	Raisecom(config-ip)#**rip metric-offset out** *vlaue*	Configure additional measurement when IP interface sends RIP router;

10.4.5 Configuring information distribution of router

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**router rip**	Enable RIP, and enter RIP configuration mode;
3	Raisecom(config-rip)#**host-route** { **enable** | **disable** }	Enable/disable receiving host router;
4	Raisecom(config-rip)#**exit** Raisecom(config)#**interface ip** *if-number*	Enter three-layer interface configuration mode;

Step	Configuration	Description
5	Raisecom(config-ip)#**rip passive-interface** { **enable** | **disable** }	Configure IP interface as passive interface/no passive interface;

10.4.6 Configuring RIP2 authentication

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface ip** *if-number*	Enter three-layer interface configuration mode;
3	Raisecom(config-ip)#**rip authentication-mode** { **none** | **text** | **md5** }	Configure RIP2 authentication mode of IP interface;
4	Raisecom(config-ip)#**rip authentication key-chain** *string*	Configure key-chain associating IP interface;

10.4.7 Adjusting and optimizing RIP network

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**router rip**	Enable RIP, and enter RIP configuration mode;
3	Raisecom(config-rip)#**timers** { **update** *update-value* | **invalid** *invalid-value* | **flush** *flush-value* | **suppress** *suppress-value* }	Configure RIP timer;
4	Raisecom(config-rip)#**validate-update-source** { **enable** | **disable** }	Enable/disable detection of source IP address of received RIP message;
5	Raisecom(config-rip)#**exit** Raisecom(config)#**interface ip** *if-number*	Enter three-layer interface configuration mode;
6	Raisecom(config-ip)#**rip split-horizon** { **enable** | **disable** }	Enable/disable split horizon function;
7	Raisecom(config-ip)#**rip poison-reverse** { **enable** | **disable** }	Enable/disable poison reverse function;

10.4.8 Configuring key-chain

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**key-chain** *string*	Create key chain, and enter KEYCHAIN configuration mode;

Step	Configuration	Description
3	Raisecom(config-keychain)#**key** *key-id* **key-string** [**0** | **7**] *string*	Configure key and key string;
4	Raisecom(config-keychain)#**key** key-id **accept-lifetime** *start-time* { **infinite** | *end-time* | **duration** *duration-time* }	Configure receipt time of key;
5	Raisecom(config-keychain)#**key** key-id **send-lifetime** *start-time* { **infinite** | *end-time* | **duration** *duration-time* }	Configure send time of key;
6	Raisecom(config-keychain)#**accept-tolerance** { *time* | **infinite** }	Configure receipt and tolerance time of key chain;

10.4.9 Checking configuration

No.	Item	Description
1	Raisecom#**show rip**	Show RIP global configuration and status;
2	Raisecom#**show rip database** [**ip** *if-number*]	Show database of RIP route;
3	Raisecom#**show rip ip** [**ip** *if-number*] [**statistics**]	Show RIP configuration and statistics of IP interface;
4	Raisecom#**show key-chain** [*chainname* [**key** *key-id*]]	Show key chain information;

10.5 Configuring OSPF

10.5.1 Preparing for configuration

Scenario

RIP is not suitable for large-scale network due to its slow convergence, route loopback and weak expansibility. Therefore, Open Shortest Path First (OSPF) is used to improve the network efficiency.

OSPF is a link-state routing protocol for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS).

Prerequisite

Before configuring OSPF, you need to finish the following operations:

- Configure the internet layer properties of the port and make the network reachable.
- Enable Layer 3 interface and related VLAN.

10.5.2 Default configuration

Default configurations about OSPF on the ISCOM5508 are listed in the following table.

Function	Default value
Global OSPF	Disabled
Peer OSPF event trap	Disabled
Router ID	Obtained from the router management module.
Management distance	110
Area default route cost	1
OSPF interface network type	Broadcast
OSPF interface priority	1
OSPF interface route cost	1
Time of failure for OSPF interface neighbor	• 40s (PTP network and Broadcast network) • 120s (PTMP network)
Interval for Hello packets sent by OSPF interface	• 10s (PTP network and Broadcast network) • 30s (PTMP network)
LSA retransmission time for OSPF interface	5s
LSA delat time for OSPF interface	1s
MTU for OSPF interface	Ignored
OSPF passive interface	N/A
Authentication mode for OSPF interface	No authentication
Authentication mode for OSPF area	No authentication

10.5.3 Managing OSPF process

- To enable OSPF on the ISCOM5508, you need to create a OSPF process and specify the area and network segment related to the OSPF process.
- For a specified Layer 3 interface on the ISCOM5508, if its IP address is in the network segment of some OSPF area, the specified Layer 3 interface is also in the OSPF area and OSPF is enabled on the interface.

Please manage OSPF process.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Create OSPF process and enter OSPF configuration mode. Use the **no router ospf** *process-id* command to disable the OSPF process.
3	Raisecom(config-router-ospf)#**network** ip-*address wild-card-mask* **area** *area-id*	Specify the network segment and area related to OSPF process. **Note** The *wild-card-mask* parameter indicates the mask of an IP address in reverse order. (It means 0 is changed to 1 and 1 is changed to 0.) In addition, the ISCOM5508 supports entering the mask of an IP address. The ISCOM5508 identifies a mask in reverse order by verifying whether the first number is set to 0. If the mask is not in reverse order, the ISCOM5508 will automatically make the mask in reverse orser.
4	Raisecom(config-router-ospf)#**distance** *distance*	(Optional) configuring OSPF management distance.
5	Raisecom(config-router-ospf)#**exit** Raisecom(config)#**reset ip ospf** *process-id* **process**	(Optional) reset OSPF process. **Note** • When OSPF is reset, all configurations remain unchanged. However, operation data (such as LSDB, route table, and neighbor information) and statistics are cleared. • After re-configuring router-id, you need to reset the OSPF process.

Note

OSPF process adopts manually-configured Router-ID as a preference. If there is no manually-configured Router-ID, the ISCOM5508 will automatically select a Router-ID, according to the following rules:

- If there is a Loopback interface that is configured with IP addresses, the maximum IP address of the Loopback interface will be taken as the Router-ID.
- If there is no Loopback interface that is configured with IP addresses, the maximum IP address of the IP interface will be taken as the Router-ID.
- IP addresses adopted by other OSPF processes cannot be selected.
- If no IP address is configured, the Router-ID cannot be selected. And then the OSPF process cannot be created. You must manually configure the Router-ID.

If the ISCOM5508 is configured with the Router-ID or selects the Router-id, you must reset the ISCOM5508 after modifying the Router-ID.

10.5.4 Configuring Stub area

Please configure the Stub area.

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router ospf` *process-id* `[ router-id` *router-id* `]`	Create OSPF process and enter OSPF configuration mode. Use the **no router ospf** *process-id* command to disable the OSPF process.
3	`Raisecom(config-router-ospf)#area` *area-id* `stub [ no summary ]`	Set an area to a Stub area. The **no-summary** parameter is only for ABR in Stub area. After configuration, ARB only sends type 3 LAS of the default route to the Stub area, without generating other type 3 LSA.
4	`Raisecom(config-router-ospf)#area` *area-id* `default-cost` *cost*	Configure the default route cost for Stub area. This command is only valid for configuring default route cost for ABR in Stub area.

Note

- All devices in Stub area must be configured with identical Stub properties.
- Default route cost command is valid only for ABR in Stub area.
- The backbone area canot be set to a Stub area.
- There is no Autonomous System Boundary Router (ASBR) in the Stub area.

10.5.5 Configuring OSPF network

Please configure the OSPF network.

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface ip` *if-number*	Enter Layer 3 interface configuration mode.
3	`Raisecom(config-ip)#ip ospf network { broadcast | ptmp | ptp }`	Configure Layer 3 interface network type.

10.5.6 Configuring route aggregation

Please configure route aggregation.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Create OSPF process and enter OSPF configuration mode. Use the **no router ospf** *process-id* command to disable the OSPF process.
3	Raisecom(config-router-ospf)#**area** *area-id* **range** *ip-address ip-mask* [**not-advertise**]	(Optional) configure inter-domain router aggregation.
4	Raisecom(config-router-ospf)#**summary-address** *ip-address ip-mask* [**not-advertise**] [**cost** *cost*]	(Optional) configure external route aggregation.

10.5.7 Configuring interface cost

Please configure interface cost.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
3	Raisecom(config-ip)#**ip ospf cost** *cost*	Set a value for Layer 3 interface cost.

10.5.8 Configuring OSPF route information

Please configure OSPF route information.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Create OSPF process and enter OSPF configuration mode. Use the **no router ospf** *process-id* command to disable the OSPF process.
3	Raisecom(config-router-ospf)#**import limit** *limit-value*	Configure a threshold for introduced external routes.
4	Raisecom(config-router-ospf)#**import** { **static** | **connected** | **rip** } [**cost** *cost*] [**type** { **1** | **2** }]	(Optional) introduce external route.
5	Raisecom(config-router-ospf)#**default-information originate** [**always**] [**cost** *cost*] [**type** { **1** | **2** }]	(Optional) introduce default route.

- Only active routes in the route table can be introduced.
- If numbers for introduced external routes exceeds the threshold, the additional routes cannot be introduced.
- If the threshold for introduced external routes is modified, the ISCOM5508 will re-introduce external routes.

10.5.9 Configuring OSPF timer

Please configure the OSPF passive interface.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
3	Raisecom(config-ip)#**ip ospf dead-interval** *time*	Configure the time for failure of OSPF neighbor.
4	Raisecom(config-ip)#**ip ospf hello-interval** *time*	Configure the interval for sending Hello packets.
5	Raisecom(config-ip)#**ip ospf retransmit-interval** *time*	Configure the LSA retransmission interval.
6	Raisecom(config-ip)#**ip ospf transmit-delay** *time*	Configure LSA transmission delay.

- If the network type is modified, the time for failure of OSPF neighbour and the interval for sending Hello packets will return to default setting.
- On the same interface, the time for failure of OSPF neighbour is 4 times longer than the interval for sending Hello packets.
- The LSA retransmission interval should not be over short. In general, the LSA retransmission interval should be longer than the time used sending and receiving packets once between two devices.

10.5.10 Configuring OSPF passive interface

Please configure the OSPF passive interface.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
3	Raisecom(config-ip)#**ip ospf passive-interface** { **enable** | **disable** }	Set Layer 3 interface to the OSPF passive interface.

- The passive interface cannot be used to transmit OSPF packets. Therefore, it cannot create an OSPF neighbour relationship with the peer device. However, the passive interface can receive OSPF packets and can control the transmission scope of OSPF packets.
- The directly-connected route for the passive interface will be sent out through LSA by other interfaces on the same device.

10.5.11 Configuring OSPF authentication

Configuring OSPF area authentication

Please configure the OSPF area authentication.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Create OSPF process and enter OSPF configuration mode. Use the **no router ospf** *process-id* command to disable the OSPF process.
3	Raisecom(config-router-ospf)#**area** *area-id* **authentication** { **none** | **simple** | **md5** }	Configure OSPF area authentication mode.

Configuring OSPF interface authtication

Please configure the OSPF interface authentication.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
3	Raisecom(config-ip)#**ip ospf authentication** { **none** | **simple** | **md5** }	Configure Layer 3 interface OSPF authentication mode.
4	Raisecom(config-ip)#**ip ospf authentication-key** { **simple** { **0** | **7** | *password* } | **md5** *key-id* [{ **0** | **7** | *password* } | **keychain** *keychain-name* }	Configure Layer 3 interface OSPF authentication password.

10.5.12 Ignoring MTU

Please configure to ignore MTU.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.

Step	Configuration	Description
2	Raisecom(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
3	Raisecom(config-ip)#**ip ospf mtu-ignore** { **enable** | **disable** }	Configure Layer 3 interface to ignore MTU.

10.5.13 Configuring OSPF Trap

Please configure the OSPF Trap on device.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Create OSPF process and enter OSPF configuration mode. Use the **no router ospf** *process-id* command to disable the OSPF process.
3	Raisecom(config-router-ospf)#**snmp-server ospf-trap** { **enable** | **disable** }	Enable/Disable the OSPF Trap.

10.5.14 Checking configurations

Please perform the following operations to check configuration result.

No.	Item	Description
1	Raisecom#**show ip ospf** [*process-id*]	Show configuration and state information about OSPF.
2	Raisecom#**show ip ospf** [*process-id*] **neighbor** [**ip** *if-numbe*] [*neighbor-id*] [statistics]	Show OSPF neighbor information.
3	Raisecom#**show ip ospf** [*process-id*] { **request-queue** | **retrains-queue** } [**ip** *if-numbe*] [*neighbor-id*]	Show information about OSPF request list/retrain list.
4	Raisecom#**show ip ospf** [*process-id*] **route**	Show OSPF route information.
5	Raisecom#**show ip ospf** [*process-id*] **database external** [**originate-router** *ip-address* | **self-originate**]	Show OSPF link state database and exterior route information.
6	Raisecom#**show ip ospf** [*process-id*] [**area** area-id] **database** [**router** | **network** | **summary** | **asbr**] [**originate-router** *ip-address* | **self-originate**]	Show OSPF link state database.
7	Raisecom#**show ip ospf** [*process-id*] **database statistics**	Show OSPF statistics.
8	Raisecom#**show ip ospf** [*process-id*] **border-routers**	Show area border router information.
9	Raisecom#**show ip ospf** [*process-id*] [**neighbor**] **statistics**	Show OSPF (neighbor) statistics.

No.	Item	Description
10	Raisecom#**show ip ospf** [*process-id*] **summay-address**	Show OSPF exterior route convergence information.

10.6 Maintenance

Command	Description
Rasiecom(config-rip)#**clear rip database** [**ip** *if-number*]	Clear database information of RIP route;
Rasiecom(config-rip)#**clear rip statistics** [**ip** *if-number*]	Clear RIP statistics;
Raisecom(config)#**clear ip ospf process-id statistics**	Clear OSPF statistics.

10.7 Configuration examples

10.7.1 Examples for configuring ARP

Networking requirements

As shown in below figure, ISCOM5508 device connects with host, and connects with upstream route by port GE 1. IP address of route is 192.168.1.10/24, and MAC address is 0050-8d4b-fd1e.

Users should configure aging time of dynamic ARP entries of ISCOM5508 as 600s, and configure responding static ARP entries on ISCOM5508 to increase security of communication between ISCOM5508 and route.

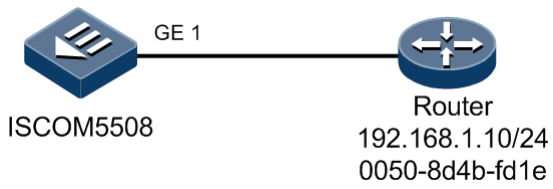

Figure 10-1 Configuring ARP

Configuration steps

Step 1 Configure aging time of dynamic ARP entries of device as 600s.

```
Raisecom#config
Raisecom(config)#arp aging-time 600
```

Step 2 Add an ARP static entry.

```
Raisecom(config)#arp 192.168.1.10 0050.8d4b.fd1e
```

Checking results

Show whether all entry information in ARP address mapping table is correct by command **show arp**.

```
Raisecom#show arp
ARP table aging-time: 600 seconds(default: 1200s)
ARP mode: Learn reply only

Ip Address       Mac Address         Type     Interface ip
-------------------------------------------------------
192.168.1.10     0050.8d4b.fd1e      static    --
Total: 1
Static: 1
Dynamic: 0
```

10.7.2 Examples for configuring static route

Networking requirements

As shown in below figure, ping between any two PC or ISCOM5508 devices.

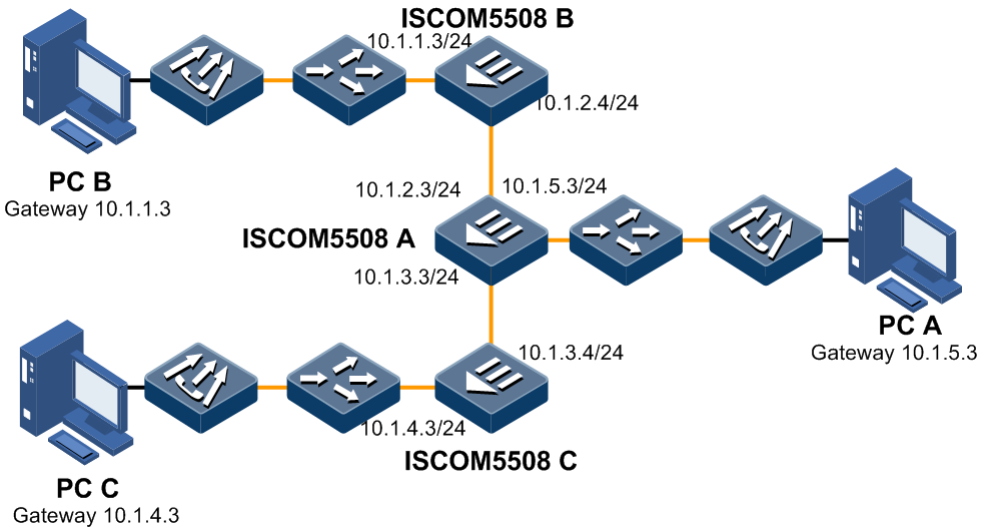

Figure 10-2 Configuring static route

Configuration steps

Step 1 Configure IP address of each device.

Step 2 Enable routing function and configure static route on ISCOM5508 A.

```
Raisecom#config
Raisecom(config)#ip routing
Raisecom(config)#ip route 10.1.1.0 255.255.255.0 10.1.2.4
Raisecom(config)#ip route 10.1.4.0 255.255.255.0 10.1.3.4
```

Step 3 Enable routing function and configure static route on ISCOM5508 B.

```
Raisecom#config
Raisecom(config)#ip routing
Raisecom(config)#ip route 10.1.5.0 255.255.255.0 10.1.2.3
Raisecom(config)#ip route 10.1.4.0 255.255.255.0 10.1.2.3
```

Step 4 Enable routing function and configure static route on ISCOM5508 C.

```
Raisecom#config
Raisecom(config)#ip routing
Raisecom(config)#ip route 10.1.1.0 255.255.255.0 10.1.3.3
Raisecom(config)#ip route 10.1.5.0 255.255.255.0 10.1.3.3
```

Step 5 Configure default gateway as 10.1.5.3 on PC A; configure default gateway as 10.1.1.3 on PC B; configure default gateway as 10.1.4.3 on PC C.

Checking results

Check whether any two devices can exchange information with each other in a ISCOM5508.

```
Raisecom#ping 10.1.1.3
Sending 5, 72-byte ICMP Echos to 10.1.1.3 , timeout is 1 seconds:
!!!!!
Success rate is 100 percent(5/5)
round-trip (ms)  min/avg/max = 0/0/0
```

10.7.3 Examples for configuring basic OSPF functions

Networking requirements

As shown in Figure 10-3, all devices in the network run OSPF protocol. The whole Autonomous System (AS) is divided into Area 0, Area 1 and Area 2, where the OLT A and OLT B are ABR and the inter-domain route for Area 0, Area 1 and Area 2. With OSPF, all devices in the network can Ping to each other and share the route information of the whole AS.

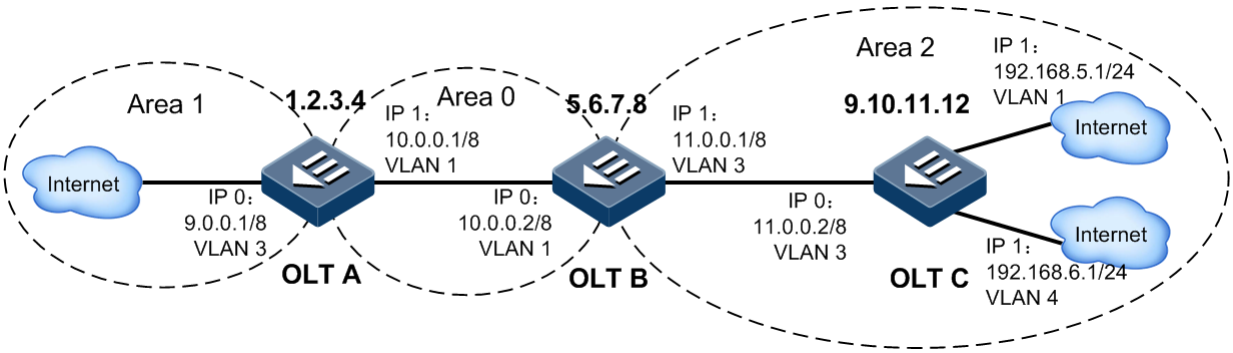

Figure 10-3 Configuring basic OSPF functions

Configuration steps

Step 1 Configure IP address and VLANs for all interfaces. Detailed commands are omitted.

Step 2 Enable Layer 3 route.

Configure OLT A.

```
Raisecom#config
Raisecom(config)#ip routing
```

Configure OLT B.

```
Raisecom#config
Raisecom(config)#ip routing
```

Configure OLT C.

```
Raisecom#config
Raisecom(config)#ip routing
```

Step 3 Configure basic OSPF functions.

Configure OLT A.

```
Raisecom(config)#router ospf 1 router-id 1.2.3.4
Raisecom(config-router-ospf)#network 9.0.0.0 0.255.255.255 area 1
Raisecom(config-router-ospf)#network 10.0.0.0 0.255.255.255 area 0
```

Configure OLT B.

```
Raisecom(config)#router ospf 1 router-id 5.6.7.8
Raisecom(config-router-ospf)#network 10.0.0.0 0.255.255.255 area 0
Raisecom(config-router-ospf)#network 11.0.0.0 0.255.255.255 area 2
```

Configure OLT C.

```
Raisecom(config)#router ospf 1 router-id 9.10.11.12
Raisecom(config-router-ospf)#network 11.0.0.0 0.255.255.255 area 2
Raisecom(config-router-ospf)#network 192.168.5.0 0.0.0.255 area 2
Raisecom(config-router-ospf)#network 192.168.6.0 0.0.0.255 area 2
```

Checking results

Use the **show ip ospf neighbor** command to check the neighbour information of the ISCOM5508, taking OLT B for an example.

```
Raisecom#show ip ospf neighbor

       OSPF Neighbor Information

   OSPF Process 1 with Router ID 5.6.7.8

Area 0.0.0.0 interface 10.0.0.2(ip0)'s neighbor(s)
RouterID: 1.2.3.4     Address: 10.0.0.1
State: Full  Mode: Slave  Priority: 1
DR: 10.0.0.2  BDR: 10.0.0.1

Area 0.0.0.2 interface 11.0.0.1(ip1)'s neighbor(s)
```

```
RouterID: 9.10.11.12     Address: 11.0.0.2
State: Full  Mode: Master  Priority: 1
DR: 11.0.0.2  BDR: 11.0.0.1
```

Use the **show ip ospf database** command to check the LSDB information of the ISCOM5508, taking OLT A for an example.

```
Raisecom#show ip ospf database

       LinkState Database Information

   OSPF Process 1 with Router ID 1.2.3.4

Area: 0.0.0.0
Type LinkState ID   AdvRouter      Age  Len  Sequence   Metric
-------------------------------------------------------------------------
Router  1.2.3.4         1.2.3.4        55   36   80000004    0
Router  5.6.7.8         5.6.7.8        56   36   80000003    0
Net  10.0.0.2         5.6.7.8        56   32   80000001    0
SumNet 9.0.0.0         1.2.3.4         93   28   80000001    1
SumNet 11.0.0.0        5.6.7.8         96   28   80000001    1
SumNet 192.168.5.0     5.6.7.8         51   28   80000001    2
SumNet 192.168.6.0     5.6.7.8         51   28   80000001    2

Area: 0.0.0.1
Type LinkState ID   AdvRouter      Age  Len  Sequence   Metric
-------------------------------------------------------------------------
Router  1.2.3.4        1.2.3.4          93   36   80000002   0
SumNet 10.0.0.0       1.2.3.4         93    28   80000001   1
SumNet 11.0.0.0       1.2.3.4        48   28    80000001   2
SumNet 192.168.5.0     1.2.3.4         48   28   80000001   3
SumNet 192.168.6.0     1.2.3.4         48   28   80000001   3
```

Use the **show ip ospf route** command to check information about the route table of the ISCOM5508, taking OLT A for an example.

```
Raisecom#show ip ospf route

       OSPF Route Information

   OSPF Process 1 with Router ID 1.2.3.4

Routing for Network
Destination     Cost   Type  NextHop        AdvRouter      Area
-------------------------------------------------------------------------
10.0.0.0/8      1     Net   10.0.0.1       5.6.7.8        0.0.0.0
9.0.0.0/8       1     Stub  9.0.0.1        1.2.3.4        0.0.0.1
11.0.0.0/8      2     SumNet  10.0.0.2       5.6.7.8        0.0.0.0
192.168.5.0/24   3     SumNet  10.0.0.2       5.6.7.8        0.0.0.0
192.168.6.0/24   3     SumNet  10.0.0.2       5.6.7.8        0.0.0.0
```

```
Total Nets: 5
Intra Area: 2  Inter Area: 3  ASE: 0
```

10.7.4 Examples for configuring OSPF DR selection

Networking requirements

As shown in Figure 10-4, OLT A, OLT A, OLT C and OLT D are in the same network segment and transmit route information to each other through OSPF protocol. Set the priorities of DR selection for OLT D and OLTC to 2 and 0 respectively. OLT A and OLT B adopt the default setting.

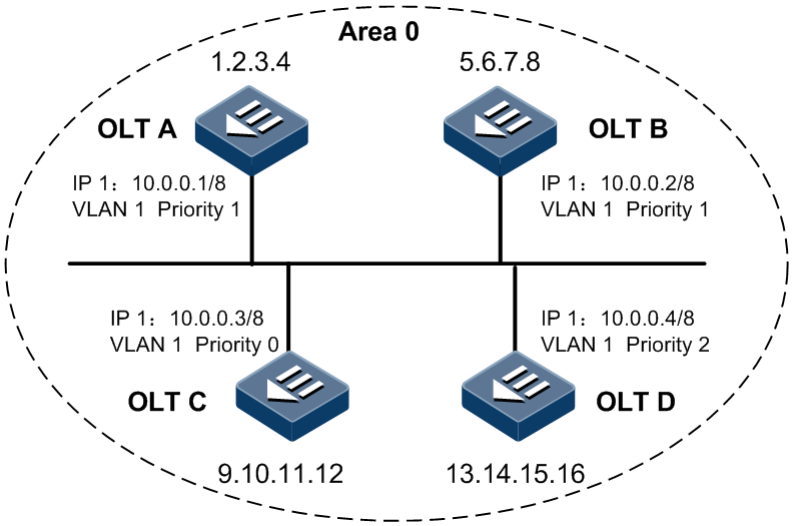

Figure 10-4 Configuring OSPF DR selection

Configuration steps

Step 1 Configure IP address and VLANs for all interfaces and enable Layer 3 route. Detailed commands are omitted.

Step 2 Configure basic OSPF functions.

Configure OLT A.

```
Raisecom#config
Raisecom(config)#router ospf 1 router-id 1.2.3.4
Raisecom(config-router-ospf)#network 10.0.0.0 0.255.255.255 area 0
Raisecom(config-router-ospf)#exit
```

Configure OLT B.

```
Raisecom#config
Raisecom(config)#router ospf 1 router-id 5.6.7.8
```

```
Raisecom(config-router-ospf)#network 10.0.0.0 0.255.255.255 area 0
Raisecom(config-router-ospf)#exit
```

Configure OLT C.

```
Raisecom#config
Raisecom(config)#router ospf 1 router-id 9.10.11.12
Raisecom(config-router-ospf)#network 10.0.0.0 0.255.255.255 area 0
Raisecom(config-router-ospf)#exit
```

Configure OLT D.

```
Raisecom#config
Raisecom(config)#router ospf 1 router-id 13.14.15.16
Raisecom(config-router-ospf)#network 10.0.0.0 0.255.255.255 area 0
Raisecom(config-router-ospf)#exit
```

Step 3 Configure OSPF DR selection priority.

Configure OLT A.

```
Raisecom(config)#interface ip 1
Raisecom(config-ip)#ip ospf priority 1
```

Configure OLT B.

```
Raisecom(config)#interface ip 1
Raisecom(config-ip)#ip ospf priority 1
```

Configure OLT C.

```
Raisecom(config)#interface ip 1
Raisecom(config-ip)#ip ospf priority 0
```

Configure OLT D.

```
Raisecom(config)#interface ip 1
Raisecom(config-ip)#ip ospf priority 2
```

Checking results

Use the **show ip ospf interface** command to check OSPF interface information of OLT A and OLT D.

- Check OLT A.

```
Raisecom#show ip ospf interface
       OSPF Interface Information

   OSPF Process 1 with Router ID 1.2.3.4

Area: 0.0.0.0
Interface 10.0.0.1/8 (ip1)  Priority: 1  AuthType: None
Cost: 1   State: DRother   Type: Broadcast
Designated Router-id/IP: 13.14.15.16/10.0.0.4
Backup Designated Router-id/IP: 5.6.7.8/10.0.0.2
Timers(second): Hello 10, Dead 40, Poll 120, Retransmit 5, Transmit Delay
1
Neighbor Count: 3  Adjacent Neighbor Count: 2
```

- Check OLT D.

```
Raisecom#show ip ospf interface
       OSPF Interface Information

   OSPF Process 1 with Router ID 13.14.15.16

Area: 0.0.0.0
Interface 10.0.0.4/8 (ip1)  Priority: 2  AuthType: None
Cost: 1   State: DR   Type: Broadcast
Designated Router-id/IP: 13.14.15.16/10.0.0.4
Backup Designated Router-id/IP: 5.6.7.8/10.0.0.2
Timers(second): Hello 10, Dead 40, Poll 120, Retransmit 5, Transmit Delay
1
Neighbor Count: 3  Adjacent Neighbor Count: 3
```

As shown in the previous configurations, OLT D is selected as a DR because of a higher priority. OLT A and OLT B have identical priority level. However, the Router-ID OLT B is larger than the one of OLT A. Therefore, the OLT B is selected as BDR.

10.7.5 Examples for introducing external routes through OSPF

Networking requirements

As shown in Figure 10-5. OLT A and OLT B communicate route information through OSPF. Configure OLT B to introduce external static routes, which can be transmitted in the AS.

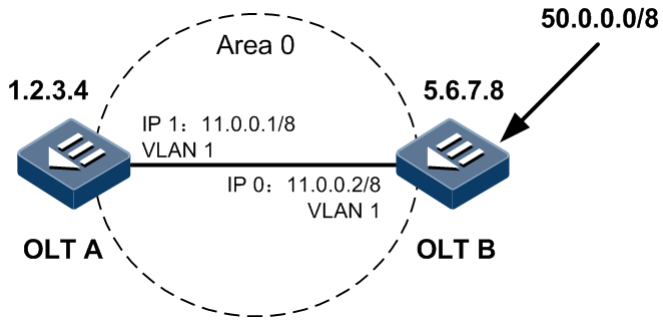

Figure 10-5 Introducing external routes through OSPF

Configuration steps

Step 1 Configure IP address and VLANs for all interfaces and enable Layer 3 route. Detailed commands are omitted.

Step 2 Configure basic OSPF functionS and introduce ASE routes.

Configure OLT A.

```
Raisecom#config
Raisecom(config)#router ospf 1 router-id 1.2.3.4
Raisecom(config-router-ospf)#network 11.0.0.0 0.255.255.255 area 0
```

Configure OLT B.

```
Raisecom#config
Raisecom(config)#ip route 50.0.0.0 255.0.0.0 11.0.0.1
Raisecom(config)#router ospf 1 router-id 5.6.7.8
Raisecom(config-router-ospf)#network 11.0.0.0 0.255.255.255 area 0
Raisecom(config-router-ospf)#import static
```

Checking results

Use the **show ip ospf database** command to check information about LSDB of OLT A and OLT B.

- Check OLT A.

```
Raisecom#show ip ospf database

       LinkState Database Information

   OSPF Process 1 with Router ID 1.2.3.4

Area: 0.0.0.0
```

```
Type LinkState ID   AdvRouter      Age  Len  Sequence   Metric
-------------------------------------------------------------------------
Router  1.2.3.4       1.2.3.4        3    36   80000009   0
Router  5.6.7.8       5.6.7.8        1160 36   80000008   0
Net  11.0.0.2       5.6.7.8        1160 32   80000001   0

AS External Database
Type LinkState ID   AdvRouter      Age  Len  Sequence   Metric
-------------------------------------------------------------------------
ASE  50.0.0.0       5.6.7.8        3    36   80000001   1
```

- Check OLT B.

```
Raisecom#show ip ospf database

       LinkState Database Information

   OSPF Process 1 with Router ID 5.6.7.8

Area: 0.0.0.0
Type LinkState ID   AdvRouter      Age  Len  Sequence   Metric
-------------------------------------------------------------------------
Router  1.2.3.4       1.2.3.4        3    36   80000009   0
Router  5.6.7.8       5.6.7.8        1160 36   80000008   0
Net  11.0.0.2       5.6.7.8        1160 32   80000001   0

AS External Database
Type LinkState ID   AdvRouter      Age  Len  Sequence   Metric
-------------------------------------------------------------------------
ASE  50.0.0.0       5.6.7.8        3    36   80000001   1
```

Use the **show ip ospf route** command to check information about the route table of OLT A.

- Check information about the route table of OLT A.

```
Raisecom#show ip ospf route
       OSPF Route Information

   OSPF Process 1 with Router ID 1.2.3.4

Routing for Network
Destination     Cost   Type  NextHop       AdvRouter      Area
-------------------------------------------------------------------------
11.0.0.0/8      1      Net   11.0.0.2      5.6.7.8        0.0.0.0
Routing for ASEs
Destination     Cost   Type  NextHop       AdvRouter
-------------------------------------------------------------------------
50.0.0.0/8      1      ASE   11.0.0.2      5.6.7.8
Total Nets: 2
Intra Area: 1  Inter Area: 0  ASE: 1
```

10.7.6 Examples for configuring Stub area of OSPF

Networking requirements

As shown in Figure 10-6, all devices in the network run OSPF protocol. The AS is divided into Area 0 and Area 1. Specified requirements are shown as follows:

- OLT B is taken as an ABR to forward routes between two areas.
- OLT C is taken as an ASBR to introduce external static toutes.
- Set Area 1 to the Stub area, introducing LSA numbers transmitted to Area 1 without influencing the reachability of routes.

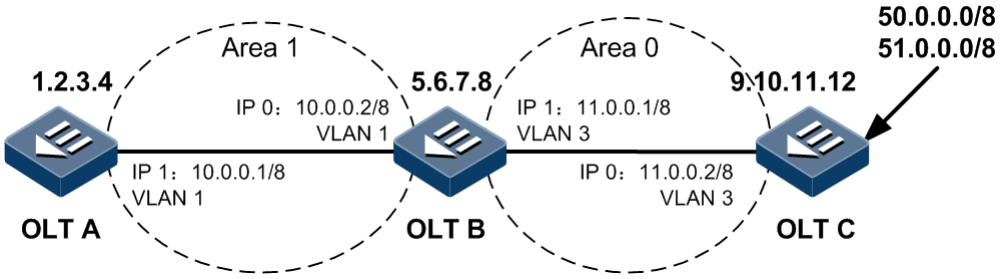

Figure 10-6 Configuring Stub area of OSPF

Configuration steps

Step 1 Configure IP address and VLANs for all interfaces and enable Layer 3 route. Detailed commands are omitted.

Step 2 Configure basic OSPF functionS.

Configure OLT A.

```
Raisecom#config
Raisecom(config)#router ospf 1 router-id 1.2.3.4
Raisecom(config-router-ospf)#network 10.0.0.0 0.255.255.255 area 1
```

Configure OLT B.

```
Raisecom#config
Raisecom(config)#router ospf 1 router-id 5.6.7.8
Raisecom(config-router-ospf)#network 10.0.0.0 0.255.255.255 area 1
Raisecom(config-router-ospf)#network 11.0.0.0 0.255.255.255 area 0
```

Configure OLT C.

```
Raisecom#config
Raisecom(config)#ip route 50.0.0.0 255.0.0.0 11.0.0.1
```

```
Raisecom(config)#ip route 51.0.0.0 255.0.0.0 11.0.0.1
Raisecom(config)#router ospf 1 router-id 9.10.11.12
Raisecom(config-router-ospf)#network 11.0.0.0 0.255.255.255 area 0
```

Step 3 Configure OLT C to introduce external static routes.

```
Raisecom(config-router-ospf)#import static
```

Step 4 Set Area 1 to the Stub area.

Configure OLT A.

```
Raisecom(config-router-ospf)#area 1 stub
```

Configure OLT A.

```
Raisecom(config-router-ospf)#area 1 stub
```

Checking results

Use the **show ip ospf database** command to check information about LSDB of OLT A and OLT B.

- Check information about LSDB of OLT A.

```
Raisecom#show ip ospf database

       LinkState Database Information

   OSPF Process 1 with Router ID 1.2.3.4

Area: 0.0.0.1
Type LinkState ID   AdvRouter      Age  Len  Sequence   Metric
-------------------------------------------------------------------------
Router  1.2.3.4       1.2.3.4       26   36   80000005   0
Router  5.6.7.8       5.6.7.8       32   36   80000006   0
Net  10.0.0.2      5.6.7.8       32   32   80000002   0
SumNet 0.0.0.0       5.6.7.8       29   28   80000001   1
SumNet 11.0.0.0      5.6.7.8       71   28   80000001   1
```

- Check information about LSDB of OLT B.

```
Raisecom#show ip ospf database

       LinkState Database Information

   OSPF Process 1 with Router ID 5.6.7.8

Area: 0.0.0.0
Type LinkState ID   AdvRouter      Age  Len  Sequence   Metric
-------------------------------------------------------------------------
Router  5.6.7.8       5.6.7.8        50   36   80000005   0
Router  9.10.11.12    9.10.11.12     54   36   80000005   0
Net  11.0.0.2       9.10.11.12     54   32   80000002   0
SumNet 10.0.0.0       5.6.7.8        60   28   80000002   1

Area: 0.0.0.1
Type LinkState ID   AdvRouter      Age  Len  Sequence   Metric
-------------------------------------------------------------------------
Router  1.2.3.4       1.2.3.4        56   36   80000005   0
Router  5.6.7.8       5.6.7.8        60   36   80000006   0
Net  10.0.0.2       5.6.7.8        60   32   80000002   0
SumNet 0.0.0.0        5.6.7.8        58   28   80000001   1
SumNet 11.0.0.0       5.6.7.8        100  28   80000001   1

AS External Database
Type LinkState ID   AdvRouter      Age  Len  Sequence   Metric
-------------------------------------------------------------------------
ASE  50.0.0.0       9.10.11.12     57   36   80000002   1
ASE  51.0.0.0       9.10.11.12     61   36   80000001   1
```

Use the **show ip ospf route** command to check information about the route table of OLT A.

```
Raisecom#show ip ospf route

       OSPF Route Information

   OSPF Process 1 with Router ID 1.2.3.4

Routing for Network
Destination     Cost   Type  NextHop        AdvRouter      Area
-------------------------------------------------------------------------
10.0.0.0/8      1      Net   10.0.0.1       5.6.7.8        0.0.0.1
0.0.0.0/0       2      SumNet  10.0.0.2       5.6.7.8        0.0.0.1
11.0.0.0/8      2      SumNet  10.0.0.2       5.6.7.8        0.0.0.1
Total Nets: 3
Intra Area: 1  Inter Area: 2  ASE: 0
```

10.7.7 Examples for forwarding aggregated route through OSPF

Networking requirements

As shown in Figure 10-7, OLT A, OLT B and OLT C communicate route information with each other through OSPF. The whole AS is divided into Area 0 and Area 1. OLT A and OLT B are in Area 0 while OLTB and OLT C are in Area 1. OLT C introduces 4 static routes. Specified requirements are shown as follows:

- To reduce the OSPF route table size, the OLT C is configured with external route aggregation. After aggregation, only one route is forwarded. the route is set to 192.168.32.0 and the mask is set to 255.255.255.128.
- To further reduce the OSPF route table size, inter-domain route aggregation is configured on OLT B. After configuration, only one route is forwarded. the route is set to 192.168.42.0 and the mask is set to 255.255.255.128.

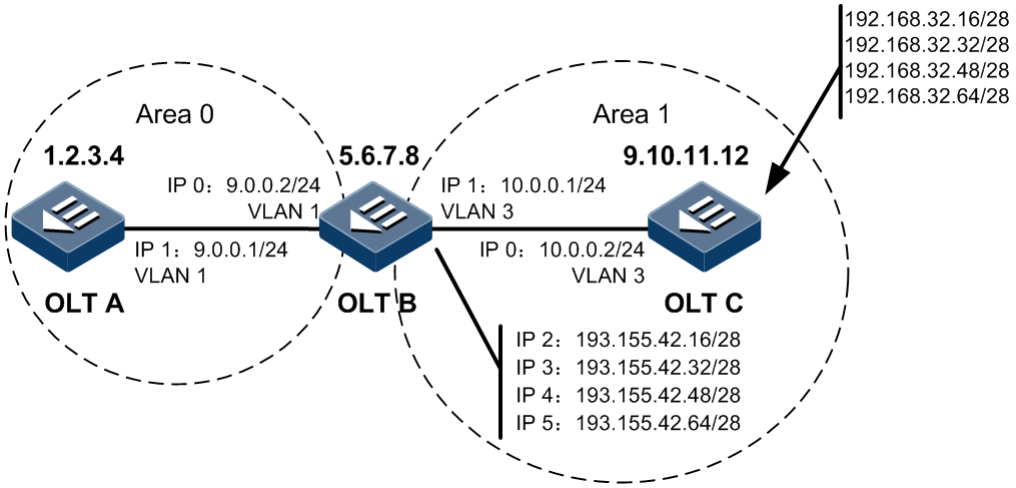

Figure 10-7 Forwarding aggregated route through OSPF

Configuration steps

Step 1 Configure IP address and VLANs for all interfaces and enable Layer 3 route. Detailed commands are omitted.

Step 2 Configure basic OSPF functions.

Configure OLT A.

```
Raisecom#config
Raisecom(config)#router ospf 1 router-id 1.2.3.4
Raisecom(config-router-ospf)#network 9.0.0.0 0.255.255.255 area 0
```

Configure OLT B.

```
Raisecom#config
```

```
Raisecom(config)#router ospf 1 router-id 5.6.7.8
Raisecom(config-router-ospf)#network 9.0.0.0 0.255.255.255 area 0
Raisecom(config-router-ospf)#network 10.0.0.0 0.255.255.255 area 1
Raisecom(config-router-ospf)#network 193.155.42.0 0.0.0.127 area 1
```

Configure OLT C.

```
Raisecom#config
Raisecom(config)#router ospf 1 router-id 9.10.11.12
Raisecom(config-router-ospf)#network 10.0.0.0 0.255.255.255 area 1
Raisecom(config-router-ospf)#import static
```

Note

You can check LSDB information and OSPF information of the ISCOM5508 by using the **show ip ospf database** and **show ip ospf route** commands.

Step 3 Configure external route aggregation on OLT C.

```
Raisecom(config-router-ospf)#summary-address 192.168.32.0 255.255.255.128
```

Note

You can check LSDB information and OSPF information of the ISCOM508 by using the **show ip ospf database** and **show ip ospf route** commands. After finishing external route aggregation, 4 external routes are aggregated into one aggregated route and the total route number is reduced to 7 from 10.

Step 4 Configure external route aggregation on OLT B.

```
Raisecom(config-router-ospf)#area 1 range 193.155.42.0 255.255.255.128
```

Checking results

Use the **show ip ospf database** command to check LSDB information of the ISCOM5508.

- Check LSDB information of OLT A.

```
Raisecom#show ip ospf database
       LinkState Database Information

   OSPF Process 1 with Router ID 1.2.3.4
Area: 0.0.0.0
```

```
Type LinkState ID   AdvRouter      Age  Len  Sequence   Metric
-------------------------------------------------------------------------
Router  1.2.3.4        1.2.3.4        146  36   8000000a   0
Router  5.6.7.8        5.6.7.8        150  36   80000005   0
Net  9.0.0.2        5.6.7.8        155  32   80000001   0
SumNet 10.0.0.0       5.6.7.8        190  28   80000001   1
SumNet 193.155.42.0   5.6.7.8        10   28   80000001   1
ASB  9.10.11.12     5.6.7.8        145  28   80000001   1

AS External Database
Type LinkState ID   AdvRouter      Age  Len  Sequence   Metric
-------------------------------------------------------------------------
ASE  192.168.32.0   9.10.11.12     54   36   80000001   2
```

- Check LSDB information of OLT B.

```
Raisecom#show ip ospf database
       LinkState Database Information

   OSPF Process 1 with Router ID 5.6.7.8

Area: 0.0.0.0
Type LinkState ID   AdvRouter      Age  Len  Sequence   Metric
-------------------------------------------------------------------------
Router  1.2.3.4        1.2.3.4        156  36   8000000a   0
Router  5.6.7.8        5.6.7.8        158  36   80000005   0
Net  9.0.0.2        5.6.7.8        163  32   80000001   0
SumNet 10.0.0.0       5.6.7.8        198  28   80000001   1
SumNet 193.155.42.0   5.6.7.8        18   28   80000001   1
ASB  9.10.11.12     5.6.7.8        153  28   80000001   1

Area: 0.0.0.1
Type LinkState ID   AdvRouter      Age  Len  Sequence   Metric
-------------------------------------------------------------------------
Router  5.6.7.8        5.6.7.8        162  84   80000004   0
Router  9.10.11.12     9.10.11.12     163  36   80000009   0
Net  10.0.0.2       9.10.11.12     163  32   80000001   0
SumNet 9.0.0.0        5.6.7.8        158  28   80000002   1

AS External Database
Type LinkState ID   AdvRouter      Age  Len  Sequence   Metric
-------------------------------------------------------------------------
ASE  192.168.32.0   9.10.11.12     62   36   80000001   2
```

Use the **show ip ospf route** command to check information about the route table of OLT A.

```
Raisecom#show ip ospf route
       OSPF Route Information

   OSPF Process 1 with Router ID 1.2.3.4
```

```
Routing for Network
Destination     Cost   Type  NextHop       AdvRouter      Area
-------------------------------------------------------------------------
9.0.0.0/8       1     Net   9.0.0.1       5.6.7.8        0.0.0.0
10.0.0.0/8      2     SumNet  9.0.0.2       5.6.7.8        0.0.0.0
193.155.42.0/25  2     SumNet  9.0.0.2       5.6.7.8        0.0.0.0
Routing for ASEs
Destination     Cost   Type  NextHop       AdvRouter
-------------------------------------------------------------------------
192.168.32.0/25  2     ASE   9.0.0.2       9.10.11.12
Total Nets: 4
Intra Area: 1  Inter Area: 2  ASE: 1
```

As shown in the previous configurations, after configuring the inter-domain route aggregation, the route table size is reduced. 4 inter-domain routes are aggregated into one route and the total route number is reduced to 4 from 7.

11 Configuring DHCP

The chapter introduces DHCP configuration and procedure of ISCOM5508 device, and provides related applications.

- Configuring DHCP Client
- Configuring DHCP Server
- Configuring DHCP Snooping
- Configuring DHCP Relay
- Configuring DHCP Option 82
- Configuration examples

11.1 Configuring DHCP Client

11.1.1 Preparing for configuration

Networking situation

Enable DHCP Client function when the device needs to get IP address from DHCP Server.

Note

At present, only interface ip 0 on ISCOM5508 device is in support of DHCP Client.

Precondition

DHCP Client, DHCP Server and DHCP Relay functions are mutually exclusive.

- The device cannot be configured DHCP Server and DHCP Relay functions after configuring DHCP Client function.
- The device cannot be configured DHCP Client function after configuring DHCP Server and DHCP Relay functions.

11.1.2 Default configuration of DHCP Client

Function	Default value
hostname	raisecomFTTH
class-id	raisecomFTTH-ROS_VERSION
client-id	raisecomFTTH-SYSMAC- IF0
IP port get IP address by DHCP	enable
DHCP Client renewing	disable
DHCP Client release IP address	disable

11.1.3 Configuring DHCP Client

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode;
2	`Raisecom(config)#interface ip 0`	Enter three-layer port configuration mode; three-layer port whose number is 0 supports DHCP client function in a device;
3	`Raisecom(config-ip)#ip address dhcp` *`vlan-id`* `[ server-ip` *`ip-address`* `]`	Apply for IP address by DHCP;

Note

If the equipment has got IP address previously from a DHCP server by DHCP, when user can use the command of **ip address dhcp** to modify DHCP server address, the device will restart the IP address application process.

11.1.4 (Optional) configuring DHCP Client information

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode;
2	`Raisecom(config)#interface ip 0`	Enter three-layer port configuration mode; three-layer port whose number is 0 supports DHCP client function in a device;
3	`Raisecom(config-ip)#ip dhcp client hostname` *`hostname`*	(Optional) Configure hostname information of DHCP client;
4	`Raisecom(config-ip)#ip dhcp client class-id` *`class-id`*	(Optional) Configure class-id information of DHCP client;

Step	Configuration	Description
5	Raisecom(config-ip)#**ip dhcp client client-id** *client-id*	(Optional) Configure client-id information of DHCP client;

11.1.5 (Optional) renewing/releasing IP address

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface ip 0**	Enter three-layer port configuration mode; three-layer port whose number is 0 supports DHCP client function in a device;
3	Raisecom(config-ip)#**ip dhcp client renew**	(Optional) renew IP address; Renew IP address automatically if three-layer port gets IP address by DHCP previously;
4	Raisecom(config-ip)#**no ip address dhcp**	(Optional) release IP address;

11.1.6 Checking configuration

No.	Item	Description
1	Raisecom#**show ip dhcp client**	Show configuration information of DHCP Client and the information obtained from DHCP Server;

11.2 Configuring DHCP Server

11.2.1 Preparing for configuration

Networking situation

User needs to configure DHCP Server function when using ISCOM5508 to provide dynamic IP address for other devices.

Precondition

- DHCP Server, DHCP Client and DHCP Relay functions are mutually exclusive.
  - The device cannot be configured DHCP Client and DHCP Relay functions after configuring DHCP Server function.
  - The device cannot be configured DHCP Server function after configuring DHCP Client and DHCP Relay functions.

- Port DHCP Server can take effect after enabling global DHCP Server function.

11.2.2 Default configuration of DHCP Server

Function	Default value
Global DHCP Server	disable
IP port DHCP Server	disable
address pool	N/A
DHCP Option 82 function	support
time-out period of least table	• the maximum time-out period: 10080 minutes; • the minimum time-out period: 30 minutes; • default time-out period: 30 minutes;
adjacent agent address	N/A

11.2.3 Configuring DHCP Server

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip dhcp server ip-pool** *ip-pool-name start-ip-address end-ip-address ip-mask* **ip** *if-number* [**gatway** *ip-address* | **dns** *ip-address* | **secondary-dns** *ip-address*]	Configure IP address pool of DHCP Server;
3	Raisecom(config)#**interface ip** *if-number*	Enter three-layer port configuration mode;
4	Raisecom(config-ip)#**ip address** *ip-address ip-mask vlan-id*	Configure IP address of DHCP Server;
5	Raisecom(config-ip)#**ip dhcp server**	Enable IP port DHCP Server service;
6	Raisecom(config-ip)#**exit**	Return to global configuration mode;
7	Raisecom(config)#**ip dhcp server**	Enable global DHCP Server service;

11.2.4 (Optional) configuring time-out period of leasing table

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip dhcp server default-least** *second*	(Optional) Configure default least time-out period of DHCP Server IP address pool;
3	Raisecom(config)#**ip dhcp server max-least** *second*	(Optional) Configure the maximum least time-out period of DHCP Server IP address pool;

Step	Configuration	Description
4	Raisecom(config)#**ip dhcp server min-least** *second*	(Optional) Configure the minimum least time-out period of DHCP Server IP address pool;

11.2.5 (Optional) configuring IP address of neighbor

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip dhcp server relay-ip** *ip-address ip-mask*	Configure IP address of adjacent agent;

11.2.6 (Optional) configuring DHCP Server information

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip dhcp server tftp-server** *ip-address* **ip-pool** *ip-pool-name*	(Optional) Configure TFTP server address;
3	Raisecom(config)#**ip dhcp server bootfile** *file-name* **ip-pool** *ip-pool-name*	(Optional) Configure boot file name;
4	Raisecom(config)#**no ip dhcp server relay information option**	(Optional) disable DHCP Server supporting DHCP Option 82 function;
5	Raisecom(config)#**ip dhcp server option number** { **ascii** *ascii-string* | **hex** hex-*string* | **ip-address** *ip-address* } **ip-pool** *ip-pool-name*	(Optional) Configure options defined by users;

11.2.7 Checking configuration

No.	Item	Description
1	Raisecom#**show ip dhcp server**	Show configuration information of DHCP Server function;
2	Raisecom#**show ip dhcp server ip-pool**	Show configuration information of DHCP Server IP address pool;
3	Raisecom#**show ip dhcp server relay-ip**	Show configuration information of adjacent agent's IP address;
4	Raisecom#**show ip dhcp server lease**	Show allocated IP address and related information;

11.3 Configuring DHCP Snooping

11.3.1 Preparing for configuration

Networking situation

DHCP Snooping is a security feature of DHCP, being used to guarantee DHCP client gets IP address from legal DHCP server and record corresponding relationship between DHCP client IP and MAC address.

Option field of DHCP packet records location of DHCP client. Administrator can locate DHCP client through Option field and control client security and accounting. ISCOM5508 device configured with DHCP Snooping and Option can perform related process according to Option field existence status in packet.

Precondition

- DHCP Snooping, DHCP Relay and DHCP Server functions are mutually exclusive.
  - The device cannot be configured DHCP Relay and DHCP Server functions after configuring DHCP Snooping function.
  - The device cannot be configured DHCP Snooping function after configuring DHCP Relay and DHCP Server functions.
- Port DHCP Snooping can take effect after enabling global DHCP Snooping function.
- When enabling DHCP Snooping and DHCP Client functions simultaneously, user must make sure the DHCP Server connection port is trust port of DHCP Snooping so as to apply for dynamic IP address correctly.

11.3.2 Default configuration of DHCP Snooping

Default configuration of DHCP Snooping on ISCOM5508 device.

Function	Default value
Global DHCP Snooping function	disable
Port DHCP Snooping function	enable
Port DHCP Snooping trust status	not trust
DHCP Option 82 function	not support

Default configuration of DHCP Snooping on Raisecom ONU device.

Function	Default value
Global DHCP Snooping function	disable
Port DHCP Snooping function	disable
Port DHCP Snooping trust status	not trust
DHCP Option 82 function	disable

11.3.3 Configuring global DHCP Snooping

Configuring OLT global DHCP Snooping

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip dhcp snooping**	Enable global DHCP Snooping function;

Configuring ONU global DHCP Snooping

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**ip dhcp snooping** { **enable** | **disable** }	Enable/disable ONU global DHCP Snooping function;

11.3.4 Configuring port DHCP Snooping

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip dhcp snooping port-list** { **all** | *port-list* }	Enable port DHCP Snooping function;

11.3.5 Configuring port DHCP Snooping trust

Configuring DHCP Snooping trust of OLT port

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enable port DHCP Snooping function;
3	Raisecom(config-port)#**ip dhcp snooping trust**	Configure trust port;

Configuring DHCP Snooping trust of ONU port

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter ONU UNI Ethernet port configuration mode;
4	Raisecom(fttx-onu-uni*/*/*:*)#**ip dhcp snooping trust** { **enable** | **disable** }	Enable/disable ONU port DHCP Snooping trust;

Note

Generally, user needs to make sure the device connection DHCP Server port is in trust status, while the DHCP Client port is in untrusted status.

11.3.6 (Optional) configuring DHCP Snooping supporting DHCP Option 82

Configuring OLT DHCP Snooping supporting DHCP Option 82

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip dhcp snooping information option**	Configure DHCP Snooping to support Option 82 function;

Configuring ONU DHCP Snooping supporting DHCP Option 82

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**ip dhcp information option82** { **enable** | **disable** }	Enable/disable DHCP Snooping to support DHCP Option 82 function;
4	Raisecom(fttx-onu*/*:*)#**ip dhcp snooping information option82 user-defined** { **enable** | **disable** }	(Optional) Enable/disable DHCP Option 82 option function defined by users;
5	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter ONU UNI Ethernet port configuration mode;
6	Raisecom(fttx-onu*/*:*)#**ip dhcp snooping option82 policy** { **drop** | **keep** | **replace** }	(Optional) Configure processing policy of message carried with option 82;

If enabling DHCP Snooping without configuring DHCP Snooping supporting Option 82 function, the device will do nothing to Option 82 fields in the packets. For packets without Option 82 fields, the device also doesn't do insertion operation.

11.3.7 Checking configuration

Checking OLT configuration

No.	Item	Description
1	Raisecom#**show ip dhcp snooping** [**binding**]	Show configuration information of DHCP Snooping function on OLT;

Checking ONU configuration

No.	Item	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **ip dhcp snooping** [**binding**]	Show configuration information of DHCP Snooping function in ONU device;
2	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** *uni-id* **ip dhcp snooping**	Show configuration information of DHCP Snooping function on ONU port;
3	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** *uni-id* **ip dhcp snooping statistics**	Show statistics information of DHCP message on ONU port;

11.4 Configuring DHCP Relay

11.4.1 Preparing for configuration

Networking situation

When DHCP Client and DHCP Server are not in the same network segment, user can use DHCP Relay function to make DHCP Client and DHCP Server in different network segment bear relay service, and relay DHCP protocol message across network segment to destination DHCP server, so that DHCP Client in different network segment can share the same DHCP Server.

Precondition

- DHCP Relay, DHCP Client and DHCP Snooping functions are mutually exclusive.
  - The device cannot be configured DHCP Client and DHCP Snooping functions after configuring DHCP Relay function.

  - The device cannot be configured DHCP Relay function after configuring DHCP Client and DHCP Snooping functions.
- Port DHCP Relay can take effect after enabling global DHCP Relay function.
- For the situation of DHCP Client connecting DHCP Server through multiple DHCP Relay it is recommended not more than 4 DHCP Relay.

11.4.2 Default configuration of DHCP Relay

Function	Default value
Global DHCP Relay function	disable
Port DHCP Relay function	enable
port destination IP address	N/A
Port DHCP Relay trust status	not trust
DHCP Option 82 function	not support
Processing policy of request message including option 82	Replace

11.4.3 Configuring global DHCP Relay

Configuring OLT global DHCP Relay

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip dhcp relay**	Enable global DHCP Relay function;

Configuring ONU global DHCP Relay

Step	Configuration	Description
1	Raisecom#**fttx**	Enter EPON global configuration mode;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**ip dhcp relay** { **enable** | **disable** }	Enable/disable global DHCP Relay function;

11.4.4 Configuring port DHCP Relay

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;

Step	Configuration	Description
2	Raisecom(config)#**interface ip** *if-number*	Enter three-layer port configuration mode;
3	Raisecom(config-ip)#**ip dhcp relay**	Enable port DHCP Relay function;

11.4.5 Configuring destination IP address of port

Configuring destination IP address of OLT port

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)# **ip dhcp relay ip-list** { **all** | *port-list* } **target-ip** *ip-address*	(Optional) Configure destination IP address of global port;
3	Raisecom(config)#**interface ip** *if-number*	Enter three-layer port configuration mode;
4	Raisecom(config-ip)#**ip dhcp relay target-ip** *ip-address*	Configure destination IP address of three-layer port;

Note

Each port can set a maximum of 4 destination IP addresses.

Configuring destination IP address of ONU port

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**ip-if** *ip-if* **address** *ip-address ip-mask* [**vlan** *vlan-list*]	Create IP interface of ONU DHCP Relay;
4	Raisecom(fttx-onu*/*:*)#**ip dhcp relay ip-if** *ip-list* **target-ip** *ip-address*	Configure target DHCP server address of IP interface; Use the command **no ip dhcp relay ip-if** *ip-list* **target-ip** to recover IP address of DHCP server as default value

Caution

DHCP Relay IP interface VLAN and PON interface management VLAN cannot be the same, and DHCP Relay IP interface IP address and PON interface management IP address cannot belong to the same subnet.

11.4.6 Configuring DHCP Relay trust of port

Configuring DHCP Relay trust of OLT port

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip dhcp relay information trusted port-list** { **all** | *port-list* }	Configure global port DHCP Relay trust;

Configuring DHCP Relay trust of ONU port

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**uni Ethernet** *uni-id*	Enter ONU UNI Ethernet port configuration mode;
4	Raisecom(fttx-onu*/*/*:*)#**ip dhcp relay trust** { **enable** | **disable** }	enable/disable ports as DHCP Relay trust ports;

Note

Port trust can take effect only when DHCP Relay is in support of DHCP Option 82.

11.4.7 (Optional) configuring DHCP Relay supporting DHCP Option 82

Configuring OLT DHCP Relay supporting DHCP Option 82

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip dhcp relay information**	Configure DHCP Relay to support DHCP Option 82 function;

Configuring ONU DHCP Relay supporting DHCP Option 82

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;

Step	Configuration	Description
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**ip dhcp relay information option82 user-defined** { **enable** | **disable** }	Configure DHCP Relay to support DHCP Option 82 function;

11.4.8 (Optional) configuring processing policy of DHCP Relay demand message

Configuring processing policy of OLT DHCP Relay demand message

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip dhcp relay information policy** { **drop** | **keep** | **replace** | **schedule-list** *list-id* }	Configure processing policy of DHCP Relay request message;

Configuring processing policy of ONU DHCP Relay demand message

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**uni Ethernet** *uni-id*	Enter ONU UNI Ethernet port configuration mode;
4	Raisecom(fttx-onu*/*/*:*)#**ip dhcp relay option82 policy** { **drop** | **keep** | **replace** }	Configure processing policy of DHCP Relay request message; Use the command **no ip dhcp relay option82 policy** to recover default configuration;

11.4.9 Checking configuration

Checking OLT configuration

No.	Item	Description
1	Raisecom#**show ip dhcp relay**	Show configuration information of DHCP Relay function;
2	Raisecom#**show ip dhcp relay statistics**	Show statistics information of DHCP Relay function;

No.	Item	Description
3	Raisecom#**show ip dhcp relay information**	Show address information of adjacent DHCP Relay;

Checking ONU configuration

No.	Item	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **ip dhcp relay**	Show configuration information of DHCP Relay function;
2	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **ip-if**	Show IP interface information of DHCP Relay function;
3	Raisecom# **show interface onu** *slot-id/olt-id/onu-id* **ip dhcp relay ip-if**	Show IP interface target server address information of DHCP Relay function;
4	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** [**uni-id**] **ip dhcp relay**	Show configuration information of DHCP Relay port function;
5	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** [**uni-id**] **ip dhcp relay statistics**	Show DHCP message statistics information of DHCP Relay port;

11.5 Configuring DHCP Option 82

11.5.1 Preparing for configuration

Networking situation

RFC 3046 defines DHCP Option 82 (DHCP Relay Agent Information Option) and adds some options information in DHCP request to make DHCP Server determine user location more accurately so as to take different address assignment strategy to different user.

Precondition

Before configuring DHCP Option 82 function, user needs to enable DHCP Snooping function or the DHCP Relay function.

Note

- Before configuring DHCP Option 82 function, user needs to enable "user-defined DHCP Option 82 options function" firstly.
- Please refer to "(Optional) Configure DHCP Snooping supporting DHCP Option 82 function" for the method to enable "user-defined DHCP Option 82 options function".

11.5.2 Default configuration of DHCP Option 82

Default configuration of DHCP Option 82 in ISCOM5508 device.

Function	Default value
global DHCP Option attach-string	N/A
global remote-id	switch-mac
port circuit-id	N/A

Default configuration of DHCP Option 82 in Raisecom ONU device.

Function	Default value
global DHCP Option attach-string	N/A
global remote-id mode	onu-mac
port circuit-id	N/A

11.5.3 Configuring global DHCP Option attach-string

Configuring OLT global DHCP Option attach-string

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip dhcp information option attach-string** *attach-string*	Configure additional information of Option 82 field on OLT;

Configuring ONU global DHCP Option attach-string

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**ip dhcp information option82 attach-string** *attach-string*	Configure additional information of Option 82 field on ONU;

11.5.4 Configuring global DHCP Option remote-id

Configuring OLT global DHCP Option remote-id

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip dhcp information option remote-id** { **switch-mac** | **client-mac** | **switch-mac-string** | **client-mac-string** | **hostname** | **string** *string* }	Configure RID sub-option information of Option 82 field on OLT;

Configuring ONU global DHCP Option remote-id

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**ip dhcp information option82 remote-id string** *string*	Configure RID sub-option information of Option 82 field in ONU device;
4	Raisecom(fttx-onu*/*:*)#**ip dhcp information option82 remote-id mode** { **client-mac** | **client-mac-string** | **hostname** | **onu-mac** | **onu-mac-string** | **user-defined** *string* }	Configure filling mode of RID sub-option of Option 82 field in ONU device;

11.5.5 Configuring port DHCP Option circuit-id

Configuring OLT port DHCP Option circuit-id

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer port configuration mode;
3	Raisecom(config-port)#**ip dhcp information option circuit-id** *string*	Configure CID sub-option information of Option82 field on OLT port;

Configuring ONU port DHCP Option circuit-id

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter ONU UNI Ethernet port configuration mode;
4	Raisecom(fttx-onu-uni*/*/*:*)#**ip dhcp information option82 circuit-id** *string*	Configure CID sub-option information of Option82 field on ONU port;

11.5.6 Checking configuration

Checking OLT configuration

No.	Item	Description
1	Raisecom(config)#**show ip dhcp information**	Show DHCP Option configuration of OLT device;

Checking ONU configuration

No.	Item	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **ip dhcp information option82**	Show global DHCP Option82 configuration of ONU device;
2	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** *uni-id* **ip dhcp information option82**	Show port DHCP Option82 configuration of ONU device;

11.6 Configuration examples

11.6.1 Examples for configuring DHCP Client

Networking requirements

As shown in below figure, ISCOM5508 device gets IP address and other configuration information by DHCP Server.

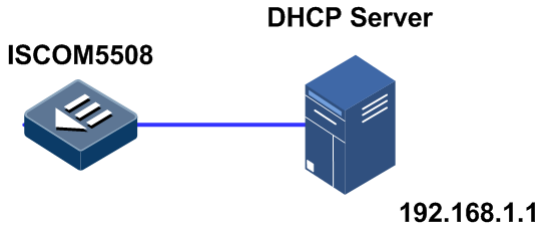

Figure 11-1 DHCP Client networking

Configuration steps

Step 1 Configure DHCP client information.

```
Raisecom#config
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip dhcp client hostname raisecom
```

Step 2 Apply for IP address by DHCP.

```
Raisecom(config-ip)#ip address dhcp server-ip 192.168.1.1
```

Checking results

Show security configuration of all ports in a device by command **show ip dhcp client**.

```
Raisecom(config)#show ip dhcp client
  Hostname:              raisecom
  Class-ID:              raisecomFTTH-ROS_4.9.771
  Client-ID:             raisecomFTTH-000e5e034be5-IF0

  Assigned IP Addr:      192.168.1.2
  Subnet mask:           255.255.255.0
  Default Gateway:       --
  Client lease Starts:       Jan-01-2000 00:00:00
  Client lease Ends:         Jan-01-2000 00:30:00
  Client lease duration:     1800(sec)
  DHCP Server:               192.168.1.1

  Tftp server name:          --
  Tftp server IP Addr:       --
  Startup_config filename:   --
  NTP server IP Addr:        --
  Root path:                 --
```

11.6.2 Examples for configuring DHCP Server

Networking requirements

As shown in below figure, ISCOM5508 which works as DHCP Server device needs to provide dynamic IP address to client device. And configure default out-time period of leasing table as 60 minutes.

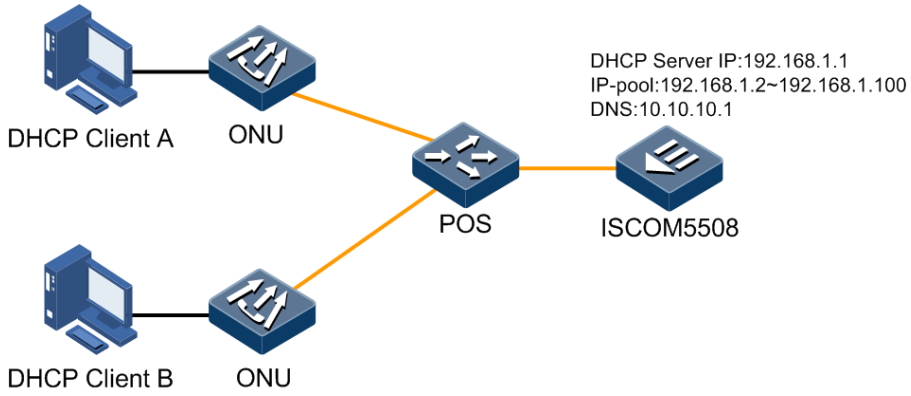

Figure 11-2 Configuring DHCP Server

Configuration steps

Step 1 Configure DHCP Server gateway address.

```
Raisecom#config
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address 192.168.1.1 255.255.255.0 1
Raisecom(config-ip)#ip dhcp server
Raisecom(config-ip)#exit
```

Step 2 Configure DHCP Server IP address pool.

```
Raisecom(config)#ip dhcp server ip-pool raisecom1 192.168.1.2
192.168.1.100 255.255.255.0 ip 0 gateway 192.168.1.1 dns 10.10.10.1
```

Step 3 Configure out-time period of leasing table.

```
Raisecom(config)# ip dhcp server default-least 60
```

Step 4 Enable global DHCP Server service.

```
Raisecom(config)#ip dhcp server
```

Checking results

Show DHCP Server configuration by command **show ip dhcp server**.

```
Raisecom(config)#show ip dhcp server
DHCP Server: Enabled
IP Interface Enabled: 1
Total Number: 1
Option 82: Enabled

Max lease time: 10080 m
Min lease time: 30 m
Default lease time: 60 m

Statistics information:
Running time:  0 hours 0 minutes 36 seconds
Bootps:  1
Discover: 1
Request: 0
Release: 0
Offer: 0
Ack: 0
Nack: 0
Decline: 0
Information: 0
Unknows: 0
Total: 2
```

Show DHCP Server configuration by command **show ip dhcp server ip-pool**.

```
Raisecom(config)#show ip dhcp client ip-pool
-----------------------------------------
Name of IP pool table: raisecom1
Status of IP pool table: active
IP address range: 192.168.1.2 - 192.168.1.100
Mask: 255.255.255.0
Including IP Interface: 1
IP address of gateway: 192.168.1.1
IP address of DNS server: 10.10.10.1
IP address of secondary DNS server: 0.0.0.0
IP address of TFTP server: 0.0.0.0
Boot-file name:
-----------------------------------------
Valid IP pool count: 1
Valid IP address count: 99
Alloted IP address count: 0
```

11.6.3 Examples for configuring DHCP Snooping

Networking requirements

As shown in below figure, ISCOM5508 which works as DHCP Snooping device needs to ensure that DHCP client can get IP address from legal DHCP server, and supports Option 82 function for helping management on client. Configure information filling of electric circuit ID sub-option as Raisecom, and information filling of remote ID sub-option as user01.

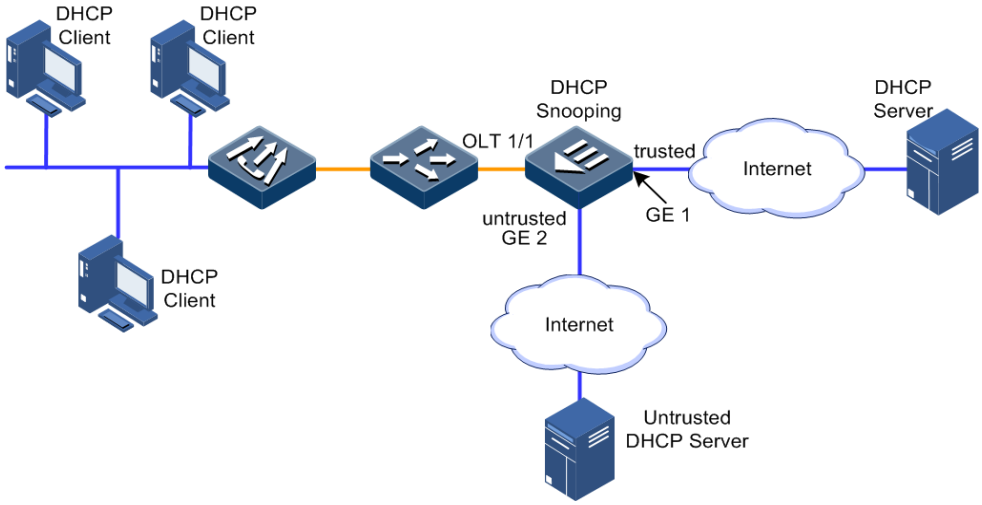

Figure 11-3 Configuring DHCP Snooping

Configuration steps

Step 1 Configure global DHCP Snooping function.

```
Raisecom#config
Raisecom(config)#ip dhcp snooping
```

Step 2 Configure trust port.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#ip dhcp snooping trust
Raisecom(config-port)#exit
```

Step 3 Support option82 function and configure option82 field.

```
Raisecom(config)#ip dhcp snooping information option
Raisecom(config)#ip dhcp information option remote-id string user01
Raisecom(config)#interface port 1
Raisecom(config-port)#ip dhcp information option circuit-id raisecom
```

Checking results

Check whether DHCP client configuration is correct by command **show ip dhcp information option**.

```
Raisecom#show ip dhcp information option
DHCP Option Config Information
  Circuit-ID :  default
  Remote-ID Mode:  string
  Remote-ID String:
  Port:  1    Circuit ID:  raisecom
  Port:  2    Circuit ID:  raisecom
  Port:  3    Circuit ID:  raisecom
  Port:  4    Circuit ID:  raisecom
  Port:  5    Circuit ID:  raisecom
  Port:  6    Circuit ID:  raisecom
ipv4Global
code: 82    content :
ip Port
port: 1
code: 82    content : raisecom
port: 2
port: 3
port: 4
port: 5
port: 6
```

11.6.4 Examples for configuring DHCP Relay

Networking requirements

As shown in below figure, ISCOM5508 which works as DHCP Relay device should ensure that DHCP client in different subnet can get IP address from DHCP server, and supports Option 82 function for helping management on client.

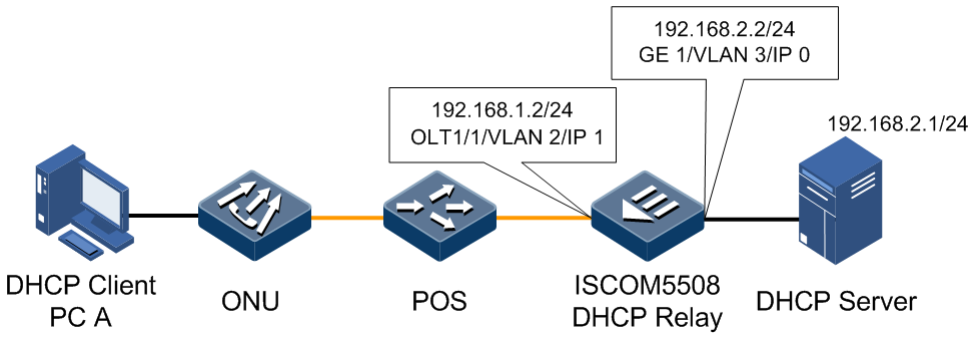

Figure 11-4 Configuring DHCP Relay

Configuration steps

Step 1 Configure global DHCP Relay function.

```
Raisecom#config
Raisecom(config)#ip dhcp relay
```

Step 2 Configure IP address of destination port of IP port 1.

```
Raisecom(config)#ip dhcp relay ip-list 1 target-ip 192.168.2.1
```

Step 3 Support option82 function.

```
Raisecom(config)#ip dhcp relay information option
```

Step 4 Configure port 1 as DHCP Relay trust port.

```
Raisecom(config)#ip dhcp relay information trusted post-list 1
```

Checking results

Check whether DHCP Relay configuration is correct by command **show ip dhcp relay**.

```
Raisecom#show ip dhcp relay
DHCP Relay: Enabled
 IP Interface   Enabled Status   Target IP Address
 ---------------------------------------------------
     0          Enabled           --
     1          Enabled       192.168.2.1
     2          Enabled           --
     3          Enabled           --
     4          Enabled           --
     5          Enabled           --
     6          Enabled           --
     7          Enabled           --
     8          Enabled           --
     9          Enabled           --
     10         Enabled           --
     11         Enabled           --
     12         Enabled           --
     13         Enabled           --
     14         Enabled           --
```

Show trust state of DHCP Relay port and configuration of DHCP Option82 by command **show ip dhcp relay information**.

```
Raisecom#show ip dhcp relay information
Option 82: Enabled
Policy: Replace
 Port     Trusted
 -----------------
 1         yes
 2         no
 3         no
 4         no
 5         no
 6         no
 7         no
 8         no
```

11.6.5 Examples for onfiguring DHCP Option 82

Networking requirements

DHCP Option 82 function is often used together with DHCP Snooping function or DHCP Relay function to determine user location more accurately so as to take different strategy to different user.

In port configuration mode, some vendor requires to use DHCP Option 82 to locate user position more accurately. The location requirement is as below:

<Access-Node-Identifier> / PON / <rack> / <shelf> / <slot> / <PON>: <ONU>. <ONU-slot>.<UNI>

- <Access-Node-Identifier>: node name
- <rack> : rack No.
- <shelf>: sub-frame No.
- <slot>: slot No.
- <PON>: PON port No.
- <ONU>: ONU No.
- <ONU-SLOT>: ONU sub-modules No.
- <UNI>: user physical port No.

Configuration steps

Step 1 Configure port DHCP Option circuit-id.

```
Raisecom#config
Raisecom(config)#interface port 7
Raisecom(config-port)#ip dhcp information option circuit-id
CHINA/PON/1/1/08/01:28.1.10
```

Checking results

Show trust state of DHCP Relay port and configuration of DHCP Option82 by command **show ip dhcp information option**.

```
Raisecom#show ip dhcp information option
DHCP Option Config Information
  Circuit-ID :  default
  Remote-ID Mode:  switch-mac
  Port:  7   Circuit ID:  CHINA/PON/1/1/08/01:28.1.10
```

12 Configuring QoS

The chapter introduces basic principles and configuration procedure of QoS features in ISCOM5508 device, and provides related applications.

- Configuring priority trust
- Configuring flow classification and flow policy
- Configuring priority mapping and queue scheduling
- Configuring speed limit of flow
- Maintenance
- Configuration examples

12.1 Configuring priority trust

12.1.1 Preparing for configuration

Networking situation

User can choose priority for trusted packets, while the untrusted priority packets are processed by traffic classification and traffic policy. After configuring priority trust, device operates packets according to their priorities and provides related service.

12.1.2 Default configuration of priority trust

Default configuration of priority trust on ISCOM5508 device.

Function	Default value
Global QoS function	enable
Type of priority trust	cos

Default configuration of priority trust on Raisecom ONU device.

Function	Default value
priority trust of UNI port	Not trust

12.1.3 Configuring priority trust of OLT

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**mls qos** { **enable** | **disable** }	Enable/disable QoS function globally;
3	Raisecom(config)#**mls qos trust** { **cos** | **dscp** }	Configure type of priority trust;

12.1.4 Configuring priority trust of ONU

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter UNI Ethernet port configuration mode;
4	Raisecom(fttx-onu-uni*/*/*:*)#**qos cos trust**	Configure CoS priority trust; Use **no qos cos trust** to configure no trust CoS priority;

12.1.5 Checking configuration

No.	Item	Description
1	Raisecom#**show mls qos**	Show priority trust configuration of OLT;
2	Raisecom(fttx)#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** [*uni-id*] **qos**	Show QoS configuration of ONU UNI port;

12.2 Configuring flow classification and flow policy

12.2.1 Preparing for configuration

Networking situation

Flow classification is the base of QoS; User can classify packets according to packet features, such as packet priority, source MAC, destination MAC, source IP, destination IP, etc. After classification, the device can take different operation to different packet and provide corresponding service.

Flow classification configuration won't take effect until user binds it to flow policy. Applying flow policy is related to the current network loading condition. Usually, packets flow rate is limited according to configured speed when it enters network, and re-mark priority according to packet service feature.

12.2.2 Configuring flow classification of OLT

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**mls qos** { **enable** | **disable** }	Enable/disable QoS function globally;
3	Raisecom(config)#**class-map** *class-map-name* { **match-all** | **match-any** }	Create flow classification and enter configuration mode of flow classification;
4	Raisecom(config-cmap)#**description** *description*	(Optional) Configure description information of flow classification;
5	Raisecom(config-cmap)#**match** { **access-list-map** | **ip-access-list** | **mac-access-list** } *acl-number*	Configure flow classification based on ACL;
6	Raisecom(config-cmap)#**match class-map** *class-map-name*	Configure flow classification based on flow classification rules;
7	Raisecom(config-cmap)#**match ip dscp** *dscp-value*	Configure flow classification based on DSCP priority;
8	Raisecom(config-cmap)#**match ip precedence** *ip-precedence-value*	Configure flow classification based on IP priority;
9	Raisecom(config-cmap)#**match vlan** *vlan-id* [**double-tagging inner**]	Configure flow classification based on single layer of VLAN or flow classification of internal VLAN of double layers of VLAN;

12.2.3 Configuring flow policy of OLT

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;

Step	Configuration	Description
2	Raisecom(config)#**policy-map** *policy-map-name*	Create flow policy and enter flow policy configuration mode;
3	Raisecom(config-pmap)#**description** *description*	(Optional) Configure description information of flow policy;
4	Raisecom(config-pmap)#**class-map** *class-map-name*	Bind flow classification on flow policy, it's only for matched message of flow classification; Use **no class-map** *class-map-name* to delete flow classification in flow policy; **Note** The flow classification which binds flow policy needs a kind of rules at least, otherwise it fails;
5	Raisecom(config-pmap-c)#**police** *policer-name*	(Optional) apply speed limit for the flow which match flow classification; We should create speed limit rules before using the command, refer to section 12.2.4 Configuring flow limit speed rules of OLT.
6	Raisecom(config-pmap-c)#**copy-to-mirror**	(Optional) apply flow mirroring for the flow which match flow classification;
7	Raisecom(config-pmap-c)#**redirect-to port** *port-id*	(Optional) apply redirection for the flow which match flow classification;
8	Raisecom(config-pmap-c)#**set** { **cos** *cos-value* | **ip dscp** *ip-dscp-value* | **ip precedence** *ip-precedence-value* | **vlan** *vlan-id* }	(Optional) apply resetting for the flow which match flow classification;
9	Raisecom(config-pmap-c)#**statistics enable**	(Optional) apply flow statistics for the flow which match flow classification;
10	Raisecom(config-pmap-c)#**quit** Raisecom(config-pmap)#**quit** Raisecom(config)#**service-policy** *policy-name* { **egress** *port-id* | **ingress** *port-id* }	Apply flow policy on egress or ingress port;

12.2.4 Configuring flow limit speed rules of OLT

When taking flow limit speed based on flow policy to packets, user needs to create flow limit speed rule and quote this rule in the flow classification bound to flow policy.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;

Step	Configuration	Description
2	Raisecom(config)#**mls qos aggregate-policer** *policer-name rate burst* [**exceed-action** { **drop** | **policed-dscp-transmit** *dscp-id* }]	(Optional) Create speed limit rules whose type is aggregate; All classes share the policer in a policy;
3	Raisecom(config)#**mls qos class-policer** *policer-name rate burst* [**exceed-action** { **drop** | **policed-dscp-transmit** *dscp-id* }]	(Optional) Create speed limit rules whose type is class; All match rules in a class share the policer;
4	Raisecom(config)#**mls qos single-policer** *policer-name rate burst* [**exceed-action** { **drop** | **policed-dscp-transmit** *dscp-id* }]	(Optional) Create speed limit rules whose type is single; All match rules in a class-map share the policer.

12.2.5 Configuring flow classification and flow policy of ONU

Flow classification and flow policy can divide the packets into different flow according to service demand and packets features so as to distinguish and achieve different service. Port flow filter refers to forward and discard the qualified flow.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**create class** *rule-id* **match** { **cos** *cos-vlaue* | **pre** *pre-value* | **dip** *ip-address* | **sip** *ip-address* | **dmac** *mac-address* | **smac** *mac-address* | **l4-dport** *port-number* | **l4-sport** *port-number* | **dscp** *dscp-value* | **eth-type** *type-vlaue* | **protocol** { *protocol-number* | **icmp** | **igmp** | **tcp** | **udp** } | **vlan** *vlan-id* } { **always-match** | **equal** | **exist** | **greater-equal** | **less-equal** | **never-match** | **not-equal** | **not-exist** }	Define classification rules of data flow; Use **no class** {**all** | *rule-id*} to delete flow classification rules;
3	Raisecom(fttx)#**create policy** *rule-id* **class** *rule-list* **queue-map** *queue-id* **pri-marking** *priority* [**weight** *weight-value*]	Configure flow policy; Use **no policy** {**all** | *rule-id*} to delete flow policy;
4	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
5	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter ONU UNI Ethernet port configuration mode;
6	Raisecom(fttx-onu-uni*/*/*:*)#**policy** *rule-list*	Apply flow policy on UNI port; Use **no policy** to delete flow policy on UNI;
7	Raisecom(fttx-onu-uni*/*/*:*)#**filter** { **permit** | **deny** } { **match-all** | **match-any** } **policy** *rule-list*	(Optional) Configure filtering rules;

Step	Configuration	Description
8	Raisecom(fttx-onu-uni*/*/*:*)#**qos cos-override** { **enable** | **disable** }	(Optional) Enable/disable port priority override function;
9	Raisecom(fttx-onu-uni*/*/*:*)#**qos map cos-cos** *value0 value1 value2 value3 value4 value5 value6 value7*	(Optional) Configure priority resetting;

12.2.6 Checking configuration

No.	Item	Description
1	Raisecom#**show class-map** [*class-map-name*]	Show flow classification rules configuration of OLT;
2	Raisecom#**show mls qos policer** [*policer-name* | **aggregate-policer** | **class-policer** | **single-policer**]	Show speed limit rules configuration of OLT;
3	Raisecom#**show policy-map** [*policy-map-name* | **class** *class-map-name*]	Show flow policy configuration of OLT;
4	Raisecom(fttx)#**show onu-remote class** { **all** | *rule-list* }	Show flow classification configuration of ONU;
5	Raisecom(fttx)#**show onu-remote policy** { **all** | *rule-list* }	Show flow policy configuration information of ONU;
6	Raisecom(fttx)#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** [*uni-id*] **policy**	Show applied flow classification policy on UNI;

12.3 Configuring priority mapping and queue scheduling

12.3.1 Preparing for configuration

Networking situation

When network has congestion, user want to balance delay and delay jitter of various packets, packets of key services (like video and voice) can be processed preferentially; packets of secondary services (like E-Mail) with identical priority can be fairly processed, different priority can be processed according to its weight value. User can configure queue schedule in this situation. Selection of schedule algorithm is depended on service condition and customer requirements.

Priority mapping is precondition for queue schedule. User can map priority of packets to different local priority, and device perform queue schedule for the packets according to local priority. Generally speaking, IP packets need to configure mapping relationship between DSCP priority and local priority; VLAN packets need to configure mapping relationship between CoS priority and local priority.

12.3.2 Default configuration of priority mapping and queue scheduling

Default configuration of priority mapping and queue scheduling on ISCOM5508 device.

Function	Default value
OLT queue scheduling mode	SP
ONU queue scheduling mode	SP

Mapping of COS priority and local priority on ISCOM5508 device:

Local Priority	0	1	2	3	4	5	6	7
CoS	0	1	2	3	4	5	6	7

Mapping of DSCP priority and local priority on ISCOM5508 device:

Local Priority	0	1	2	3	4	5	6	7
DSCP	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63

Mapping of local priority and queue on ISCOM5508 device:

Local Priority	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

Weight of SP, DRR and WRR in ISCOM5508:

Queue	1	2	3	4	5	6	7	8
SP weight	1	1	1	1	1	1	1	1
DRR weight	1	1	1	1	1	1	1	1
WRR weight	1	1	1	1	1	1	1	1

Mapping of priority and queue of Raisecom ONU:

CoS	0	1	2	3	4	5	6	7
Queue	0	0	1	1	2	2	3	3

Queue weight of Raisecom ONU (the lager weight, the higher priority. 0 stands for the highest priority):

Queue	0	1	2	3	4	5	6	7
Weight	1	2	4	8	0	0	0	0

12.3.3 Configuring priority mapping of OLT

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**mls qos** { **enable** | **disable** }	Enable/disable QoS function globally;
3	Raisecom(config)#**mls qos mapping cos** *cos-value* **to localpriority** *local-priority*	(Optional) Configure mapping of CoS priority and internal priority;
3	Raisecom(config)#**mls qos mapping dscp** *dscp-value* **to localpriority** *local-priority*	(Optional) Configure mapping of DSCP priority and internal priority;

12.3.4 Configuring internal priority of OLT based on port

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer port configuration mode;
3	Raisecom(config-port)#**mls qos port-priority** *local-priority*	Configure internal priority based on port;

12.3.5 Configuring SP queue scheduling of OLT

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer port configuration mode;
3	Raisecom(config-port)#**mls qos queue scheduler sp**	Configure scheduler of message queue as SP;

12.3.6 Configuring WRR queue scheduling of OLT

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer port configuration mode;

Step	Configuration	Description
3	Raisecom(config-port)#**mls qos queue scheduler wrr**	Configure scheduler of message queue as WRR;
4	Raisecom(config-port)#**mls qos queue wrr** *weight1 weight2 weight3 weight4 weight5 weight6 weight7 weight8*	Configure priority of each queue; If priority of a queue is 0, the queue will be configured by SP scheduling;

12.3.7 Configuring DRR queue scheduling of OLT

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer port configuration mode;
3	Raisecom(config-port)#**mls qos queue scheduler drr**	Configure scheduler of message queue as DRR;
4	Raisecom(config-port)#**mls qos queue drr** *weight1 weight2 weight3 weight4 weight5 weight6 weight7 weight8*	Configure scheduler of message queue as DRR, and configure priority of each queue; If priority of a queue is 0, the queue will be configured by SP scheduling;

12.3.8 Configuring priority mapping of ONU

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**queue cos-map** *value0 value1 value2 value3 value4 value5 value6 value7*	Configure mapping of CoS priority and queue;

12.3.9 Configuring queue scheduling of ONU

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;

Step	Configuration	Description
3	Raisecom(fttx-onu*/*:*)#**queue** { **preempt-wrr** | **strict-priority** | **wrr-weight** }	Configure queue scheduling mode of ONU PON port;
4	Raisecom(fttx-onu*/*:*)#**queue weight** *weight0 weight1 weight2 weight3 weight4 weight5 weight6 weight7*	Configure weight of queue;

12.3.10 Checking configuration

No.	Item	Description
1	Raisecom#**show mls qos mapping** { **cos** | **dscp** | **localpriority** }	Show priority mapping configuration of OLT;
2	Raisecom#**show mls qos queue**	Show queue scheduling configuration;
3	Raisecom(fttx)#**show interface onu** *slot-id/olt-id/onu-id* **queue**	Show queue scheduling mode of ONU;

12.4 Configuring speed limit of flow

12.4.1 Preparing for configuration

Networking situation

When network has congestion, user can configure speed limit over port or VLAN to restrict burst traffic flow at a port or a VLAN to make it transports in a well-proportioned rate, so as to remove network congestion.

Precondition

Related VLAN must be created before configuring speed limit over VLAN or QinQ.

12.4.2 Configuring flow speed limit of OLT based on port

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**rate-limit port** *port-id* { **both** | **egress** | **ingress** } *rate-value* [*burst-value*]	Configure speed limit based on port;

12.4.3 Configuring flow speed limit of OLT based on VLAN or QinQ

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**rate-limit vlan** *vlan-id rate-value burst-value* [**statistics**]	Configure speed limit based on VLAN;
3	Raisecom(config)#**rate-limit double-tagging-vlan outer** { *outer-vlan-id* | **any** } **inner** { *inner-vlan-id* | **any** } *rate-value burst-value* [**statistics**]	Configure speed limit based on QinQ;

12.4.4 Configuring flow speed limit of ONU UNI port

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter ONU UNI Ethernet port configuration mode;
4	Raisecom(fttx-onu-uni*/*/*:*)#**policing** { **all** | **egress** | **ingress** } { **enable** | **disable** }	Enable/disable speed limit of UNI port;
5	Raisecom(fttx-onu-uni*/*/*:*)#**policing egress cir** *cir* [**pir** *pir*]	Configure speed limit of flow on UNI downlink direction; Use **no policing egress cir** to return to default configuration;
6	Raisecom(fttx-onu-uni*/*/*:*)#**policing ingress cir** *cir* [**cbs** *cbs*] [**ebs** *ebs*]	Configure speed limit of flow on UNI downlink direction; Use **no policing ingress cir** to return to default configuration;

12.4.5 Checking configuration

No.	Item	Description
1	Raisecom#**show rate-limit port-list**	Show speed limit configuration based on port;
2	Raisecom#**show rate-limit vlan**	Show speed limit configuration based on VLAN or QinQ;
3	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** [*uni-id*] **policing**	Show speed limit configuration on uplink/downlink port of ONU UNI Ethernet port;

12.5 Maintenance

Command	Description
Raisecom(config)#**clear service-policy statistics** { **egress** | **ingress** } **port** *port-id* [**class-map** *class-map-name*]	Clear message statistics information of QoS;

12.6 Configuration examples

12.6.1 Examples for configuring flow speed limit based on flow policy

Networking requirements

As shown in below figure, User A, User B, User C belongs to VLAN1, VLAN2, and VLAN3 respectively, and connects with each other by ONU A, ONU B, ONU C and OLT.

User A provides voice and video, User B provides voice, video and data, and User C provides video and data.

- For User A, we provide 25M guaranteed bandwidth, burst flow allows 100KB, discard redundant flow;
- For User B, we provide 35M guaranteed bandwidth, burst flow allows 100KB, discard redundant flow;
- For User C, we provide 30M guaranteed bandwidth, burst flow allows 100KB, discard redundant flow;

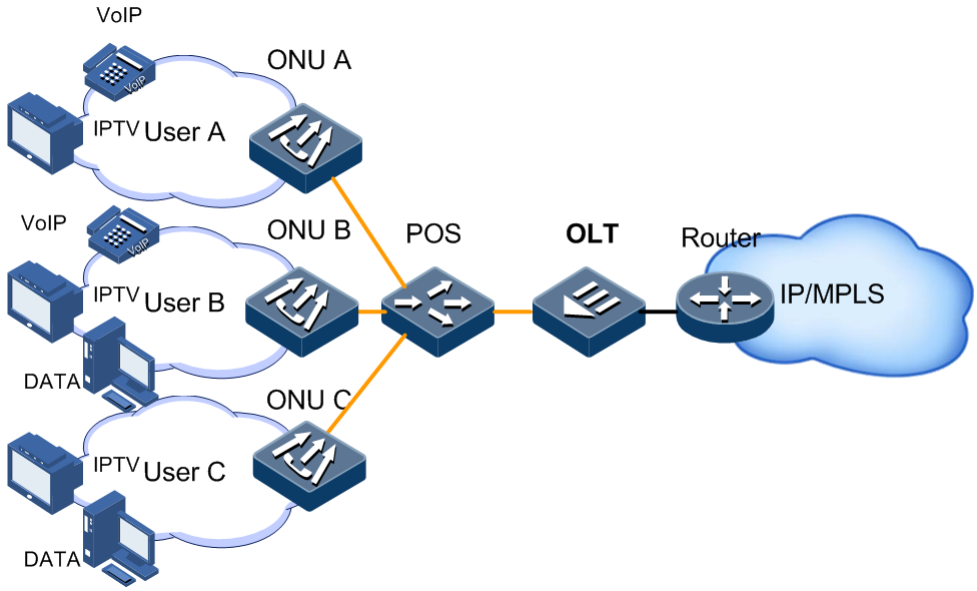

Figure 12-1 Configuring speed limit based on flow policy

Configuration steps

Step 1 Create and configure flow classification according to VLAN ID for different users.

```
Raisecom#config
Raisecom(config)#mls qos enable
Raisecom(config)#class-map map-a match-any
Raisecom(config-cmap)#match vlan 1
Raisecom(config-cmap)#quit
Raisecom(config)#class-map map-b match-any
Raisecom(config-cmap)#match vlan 2
Raisecom(config-cmap)#quit
Raisecom(config)#class-map map-c match-any
Raisecom(config-cmap)#match vlan 3
Raisecom(config-cmap)#quit
```

Step 2 Create speed limit of flow rules.

```
Raisecom(config)#mls qos single-policer usera 25000 100 exceed-action
drop
Raisecom(config)#mls qos single-policer userb 35000 100 exceed-action
drop
Raisecom(config)#mls qos single-policer userc 30000 100 exceed-action
drop
```

Step 3 Create and configure flow policy.

```
Raisecom(config)#policy-map rule1
Raisecom(config-pmap)#class-map map-a
Raisecom(config-pmap-c)#police usera
Raisecom(config-pmap-c)#exit
Raisecom(config-pmap)#class-map map-b
Raisecom(config-pmap-c)#police userb
Raisecom(config-pmap-c)#exit
Raisecom(config-pmap)#class-map map-c
Raisecom(config-pmap-c)#police userc
Raisecom(config-pmap-c)#quit
Raisecom(config-pmap)#quit
Raisecom(config)#service-policy rule1 ingress 7
```

Checking results

Show whether configuration of flow classification is correct.

```
Raisecom#show class-map map-a
 Class Map match-any map-a (id 0)
    Match vlan 1
Raisecom#show class-map map-b
 Class Map match-any map-b (id 1)
    Match vlan 2
Raisecom#show class-map map-c
 Class Map match-any map-c (id 2)
    Match vlan 3
```

Show whether configuration of flow speed limit rule is correct.

```
Raisecom(config)#show mls qos policer usera
single-policer usera cir 25000  cbs 100 exceed-action drop
 Used by policy map usera
Raisecom(config)#show mls qos policer userb
single-policer usera cir 35000  cbs 100 exceed-action drop
 Used by policy map userb
Raisecom(config)#show mls qos policer userc
single-policer usera cir 30000  cbs 100 exceed-action drop
 Used by policy map userc
```

Show whether configuration of flow policy is correct.

```
Raisecom(config)#show policy-map rule1
  Policy Map rule1
    Class map-a
        police usera
    Class map-2
```

```
    police userb
class map-c
    police userc
```

12.6.2 Examples for configuring queue scheduling

Networking requirements

As shown in below figure, User A provides voice and video, User B provides voice, video and data, and User C provides video and data.

CoS priority of voice service is 5, CoS priority of video service is 4, and CoS priority of data service is 2. Internal priority of the above services is 6, 5, and 2 respectively.

- For voice service, SP scheduling is necessary;
- For video service, WRR scheduling is necessary, weight is 15;
- For data service, WRR scheduling is necessary, weight is 12, and we need configure discard threshold is 15 for avoiding network congestion.

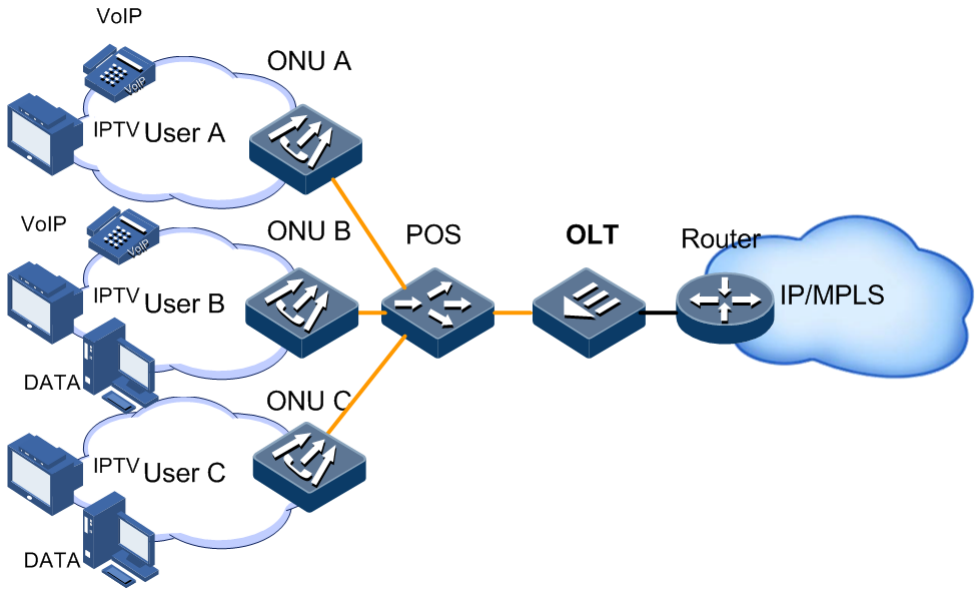

Figure 12-2 Configuring queue scheduling

Configuration steps

Step 1 Configure port priority trust.

```
Raisecom#config
Raisecom(config)#mls qos enable
Raisecom(config)#mls qos trust cos
```

Step 2 Configure mapping of CoS priority and internal priority.

```
Raisecom(config)#mls qos mapping cos 5 to localpriority 6
Raisecom(config)#mls qos mapping cos 4 to localpriority 5
Raisecom(config)#mls qos mapping cos 2 to localpriority 2
```

Step 3 Configure SP+WRR queue scheduling.

```
Raisecom(config)#mls qos queue wrr 1 1 12 1 1 15 0 0
```

Checking results

Show whether mapping configuration of specific priority is correct by command **show mls qos mapping**.

```
Raisecom(config)#show mls qos mapping cos

  CoS-LocalPriority Mapping:

           CoS:   0  1  2  3  4  5  6  7
 ------------------------------------------------
 LocalPriority:   0  1  2  3  5  6  6  7
```

Show whether configuration of queue scheduling is correct by command **show mls qos queue**.

```
Raisecom(config)#show mls qos queue

  Queue    Weight(WRR)
-------------------------
  1       1
  2       1
  3       12
  4       1
  5       1
  6       15
  7       0
  8       0

  Queue    Weight(DRR)
-------------------------
  1       0
  2       0
  3       0
  4       0
  5       0
  6       0
  7       0
  8       0
```

12.6.3 Examples for configuring flow speed limit based on VLAN

Networking requirements

As shown in below figure, User A, User B, User C belongs to VLAN1, VLAN2, and VLAN3 respectively, and connects with each other by ONU A, ONU B, ONU C and OLT.

User A provides voice and video, User B provides voice, video and data, and User C provides video and data.

- For User A, we provide 25M guaranteed bandwidth, burst flow allows 100KB, discard redundant flow;
- For User B, we provide 35M guaranteed bandwidth, burst flow allows 100KB, discard redundant flow;
- For User C, we provide 30M guaranteed bandwidth, burst flow allows 100KB, discard redundant flow;

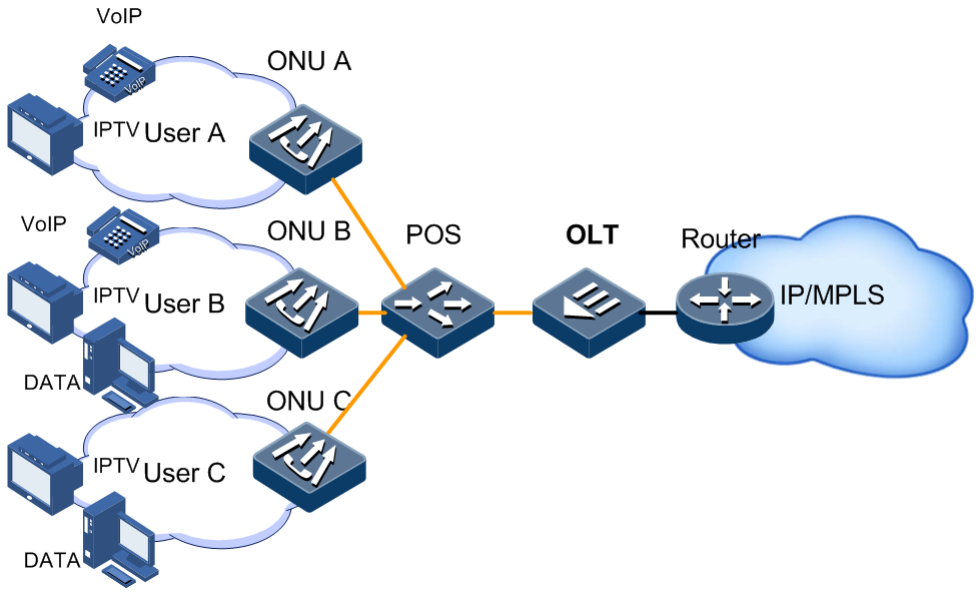

Figure 12-3 Configuring speed limit based on port

Configuration steps

Step 1 Configure speed limit based on VLAN.

```
Raisecom#config
Raisecom(config)#rate-limit vlan 1 25000 100
Raisecom(config)#rate-limit vlan 2 35000 100
Raisecom(config)#rate-limit vlan 3 30000 100
```

Checking results

Show whether configuration of speed limit based on VLAN is correct by command **show rate-limit port-list**.

```
Raisecom(config)#show rate-limit vlan
CVLAN: Customer VLAN(inner VLAN)
SPVLAN:Service provider VLAN(outer VLAN)
StatisHw:Statistics Hardware
Inp: Inprofile
OutP:Outprofile
Type   CVLAN SPVLAN Rate(kbps)  Burst(kB)   StatHw   Inp(Pkts)
Outp(Pkts)
-------------------------------------------------------------------------
single 1   --    25063       128        Yes     0                       0
single 2   --    35063       128        Yes     0                       0
single 3    --   30063       128        No      --                      -
```

13 Configuring OAM

The chapter introduces basic principles and procedure of OAM features in ISCOM5508 device, and provides related applications.

- Configuring CFM
- Configuring SLA
- Configuration examples

13.1 Configuring CFM

13.1.1 Preparing for configuration

Networking situation

To develop Ethernet technology application in telecommunication network, Ethernet needs to realize service level identical to telecommunication transmission network. CFM provides full OAM tool to solve this problem through telecommunication Ethernet.

CFM provides the below OAM functions:

- Fault detection function (CC, Continuity Check)
  - This function is realized by MEP sends CCM (Continuity Check Message) periodically, other MEP in one service instance receives packet to confirm status of RMEP. If device fault or link configuration uncorrected may cause MEP cannot receive and process CCM from RMEP. If MEP hasn't received remote CCM packet in 3.5 CCM interval, the link is considered to be fault, system will send fault trap according to alarm priority configuration.
- Fault acknowledgement function (LB, LoopBack)
  - This function confirm connectivity between two MP by sending LBM (LoopBack Message) from source MEP and answering LBR (LoopBack Reply) by destination MP. Source MEP sends LBM to MP for fault acknowledgement, the MP receives LBR and sends a LBR to source MEP, if source MEP received LBR the path is connective, if source MEP doesn't receive LBR the path is not connective.
- Fault location function (LT, LinkTrace)

  - Source MEP sends LTM (LinkTrace Message) to destination MP, each MP device on LTM transmitting path answers LTR (LinkTrace Reply) to source MEP, the function records efficient LTR and LTM fault location point.
- Alarm indicator signal function (AIS, Alarm Indication Signal)
  - This function is used to stop alarm when detected fault at server layer (sub-layer). MEP (including server MEP) sends AIS frame to client MD when detected fault. ETH-AIS frame is transmitted on MEP (or server MEP). When receiving AIS frame, it doesn't contain peer MEP information of fault, the MEP must inhibit all peer MEP trap regardless the connectivity status. It is able to inhibit client alarm information when server layer has fault through AIS function, then network is easier to manage and maintain.
- Ethernet signal lock function (LCK, Lock)
  - This function is used to notify management lock for server layer (sub-layer) MEP and the followed data service traffic halt. The service traffic is sent for MEP expected to receive traffic. Then MEP receives ETH-LCK frame can identify it is fault or management lock of server layer MEP. Lock is OAM function according to requirement, a typical application of MEP lock is when performing diagnostic test when service halts.

Anyway, CFM implements end-to-end service OAM technology, reducing service provider operation cost and improve completion.

Precondition

Users should complete the following tasks before configuring CFM:

- Connect with ports and configure physical parameters of port, and physical layer state of port is up;
- Create VLAN;
- Add port into VLAN.

13.1.2 Default configuration of CFM

Function	Default value
Global CFM function status	disable
CFM function status on port	enable
MD status	nonexistent
MEP status based on service instance	Up direction
aging time of remote MEP	100minutes
Saving time of error CCM message	100minutes
status of MEP sending CCM message	Not sent
Mode of MEP sending CCM message	passive mode
Time interval of sending CCM message	1s

Function	Default value
dynamic import function learned by service instance remote MEP	Not take effect
cc check function of remote MEP	disable
CFM OAM message priority	6
two-layer ping function status	The number of sending LBM message is 5, the length of message TLV is 64.
switch status of LinkTrace database	disable
Saving time of LinkTrace database	100minutes
AIS sending function status	disable
AIS sending period	1s
alarm suppression function status	enable
LCK message sending function status	disable

13.1.3 Enabling CFM

CC and LT functions take effect only if CFM enables on device.

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode;
2	`Raisecom(config)#ethernet cfm { enable | disable }`	Enable/disable CFM function globally;
3	`Raisecom(config)#interface port` *port-id*	Enter physical layer port configuration mode;
4	`Raisecom(config-port)#ethernet cfm { enable | disable }`	(Optional) enable CFM function on port;

13.1.4 Configuring basic function of CFM

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode;

Step	Configuration	Description
2	Raisecom(config)#**ethernet cfm domain** [**md-name** *domain-name*] **level** *level*	Create maintenance field, use parameter **md-name** to specify name of maintenance field as 802.1ag. MA and CCM are all 802.1ag; the maintenance field is Y.1731 if it doesn't specify name, and MA and CCM are all Y.1731. If it specifies name of maintenance field, the name is unique, otherwise configuration of maintenance field fails. **Note** Level of different maintenance fields is different; otherwise configuration of maintenance field fails.
3	Raisecom(config)#**service** *cisid* **level** *level*	Create service instance and enter configuration mode of it. (name of maintenance field, name of service instance) component character string is unique in global range. Enter service instance configuration mode directly when configuring the command if there is already a service instance.
4	Raisecom(config-service)#**service vlan-list** *vlan-list* [**primary-vlan** *vlan-id*]	Configure VLAN mapping of service instance. 32 VLAN in VLAN list at most, if parameter primary-vlan doesn't specify master VLAN, the minimum VLAN works as master VALN of service instance. All MEP receive and send packets by master VLAN. **Note** All VLAN except for master VLAN map into master VLAN logically, the mapping relation is global, they can be the same, but intersect.
5	Raisecom(config-service)#**service mep** [**up** | **down**] **mepid** *mepid* **port** *port-id*	Configure MEP based on service instance; service instance must mapping with VLAN when configuring the MEP; **Note** Configure MEP port as up, the device sends CCM message to all inner ports excepting for MEP port. Configure MEP port as down, the device sends CCM message by MEP port.

13.1.5 Configuring Continuity Check (CC)

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ethernet cfm remote mep age-time** *minute*	(Optional) Configure aging time of remote MEP; By default, aging time of learned remote MEP is 100 minutes;

Step	Configuration	Description
3	Raisecom(config)#**ethernet cfm errors archive-hold-time** *minute*	(Optional) Configure saving time of error CCM message; fault information of all MEP reports is saved in the device; By default, saving time of error CCM message is 100 minutes; system will detect data in database if configuring new saving time, and clear data if it exceeds the time.
4	Raisecom(config)#**service** *cisid* **level** *level*	Enter service instance configuration mode;
5	Raisecom(config-service)#**service cc** { **enable** | **disable** } **mep** { *mepid-list* | **all** }	Enable/disable MEP sending CCM message;
6	Raisecom(config-service)#**service cc interval** { **1** | **10** | **60** | **600** | **3ms** | **10ms** | **100ms** }	(Optional) Configure sending time interval of service instance CCM message; By default, sending time interval of CCM message of service instance is 10s; the sending time interval of CCM message can't be modified if it enables.
7	Raisecom(config-service)#**service remote-mep** *mepid* [**port** *port-id*]	(Optional) Configure static remote MEP and cooperate with cc check function;
8	Raisecom(config-service)#**service remote-mep learning active**	(Optional) Configure dynamic import function learned by remote MEP; service instance will convert learned dynamic remote MEP to static remote MEP automatically if receiving CCM message; By default, dynamic import function learned by service instance remote MEP doesn't take effect;
9	Raisecom(config-service)#**service remote-mep cc-check enable**	(Optional) Configure cc check function of remote MEP; System will detect whether dynamic learned ID of remote MEP is consist with ID of static remote MEP, if not, it's a wrong CCM message; By default, disable the function;
10	Raisecom(config-service)#**service cvlan** *vlan-id*	(Optional) Configure client VLAN of CFM OAM message only in QinQ networking; By default, CFM OAM message doesn't take C-TAG, all CCM, LTM, LBM, DMM sent from MEP in service instance carry double-deck TAG, where C-TAG uses the command to configure client VLAN;
11	Raisecom(config-service)#**service priority** *priority*	(Optional) Configure priority of CFM OAM message; CCM, LBM, LTM, DMM message sent form all MEP use specific priority in service instance after configuring priority of messages; By default, priority of messages is 6;

Step	Configuration	Description
12	Raisecom(config-service)#**snmp-server trap cfm** { **all** | **ccmerr** | **macremerr** | **none** | **remerr** | **xcon** } **mep** { *mepid-list* | **all** }	(Optional) Configure fault alarm type which is allowed to send by CFM; CC function of CFM can detect five levels of faults: • level 5: cross connection fault • level 4: CCM error fault • level 3: remote MEP loss fault • level 2: port status fault • level 1: RDI fault By default, macremerr allows level 2–5 fault alarm; **Note** If CFM detects fault, same level or lower level of faults won't generate alarm before removing fault; the fault status will be cleared after 10s if CFM fault has been removed.

13.1.6 Configuring LoopBack (LB)

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**service** *cisid* **level** *level*	Enter service instance configuration mode;
3	Raisecom(config-service)#**ping** { *mac-address* | **mep** *rmepid* } [**count** *count*] [**size** *size*] [**source** *mepid*]	Execute two-layer ping function which is used in loopback; By default, the number of sending LBM message is 5, the length of message TLV is 64, and search a useful source MEP automatically; CFM need finds MAC address of destination MEP by mepid to finish ping operation if two-layer ping operation is done by specifying destination mepid. Source MEP finds remote MEP and it is steady, it will save data of remote MEP in remote MEP database in MEP. The MAC address of remote MEP can be found by mepid.

Note

- users should ensure that global CFM enables before executing the command, otherwise it fails;
- if MEP doesn't be configured in service instance, ping operation will fails because system can't find source MEP;
- if specific source is of no effect, it leads to ping operation fails;
- if specific destination MEPID executes ping operation, ping operation fails if system can't find MAC address of destination MEP;
- Ping operation fails if other users are using specific source MEP.

13.1.7 Configuring LinkTrace (LT)

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ethernet cfm traceroute cache** { **enable** | **disable** }	(Optional) Enable/disable LinkTrace database switch; if switch enables, system will find path information by database storage protocol, and it can be seen by **show ethernet cfm traceroute cache**; result of traceroute will be cleared automatically if switch disables;
3	Raisecom(config)#**ethernet cfm traceroute cache hold-time** *minute*	(Optional) Configure saving time of LinkTrace database; if LinkTrace database switch enables, user can configure the time; By default, saving time is 100minutes;
4	Raisecom(config)#**ethernet cfm traceroute cache size** *size*	(Optional) Configure the number of LinkTrace database entries. If LinkTrace database switch enables, user can configure the number of entries; By default, he number of entries is 100; system doesn't save data if switch disables.
5	Raisecom(config)#**service** *cisid* **level** *level*	Enter service instance configuration mode;
6	Raisecom(config-service)#**traceroute** { *mac-address* | **mep** *rmepid* } [**ttl** *ttl*] [**source** *mepid*]	two-layer Traceroute function is used in LinkTrace; By default, the length of message TLV is 64, and find a useful source MEP automatically; CFM need finds MAC address of destination MEP by mepid to finish ping operation if two-layer ping operation is done by specifying destination mepid. Source MEP finds remote MEP and it is steady, it will save data of remote MEP in remote MEP database in MEP. The MAC address of remote MEP can be found by mepid.

Note

- Users should ensure that global CFM enables before executing the command, otherwise it fails;
- if MEP doesn't be configured in service instance, Traceroute operation will fails because system can't find source MEP;
- if specific source is of no effect, it leads to Traceroute operation fails;
- if specific destination MEPID executes Traceroute operation, Traceroute operation fails if system can't find MAC address of destination MEP;
- Traceroute operation fails if other users are using specific source MEP.

13.1.8 Configuring Alarm Indication Signal (AIS)

- Configure AIS on server layer device.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**service** *cisid* **level** *level*	Enter service instance configuration mode;

Step	Configuration	Description
3	Raisecom(config-service)#**service ais** { **enable** | **disable** }	Enable/disable AIS sending function;
4	Raisecom(config-service)#**service ais period** { **1** | **60** }	Configure AIS sending period; By default, sending period is 1s;
5	Raisecom(config-service)#**service ais level** *level*	AIS is sent to client MD and configure the level of the client MD;

- Configure AIS on client layer device.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**service** *cisid* **level** *level*	Enter service instance configuration mode;
3	Raisecom(config-service)#**service suppress-alarms** { **enable** | **disable** } **mep** { *mepid* | **all** }	Enable/disable alarm suppression function;

13.1.9 Configuring Lock (LCK)

Configure LCK on server layer device.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**service** *cisid* **level** *level*	Enter service instance configuration mode;
3	Raisecom(config-service)#**service lck start mep** { *mepid* | **all** }	Enable LCK message sending function; By default, system doesn't enable LCK sending function; use **service lck stop mep** *mepid* to disable the function;
4	Raisecom(config-service)#**service lck period** { **1** | **60** }	Configure sending period of LCK message; By default, sending period is 1s;
5	Raisecom(config-service)#**service lck level** *level*	LCK is sent to client layer MD and configure the level of the client MD;

Configure LCK on server layer device.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**service** *cisid* **level** *level*	Enter service instance configuration mode;

Step	Configuration	Description
3	Raisecom(config-service)#**service suppress-alarms** { **enable** | **disable** } **mep** { *mepid* | **all** }	Enable/disable alarm suppression function;

13.1.10 Checking configuration

No.	Item	Description
1	Raisecom#**show ethernet cfm**	Show CFM global configuration;
2	Raisecom#**show ethernet cfm domain** [**level** *level*]	Show maintenance field and service instance configuration;
3	Raisecom#**show ethernet cfm errors** [**level** *level*]	Show error CCM database information;
4	Raisecom#**show ethernet cfm lck** [**level** *level*]	Show Ethernet lock signal;
5	Raisecom#**show ethernet cfm local-mp** [**interface port** *port-id* | **level** *level*]	Show local MEP configuration;
6	Raisecom#**show ethernet cfm remote-mep static**	Show static remote MEP information;
7	Raisecom#**show ethernet cfm remote-mep** [**level** *level* [**service** *service-instance* [**mep** *mepid*]]]	Show remote MEP information;
8	Raisecom#**show ethernet cfm suppress-alarms** [**level** *level*]	Show configuration of CFM alarm suppression function;
9	Raisecom#**show ethernet cfm traceroute-cache**	Show LinkTrace database path discovery;

13.2 Configuring SLA

13.2.1 Preparing for configuration

Networking situation

In order to guarantee user to enjoy a certain quality of network service, the operators and customers will sign SLA agreement. To fulfill SLA agreement effectively, the operators need to deploy SLA features on device to measure network performance and take measurement results as a basis for user performance guarantee.

SLA feature chooses two check points, and one configures SLA work and executes it, in order to check network performance of network between two points.

SLA feature statistics go there and back packet drop rate, return or one-way (SD/DS) delay, jitter, and so on. System will report data to upper monitor software, in order to analysis network performance.

Precondition

Users need to complete the task before configuring SLA:

Deploy CFM between the devices to detect

13.2.2 Default configuration of SLA

Function	Default value
SLA scheduling information status	disable
SLA layer-2 work services level	Level 0
Time interval of SLA jitter work detection	1s
The number of SLA jitter work detection message	10
Life cycle of SLA work scheduling	forever
Test cycle of SLA work scheduling	20s

13.2.3 Configuring basic information of SLA work

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**sla** *oper-num* **y1731-echo remote-mep** *mep-id* **level** *level* **svlan** *vlan-id* [**cvlan** *vlan-id*] [**cos** *cos-value*][**dm**]	Configure SLA y1731-echo work according to destination MEP number;
3	Raisecom(config)#**sla** *oper-num* **y1731-echo remote-mac** *mac-address* **level** *level* **svlan** *vlan-id* [**cvlan** *vlan-id*] [**cos** *cos-value*][**dm**]	Configure SLA y1731-echo work according to destination MAC;
4	Raisecom(config)#**sla** *oper-num* **y1731-jitter remote-mep** *mep-id* **level** *level* **svlan** *vlan-id* [**cvlan** *vlan-id*] [**interval** *period*] [**packets** *packets-num*] [**cos** *cos-value*] [**dm**]	Configure SLA y1731-jitter work according to destination MEP;
5	Raisecom(config)#**sla** *oper-num* **y1731-jitter remote-mac** *mac-address* **level** *level* **svlan** *vlan-id* [**cvlan** *vlan-id*] [**interval** *period*] [**packets** *packets-num*] [**cos** *cos-value*] [**dm**]	Configure SLA y1731-jitter work according to destination MAC;
6	Raisecom(config)#**sla** *oper-num* **icmp-echo dest-ipaddr** *ip-address* [**dscp** *dscp-value*]	Configure basic information of SLA icmp-echo work;
7	Raisecom(config)#**sla** *oper-num* **icmp-jitter dest-ipaddr** *ip-address* [**dscp** *dscp-value*] [**interval** *period*] [**packets** *packets-nums*]	Configure basic information of SLA icmp-jitter work;
8	Raisecom(config)#**sla y1731-echo quick-input** [**level** *level* [**svlan** *vlan-id*]] [**dm**]	Quickly create y1731-echo work;
9	Raisecom(config)#**sla y1731-jitter quick-input** [**level** *level* [**svlan** *vlan-id*]] [**dm**]	Quickly create y1731-jitter work;

Note

- Users can't modify or configure the basic information again if the basic information of a work has been configured;
- The maximum number of entries in SLA work is 100. Users can't modify or configure the basic information again if the basic information of a work has been configured.

13.2.4 Configuring SLA scheduling information and enabling work scheduling

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**sla schedule** *oper-num* [**life** { **forever** | *life-time* }] [**period** *period*]	Configure SLA scheduling information, and enables LA work scheduling; By default, disable scheduling;

13.2.5 Checking configuration

No.	Item	Description
1	Raisecom#**show sla** { **all** | *oper-num* } **configuration**	Show SLA configuration;
2	Raisecom#**show sla** { **all** | *oper-num* } **result**	Show the last test data of work;
3	Raisecom#**show sla** { **all** | *oper-num* } **statistic**	Show statistics of work scheduling; we can record 5 groups of statistics of a work (different work with different number), and if the number of groups exceeds 5, the earliest statistics will be aged;

13.3 Configuration examples

13.3.1 Examples for configuring CFM

Networking requirements

As shown in below figure, PC A communicates with PC B by ISCOM5508 A, ISCOM5508 B and ISCOM5508 C, ISCOM5508 device has CFM features to realize active detection, confirmation and location, and link between PC A and PC B realizes telecom service. ISCOM5508 A and ISCOM5508 C are MEP, ISCOM5508 B is MIP, fault in Ethernet between GE 1 of ISCOM5508 A and ISCOM5508 C can be detected, and level of maintenance field is level 3.

Figure 13-1 CFM networking application

Configuration steps

Step 1 Configure ports and add VLAN.

Configure ISCOM5508 A.

```
Raisecom#config
Raisecom(config)#create vlan 100 active
Raisecom(config)#interface port 1
Raisecom(config-port)#switch access vlan 100
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
```

Configure ISCOM5508 B.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
```

Configure ISCOM5508 C.

```
Raisecom#config
Raisecom(config)#create vlan 100 active
Raisecom(config)#interface port 1
Raisecom(config-port)#switch access vlan 100
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
```

Step 2 Configure CFM fault detection.

Configure ISCOM5508 A.

```
Raisecom(config)#ethernet cfm domain level 3
Raisecom(config)#service ma1 level 3
```

```
Raisecom(config-service)#service vlan-list 100
Raisecom(config-service)#service mep down mpid 301 port 1
Raisecom(config-service)#service remote-mep 302
Raisecom(config-service)#service cc enable mep all
Raisecom(config-service)#exit
Raisecom(config)#ethernet cfm enable
```

Configure ISCOM5508 B.

```
Raisecom(config)#ethernet cfm domain level 3
Raisecom(config)#service ma1 level 3
Raisecom(config-service)#service vlan-list 100
Raisecom(config-service)#exit
Raisecom(config)#ethernet cfm enable
```

Configure ISCOM5508 C.

```
Raisecom(config)#ethernet cfm domain level 3
Raisecom(config)#service ma1 level 3
Raisecom(config-service)#service vlan-list 100
Raisecom(config-service)#service mep down mpid 302 port 1
Raisecom(config-service)#service remote-mep 301
Raisecom(config-service)#service cc enable mep all
Raisecom(config-service)#exit
Raisecom(config)#ethernet cfm enable
```

Step 3 Execute CFM fault confirmation.

Take ISCOM5508 A as an example.

```
Raisecom(config)#service ma1 level 3
Raisecom(config-service)#ping mep 302 source 301
Sending 5 ethernet cfm loopback messages to BBBB, timeout is 2.5 seconds:
!!!!!
Success rate is 100 percent (5/5).
Ping statistics from BBBB:
Received loopback replys:< 5/0/0 > (Total/Out of order/Error)
Ping successfully.
```

Step 4 Execute CFM fault location.

Take ISCOM5508 A as an example.

```
Raisecom(config)#service ma1 level 3
Raisecom(config-service)#traceroute mep 302 source 301
```

```
TTL: 100
Tracing the route to 000E.5E00.000c on level 3 service 3.
Traceroute send via port1.
------------------------------------------------------------------------
Hops  HostMac    Ingress/EgressPort  IsForwarded  RelayAction  NextHop
------------------------------------------------------------------------
 1  000E.5E00.000b    port1/port2        Yes        rlyFdb  000E.5E00.000c
```

Checking results

Use **show ethernet cfm** on ISCOM5508 to show CFM configuration.

Take ISCOM5508 A as an example.

```
Raisecom#show ethernet cfm
Global CFM Status: enable
Port CFM Enabled Portlist:port 1-2,port 1-4
Archive hold time of error CCMs: 100
Remote mep aging time: 100
Device mode: Slave
```

13.3.2 Examples for configuring SLA

Networking requirements

As shown in below figure, PC A communicates with PC B by ISCOM5508 A, ISCOM5508 B and ISCOM5508 C, ISCOM5508 device has CFM features to realize telecom service on Ethernet link between ISCOM5508 A and ISCOM5508 B. ISCOM5508 A has SLA features and it is executed periodically to realize SLA protocol and detect network performance between ISCOM5508 A and ISCOM5508 C.

ISCOM5508 A takes layer-2 delay test on ISCOM5508 C. We configure y1731-echo on ISCOM5508 A work, work number is 2, remote MEP is 2, level of maintenance field is level 3, VLAN-ID is 100, level of service is level 0, life cycle of scheduling is 20s and period of test is 10s.

Figure 13-2 SLA networking application

Configuration steps

Step 1 Configure CFM on ISCOM5508 device.

The detail refers to section 13.1 Configuring CFM.

Step 2 Configure y1731-echo work on ISCOM5508 A and enable work scheduling.

```
Raisecom#config
Raisecom(config)#sla 2 y1731-echo remote-mep 302 level 3 svlan 100 cos 0
Raisecom(config)#sla schedule 2 life 20 period 10
```

Checking results

Check whether SLA configuration is correct by **show sla configuration** on ISCOM5508 A.

```
Raisecom(config)#show sla 2 configuration
------------------------------------------------------------------------
Operation <2>:
   Type: Y.1731 echo
   StartTime:  0 days, 0 : 0 : 50
------------------------------------------------------------------------
   Cos:                    0
   Service Vlan ID:          100
   Customer Vlan ID:         0
   MD Level:                3
   Remote MEP ID:            302
   Timeout(sec):            5
   Schedule Life(sec):        20
   Schedule Period(sec):      10
   Schedule Status:          Completed!
```

14 Configuring system security

The chapter introduces system security configuration and procedure of ISCOM5508 device and provides related configuration applications.

- Configuring ACL
- Configuring RADIUS
- Configuring TACACS+
- Configuring storm suppression
- Configuring IP Source Guard
- Configuring DAI
- Configuring port security MAC
- Configuring defending against DoS attack
- Maintenance
- Configuration examples

14.1 Configuring ACL

14.1.1 Preparing for configuration

Networking situation

Network device needs to configure ACL to filter data packet in order to indentify objects which need to be filtered. And then the device can enable or disable corresponding data packets to pass through according to predefined policy.

ACL can be divided into the following types:

- IP ACL: make classification rules according to data packet attribute information, such as data packet IP header carried source or destination address, the used TCP or UDP port number and etc.
- MAC ACL: make classification rules according to layer-2 information, such as layer-2 frame header carried source MAC address, destination MAC address, layer-2 protocol type and etc.

- MAP ACL: to access control list mapping table MAP ACL can define more protocols and more detailed protocol field than IP ACL and MAC ACL as well as match any bytes in the first 64 bytes of layer-2 data frame according to user definition.

There are four modes for ACL application according to the difference of actual Networking situation:

- Based on the whole device
- Based on ports
- Based on the flow from ingress port to egress port
- Based on VLAN

14.1.2 Configuring IP ACL

Configuring OLT IP ACL

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip-access-list** *list-number* { **deny** | **permit** } *protocol* { *source-ip-address mask* | **any** } [*source-protocol-port*] { *destination-ip-address mask* | **any** } [*destination-protocol-port*]	Configure IP ACL of OLT device;

Configuring ONU IP ACL

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**create class** *class-number* **match** { **dip** | **sip** | **protocol** | **dscp** | **pre** | **14-sport** | **14-dport** } *value* { **never-match** | **equal** | **not-equal** | **exist** | **not-exist** | **always-match** }	Configure IP ACL of ONU device;

14.1.3 Configuring MAC ACL

Configuring OLT MAC ACL

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom (config)#**mac-access-list** *list-number* { **deny** | **permit** } [*protocol* | **arp** | **ip** | **rarp** | **any**] { *source-mac-address* | **any** } { *destination-mac-address* | **any** }	Configure MAC ACL of OLT device;

Configuring ONU MAC ACL

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**creat class** *class-number* **match** { **dmac** | **smac** | **cos** | **vid** | **eth-type** | **vlan** } *value* { **never-match** | **equal** | **not-equal** | **exist** | **not-exist** | **always-match** }	Configure MAC ACL of ONU device;

14.1.4 Configuring MAP ACL

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**access-list-map** *list-number* { **deny** | **permit** }	Create MAP ACL list, and enter ACL MAP configuration mode;
3	Raisecom(config-aclmap)#**match mac** { **destination** | **source** } *mac-address* [*mac-address-mask*]	(Optional) Define matching rules of source or destination MAC address; By default, it doesn't match MAC address;
4	Raisecom(config-aclmap)#**match cos** *cos-value*	(Optional) Define matching rules of CoS value; By default, it doesn't match CoS value;
5	Raisecom(config-aclmap)#**match ethertype** *ethertype* [*ethertype-mask*]	(Optional) define matching rules of Ethernet frame type; By default, it doesn't match Ethernet frame type; ethertype and ethertype-mask are hexadecimal digit with HHHH format; **Caution** Range of *ethertype* is 0x0600–0xFFFF when configuring **ethertype** *ethertype*;
6	Raisecom(config-aclmap)#**match** { **arp** | **eapol** | **flowcontrol** | **ip** | **ipv6** | **loopback** | **mpls** | **mpls-mcast** | **pppoe** | **pppoedisc** | **x25** | **x75** }	(Optional) Define matching rules of upper protocol type in two-layer message's header
7	Raisecom(config-aclmap)#**match arp opcode** { **reply** | **request** }	(Optional) Define matching rules of ARP protocol type (responding packet /requesting packet); by default, it doesn't match ARP protocol type;
8	Raisecom(config-aclmap)#**match arp** { **sender-mac** | **target-mac** } *mac-address*	(Optional) define matching rules of ARP message's MAC address; by default, it doesn't match MAC address of ARP message;
9	Raisecom(config-aclmap)#**match arp** { **sender-ip** | **target-ip** } *ip-address* [*ip-address-mask*]	(Optional) Define matching rules of ARP message 's IP address; by default, it doesn't match IP address of ARP message;

Step	Configuration	Description
10	Raisecom(config-aclmap)#**match ip** { **destination-address** | **source-address** } *ip-address* [*ip-address-mask*]	(Optional) Define matching rules of source or destination IP address; by default, it doesn't match IP address;
11	Raisecom(config-aclmap)#**match ip precedence** { *precedence-value* | **critical** | **flash** | **flash-override** | **immediate** | **internet** | **network** | **priority** | **routine** }	(Optional) Define matching rules of IP message priority; by default, it doesn't match IP message priority;
12	Raisecom(config-aclmap)#**match ip tos** { *tos-value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal** }	(Optional) Define matching rules of IP message priority ToS value; by default, it doesn't match IP message priority ToS value;
13	Raisecom(config-aclmap)#**match ip dscp** { *dscp-value* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41** | **af42** | **af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **default** | **ef** }	(Optional) Define matching rules of IP message DSCP value; by default, it doesn't match IP message DSCP value;
14	Raisecom(config-aclmap)#**match ip protocol** *protocol-id*	(Optional) define matching rules of IP message protocol value; by default, it doesn't be matched;
15	Raisecom(config-aclmap)#**match ip tcp** { **destination-port** | **source-port** } { *port-number* | **bgp** | **domain** | **echo** | **exec** | **finger** | **ftp** | **ftp-data** | **gopher** | **hostname** | **ident** | **irc** | **klogin** | **kshell** | **login** | **lpd** | **nntp** | **pim-auto-rp** | **pop2** | **pop3** | **smtp** | **sunrpc** | **syslog** | **tacacs** | **talk** | **telnet** | **time** | **uucp** | **whois** | **www** }	(Optional) Define matching rules of TCP message port number; by default, it doesn't match port number of TCP message;
16	Raisecom(config-aclmap)#**match ip tcp** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }	(Optional) Define matching rules of TCP protocol flag bit; by default, it doesn't match TCP protocol flag bit;
17	Raisecom(config-aclmap)#**match ip udp** { **destination-port** | **source-port** } { *port-number* | **biff** | **bootpc** | **bootps** | **domain** | **echo** | **mobile-ip** | **netbios-dgm** | **netbios-ns** | **netbios-ss** | **ntp** | **pim-auto-rp** | **rip** | **snmp** | **snmptrap** | **sunrpc** | **syslog** | **tacacs** | **talk** | **tftp** | **time** | **who** }	(Optional) Define matching rules of UDP message port number; by default, it doesn't match port number of UDP message;
18	Raisecom(config-aclmap)#**match ip icmp** *icmp-type* [*icmp-code*]	(Optional) Define matching rules of ICMP message type; by default, it doesn't match ICMP message type;
19	Raisecom(config-aclmap)#**match ip igmp** { *igmp-type* | **dvmrp** | **leave-v2** | **pim-v1** | **query** | **report-v1** | **report-v2** | **report-v3** }	(Optional) Define matching rules of IGMP message type; by default, it doesn't match IGMP message type;

Step	Configuration	Description
20	Raisecom(config-aclmap)#**match user-define** *rule-string rule-mask offset*	(Optional) Configure matching rules user-defined field, that is, use rule mask and offset to distill any bytes in the first sixty four bytes from data frame, and then preparing with user-defined rules to take corresponding measures; **Note** The rules must be an even number of hexadecimal digit, offset includes 802.1q VLAN Tag field, that is, device receives untag packet;
21	Raisecom(config-aclmap)#**match cvlan** *vlan-id*	(Optional) Define matching rules of inner VLAN ID message;
22	Raisecom(config-aclmap)#**match cvlan-cos** *vlan-id*	(Optional) Define matching rules of inner VLAN message CoS value;
23	Raisecom(config-aclmap)#**match svlan-cos** *vlan-id*	(Optional) Define matching rules of outer VLAN ID message;

14.1.5 Applying ACL on devices

Note

ACL takes effect on devices if ACL is added into filter. Many ACL matching rules can be added into filter to generate many filter rules. The priority of the rules can be defined by the order of adding ACL matching rules. Order can be defined reasonably to filter messages correctly.

Applying ACL on OLT devices

- Apply ACL based on the whole device

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**filter** { **ip-access-list** | **mac-access-list** | **access-list-map** } { *list-number* | **all** } [**statistics**]	The configuration is based on the whole device filtering. The system will count according to filtering rules if **statistics** parameter has been configured;
3	Raisecom(config)#**filter** { **enable** | **disable** }	Enable /disable filter to bring rules into effect. Filtering rules which is set before or later will take effect if filter enables;

- Apply ACL based on ports

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**filter** { **ip-access-list** | **mac-access-list** | **access-list-map** } { *acllist-number* | **all** } { **ingress** | **egress** } **port-list** *port-list* [**statistics**]	Configure filtering based on port; The system will count according to filtering rules if **statistics** parameter has been configured;
3	Raisecom(config)#**filter** { **enable** | **disable** }	Enable /disable filter to bring rules into effect. Filtering rules which is set before or later will take effect if filter enables;

- Apply ACL based on flow from ingress to egress

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**filter** { **ip-access-list** | **mac-access-list** | **access-list-map** } { *list-number* | **all** } **from** *port-id* **to** *port-id* [**statistics**]	Configure flow filtering from ingress to egress port; The system will count according to filtering rules if **statistics** parameter has been configured;
3	Raisecom(config)#**filter** { **enable** | **disable** }	Enable /disable filter to bring rules into effect. Filtering rules which is set before or later will take effect if filter enables;

- Apply ACL based on VLAN

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**filter** { **ip-access-list** | **mac-access-list** | **access-list-map** } { *list-number* | **all** } **vlan** *vlan-id* [**statistics** | **double-tagging inner**]	Configure VLAN filtering; The system will count according to filtering rules if **statistics** parameter has been configured;
3	Raisecom(config)#**filter enable**	Enable /disable filter to bring rules into effect. Filtering rules which is set before or later will take effect if filter enables; by default, system disable the filter;

Applying ACL on ONU device

Note

Raisecom ONU ACL filtering function has the following configuration limits:

- All ports support 100 filtering based on VLAN at most. Single port ONU supports 6 filtering based on VLAN at most;

- All ports support 100 filtering based on MAC at most. Single port ONU supports 100 filtering based on MAC SA at most and 100 filtering based on MAC DA at most;
- Support filtering based on destination IP address, source IP address, types of IP, TCP interface, and UDP interface. At the same time, type of rule is deny;
- Support 24 filtering based on destination IP address, source IP address, types of IP, TCP interface, and UDP interface. The number of one type of filtering which can be configured is 16 at most, the total number is 24 at most;
- Support 23 IPACL at most, and the total number of IPACL and MAC ACL with same type of Ethernet is 32at most.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**create policy** *policy-id* **class** *class-id* **queue-map** *queue* **pri-marking** *cos*	Configure Policy filter;
3	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
4	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter port configuration mode of ONU UNI Ethernet;
5	Raisecom(fttx-onu-uni*/*/*:*)#**filter** { **permit**| **deny** } { **match-all** | **match-any** } **policy** *policy-id*	Enable Policy filter on port;

14.1.6 Checking configuration

Checking OLT configuration

No.	Item	Description
1	Raisecom#**show ip-access-list** [*list-number*]	Show whether IP ACL configuration is correct;
2	Raisecom#**show mac-access-list** [*list-number*]	Show whether MAC ACL configuration is correct;
3	Raisecom#**show access-list-map** [*list-number*]	Show whether MAP ACL configuration is correct;
4	Raisecom#**show filter** [filter-*numbert*]	Show whether filter configuration is correct;

Checking ONU configuration

No.	Item	Description
1	Raisecom#**show onu-remote calss** { **all** | **class-number** }	Show configured ACL rules;
2	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** *uni-id* **filter**	Show configured filter on ONU port;

14.2 Configuring RADIUS

14.2.1 Preparing for configuration

Networking situation

Users can use RADIUS server to execute authentication and charging in network to control visitation in device and network. The device can be used as proxy device of RADIUS server, and device authorized users to visit network according to result which feedback from RADIUS server.

14.2.2 Default configuration of RADIUS

Function	Default value
RADIUS charging function	disable
IP address and UDP port number of RADIUS charging server	IP address: 0.0.0.0 UDP port number: 1813
common key communicating with RADIUS charging server	N/A
charging fail strategy	online
Sending time of charging updating message	0

14.2.3 Configuring RADIUS authentication

Step	Configuration	Description
1	Raisecom#**radius** [**backup**] *ip-address* [**auth-port** *port-id*]	Specify IP address and port number of RADIUS authentication server; Configure **backup** parameter to specify backup RADIUS authentication server;
2	Raisecom#**radius-key** *word*	Configure common key of RADIUS authentication;
3	Raisecom#**user login** { **local-user** | **radius-user** | **local-radius** | **radius-local** [**server-no-response**] }	Configure login authentication by RADIUS;
4	Raisecom#**enable login** { **local-user** | **radius-user** | **local-radius** | **radius-local** [**server-no-response**] }	Configure authentication which is used to enter privilege mode as RADIUS;

14.2.4 Configuring RADIUS charging

Step	Configuration	Description
1	Raisecom#**aaa accounting login enable**	Enable RADIUS charging function; Use command **aaa accounting login disable** to disable RADIUS charging function;

Step	Configuration	Description
2	Raisecom#**radius** [**backup**] **accounting-server** *ip-address* [*account-port*]	Specify IP address and UDP port number of RADIUS charging server; Configure backup parameter to specify backup RADIUS charging server;
3	Raisecom#**radius accounting-server key** *string*	Configure common key communicating with RADIUS charging server; the key must be consist with common key in RADIUS charging server, otherwise charging fails;
4	Raisecom#**aaa accounting fail** { **online** | **offline** }	Configure charging fail strategy;
5	Raisecom#**aaa accounting update** *period*	Configure sending cycle of charging updating message; if it is configured as 0, charging updating message won't be sent; **Note** RADIUS charging server can record access time and operation of all users by monitoring charging start message, charging updating message and charging end message;

14.2.5 Checking configuration

No.	Item	Description
1	Raisecom#**show radius-server**	Show whether RADIUS server configuration is correct;

14.3 Configuring TACACS+

14.3.1 Preparing for configuration

Networking situation

Users can use TACACS+ server to execute authentication and charging in network to control visitation in device and network. TACACS+ is more safe and reliable than RADIUS. The device can be used as proxy device of TACACS+ server, and device authorized users to visit network according to result which feedback from TACACS+ server.

14.3.2 Default configuration

By default, ISCOM5508 doesn't configure TACACS+ authentication server address and common key. User login mode and enable login mode are local-user.

14.3.3 Configuring TACACS+ authentication

Step	Configuration	Description
1	Raisecom#**tacacs-server** [**backup**] *ip-address*	Specify IP address of TACACS+ authentication server; Configure **backup** parameter to specify backup TACACS+ authentication server ;
2	Raisecom#**tacacs-server key** *string*	Configure common key of TACACS+ authentication;
3	Raisecom#**user login** { **local-user** | **tacacs-user** | **local-tacacs** | **tacacs-local** [**server-no-response**] }	Configure login authentication by TACACS+;
4	Raisecom#**enable login** { **local-user** | **tacacs-user** | **local-tacacs** | **tacacs-local** [**server-no-response**] }	Configure authentication which is used to enter privilege mode as TACACS+;

14.3.4 Checking configuration

No.	Item	Description
1	Raisecom#**show tacacs-server**	Show whether TACACS+ server configuration is correct;

14.4 Configuring storm suppression

14.4.1 Preparing for configuration

Networking situation

Configure storm suppression on layer-2 network to suppress generation of broadcast storm when broadcast messages increase in network, in order to ensure forwarding of normal unicast messages.

DLF flow, multicast flow and broadcast flow will generate broadcast flow, so device should limit bandwidth on layer-2 device.

- DLF flow: destination MAC doesn't exist in unicast flow in MAC table and layer-2 device sends the flow in broadcast mode;
- Unknown multicast flow: destination MAC is multicast flow and layer-2 device sends the flow in broadcast mode;
- Broadcast flow: destination MAC is broadcast flow and layer-2 device sends the flow in broadcast mode;

Precondition

Device should connect with ports and configure physical parameters before configuring storm suppression, and state of physical layer is up.

14.4.2 Default configuration

Default configuration of storm suppression on ISCOM5508 device:

Function	Default value
broadcast packet storm suppression	enable
multicast group packet storm suppression	disable
DLF storm suppression	disable
packet rate threshold of storm suppression	1024pps

Default configuration of storm suppression on Raisecom ONU device:

Function	Default value
broadcast packet storm suppression	enable
multicast group packet storm suppression	enable
DLF storm suppression	disable
rate threshold of storm suppression	1000 Kbit/s
burst length threshold of storm suppression	4 byte
packet rate threshold of storm suppression	1000 pps

14.4.3 Configuring storm suppression

Configuring OLT storm suppression

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**storm-control** { **broadcast** | **dlf** | **multicast** | **all** } { **enable** | **disable** }	enable /disable storm suppression function on broadcast flow, multicast flow and DLF flow;
3	Raisecom(config)#**storm-control pps** *value*	(Optional) Configure packet rate threshold of storm suppression;

Configuring ONU storm suppression

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;

Step	Configuration	Description
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)#**storm-control** { **broadcast** | **dlf** | **multicast** | **all** } { **enable** | **disable** }	enable /disable storm suppression function on broadcast flow, multicast flow and DLF flow;
4	Raisecom(fttx-onu*/*:*)#**storm-control bps** *rate* [*burst*]	(Optional) Configure rate and burst length threshold of storm suppression;
5	Raisecom(fttx-onu*/*:*)#**storm-control pps** *rate*	(Optional) Configure packet rate threshold of storm suppression;

14.4.4 Checking configuration

Checking OLT configuration

No.	Item	Description
1	Raisecom#**show storm-control**	Show whether OLT storm suppression configuration is correct;

Checking ONU configuration

No.	Item	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **storm-control**	Show whether ONU storm suppression configuration is correct;

14.5 Configuring IP Source Guard

14.5.1 Preparing for configuration

Networking situation

IP Source Guard has two kinds of working modes:

- Static binding working mode: set binding relation manually;
- Dynamic binding working mode: cooperate with DHCP Snooping to generate dynamic binding relation;

Source binding table of IP Source Guard supports the following combination:

- Port +IP
- Port +IP+MAC
- Port +IP+VLAN

- Port +IP+MAC+VLAN

Precondition

Enable DHCP Snooping before configuring dynamic binding relation of IP Source Guard.

14.5.2 Default configuration

Function	Default value
port trust state	distrust
static binding Function	disable
dynamic binding Function	disable

14.5.3 Configuring port trust state of IP Source Guard

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-port)#**ip verify source trust**	Configure port as trust port ; Use **no ip verify source trust** to configure port as distrust port ;

14.5.4 Configuring static binding of IP Source Guard

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip verify source**	enable global static binding Function;
3	Raisecom(config)#**ip source binding** *ip-address* [*mac address*][**vlan** *vlan-id*] **port** *port-id*	Configure static binding relation;

Note

- Manually configured static binding relation will cover dynamic binding relation. The dynamic binding relation will be recovered if the static binding relation is deleted.
- System shows operation successfully if it deletes inexistent static binding relation.

14.5.5 Configuring dynamic binding of IP Source Guard

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip verify source dhcp-snooping**	Configure dynamic binding relation;

14.5.6 Checking configuration

No.	Item	Description
1	Raisecom#**show ip verify source**	Show port trust configuration and static /dynamic binding function configuration on device;
2	Raisecom#**show ip source binding** [**port** *port-id*]	Show static binding relation table on device;

14.6 Configuring DAI

14.6.1 Preparing for configuration

Networking situation

DAI is used to prevent common ARP spoofing attacks in network. DAI has two kinds of working modes:

- Static binding working mode: set binding relation manually;
- Dynamic binding working mode: cooperate with DHCP Snooping to generate dynamic binding relation;

Source binding table of DAI supports the following combination:

- Port +IP
- Port +IP+MAC
- Port +IP+VLAN
- Port +IP+MAC+VLAN

Precondition

Enable DHCP Snooping before configuring dynamic binding relation of DAI.

14.6.2 Default configuration

Default configuration of DAI on ISCOM5508 as follows:

Function	Default value
DAI port trust	distrust
DAI static binding Function	disable
DAI dynamic binding Function	disable
DAI static binding table	N/A
port ARP speed limit of ARP message Function	disable
port ARP speed limit of ARP message rate	100
ARP speed limit of ARP message recover function	disable
ARPrecovery time of ARP message speed limit	30s

Default configuration of DAI on Raisecom ONU as follows:

Function	Default value
DAI port trust	distrust
DAI static binding Function	disable
DAI dynamic binding Function	disable
DAI static binding table	N/A

14.6.3 Configuring port trust state of DAI

Configuring port trust state of OLT DAI

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-port)#**ip arp-inspection trust**	Configure port as trust port;

Configuring port trust state of ONU DAI

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;

Step	Configuration	Description
3	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter ONU UNI Ethernet port configuration mode;
4	Raisecom(fttx-onu-uni*/*/*:*)#**ip arp-inspection trust** { **enable** | **disable** }	Enable /disable port as ARP trust port;

14.6.4 Configuring static binding of DAI

Configuring static binding of OLT DAI

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip arp-inspection static-config**	Enable global static binding Function;
3	Raisecom(config)#**ip arp-inspection binding** *ip-address* [*mac-address*][**vlan** *vlan-id*] **port** *port-id*	Configure static binding relation;

Configuring static binding of ONU DAI

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)# **ip arp-inspection static** { **enable** | **disable** }	Enable /disable static ARP binding Function;
4	Raisecom(fttx-onu*/*:*)#**ip arp-inspection binding** *ip-address* [*mac-address*] [**vlan** *vlan-id*] **uni ethernet** *uni-id*	Add a static ARP binding rule on ONU port;
5	Raisecom(fttx-onu*/*:*)#**no ip arp-inspection binding** {*ip-address* | all }	(Optional) Delete global static ARP binding rules;
6	Raisecom(fttx-onu*/*:*)#**no ip arp-inspection binding uni ethernet** *uni-id*	(Optional) Delete on port all static ARP binding rules;

14.6.5 Configuring dynamic binding of DAI

Configuring dynamic binding of OLT DAI

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;

Step	Configuration	Description
2	Raisecom(config)#**ip arp-inspection dhcp-snooping**	Enable global dynamic binding function;

Configuring dynamic binding of ONU DAI

Step	Configuration	Description
1	Raisecom#**fttx**	Enter global configuration mode of EPON system;
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode;
3	Raisecom(fttx-onu*/*:*)# **ip arp-inspection** { **dhcp-snooping** | **both** } { **enable** | **disable** }	Enable /disable dynamic ARP binding function;

Note

Dynamic ARP binding function must be used with DHCP Snooping, otherwise all ARP messages on entrust ports will be discarded.

14.6.6 Configuring speed limit of port ARP message

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-port)#**ip arp-rate-limit rate** *rate-value*	Configure port ARP speed limit of ARP message rate;
4	Raisecom(config-port)#**ip arp-rate-limit enable**	Enable port ARP speed limit of ARP message ;

14.6.7 Configuring recovery time of ARP message speed limit

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**ip arp-rate-limit recover time** *seconds*	Configure ARP recovery time of ARP message speed limit;
3	Raisecom(config)#**ip arp-rate-limit recover enable**	Enable ARP speed limit of ARP message recover function;

14.6.8 Checking configuration

Checking OLT configuration

No.	Item	Description
1	Raisecom#**show ip arp-inspection**	Show DAI port trust configuration and static /dynamic binding function configuration on device;
2	Raisecom#**show ip arp-inspection binding**	Show DAI static binding relation table of device;
3	Raisecom#**show ip arp-rate-limit**	Show ARP speed limit of ARP message function configuration and overspeed port state of device;

Checking ONU configuration

No.	Item	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **uni ethernet** [*uni-id*] **ip arp-inspection**	Show on device DAI port trust configuration;
2	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **ip arp-inspection**	Show DAI function configuration on device;
3	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **ip arp-inspection binding** [**uni ethernet** *uni-id*]	Show ARP static binding rules on device;

14.7 Configuring port security MAC

14.7.1 Preparing for configuration

Networking situation

Users can configure port security MAC address to limit and identify part of users to visit network on security port.

14.7.2 Default configuration

Default configuration of port security MAC on ISCOM5508 device:

Function	Default value
security port function	disable
Sticky learning switch of security port	disable
dynamic learning Trap switch of security port	disable

Function	Default value
the maximum number of MAC of security port	1
MAC aging time of security port	30 minutes
violation mode of security port	Protect mode

- We don't suggest users configure security port on TRUNK member ports;
- We don't suggest that users enable security port and use MAC address management mode to configure static security MAC address at the same time;
- Security port and dot1x can't be configured at the same time;
- Security port and limited number of MAC addresses on port VLAN can't be configured at the same time;

14.7.3 Configuring the maximum number of MAC

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-port)#**switchport port-security maximum** *maximum*	Configure the maximum number of security MAC of security port;

14.7.4 Configuring static MAC address

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-port)#**switchport port-security mac-address** *mac-address* **vlan** *vlan-id*	Configure static MAC address of security port;
4	Raisecom(config-port)#**switchport port-security**	Enable port security function;

14.7.5 Configuring dynamic MAC address

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;

Step	Configuration	Description
2	Raisecom(config)#**port-security aging-time** *minutes*	(Optional) Configure aging time of security port;
3	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
4	Raisecom(config-port)#**switchport port-security**	Enable port security function;
5	Raisecom(config-port)#**switchport port-security trap enable**	(Optional) enable learning dynamic MAC address report NM of security port;

14.7.6 Configuring sticky MAC address

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-port)#**switchport port-security**	Enable port security function;
4	Raisecom(config-port)#**switchport port-security mac-address sticky** *mac-address* **vlan** *vlan-id*	(Optional) Configure Sticky MAC address of security port manually;
5	Raisecom(config-port)#**switchport port-security mac-address sticky**	Enable Sticky switch; **Note** Dynamic MAC address is transferred as Sticky MAC address if Sticky switch enables; manual configured Sticky MAC address takes effect;

14.7.7 Configuring MAC violation mode

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-port)#**switchport port-security**	Enable port security function;
4	Raisecom(config-port)#**switchport port-security violation** { **protect** | **restrict** | **shutdown** }	Configure MAC violation mode of security port;

14.7.8 Clearing MAC address

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**interface port** *port-id*	Enter port configuration mode on physical layer;
3	Raisecom(config-port)#**switchport port-security**	Enable port security function;
4	Raisecom(config-port)#**clear port-security** { **all** | **configured** | **dynamic** | **sticky** }	Clear MAC address of security port;

14.7.9 Checking configuration

No.	Item	Description
1	Raisecom#**show port-security**	Show all port security configuration on device;
2	Raisecom#**show port-security mac-address**	Show port security MAC address configuration and learning situation on device;

14.8 Configuring defending against DoS attack

14.8.1 Preparing for configuration

Networking situation

DoS attack is a common attack on network and computers and make network or computer can't provide normal services. So users should configure defending against dos attacks on ISCOM5508 device.

14.8.2 Default configuration

Function	Default value
defending against dos attacks function	disable
defending against ICMP redirection	disable
defending against abnormal protocol message attacks	disable
SYN Flood precaution rules of WinNuke attacks	N/A
ICMP Flood precaution rules of WinNuke attacks	N/A
WinNuke precaution rules of WinNuke attacks	N/A
Smurf precaution rules of WinNuke attacks	N/A

14.8.3 Configuring defending against dos attacks

- Defending against dos attacks use global configuration switch, and system will search existing SYN Flood, ICMP Flood, Smurf, WinNuke defending against attack rules, and send them to hardware. If ICMP redirection has been enabled, enable ICMP redirection on hardware; if detection of protocol message has been enabled, enable detection of protocol message on hardware.
- System will delete all SYN Flood, ICMP Flood, Smurf, WinNuke defending against attack rules if disable defending against dos attacks, and disable ICMP redirection and detection of protocol message.

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode;
2	`Raisecom(config)#dos-defence`	enable global defending against dos attacks;

14.8.4 Configuring defending against ICMP redirection

The device will discard ICMP redirection message on all ports if enable global defending against dos and configure defending against ICMP redirection.

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode;
2	`Raisecom(config)#dos-defence icmp-redirection`	enable defending against ICMP redirection;

14.8.5 Configuring detection of abnormal protocol message

ISCOM5508 device support to detect the following abnormal packets:

- IPv4/IPv6 message of SIP=DIP;
- Flag bit 0 of TCP_SYN;
- TCP messages whose control mark is 0, and series number is 0;
- TCP messages whose series number is 0 and include FIN, URG, PSH flag bit;
- TCP messages which include SYN and FIN mark;
- TCP messages whose source port=destination port;
- The first TCP subsection message doesn't include the whole TCP header;
- Subsection bias is 1 in TCP header;
- UDP message whose source port=destination port;
- ICMP message of subsection;

The device will discard the above abnormal messages on all ports if enable global defending against dos and configure detection of abnormal protocol message.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**dos-defence protocol-check**	enable detection of abnormal protocol messages;

14.8.6 Configuring precaution rules of SYN Flood attacks

The device will match TCP message according to configured SYN Flood rules if enable global defending against dos and configure precaution rules of SYN Flood attacks. Device will suppress a message if it exceeds configured rate or burst of the rules, in order to prevent SYN Flood.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**dos-defence syn-flood ip** *ip-address rate burst*	Configure SYN Flood precaution rules of WinNuke attacks;

14.8.7 Configuring precaution rules of ICMP Flood attacks

The device will match TCP message according to configured SYN Flood rules if enable global defending against dos and configure precaution rules of ICMP Flood attacks. Device will suppress a message if it exceeds configured rate or burst of the rules, in order to prevent ICMP Flood.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**dos-defence icmp-flood ip** *ip-address rate burst*	Configure SYN Flood precaution rules of WinNuke attacks;

14.8.8 Configuring precaution rules of WinNuke attacks

- The device will detect configured WinNuke rules if enable global defending against dos and configure precaution rules of WinNuke attacks. The device will suppress matched messages with rules to prevent WinNuke attacks.
- Users need to input the device IP address, IP address mask code and TCP port to configure WinNuke rules.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**dos-defence winnuke ip** *ip-address ip-mask* **port** { *port-id* | **netbios-ssn** | **netbios-dgm** | **netbios-ns** | **ident** | **domain** }	Configure WinNuke precaution rules of WinNuke attacks;

14.8.9 Configuring precaution rules of Smurf attacks

- The device will detect configured Smurf rules if enable global defending against dos and configure precaution rules of WinNuke attacks. The device will suppress matched messages with rules to prevent Smurf attacks.
- Users need to input destination IP address and IP address mask code to configure Smurf rules.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode;
2	Raisecom(config)#**dos-defence smurf ip** *ip-address ip-mask*	Configure Smurf precaution rules of WinNuke attacks;

14.8.10 Checking configuration

No.	Item	Description
1	Raisecom#**show dos-defence**	Show defending against dos attacks function configuration;
3	Raisecom#**show dos-defence icmp-redirection**	Show defending against ICMP redirection configuration;
4	Raisecom#**show dos-defence protocol-check**	Show detection of abnormal protocol messages configuration;
5	Raisecom#**show dos-defence syn-flood**	Show SYN Flood precaution rules of WinNuke attacks;
6	Raisecom#**show dos-defence icmp-flood**	Show ICMP Flood precaution rules of WinNuke attacks;
7	Raisecom#**show dos-defence winnuke**	Show WinNuke precaution rules of WinNuke attacks;
8	Raisecom#**show dos-defence smurf**	Show Smurf precaution rules of WinNuke attacks;

14.9 Maintenance

Command	Description
Raisecom(config)#**clear filter statistics** [*filter-number*]	Clear statistics of filters;

14.10 Configuration examples

14.10.1 Examples for configuring ACL

Networking requirements

As shown in below figure, configure ACL on ISCOM5508 to disable access from 192.168.1.1 to 192.168.1.100, in order to limit access to server from users.

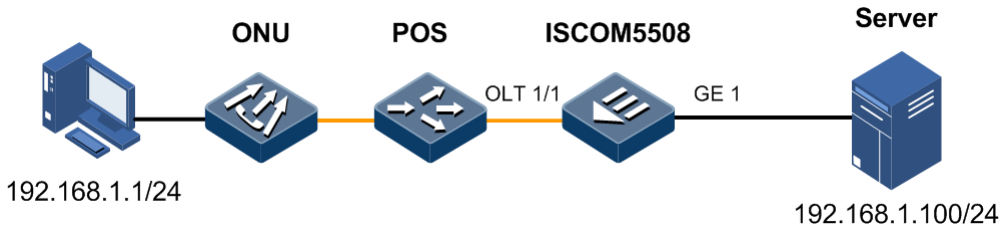

Figure 14-1 ACL application

Configuration steps

Step 1 Configure IP ACL.

```
Raisecom#config
Raisecom(config)#ip-access-list 1 permit ip any any
Raisecom(config)#ip-access-list 2 deny ip 192.168.1.1 255.255.255.0
192.168.1.100 255.255.255.0
```

Step 2 Apply ACL on port OLT 1/1 of ISCOM5508.

```
Raisecom(config)#filter ip-access-list 2 ingress port 7
Raisecom(config)#filter enable
```

Checking results

Check whether IP ACL configuration is correct by command **show ip-access-list**.

```
Raisecom#show ip-access-list
Src Ip: Source Ip Address
Dest Ip: Destination Ip Address
List  Access   Protocol Ref. Src Ip:Port         Dest Ip:Port
------------------------------------------------------------------------
---
1    permit   IP      1    0.0.0.0:0           0.0.0.0:0
2    deny     IP      1    192.168.1.0:0       192.168.1.0:0
```

Check whether filter configuration is correct by command **show filter**.

```
Raisecom#show filter
Rule filter: Enable
Filter list(Larger order number, Higher priority):
Order ACL-Index  IPort   EPort   VLAN VLANType Hardware StatHw   Pkts
-----------------------------------------------------------------
1    IP  1        7   --       --   --      Yes     No      --
2    IP  2        7   --       --   --      Yes     No      --
```

14.10.2 Examples for configuring RADIUS

Networking requirements

As shown in below figure, users need to deploy RADIUS authentication and charging on ISCOM5508 to authenticate4 and record operations, in order to control access to device by users. Please update sending time interval of message as two minutes, and off line if charging fails.

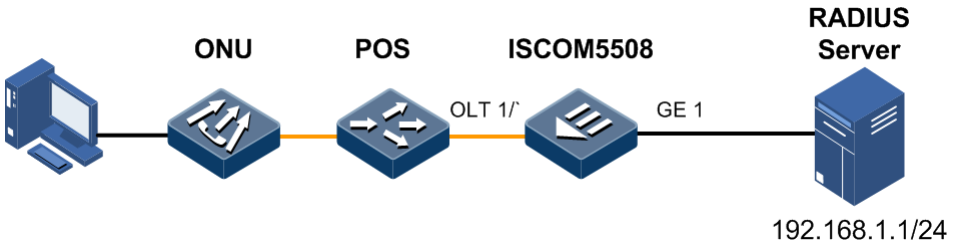

Figure 14-2 RADIUS application

Configuration steps

Step 1 Login users will be authenticated by RADIUS.

```
Raisecom#radius 192.168.1.1
Raisecom#radius-key raisecom
Raisecom#user login radius-user
```

Step 2 Login users will be charged by RADIUS.

```
Raisecom#aaa accounting login enable
Raisecom#radius accounting-server 192.168.1.1
Raisecom#radius accounting-server key raisecom
Raisecom#aaa accounting fail offline
Raisecom#aaa accounting update 120
```

Checking results

Check whether RADIUS configuration is correct by command **show radius-server**.

```
Raisecom#show radius-server
Authentication server IP:      192.168.1.1 port:1812
Backup authentication server IP:0.0.0.0 port:1812
Authentication server key:     raisecom
Accounting server IP:          192.168.1.1 port:1813
Backup accounting server IP:    0.0.0.0 port:1813
Accounting server key:         raisecom
Accounting login:              enable
Update interval:               120
Accounting fail policy:        offline
```

14.10.3 Examples for configuring TACACS+

Networking requirements

As shown in below figure, TACACS+ authentication will be deployed to authenticate users on ISCOM5508, in order to control access device by users.

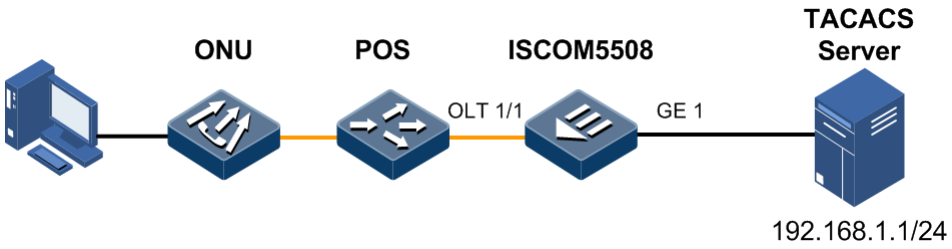

Figure 14-3 TACACS+ application

Configuration steps

Login users will be authenticated by TACACS+.

```
Raisecom#tacacs-server 192.168.1.1
Raisecom#tacacs-server key raisecom
```

```
Raisecom#user login tacacs-user
```

Checking results

Check whether TACACS+ configuration is correct by command **show tacacs-server**.

```
Server Address:                192.168.1.1
Backup Server Address:          --
Sever Shared Key:              raisecom
Total Packet Sent:             0
Total Packet Recv:             0
Accounting server Address:       --
Backup Accounting server Address: --
```

14.10.4 Examples for configuring storm suppression

Networking requirements

As shown in below figure, storm suppression will be deployed on ISCOM5508 to limit broadcast message and unknown unicast message, and threshold is 2000pps.

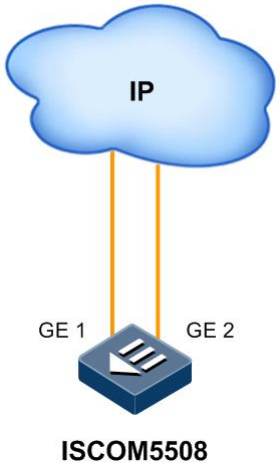

Figure 14-4 Storm suppression application

Configuration steps

Configure storm suppression on ISCOM5508.

```
Raisecom#config
Raisecom(config)#storm-control broadcast enable
Raisecom(config)#storm-control dlf enable
Raisecom(config)#storm-control pps 2000
```

Checking results

Check whether storm suppression is correct by command **show storm-control**.

```
Raisecom#show storm-control
Threshold: 2000 pps
Broadcast: Enable
Multicast: Disable
Unicast destination lookup failed(DLF): Enable
```

14.10.5 Examples for configuring IP Source Guard

Networking requirements

As shown in below figure, we need to configure IP Source Guard on ISCOM5508 to prevent IP embezzlement, and the requirements as below:

- Uplink port GE 1 allows all messages to pass;
- Downlink port OLT 1/1 allows IP message with specific 10.10.10.1 to pass;
- Other ports allows messages to pass which accords with DHCP Snooping learned dynamic binding relation;

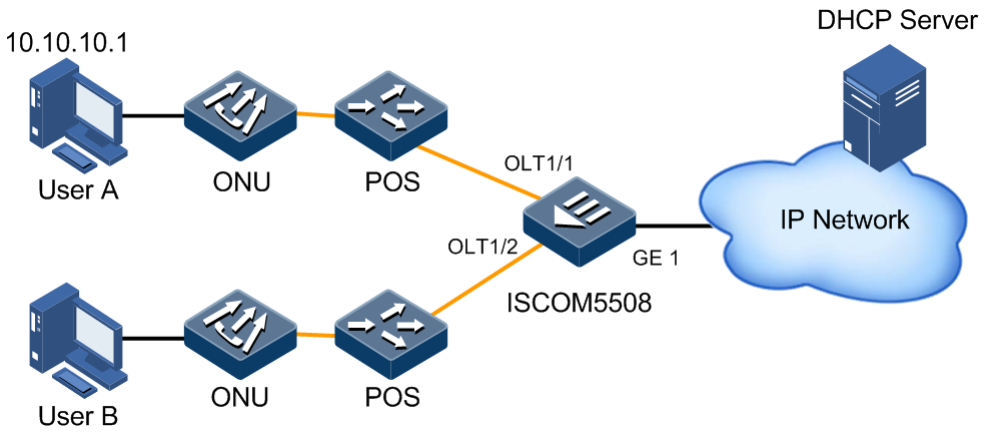

Figure 14-5 IP Source Guard application

Configuration steps

Step 1 Configure GE 1 port as trust port.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)# ip verify source trust
Raisecom(config-port)#exit
```

Step 2 Configure static binding relation.

```
Raisecom(config)#ip verify source
Raisecom(config)#ip source binding 10.10.10.1 port 7
```

Step 3 Configure global dynamic binding relation.

```
Raisecom(config)#ip verify source dhcp-snooping
```

Checking results

Show static binding table configuration by command **show ip source binding**.

```
Raisecom#show ip source binding
History Max Entry Num: 1
Current Entry Num: 1
 Ip Address       Mac Address     VLAN   Port   Type          Inhw
 ------------------------------------------------------------------------
 10.10.10.1       --              --       7     static        yes
```

Show port trust configuration and static dynamic/static binding configuration by command **show ip verify source**.

```
Raisecom#show ip verify source
Static Bind: Enable
Dhcp-Snooping Bind: Enable
 Port     Trust
 --------------------
 1     yes
 2     no
 3     no
 4     no
 5     no
 6     no
 7     no
 8     no
 9     no
 10    no
```

14.10.6 Examples for configuring DAI

Networking requirements

Configure DAI on ISCOM5508 to prevent ARP attacks, and requirements as below:

- Uplink port 1 allows all ARP message to pass;
- Downlink port 7 allows ARP message which specify 10.10.10.1 to pass;
- Other ports allows ARP messages to pass which accords with DHCP Snooping learned dynamic binding relation;
- Downlink port 8 configures ARP message speed limit, rate of speed limit is 20 and recover time of speed limit is 15 minutes.

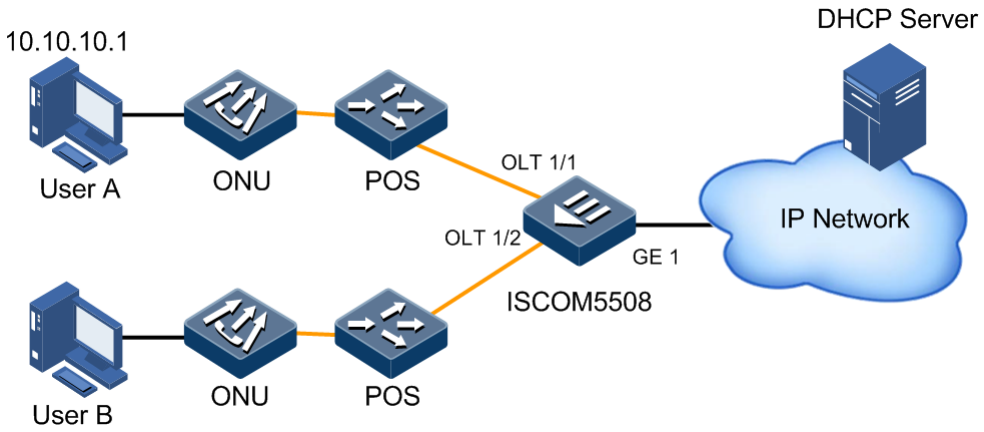

Figure 14-6 DAI application

Configuration steps

Step 1 Configure port 1 as trust port.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)# ip arp-inspection trust
Raisecom(config-port)#exit
```

Step 2 Configure static binding relation.

```
Raisecom(config)#ip arp-inspection static-config
Raisecom(config)#ip arp-inspection binding 10.10.10.1 port 7
```

Step 3 Configure global dynamic binding relation.

```
Raisecom(config)#ip arp-inspection dhcp-snooping
```

Step 4 Configure port ARP speed limit.

```
Raisecom(config)#interface port 8
Raisecom(config-port)#ip arp-rate-limit rate 20
Raisecom(config-port)#ip arp-rate-limit rate enable
Raisecom(config-port)#exit
```

Step 5 Configure recover time of ARP message speed limit.

```
Raisecom(config)#ip arp-rate-limit recover time 15
Raisecom(config)#ip arp-rate-limit recover enable
```

Checking results

Show port trust configuration and static dynamic/static binding configuration by command **show ip arp-inspection**.

```
Raisecom#show ip arp-inspection
static config arp inspection Running: Enable
dhcp snooping arp inspection Running: Enable
 Port   Trust
 -------------
 1      yes
 2      no
 3      no
 4      no
 5      no
 6      no
 7      no
 8      no
```

Show static binding table configuration by command **show ip arp-inspection binding**.

```
Raisecom#show ip arp-inspection binding
Ip Address       Mac Address     VLAN   Port    Type          Inhw
 ------------------------------------------------------------------------
 10.10.10.1       --             --    7       static        yes
 Current Rules Num: 1
 History Max Rules Num: 1
```

Show port speed limit configuration and recover time of speed limit configuration by command **show ip arp-rate-limit**.

```
Raisecom#show ip arp-rate-limit
arp rate limit auto recover: enable
arp rate limit auto recover time: 15 second
Port    Enable-Status    Rate(Num/Sec)    Overload
-------------------------------------------------
1       Disabled         100              No
2       Disabled         100              No
3       Disabled         100              No
4       Disabled         100              No
5       Disabled         100              No
6       Disabled         100              No
7       Disabled         100              No
8       Enabled          20               Yes
```

14.10.7 Examples for configuring port security

Networking requirements

As shown in below figure, ISCOM5508 downlinks three user networks:

- Port OLT 1/1 allows three user access networks. One specifies MAC address of users as 0000.0000.0001. The other two users are dynamic learning, they can receive trap information if they learned a NM, and aging time of the MAC address is ten minutes. Violation mode uses protect mode;
- Port OLT 1/2 allows two users to access network at most. MAC address of the two users won't be aging once they are confirmed.
- Port OLT 1/3 allows one user to access network at most, the MAC address of the user is 0000.0000.0002, MAC address can be aging or not. Violation mode uses shutdown mode.

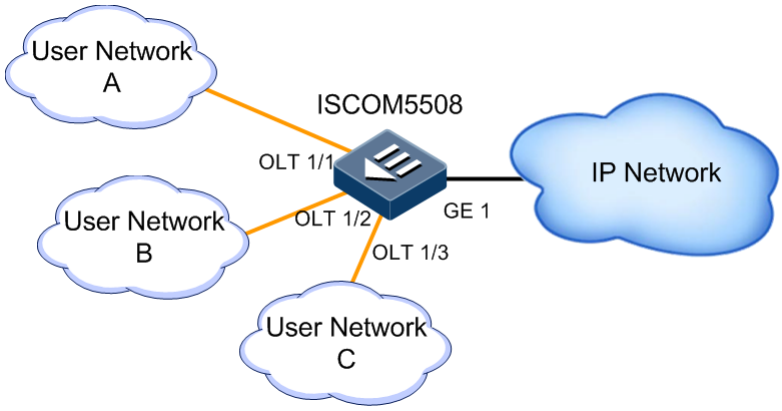

Figure 14-7 Port security application

Configuration steps

Step 1 Configure port security mode of port OLT 1/1.

```
Raisecom#config
Raisecom(config)#interface port 7
```

```
Raisecom(config-port)#switchport port-security
Raisecom(config-port)#switchport port-security maximum 3
Raisecom(config-port)#switchport port-security mac-address 0000.0000.0001
vlan 1
Raisecom(config-port)#switchport port-security violation protect
Raisecom(config-port)#switchport port-security trap enable
Raisecom(config-port)#port-security aging-time 10
```

Step 2 Configure port security mode of port OLT 1/2.

```
Raisecom(config)#interface port 8
Raisecom(config-port)#switchport port-security
Raisecom(config-port)#switchport port-security maximum 2
Raisecom(config-port)#switchport port-security mac-address sticky
Raisecom(config-port)#switchport port-security violation restrict
```

Step 3 Configure port security mode of port OLT 1/3.

```
Raisecom(config)#interface port 9
Raisecom(config-port)#switchport port-security
Raisecom(config-port)#switchport port-security maximum 1
Raisecom(config-port)#switchport port-security mac-address sticky
0000.0000.0002 vlan 1
Raisecom(config-port)#switchport port-security violation shutdown
```

Checking results

Show security configuration of all ports on device by command **show port-security**.

```
Raisecom#show port-security
Port security aging time:10 (min)
port status  Max-Num   Cur-Num  His-Num     vio-Count vio-action Dynamic-
Trap
-------------------------------------------------------------------------
-
1   Disable 1        0      0          0       protect   Disable
2   Disable 1        0      0          0       protect   Disable
3   Disable 1        0      0          0       protect   Disable
4   Disable 1        0      0          0       protect   Disable
5   Disable 1        0      0          0       protect   Disable
6   Disable 1        0      0          0       protect   Disable
7   Enable  3       1      0          0       protect   Enable
8   Enable  2       0      0          0       restrict   Disable
9   Enable  1       1      0          0       shutdown  Disable
```

Show MAC address configuration and learning situation of port security by **show port-security mac-address port-list** *portnum*.

```
Raisecom#show port-security mac-address
VLAN  Security-MAC-Address  Flag    Port  Age(min)
------------------------------------------------------------------------
1     0000.0000.0001       static      7     --
1     0000.0000.0002       sticky      8     --
1     0000.0000.0003       sticky      8     --
```

14.10.8 Examples for configuring defending against dos attacks

Networking requirements

As shown in below figure, we configure defending against dos attacks:

- Configure detection of abnormal protocol message;
- Configure defending against ICMP redirection;
- Configure precaution rules of WinNuke attacks, protected IP address is 192.168.1.1, port is 139, corresponding to Netbios session service.

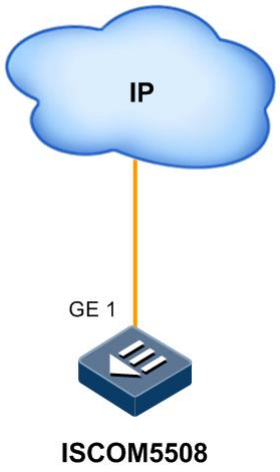

Figure 14-8 Defending against DoS attack application

Configuration steps

Step 1 Configure defending against ICMP redirection and detection of abnormal protocol message.

```
Raisecom#config
Raisecom(config)#dos-defence icmp-redirection
Raisecom(config)#dos-defence protocol-check
```

Step 2 Configure precaution rules of WinNuke attacks.

```
Raisecom(config)#dos-defence winnuke ip 192.168.1.1 255.255.255.0 port
netbios-ssn
```

Step 3 Enable global defending against dos attacks.

```
Raisecom(config)#dos-defence
```

Checking results

Show defending against ICMP redirection configuration by command **show dos-defence icmp-redirection**.

```
Raisecom#show dos-defence icmp-redirection
Dos-defence: Enable
DOS-defence ICMP-redirection: Enabled
Hardware: Yes
```

Show detection of abnormal protocol message by **show dos-defence protocol-check**.

```
Raisecom#show dos-defence protocol-check
Dos-defence: Enable
dos-defence protocol-check: Enabled
Hardware: Yes
```

Show global defending against dos attacks by **show dos-defence**.

```
Raisecom#show dos-defence
Dos-defence: Enable
```

15 Configuring link security

This chapter introduces ISCOM5508 device link security configuration information and configuration process as well as provides related configuration applications.

- Configuring OLT trunk fiber protection (Type B)
- Configuring PON full protection (Type C)
- Configuring PON full protection (Type D)
- Configuring OLT uplink port dual-adscription protection
- Configuring cross OLT PON port dual-adscription protection (Type B)
- Configuring hand in hand uplink port protection
- Configuring link aggregation
- Configuring failover
- Configuring Ethernet ring
- Configuring loopback detection
- Configuring layer-2 protocol transparent transmission
- Configuring ELPS
- Configuring ERPS
- Configuring port backup
- Maintenance
- Configuration examples

15.1 Configuring OLT trunk fiber protection (Type B)

15.1.1 Preparing for configuration

Networking situation

OLT trunk fiber protection (Type B) applies to the following situations:

- PON ports protection with the same OLT PON board.
- PON ports protection with cross OLT PON board.

Preconditions

When creating type B protection, backup link cannot contain created ONU.

15.1.2 Configuring OLT trunk fiber protection (Type B)

Caution

- OLT trunk fiber protection (Type B) protection group member PON ports must enable ports isolation to ensure the normal service switching.
- OLT trunk fiber protection (Type B) protection group member PON ports cannot be close.

Please configure OLT trunk fiber protection (Type B):

Step	Configuration	Description
1	Raisecom#**fttx**	Enter EPON system global configuration mode.
2	Raisecom(fttx)#**protect-group** *group-id* **primary** *slot-id/olt-id* **secondary** *slot-id/olt-id* **type backbone-pon-protect**	Configure to create OLT trunk fiber protection group.
3	Raisecom(fttx)#**protect-group** *group-id* { **enable** | **disable** }	Enable/Disable protection group.
4	Raisecom(fttx)#**sync-data protect-group** { *group-id* | **all** }	Synchronize the main PON port and main ONU link configuration data to standby PON port and standby ONU link configuration data.
5	Raisecom(fttx)#**protect-group** *group-id* **auto-recover-time** *second*	(Optional) Configure recovery time.
6	Raisecom(fttx)#**protect-group** *group-id* **force-switch**	(Optional) Configure force switch.
7	Raisecom(fttx)#**protect-group** *group-id* **lock** { **primary** | **secondary** | **null** }	(Optional) Configure to lock work link of protection group.

15.1.3 Configuring ONU trunk fiber protection (Type B)

Under the circumstance of OLT trunk fiber switching, user needs to configure Holdover function on ONU to prevent ONU deregistration, which will lead to the service interruption.

Please configure OLT trunk fiber protection (Type B):

Step	Configuration	Description
1	Raisecom#**fttx**	Enter EPON system global configuration mode.
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode.
3	Raisecom(fttx-onu*/*:*)#**protect-group holdover time** *period*	Configure ONU Holdover time. The configured time should be greater than 200ms.

Step	Configuration	Description
4	Raisecom(fttx-onu*/*:*)#**protect-group holdover** { **activated** | **deactivated** }	Enable/disable Holdover function

15.1.4 Checking configuration

Check the configuration result by the commands below:

No.	Item	Description
1	Raisecom#**show protect-group** *group-id*	Show the configuration information and operation status of protection group.

15.2 Configuring PON full protection (Type C)

15.2.1 Preparing for configuration

Networking situation

PON full protection (Type C) provides protection to dual OLT PON ports, dual ONU PON ports, trunk fiber, optical splitter, and wiring fiber double link redundancy.

Preconditions

The PON full protection (Type C) configuration must abide by the following preconditions:

- There is no online ONU on main link.
- There is no created ONU on standby link.

15.2.2 Configuring OLT PON full protection (Type C)

Caution

- PON full protection group members PON ports must enable ports isolation to ensure the normal service switching.
- PON full protection group members PON ports cannot be close.

Please configure PON full protection (Type C):

Step	Configuration	Description
1	Raisecom#**fttx**	Enter EPON system global configuration mode.
2	Raisecom(fttx)#**protect-group** *group-id* **primary** *slot-id/olt-id* **secondary** *slot-id/olt-id* **type full-pon-protect**	Configure OLT PON full protection group.

Step	Configuration	Description
3	Raisecom(fttx)#**protect-group** *group-id* { **enable** | **disable** }	Enable/disable protection group.
4	Raisecom(fttx)#**sync-data protect-group** *group-id* { *group-id* | **all** }	Synchronize the main PON port and main ONU link configuration data to standby PON port and standby ONU link configuration data.

15.2.3 Configuring ONU PON full protection (Type C)

Please configure PON full protection (Type C):

Step	Configuration	Description
1	Raisecom#**fttx**	Enter EPON system global configuration mode.
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode.
3	Raisecom(fttx-onu*/*:*)#**protect-group holdover time** *period*	Configure ONU Holdover time. The configured time should be greater than 200ms.
4	Raisecom(fttx-onu*/*:*)#**protect-group holdover** { **activated** | **deactivated** } **time** *period*	Enable/disable Holdover function
5	Raisecom(fttx-onu*/*:*)#**protect-group primary** *pon-port-id*	(Optional) Configure ONU full protection group primary port.
6	Raisecom(fttx-onu*/*:*)#**protect-group auto-recover-time** *second*	(Optional) configure recovery time.

15.2.4 Checking configuration

Check the configuration result by the commands below:

No.	Item	Description
1	Raisecom#**show protect-group** *group-id*	Show configuration information and operation status of OLT protection group.
2	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **protect-group**	Show configuration information and operation status of ONU (type C) protection group.
3	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **detail-information**	Show ONU information

15.3 Configuring PON full protection (Type D)

15.3.1 Preparing for configuration

Networking situation

PON full protection (Type D) provides protection to dual OLT PON ports, dual ONU PON ports, trunk fiber, optical splitter, and wiring fiber double link redundancy.

Preconditions

N/A

15.3.2 Configuring OLT PON full protection (Type D)

Caution

- PON full protection group members PON ports must enable ports isolation to ensure the normal service switching.
- PON full protection group members PON ports cannot be close.

Please configure PON full protection (Type D):

Step	Configuration	Description
1	Raisecom#**fttx**	Enter EPON system global configuration mode.
2	Raisecom(fttx)#**protect-onu-group** *group-id* **primary** *slot-id/olt-id/onu-id* **secondary** *slot-id/olt-id/onu-id*	Configure OLT PON full protection group.
3	Raisecom(fttx)#**sync-data protect-onu-group** *group-id* { *group-id* | **all** }	Synchronize the main PON port and main ONU link configuration data to standby PON port and standby ONU link configuration data.
4	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode.
5	Raisecom(fttx-onu*/*:*)#**device-mac** *mac-adress*	Configure specified device MAC address to join protection group ONU.

15.3.3 (Optional) configuring ONU PON full protection (Type D)

Please configure PON full protection (Type D):

Step	Configuration	Description
1	Raisecom#**fttx**	Enter EPON system global configuration mode.
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode.

Step	Configuration	Description
3	Raisecom(fttx-onu*/*:*)#**protect-group primary** *pon-port-id*	Configure ONU full protection group primary port.

15.3.4 Checking configuration

Check the configuration result by the commands below:

No.	Item	Description
1	Raisecom#**show protect-group** *group-id*	Show configuration information and operation status of OLT protection group.
2	Raisecom#**show protect-onu-group** *group-id*	Show configuration information and operation status of ONU type D protection group.
3	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **detail-information**	Show ONU information.
4	Raisecom#**show interface onu** *slot-id/olt-id/onu-list* **mac**	Show ONU MAC address.

15.4 Configuring OLT uplink port dual-adscription protection

15.4.1 Preparing for configuration

Networking situation

OLT uplink port dual-adscription protection is used between OLT uplink port and upper device to provide main and standby links for OLT uplink service so as to improve service security.

Preconditions

N/A

15.4.2 Configuring OLT uplink port dual-adscription protection

Please configure OLT uplink port dual-adscription protection:

Step	Configuration	Description
1	Raisecom#**fttx**	Enter EPON system global configuration mode.

Step	Configuration	Description
2	Raisecom(fttx)#**protect-group** *group-id* **primary** *slot-id/olt-id* **secondary** *slot-id/olt-id* **type uplink-protect**	Configure uplink port dual-adscription protection group.
3	Raisecom(fttx)#**protect-group** *group-id* { **enable** | **disable** }	Enable/disable protection group.
4	Raisecom(fttx)#**protect-group** *group-id* **auto-recover-time** *second*	(Optional) Configure recovery time.
5	Raisecom(fttx)#**protect-group** *group-id* **force-switch**	(Optional) Configure force switching.
6	Raisecom(fttx)#**protect-group** *group-id* **lock** { **primary** | **secondary** | **null** }	(Optional) Configure to lock the work link of protection group.

15.4.3 Checking configuration

Check the configuration result by the commands below:

No.	Item	Description
1	Raisecom#**show protect-group** *group-id*	Show configuration information and operation status of protection group.

15.5 Configuring cross OLT PON port dual-adscription protection (Type B)

15.5.1 Preparing for configuration

Networking situation

Cross OLT PON port dual-adscription protection (Type B) applies to the protection between different OLT PON ports.

Preconditions

Cross OLT PON port dual-adscription protection (Type B) configuration must abide by the following preconditions:

- The main/standby member ports cannot be close.
- The two OLT can take normal layer-3 communications.
- There should not be created ONU on standby link.

15.5.2 Configuring cross OLT PON port dual-adscription protection (Type B)

Please ensure the protection group configuration parameters (enable/disable status, recovery time, and lock status) and alarm status on both OLT consistent. Otherwise, the two OLT cannot take protection switching.

Please configure cross OLT PON port dual-adscription protection (Type B):

Step	Configuration	Description
1	Raisecom#**fttx**	Enter EPON system global configuration mode.
2	Raisecom(fttx)#**protect-group** *group-id* **primary** *slot-id/olt-id* **secondary** *slot-id/olt-id* **type backbone-pon-protect-extend local-port-role** { **primary** | **secondary** } **peer-device-description** *device-descrition* **peer-device-ip-address** *ip-address*	Configure cross OLT PON port protection group.
3	Raisecom(fttx)#**protect-group** *group-id* { **enable** | **disable** }	Enable/disable protection group.
4	Raisecom(fttx)#**protect-group** *group-id* **auto-recover-time** *second*	(Optional) Configure recovery time.
5	Raisecom(fttx)#**protect-group** *group-id* **force-switch**	(Optional) Configure force switching.
6	Raisecom(fttx)#**protect-group** *group-id* **lock** { **primary** | **secondary** | **null** }	(Optional) Configure to lock the work link of protection group.

Main/standby OLT configuration cannot take auto synchronization; user needs to synchronize the configuration data of each member port and all ONU on both OLT manually.

15.5.3 Checking configuration

Check the configuration result by the commands below:

No.	Item	Description
1	Raisecom#**show protect-group** *group-id*	Show configuration information and operation status of protection group.

15.6 Configuring hand in hand uplink port protection

15.6.1 Preparing for configuration

Networking situation

Hand in hand networking takes two OLT devices primary and standby backup mode, when one OLT uplink port is abnormal, the registered ONU can "linkage" switch to the other OLT so as to ensure the normal service operation. Thus users need to configure hand in hand uplink port protection.

Preconditions

N/A

15.6.2 Default configuration of hand in hand uplink port protection

Function	Default value
Protection object	N/A
hand in hand uplink port protection function	disable
Cycle	5 mins

15.6.3 Configuring hand in hand uplink port protection

Step	Configuration	Description
1	`Raisecom#fttx`	Enter EPON system global configuration mode.
2	`Raisecom(config)#extend-uplink-protect type { ge` *slot-id/port-id* `| trunk group` *trunk-id* `}`	Configure hand in hand uplink port protection objects. **Note** When hand in hand uplink port protection object is GE port, the input slot port No. must be existed and the type is GE port. When hand in hand uplink port protection object is Trunk group, the input Trunk group No. must be existed. By default, the system enables protection function when hand in hand uplink port protection object is configured.
3	`Raisecom(config)#extend-uplink-protect { enable | disable }`	(Optional) Configure to enable/disable hand in hand uplink port protection function.
4	`Raisecom(config)#extend-uplink-protect cycle time`	(Optional) Configure hand in hand uplink port protection cycle.

15.6.4 Checking configuration

Check the configuration result by the commands below:

No.	Item	Description
1	Raisecom#**show extend-uplink-protect**	Show OLT hand in hand uplink port protection information.

15.7 Configuring link aggregation

15.7.1 Prepare for configuration

Networking situation

Link aggregation function can provide higher communication bandwidth and reliability for link between two devices. It aggregates several physical Ethernet interface together and make one logical link. This function realizes uplink and downlink flow load sharing among member interfaces and then increases bandwidth; at the same time, the member interfaces are dynamic to one another which improve link reliability.

Preconditions

Before configuring link aggregation, please configure port physical parameters and make port physical layer status Up.

15.7.2 Default configuration of link aggregation

The default configuration of link aggregation is as below:

Function	Default value
Link aggregation function	Enable
LACP link aggregation function	Enable
Link aggregation group	N/A
Load-sharing mode	sxordmac
System LACP priority	32768

15.7.3 Configuring link aggregation in manual mode

Please configure manual link aggregation for the device as below:

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**trunk group** *group-id* **port** *port-list*	Configure manual link aggregation group.
3	Raisecom(config)#**trunk** { **enable** | **disable** }	Enable/disable link aggregation group.
4	Raisecom(config)#**trunk loading-sharing mode** { **smac** | **dmac** | **sxordmac** | **sip** | **dip** | **sxordip** }	(Optional) Configure the load-sharing mode for link aggregation.

In one link aggregation group, the member ports take part in load-sharing must have identical configuration, or else, it may cause data forwarding problem. The configuration includes STP, QoS, QinQ, VLAN, port attributes, and MAC address learning:

- STP configuration: port STP enable/disable status, link attributes connects to the interface (point-to-point or not), port path overhead, STP priority, packets sending rate limit, loopback protection, root protection, edge port or not.
- QoS configuration: flow monitor, flow reshaping, jam avoidance, port rate limit, SP queue, WRR queue, port priority, port trust mode.
- QinQ configuration: port QinQ enable/disable status, added outer VLAN Tag, policy for adding outer VLAN Tag by different inner VLANID.
- VLAN configuration: port permitting VLAN, default VLAN ID, port link type (Trunk, Hybrid, Access), sub-net VLAN configuration, VLAN packets with Tag configuration or not.
- Port attributes configuration: port is added into isolation group or not, port speed, duplex mode, link up/down status.
- MAC address learning configuration: MAC address learning enable/disable, port with maximum learning MAC address number limit or not, whether MAC address table can control forwarding when it is full.

15.7.4 Configuring static LACP link aggregation

Please configure static LACP link aggregation for the device as below:

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**lacp system-priority** *system-priority*	(Optional) Configure system LACP priority. The higher priority end is active port. LACP chooses active and backup ports according to the active end configuration. The smaller the number is, the higher the priority is. By default, system LACP priority is 32768. The smaller system MAC address device will be chosen as active port if devices system LACP priorities are identical.
3	Raisecom(config)#**trunk group** *group-id port-list* **lacp-static**	Configure static LACP link aggregation group.

Step	Configuration	Description
4	Raisecom(config)#**trunk** { **enable** | **disable** }	Enable/Disable link aggregation group.
5	Raisecom(config)#**interface port** *port-id*	(Optional) Enter physical layer port configuration mode.
6	Raisecom(config-port)#**lacp port-priority** *port-priority*	(Optional) Configure port LACP priority. The priority influents default port selection for LACP. The smaller the number is, the higher the priority is.
7	Raisecom(config-port)#**lacp mode** { **active** | **passive** }	(Optional) Configure LACP mode for member port. By default, it is in active mode. LACP connection will fail when both ends on the same link are in passive mode.

Note

- In static LACP link aggregation group, member port can be in active or standby status. Both active port and standby port can receive/transmit LACP packets, but standby port cannot forward client packets.
- System chooses default port in the order of neighbor discover, maximum port speed, highest port LACP priority, minimum port ID. The default port is in active status, and has identical speed with default port, identical peer device and identical device operation key is also in active status; other ports are in standby status.

15.7.5 Checking configuration

Check the result by the commands below after configuration:

No.	Item	Description
1	Raisecom#**show lacp internal**	Show local system LACP port status, mark, port priority, management key, operation key and status of port status machine.
2	Raisecom#**show lacp neighbor**	Show neighbor LACP information, including mark, port priority, device ID, Age, operation key value, port ID and status of port status machine.
3	Raisecom#**show lacp statistics**	Show port LACP statistic information, including total Tx/Rx number LACP packets, Tx/Rx number of Marker packets, Tx/Rx number of Marker Response packets as well as error packets.
4	Raisecom#**show lacp sys-id**	Show global enable/disable condition of local system LACP, device ID, including system LACP priority and system MAC address.
5	Raisecom#**show trunk**	Show configuration attributes of all link aggregation group.

15.8 Configuring failover

15.8.1 Preparing for configuration

Networking situation

If middleware uplink failure cannot be notified to downlink device promptly, then the flow cannot switch to standby link, which will lead to flow interruption.

The failover feature will add the uplink/downlink port of middleware to the same failover group and take real-time monitoring to uplink port. Once all the uplink port fails, the downlink ports will be set to Down status, and when one uplink port is restored, the downlink port will also restore to Up status, and uplink failure will be notified to downlink device timely. Downlink port failure does not affect the uplink port.

Preconditions

Before configuring failover, please connect port and configure port physical parameters so as to make port physical layer status Up.

15.8.2 Default configuration of failover

The default configuration of ISCOM5508 device failover function is as follows:

Function	Default value
Uplink/downlink interface of failover group	N/A

15.8.3 Configuring failover

Please configure failover on the device:

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#link-state-tracking group` *groupNumber*	Create and enable failover group. If this failover group has already created, use this command to enable it.
3	`Raisecom(config)#interface port` *port-id*	Enter physical port configuration mode.
4	`Raisecom(config-port)#link-state-tracking group` *group-number* `{ downstream | upstream }`	Configure failover group which port belongs to and port type. One port only can belong to one failover group and only can be uplink port or downlink port.

Note

- A failover group can have many uplink ports, and as long as there is an uplink port UP, there is not failover; only when all the uplink ports DOWN, there is failover.
- In global configuration mode, use the command of **no link-state-tracking group** *group-number* to disable failover function, if there is no port in this failover group, the failover group will be deleted.
- In port mode, use the command of **no link-state-tracking group** to delete a port from failover group, if there is no port in this failover group after deletion and the failover group is in disable status, and then the failover group will be deleted simultaneously.

15.8.4 Checking configuration

Check the result by the commands below after configuration:

No.	Item	Description
1	Raisecom#**show link-state-tracking group** [*group-number*] [*detail*]	Show failover group configuration and status information. This command cannot show created and disabled failover group information without member port.
2	Raisecom#**show link-admin-status port** *port-list*	Show port management information.

15.9 Configuring Ethernet ring

15.9.1 Preparing for configuration

Networking situation

As a Metro Ethernet technology, Ethernet ring solves the problems of weak protection to traditional data network and long time to fault recovery, which, in theory, can provide 50ms rapid protection features and is compatible with traditional Ethernet protocol, is an important technology options and solutions of metro broadband access network optimization transformation.

Ethernet ring technology is RAISECOM independent research and development protocol, which through simple configuration achieves the elimination of ring loop, fault protection switching, and automatic fault recovery function and makes the fault protection switching time less than 50ms.

Preconditions

Ethernet ring function and spanning tree function are mutually exclusive; they cannot be enabled at the same time, so please disable spanning tree function when configuring Ethernet ring function.

15.9.2 Default configuration of Ethernet ring

The default configuration of ISCOM5508 device Ethernet ring is as follows:

Function	Default value
Ethernet ring function status	Disable
Hello messages transmitting interval	1s
Fault recovery delay time	5s
Bridge priority	1
Ring port aging time	15s
Ring protocol messages VLAN	2
Ring description information	Ethernet ring *ring-id*

Caution

For all devices in the same ring, the parameters such as fault recovery time, hello message transmitting interval, ring protocol message, and ring port aging time should be consistent with master node.

15.9.3 Creating Ethernet ring

Please create Ethernet ring as below:

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface port` *primaryport-id*	Enter physical layer port configuration mode. This port is the first port of ring node.
3	`Raisecom(config-port)#ethernet ring` *ring-id secondaryport*-id	Create ring and configure corresponding ring port. This port is the second port of ring node.
4	`Raisecom(config-port)#exit`	Exit physical layer port configuration mode
5	`Raisecom(config)#ethernet ring` *ring-id* `enable`	Enable Ethernet ring function.

15.9.4 Configuring basic function of ring

Note

Master node election: at the beginning, all nodes consider themselves the master node, one of two interfaces is Block, so no data loop on the ring; when two interfaces on the ring node receive the same Hello packets for many times, the node considers that the ring topology is stable and can elect master node. Other nodes will not

enable the blocked interface, usually only one master node, which ensures only one blocked interface, and ensures the connectivity of the nodes on the ring.

Please configure the basic function of ring on the device as below:

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet ring** *ring-id* **hello-time** *hello-time*	(Optional) Configure Hello messages transmitting interval for Ethernet ring. **Note** Ethernet ring Hello message transmitting interval should be less than half of ring port aging time.
3	Raisecom(config)#**ethernet ring** *ring-id* **restore-delay** *delay-time*	(Optional) Configure fault recovery delay time for Ethernet ring. The link can be restored to the original work link until the recovery delay time timeout.
4	Raisecom(config)#**ethernet ring** *ring-id* **priority** *priority*	(Optional) Configure bridge priority for Ethernet ring.
5	Raisecom(config)#**ethernet ring** *ring-id* **description** *string*	(Optional) Configure ring description information. The description information cannot exceed 32 bytes.
6	Raisecom(config)#**ethernet ring** *ring-id* **hold-time** *hold-time*	(Optional) Configure port aging time for Ethernet ring. If Ethernet ring port hasn't received Hello messages in aging time, age this port. If the node port is in Block state, it will enable the blocked port temporarily to ensure the normal communication of all nodes on Ethernet ring.
7	Raisecom(config)#**ethernet ring** *ring-id* **protocol-vlan** *vlan-id*	(Optional) Configure protocol VLAN for Ethernet ring.
8	Raisecom(config)#**ethernet ring upstream-group** { *group-list* }	(Optional) Configure uplink port group for Ethernet ring.

Note

- Uplink port group must be combined with failover function to support dual-adscription topology application.
- Uplink port group number must correspond with failover group number.
- In configuring Ethernet ring, the device port must allow Ethernet ring protocol VLAN through; the default Ethernet ring protocol VLAN of ISCOM5508 device is VLAN 2.

15.9.5 Checking configuration

Check the configuration result by the commands below:

No.	Item	Description
1	Raisecom#**show ethernet ring** [*ring-id*]	Show Ethernet ring information.

No.	Item	Description
2	Raisecom#**show ethernet ring port**	Show Ethernet ring port information.

15.9.6 Maintenance

User can maintain Ethernet ring operation and configuration situation by the commands below:

Command	Description
Raisecom(config)#**clear ethernet ring** *ring-id* **statistics**	Clear ring port statistic information.

15.10 Configuring loopback detection

15.10.1 Preparing for configuration

Networking situation

In network, the hosts or layer-2 devices under access devices may form loopback by network cable intentionally or involuntary. Enable loopback detection function at downlink port of access device to avoid the network jam formed by unlimited copies of data flow caused by downlink port loopback. Block the loopback port once there is a loopback.

In EPON system, it is generally ONU that takes on loopback detection function. Common loopback types are as follows:

- Self loopback: loopback under the same Ethernet port in the same ONU.
- Inner loopback: loopback under different Ethernet port in the same ONU.
- Outer loopback: loopback between Ethernet ports in different ONU.

Preconditions

Configure port physical parameters to make it Up before configuring loopback detection.

15.10.2 Default configuration of loopback detection

The default configuration of Raisecom ONU device loopback detection is as below:

Function	Default value
Port-based loopback detection function status	Enable
Loopback detection period	4s
VLAN to enable loopback detection	N/A
Disable loopback port Rx/Tx packets time	infinite

15.10.3 Configuring basic loopback detection

Note

- Loopback detection function and STP are exclusive, only one can be enabled at one time.
- The straight connection device cannot enable loopback detection in both ends simultaneously; otherwise the interfaces at both ends will be blocked.

Please configure loopback detection function as below:

Step	Configuration	Description
1	Raisecom#**fttx**	Enter EPON system global configuration mode.
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode.
3	Raisecom(fttx-onu*/*:*)#**loopback-detection vlan** *vlan-id*	(Optional) Configure the VLAN to enable loopback detection.
4	Raisecom(fttx-onu*/*:*)#**loopback-detection hello-time** *second*	(Optional) Configure loopback detection period.
5	Raisecom(fttx-onu*/*:*)#**uni ethernet** *uni-id*	Enter ONU UNI Ethernet port configuration mode.
6	Raisecom(fttx-onu-uni*/*/*:*)#**loopback-detection** { **enable** | **disable** }	Enable/disable port loopback detection function.
7	Raisecom(fttx-onu-uni*/*/*:*)#**loopback-detection down-time** { *second* | **infinite** }	(Optional) Configure to disable loopback port Rx/Tx packets time.

15.10.4 Checking configuration

Check the configuration result by the commands below:

No.	Item	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **loopback-detection**	Show ONU port loopback detection configuration.

15.11 Configuring layer-2 protocol transparent transmission

15.11.1 Prepare for configuration

Networking situation

Part of layer-2 protocol messages destination multicast addresses in carrier network cannot be forwarded. To make layer-2 protocol messages in one user network to cross carrier and achieve the same user network in different regions unified operating the same layer-2 protocol,

user needs to configure layer-2 protocol transparent transmission. Layer-2 protocol transparent transmission function can modify the destination multicast address so that it can be forwarded in carrier network and decapsulate to original destination multicast address in the exit of carrier network to achieve the same user network in different regions unified operating the same layer-2 protocol.

Preconditions

Configure port physical parameters to make port physical status Up before configuring layer-2 protocol transparent transmission function.

15.11.2 Default configuration of layer-2 protocol transparent transmission

The default configuration of ISCOM5508 device layer-2 protocol transparent transmission is as below:

Function	Default value
Layer-2 protocol transparent transmission function status	Disable
Destination MAC address of transparent transmission message	010E.5E00.0003
Transparent transmission message CoS	5
Specified VLAN of transparent transmission message	N/A
Specified egress port of transparent transmission message	N/A
Packet loss threshold and ban threshold of transparent transmission message	N/A
Port OFF threshold of transparent transmission message	N/A

15.11.3 Configuring layer-2 protocol transparent transmission

Please configure transparent transmission parameter for the device as below:

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#relay destination-address` *mac-address*	(Optional) Configure destination MAC for transparent transmission message.
3	`Raisecom(config)#relay cos` *cos-value*	(Optional) Configure CoS value for transparent transmission message.
4	`Raisecom(config)#interface port` *port-id*	Enter physical layer port configuration mode.
5	`Raisecom(config-port)#relay port` *port-id*	Configure specified egress port for transparent transmission message.

Step	Configuration	Description
6	Raisecom(config-port)#**relay vlan** *vlan-id*	Configure specified VLAN for transparent transmission message.
7	Raisecom(config-port)#**relay** { **all** | **stp** | **dot1x** | **lacp** }	Configure port transparent transmission message type.

15.11.4 Checking configuration

Check the configuration result by the commands below:

No.	Item	Description
1	Raisecom#**show relay**	Show transparent transmission configuration and status.
2	Raisecom#**show relay statistics** [**port-list** *port-list*]	Show statistics information of transparent transmission message.

15.12 Configuring ELPS

15.12.1 Preparing for configuration

Networking situation

Configuring ELPS feature in Ethernet can make Ethernet reliability up to telecommunication level (network self-heal time less than 50ms). It is an end-to-end protection technology used for protecting an Ethernet link.

ELPS is in support of two protection modes: 1+1 and 1:1.

- 1+1 protection switching mode: deploys a protection path for each working path. In protection domain, source end transmits traffic at both working path and protection path, but destination end only choose one path to receive traffic.
- 1:1 protection switching mode: deploys a protection path for each working path. Traffic just be transmitted in either working path or protection path, need APS protocol for negotiation and the source end and destination end choose the same path.

One-way switching and bi-directional switching can be chosen according to whether both ends switches at the same time when link error.

- One-way switching: the fault of when one direction at a link causes one end can receive traffic, but the other end cannot receive. In this case, the end cannot receive traffic detects link error and performs switching, while the normal end doesn't detect and switch. The result of switching is that two ends of ELPS may choose different link to receive traffic.
- Bi-directional switching: when link is error, even only one direction has fault, both ends of the link require APS protocol to negotiate and switch to backup link at the same time.

The result of switching is that two ends of ELPS should choose one link for transmitting and receiving.

ISCOM5508 device doesn't differentiate one-way and bi-directional switching until in 1+1 mode, only bi-directional switching is available in 1:1 mode.

ELPS provides two modes for fault detection:

- Detecting fault over physical interface status: to get link fault quickly and switching in time, available to neighbor devices.
- Detecting fault over CFM: available to one-way detection or multi-devices accrossing detection.

Preconditions

Finish the following tasks before configuring ELPS:

- Connect port and configure physical parameters for it, the port is Up at physical layer.
- Create VLAN.
- Add port into VLAN.
- Configure CFP detection among devices (make preparation in CFP detection mode).

User cannot configure ELPS function together with loopback detection and port backup functions because they are mutually exclusive.

15.12.2 Default configuration of ELPS

The default configuration of ISCOM5508 device ELPS is as below:

Function	Default value
ELPS protection group	N/A
ELPS protection group protection mode	Revertive mode
WTR timer	5min
HOLDOFF timer	0
ELPS information reports to NMS through Trap	Disable
Failure detection mode	Physical link

15.12.3 Creating protection line

Please configure to enable ELPS on the device as below:

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode.

Step	Configuration	Description
2	Raisecom(config)#**ethernet line-protection** *line-id* **working port** *port-id vlanlist* **protection port** *Port-id vlanlist* { **one-plus-one-bi** | **one-plus-one-uni** | **one-to-one** } [**non-revertive**] [**protocol-vlan** *vlan-id*]	Create ELPS protection line and configure protection mode. The protection group becomes non-revertive mode if configure the parameter of non-revertive. In revertive mode, when work link fault recovers, the flow will switch back to work link from protection line; it doesn't switch back in non-revertive mode. **Note** If ELPS port is Trunk port, Trunk attributes configuration must be before enabling ELPS.
3	Raisecom(config)#**ethernet line-protection** *line-id* **name** *string*	(Optional) Configure ELPS protection line name.
4	Raisecom(config)#**ethernet line-protection** *line-id* **wtr-timer** *wtr-timer*	(Optional) Configure WTR timer. In revertive mode, the flow can restore to work in work link after waiting for WTR timer overtime when work link fault restores. **Note** It is better to configure WTR timer at both ends consistent, or else it will not ensure the fast switching in 50ms.
5	Raisecom(config)#**ethernet line-protection** *line-id* **hold-off-timer** *holdoff-timer*	(Optional) Configure HOLDOFF timer. After configuring HOLDOFF timer, system delays to solve the fault when work link has fault, that is to say, it switches to protection link after a delay time to avoid frequent switch caused by work link change. **Note** The greater HOLDOFF timer value will influence 50ms switching performance, so it is recommended to use default value 0.
6	Raisecom(config)#**ethernet line-protection trap** { **enable** | **disable** }	(Optional) Enable/disable ELPS fault information reports to NMS. It is disabled by default.

Note

Please configure port protection function on corresponding port when configuring 1+1 protection.

15.12.4 Configuring ELPS fault detection mode

Please configure ELPS for the device as below.

Note

The work path and protection path can configure different fault detection mode, but it is better to keep their configuration consistent.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet line-protection** *line-id* { **working** | **protection** } **failure-detect physical-link**	Configure physical link detection mode for working path and protection path.
	Raisecom(config)#**ethernet line-protection** *line-id* { **working** | **protection** } **failure-detect cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	Configure CC detection mode for working path and protection path. The fault detection mode takes effective after user finishes CFM related configuration.
	Raisecom(config)#**ethernet line-protection** *line-id* { **working** | **protection** } **failure-detect physical-link-or-cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	Configure physical link or CC detection mode for working link or protection link. Any fault of physical link or CC will be reported. The fault detection mode takes effective after user finishes CFM related configuration.

15.12.5 (Optional) configuring ELPS switching control

Please configure ELPS for the device as below.

Note

By default, the flow will switch to protection link when work link has fault. Thus user needs to configure ELPS switching control just in some special situations.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet line-protection** *line-id* **lockout**	Lockout protection switch. The flow won't switch to protection link even if work link has fault.
3	Raisecom(config)#**ethernet line-protection** *line-id* **force-switch**	Switching flow to protection link from work link by force.
4	Raisecom(config)#**ethernet line-protection** *line-id* **manual-switch**	Switching flow to protection link from work link by manual, priority of this command is lower than force switch and auto-switch.
5	Raisecom(config)#**ethernet line-protection** *line-id* **manual-switch-to-work**	The flow will switch back to work link from protection link in non-revertive mode.
6	Raisecom(config)#**clear ethernet line-protection** *line-id* **end-to-end command**	Clear end-to-end switching control commands, including commands of lockout, force-switch, manual-switch and manual-switch-to-work.

15.12.6 Checking configuration

Check the configuration result by the commands below:

No.	Item	Description
1	Raisecom#**show ethernet line-protection** [*line-id*]	Show protection line configuration.
2	Raisecom#**show ethernet line-protection statistics**	Show protection line statistics information.
3	Raisecom#**show ethernet line-protection aps**	Show APS protocol information.

15.13 Configuring ERPS

15.13.1 Preparing for configuration

Networking situation

With the development of Ethernet to telecom level network, voice and video multicast services bring forth higher requirements on Ethernet redundant protection and fault-restore time. The fault-restore convergent time of current STP system is in second level that is far away to meet requirement. By defining different roles for nodes in a ring, ERPS can break loop link and avoid broadcast storm in normal condition. Then the service link can switch to backup link if the ring link or node faults and remove loop, perform fault protection switch and automatic fault restore, what's more, the protection switch time is lower than 50ms. It is in support of single ring, crossed rings and tangent rings networking modes.

ERPS provides two fault detection modes:

- Fault detection over physical interface status: to get link fault and switching quickly, available to adjacent devices.
- Fault detection over CFM: available to unidirectional detection or multiple devices cross over detection.

Preconditions

Finish the following tasks before configuring ERPS:

- Connect port and configure physical parameters for it, the port is Up at physical layer.
- Create VLAN.
- Add port into VLAN.
- Configure CFP detection among devices (make preparation in CFP detection mode)

15.13.2 Default configuration of ERPS

The default configuration of ERPS is as below:

Function	Default value
ERPS protection ring	N/A
ERPS protection ring protection mode	Revertive mode
Guard timer	500ms
WTB timer	5min
HOLDOFF timer	0
ERPS information reported to NMS through Trap	Disable
Fault detection mode	Physical link

15.13.3 Creating ERPS protection ring

Please configure ERPS for the device as below.

Caution

- Only one device set can be configured as RPL (Ring Protection Link) Owner in a ring, and one device set as RPL Neighbour, other devices can only be configured as ring forwarding node.
- Tangent ring can be taken as two independent rings in fact, the configuration is identical to common single ring; crossover rings has a master ring and a sub-ring, the configurations please refer to the section of "Create ERPS protection ring".

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ethernet ring-protection` *ring-id* `east port` *port-id* `west port` *port-id* `node-type rpl-owner rpl { east | west } [ not-revertive ] [ protocol-vlan` *vlan-id* `] [ block-vlanlist` *vlanlist* `]`	Create ring and configure node as RPLOwner. By default, protocol VLAN is 1, blocked VLAN range is 1-4094. Protection ring changes to non-revertive mode when configuring not-revertive parameter. The difference between non-revertive mode and revertive mode is: in revertive mode, when work link fault restores, the flow will switch back to work link from protection link, but it doesn't switch in non-revertive mode. **Note** The east-bound and western-bound ports cannot be identical.

Step	Configuration	Description
	Raisecom(config)#**ethernet ring-protection** *ring-id* **east port** *port-id* **west port** *port-id* **node-type rpl-neighbour rpl** { **east** | **west** } [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlanlist*]	Create ring and configure node as RPL Neighbour.
	Raisecom(config)#**ethernet ring-protection** *ring-id* **east port** *port-id* **west port** *port-id* [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlanlist*]	Create ring and configure node as ring forwarding node.
3	Raisecom(config)#**ethernet ring-protection** *ring-id* **name** *string*	(Optional) Configure ring name. The length of name cannot exceed 32 strings.
4	Raisecom(config)#**ethernet ring-protection** *ring-id* **version** { **1** | **2** }	(Optional) Configure protocol version. All nodes in one ring must be consistent, version 1 differentiates ring via protocol VLAN, so different rings need to configure different protocol VLAN, and so do version 2.
5	Raisecom(config)#**ethernet ring-protection** *ring-id* **guard-time** *guard-time*	(Optional) During fault node restore time, after configuring Guard timer, it doesn't deal with APS protocol packets. In some big ring network, restoring node fault immediately may receive fault notice from neighbor node and cause link Down. Configure ring Guard timer can solve this problem.
6	Raisecom(config)#**ethernet ring-protection** *ring-id* **wtr-time** *wtr-time*	(Optional) Configure ring WTR timer. In revertive mode, the device returns to work in work link after WTR timer timeout when work link fault restores.
7	Raisecom(config)#**ethernet ring-protection** *ring-id* **holdoff-time** *holdoff-time*	(Optional) After configuring ring HOLDOFF timer, system delays fault report time when work link has fault. That is to say, the device will switch to protection link after a delay time to avoid frequent switch caused by work link change. **Note** The greater HOLDOFF timer value will influence 50ms switching performance, so it is recommended to use default value 0.
8	Raisecom(config)#**ethernet ring-protection trap** { **enable** | **disable** }	(Optional) Enable/disable ERPS fault information reported to NMS.

15.13.4 (Optional) creating ERPS protection sub-ring

Please configure ERPS crossover rings for devices as below.

Caution

- Only the crossover rings network contains master ring and sub-ring.
- The master ring configuration is identical to the configuration of single ring or tangent ring; please refer to the section of "Create ERPS protection ring" for details.
- Un-crossed node on sub-ring is identical to configuration of single ring or tangent ring; please refer to the section of "Create ERPS protection ring" for details.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet ring-protection** *ring-id* { **east port** *port-id* | **west port** *port-id* } **node-type rpl-owner** [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlanlist*]	Create sub-ring and configure node as RPLOwner on crossover node. By default, protocol VLAN is 1, blocked VLAN range is 1-4094. Protection ring changes to non-revertive mode when configuring not-revertive parameter. The difference between non-revertive mode and revertive mode is: in revertive mode, when work link fault restores, the flow will switch back to work link from protection link, but it doesn't switch in non-revertive mode. Protection ring is in revertive mode by default. **Note** The link between two crossover nodes in crossover rings belongs to master ring, so either east-bound or wester-bound port can be configured for sub-ring.
	Raisecom(config)#**ethernet ring-protection** *ring-id* { **east port** *port-id* | **west port** *port-id* } **node-type rpl-neighbour** [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlanlist*]	Create sub-ring and configure node as RPL Neighbour on crossover nodes.
	Raisecom(config)#**ethernet ring-protection** *ring-id* { **east port** *port-id* | **west port** *port-id* } [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlanlist*]	Create sub-ring and configure node as ring forwarding node on crossover nodes.

Step	Configuration	Description
3	Raisecom(config)#**ethernet ring-protection** *ring-id* **raps-vc** { **with** | **without** }	(Optional) Configure sub-ring virtual path mode on crossover node. Protocol packets transmitting in sub-ring is different from master ring, including with mode and without mode: • with: sub-ring protocol packets transmitted by master ring. • without: sub-ring protocol packets transmitted by sub-ring protocol VLAN, so the blocked VLAN list should not include protocol VLAN. By default, sub-ring virtual path uses with. Configuration mode of two crossover nodes must be consistent.
4	Raisecom(config)#**ethernet ring-protection** *ring-id* **propagate enable**	Enable ring Propagate switch on crossover node. Sub-ring data needs to be forwarded by master ring, so the sub-ring MAC address table also exists in master ring device. When sub-ring has fault, Propagate switch notifies master ring to refresh MAC address table in time and avoid flow lost. By default, Propagate switch disable. The command of **ethernet ring-protection** *ring-id* **propagate disable** can disable this function. It is suggested to enable Propagate switch.

15.13.5 Configuring ERPS fault detection mode

Please configure ERPS for the device as below.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } **failure-detect physical-link**	Configure fault detection mode as physical link.
	Raisecom(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } **failure-detect cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	Configure fault detection mode as CC. The fault detection mode won't take effect unless configuring CFM. MA must under md level after configuring MD.
	Raisecom(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } **failure-detect physical-link-or-cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	Configure fault detection mode as physical port or CC, namely, report fault either physical link or CC detected fault. The fault detection mode won't take effect unless configuring CFM. MA must under md level after configuring MD.

15.13.6 (Optional) configuring ERPS switching control

Please configure ERPS for the device as below.

By default, the flow will switch to protection link when work link has fault. Thus user needs to configure ELPS switching control just in some special situations.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet ring-protection** *ring-id* **force-switch** { **east** | **west** }	Configure flow on the ring force switch to east-bound or western-bound.
3	Raisecom(config)#**ethernet ring-protection** *ring-id* **manual-switch** { **east** | **west** }	Configure flow on the ring manual switch to east-bound or western-bound. Priority is lower than force switch and auto-switch when work link has faults.
4	Raisecom(config)#**ethernet ring-protection** *ring-id* **wtb-time** *wtb-time*	Available to RPLOwner node, in revertive mode, after configuring WTB timer, delay blocking RPL interface when clearing manual command to avoid several force-switch or manual-switch on a ring to block RPL interface. It is 5 seconds by default.
5	Raisecom(config)#**clear ethernet ring-protection** *ring-id* **command**	Clear switching control command, including force-switch and manual-switch.

15.13.7 Checking configuration

Check the configuration result by the commands below:

No.	Item	Description
1	Raisecom)#**show ethernet ring-protection**	Show ERPS ring configuration.
2	Raisecom)#**show ethernet ring-protection status**	Show ERPS ring status information.
3	Raisecom)#**show ethernet ring-protection statistics**	Show ERPS ring statistics.

15.14 Configuring port backup

15.14.1 Preparing for configuration

Networking situation

Port backup is the other STP solution. Users can manually set the port backup to achieve the basic link redundancy after disabling STP protocol.

Preconditions

Port backup and STP/MSTP functions cannot be enabled simultaneously. Therefore, user should disable STP/MSTP functions before configuring port backup.

15.14.2 Default configuration of port backup

The default configuration of port backup is as below:

Function	Default value
Port backup group	N/A
Recovery time	15s
Recovery mode	port-up (Port connection mode)

15.14.3 Configuring port backup

Please configure the port backup function as below:

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface port` *primary-port-id*	Enter physical layer port configuration mode.
3	`Raisecom(config-port)#switchport backup port` *backup-port-id* `[ vlanlist` *vlanlist* `]`	Configure port protection group. Configure port *backup-port-id* as standby port, while *primary-port-id* as master port on VLAN list. If configured port backup group cannot specify VLAN list, the default VLAN range is 1–4049.
4	`Raisecom(config)#switchport backup restore-delay` *delay-time*	(Optional) Configure recovery time.
5	`Raisecom(config)#switchport backup restore-mode { port-up | neighbor-discover | disable }`	(Optional) Configure recovery mode.

15.14.4 (Optional) configuring port forced switch

Please configure port forced switch as below:

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface port` *primary-port-id*	Enter physical layer port configuration mode. *port-id* is the master port of port protection group.

Step	Configuration	Description
3	Raisecom(config-port)#**switchport backup** [**port** *backup-port-id*] **force-switch**	Configure port forced switch. *port-id* is the standby port of port protection group.

15.14.5 Checking configuration

Check the configuration result by the commands below:

No.	Item	Description
1	Raisecom#**show switchport backup**	Check port backup information.

15.15 Maintenance

User can maintain the link reliability operation and configuration situation by the following commands:

Command	Description
Raisecom(config)#**clear ethernet line-protection statistics**	Clear protection line statistics, including numbers of Tx/Rx ASP messages, latest switching time and latest status switching time, etc.
Raisecom(config)#**clear ethernet ring-protection** *ring-id* **statistics**	Clear protection ring statistics.

15.16 Configuration examples

15.16.1 Examples for configuring OLT trunk fiber protection (Type B)

Networking requirements

As the figure shows below, to improve the link reliability between ISCOM5508 and ONU, user needs to configure OLT trunk fiber protection (Type B) on ISCOM5508, add OLT 1/1 and OLT 1/2 to protection group, therein, OLT 1/1 is master link, OLT 1/2 is standby link. The configured switching recovery time is 10min, ONU Holdover time is 500ms.

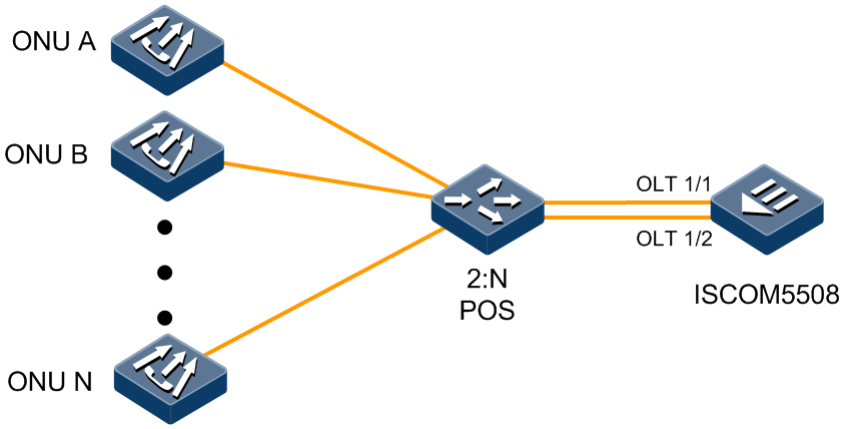

Figure 15-1 OLT trunk fiber protection (Type B) networking

Configuration steps

Step 1 Create OLT trunk fiber protection group.

```
Raisecom#fttx
Raisecom(fttx)#protect-group 1 primary 1/1 secondary 1/2 type backbone-pon-protect
```

Step 2 Configure to synchronize main PON port and main ONU link configuration data to standby PON port and standby ONU link.

```
Raisecom(fttx)#sync-data protect-group 1
```

Step 3 Configure recovery time.

```
Raisecom(fttx)#pretect-group 1 auto-recover-time 10
```

Step 4 Configure to enable protection group.

```
Raisecom(fttx)#pretect-group 1 enable
```

Step 5 Configure ONU Holdover time.

```
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#protect-group holdover time 500
Raisecom(fttx-onu1/1:1)#protect-group holdover activated time 500
```

```
Raisecom(fttx-onu1/1:1)#end
```

Step 6 Configure protection group member port isolation.

```
Raisecom#config
Raisecom(config)#interface port 7
Raisecom(config-port)#switch protect
Raisecom(config-port)#exit
Raisecom(config)#interface port 8
Raisecom(config-port)#switch protect
Raisecom(config-port)#end
```

Checking results

Use the command of **show protect-group** to show protection group configuration information and operation status.

```
Raisecom#show protect-group 1
Group ID: 1
   Group type             : Backbone pon protection
   Primary line           : 1/1
   Primary line state      : Normal
   Secondary line          : 1/2
   Secondary line state     : Normal
   Group admin status      : Enabled
   Group lock status       : Unlocked
   Group working status     : Normal
   Auto-recovery time      : 10 min
   Successful switching count: 0
   Last switching result    : Succeeded
```

15.16.2 Examples for configuring PON full protection (Type C)

Networking requirements

As the figure shows below, to improve the link reliability between ISCOM5508 and ONU, user needs to configure PON full protection (Type C) on ISCOM5508 and ONU, add OLT 1/1 and OLT 1/2 to protection group, therein, OLT 1/1 is master link, OLT 1/2 is standby link. The ONU Holdover time is 500ms.

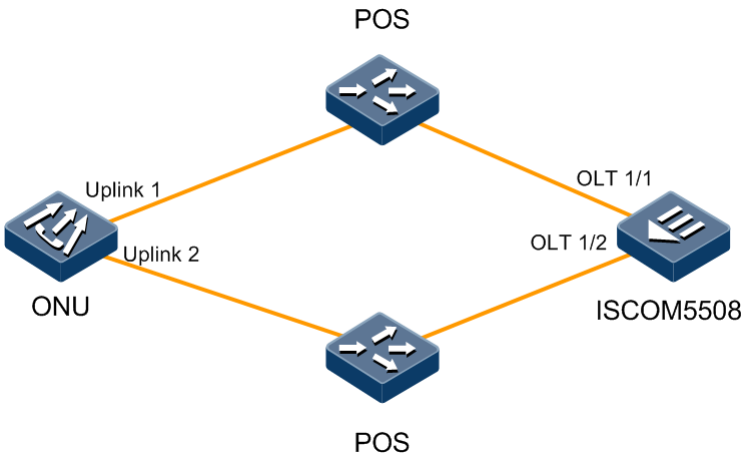

Figure 15-2 PON full protection (Type C) networking

Configuration steps

Step 1 Create OLT full protection group.

```
Raisecom#fttx
Raisecom(fttx)#protect-group 1 primary 1/1 secondary 1/2 type full-pon-protect
```

Step 2 Configure to synchronize main PON port and main ONU link configuration data to standby PON port and standby ONU link.

```
Raisecom(fttx)#sync-data protect-group 1
```

Step 3 Configure to enable protection group.

```
Raisecom(fttx)#pretect-group 1 enable
```

Step 4 Configure ONU Holdover time.

```
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#protect-group holdover time 500
Raisecom(fttx-onu1/1:1)#protect-group holdover activated time 500
Raisecom(fttx)#end
```

Step 5 Configure protection group member port isolation.

```
Raisecom#config
Raisecom(config)#interface port 7
Raisecom(config-port)#switch protect
Raisecom(config-port)#exit
Raisecom(config)#interface port 8
Raisecom(config-port)#switch protect
Raisecom(config-port)#end
```

Checking results

Use the command of **show protect-group** to show OLT protection group configuration information and operation status.

```
Raisecom#show protect-group 1
Group ID: 1
   Group type             : Full pon protection
   Primary line           : 1/1
   Primary line state      : Normal
   Secondary line          : 1/2
   Secondary line state     : LOS
   Group admin status       : Enabled
   Group lock status       : Unlocked
   Group working status     : Hotbackup
   Auto-recovery time      : 0 min
   Successful switching count: 0
   Last switching result    : Succeeded
```

Use the command of **show interface onu** *slot-id/olt-id/onu-id* **protect-group** to show ONU protection group configuration information and operation status.

```
Raisecom#show interface onu 1/1/1 protect-group
Group ID: 1
   Group type             : full pon protection
   Primary line           : 1/1
   Primary line state      : Normal
   Secondary line          : 1/2
   Secondary line state     : LOS
   Group admin status       : Enabled
   Group lock status       : Unlocked
   Group working status     : Normal
   Auto-recovery time      : 10 min
   Successful switching count: 0
   Last switching result    : Succeeded
```

15.16.3 Examples for configuring PON full protection (Type D)

Networking requirements

As the figure shows below, to improve the link reliability between ISCOM5508 and ONU, user needs to configure PON full protection (Type D) on ISCOM5508 and ONU, add OLT 1/1 and OLT 1/2 to protection group, therein, OLT 1/1 is master link, OLT 1/2 is standby link.

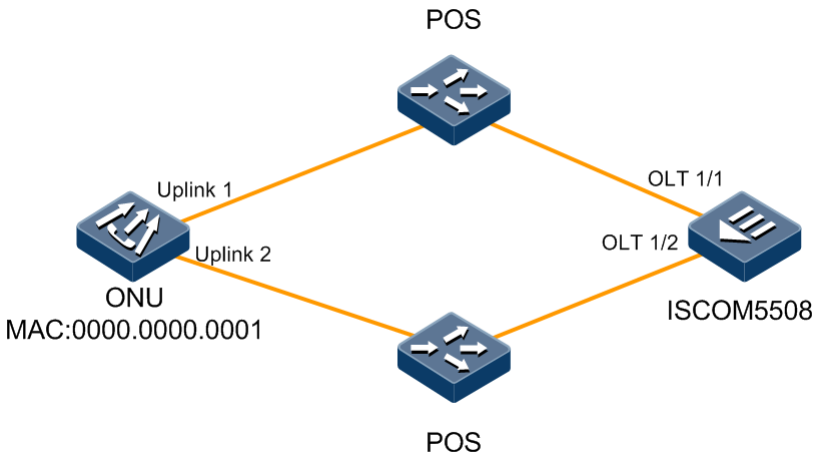

Figure 15-3 PON full protection (Type D) networking

Configuration steps

Step 1 Create OLT full protection group.

```
Raisecom#fttx
Raisecom(fttx)#protect-onu-group 1 primary 1/1/1 secondary 1/2/1
```

Step 2 Configure ONU MAC address.

```
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#device-mac 0000.0000.0001
Raisecom(fttx-onu1/1:1)#exit
Raisecom(fttx)#interface onu 1/2/1
Raisecom(fttx-onu1/2:1)#device-mac 0000.0000.0001
```

Step 3 Configure to synchronize main PON port and main ONU link configuration data to standby PON port and standby ONU link.

```
Raisecom(fttx-onu1/2:1)#exit
Raisecom(fttx)#sync-data protect-onu-group 1
Raisecom(fttx)#exit
```

Step 4 Configure protection group member port isolation.

```
Raisecom#config
Raisecom(config)#interface port 7
Raisecom(config-port)#switch protect
Raisecom(config-port)#exit
Raisecom(config)#interface port 8
Raisecom(config-port)#switch protect
Raisecom(config-port)#end
```

Checking results

Use the command of **show protect-group** to show OLT protection group configuration information and operation status.

```
Raisecom#show protect-group 1
Group ID: 1
   Group type             : Full pon protection
   Primary line           : 1/1
   Primary line state      : Normal
   Secondary line          : 1/2
   Secondary line state     : LOS
   Group admin status      : Enabled
   Group lock status       : Unlocked
   Group working status     : Hotbackup
   Auto-recovery time      : 0 min
   Successful switching count: 0
   Last switching result    : Succeeded
```

Use the command of **show interface onu** *slot-id/olt-id/onu-id* **protect-group** to show ONU protection group configuration information and operation status.

```
Raisecom#show interface onu 1/1/1 protect-group
Group ID: 1
   Group type             : Backbone pon protection
   Primary line           : 1/1
   Primary line state      : Normal
   Secondary line          : 1/2
   Secondary line state     : LOS
   Group admin status      : Enabled
   Group lock status       : Unlocked
   Group working status     : Normal
   Auto-recovery time      : 10 min
   Successful switching count: 0
   Last switching result    : Succeeded
```

15.16.4 Examples for configuring OLT uplink port dual-adscription protection

Networking requirements

As the figure shows below, to improve the link reliability between ISCOM5508 and uplink device, user needs to configure uplink port dual-adscription protection on ISCOM5508 and uplink port, add GE 1 and GE 2 to protection group, therein, GE 1 is master link, GE 2 is standby link. The configured switching recovery time is 10min.

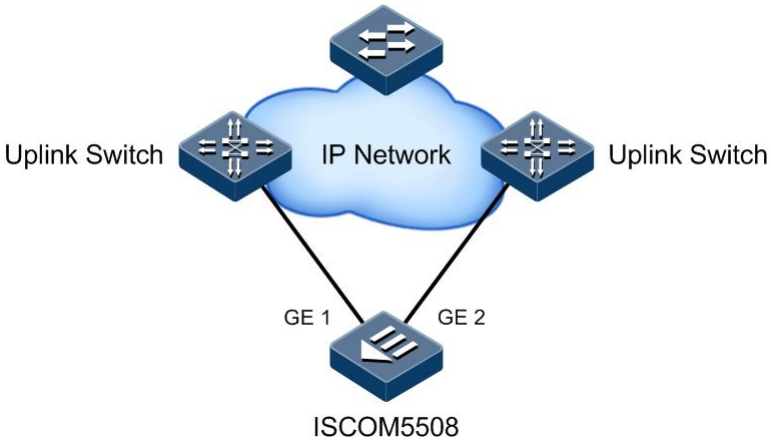

Figure 15-4 OLT uplink port dual-adscription protection networking

Configuration steps

Step 1 Create OLT uplink port dual-adscription protection group.

```
Raisecom#fttx
Raisecom(fttx)#protect-group 1 primary 1/1 secondary 1/2 type uplink-
protect
```

Step 2 Configure to enable protection group.

```
Raisecom(fttx)#pretect-group 1 enable
```

Step 3 Configure protection recovery time.

```
Raisecom(fttx)#pretect-group 1 auto-recover-time 10
```

Checking results

Use the command of **show protect-group** to show OLT protection group configuration information and operation status.

```
Raisecom#show protect-group 1
Group ID: 1
   Group type              : Uplink protection
   Primary line            : 1/1
   Primary line state       : Normal
   Secondary line          : 1/2
   Secondary line state     : LOS
   Group admin status       : Enabled
   Group lock status        : Unlocked
   Group working status     : Normal
   Auto-recovery time       : 10 min
   Successful switching count: 0
```

15.16.5 Examples for configuring cross OLT PON port dual-adscription protection (Type B)

Networking requirements

As the figure shows below, to improve overall link reliability, user can use two ISCOM5508 device to configure cross OLT PON port dual-adscription protection.

- ISCOM A is master device, IP address is 192.168.1.1, use OLT 1/1 port for downlink POS, and use GE 1 for uplink switch.
- ISCOM B is standby device, IP address is 192.168.1.2, use OLT 2/1 for downlink POS, and use GE 1 for uplink switch.

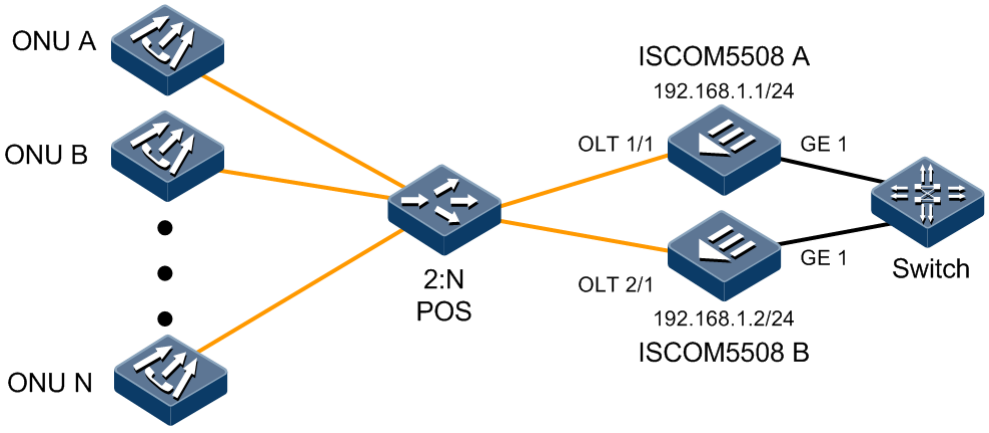

Figure 15-5 Cross OLT PON port dual-adscription protection (Type B) networking

Configuration steps

- Configure ISCOM5508 A

Step 1 Configure ISCOM5508 A IP address.

```
Raisecom#config
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address 192.168.1.1 255.255.255.0 1
Raisecom(config-ip)#end
```

Step 2 Configure ISCOM5508 A description information.

```
Raisecom#fttx
Raisecom(fttx)#device description iscom5508a
```

Step 3 Create cross OLT PON port dual-adscription protection group.

```
Raisecom(fttx)#protect-group 1 primary 1/1 secondary 2/1 type backbone-
pon-protect-extend local-port-role primary peer-device-description
iscom5508b peer-divice-ip-address 192.168.1.2
```

Step 4 Configure to enable protection group.

```
Raisecom(fttx)#pretect-group 1 enable
```

- Configure ISCOM5508 B

Step 5 Configure ISCOM5508 B IP address.

```
Raisecom#config
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address 192.168.1.2 255.255.255.0 1
Raisecom(config-ip)#end
```

Step 6 Configure ISCOM5508 B description information.

```
Raisecom#fttx
Raisecom(fttx)#device description iscom5508b
```

Step 7 Create cross OLT PON port dual-adscription protection group.

```
Raisecom#fttx
Raisecom(fttx)#protect-group 1 primary 1/1 secondary 2/1 type backbone-
pon-protect-extend local-port-role secondary peer-device-description
iscom5508a peer-divice-ip-address 192.168.1.1
```

Step 8 Configure to enable protection group.

```
Raisecom(fttx)#pretect-group 1 enable
```

Checking results

Use the command of **show protect-group** to show OLT protection group configuration information and operation status.

```
Raisecom#show protect-group 1
Group ID: 1
   Group type             : Backbone PON protection between OLTs
   Primary line           : 1/1
   Primary line state      : Normal
   Secondary line          : 2/1
   Secondary line state     : LOS
   Group admin status      : Enabled
   Group lock status       : Unlocked
   Group working status     : Normal
   Auto-recovery time      : 0 min
   Successful switching count: 1
   Last switching result    : Succeeded
   Local port role         : primary-port
   Peer device description   : iscom5508b
   Peer device IP address    : 192.168.1.2
   Last alarm status       : Normal
```

Use the command of **show protect-group** to show OLT protection group configuration information and operation status.

```
Raisecom#show protect-group 1
Group ID: 1
   Group type             : Backbone PON protection between OLTs
   Primary line           : 1/1
   Primary line state      : Normal
   Secondary line          : 2/1
   Secondary line state     : LOS
   Group admin status      : Enabled
   Group lock status       : Unlocked
   Group working status     : Normal
   Auto-recovery time      : 0 min
```

```
Successful switching count: 1
Last switching result    : Succeeded
Local port role         : secondary-port
Peer device description   : iscom5508b
Peer device IP address    : 192.168.1.1
Last alarm status       : Normal
```

15.16.6 Examples for configuring manual link aggregation

Networking requirements

As the figure shows below, to improve link reliability between ISCOM5508 and uplink aggregation switch, user can configure manual link aggregation on ISCOM5508, add GE 1 and GE 2 to link aggregation group, form a single logical port. Link aggregation group will take MAC load-sharing according to source MAC.

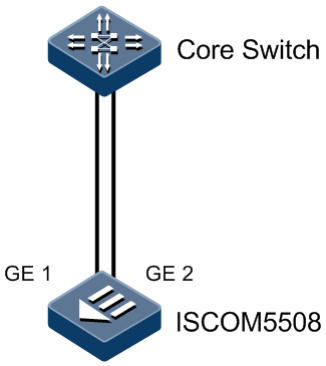

Figure 15-6 Manual link aggregation networking

Configuration steps

Step 1 Create manual link aggregation group, the group No. is 1.

```
Rraisecom#config
Rraisecom(config)#trunk group 1 port 1-2
```

Step 2 Configure aggregation link load-sharing mode.

```
Rraisecom(config)#trunkloading-sharing mode smac
```

Step 3 Enable link aggregation function.

```
Rraisecom(config)#trunk enable
```

Checking results

Use the command of **show trunk** to show manual link aggregation global configuration.

```
Raisecom#show trunk
Trunk: Enable
Loading sharing mode: SMAC
Trunk Group Mode   Member Ports        Efficient Ports
------------------------------------------------------------
1           manual     1,2                    --
```

15.16.7 Examples for configuring static LACP link aggregation

Networking requirements

As the figure shows below, to improve link reliability between ISCOM5508 and uplink switch, user can configure static LACP link aggregation on ISCOM5508 and uplink switch, add GE 1 and GE 2 to link aggregation group, therein, GE 1 is master link, and GE 2 is standby link.

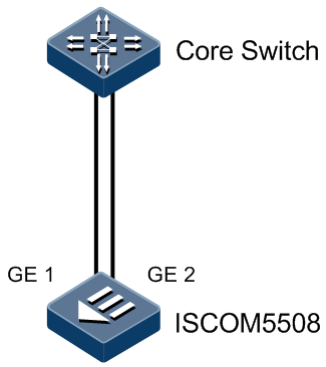

Figure 15-7 Static LACP link aggregation networking

Configuration steps

Step 1 Create static LACP link aggregation group.

```
Raisecom#config
Raisecom(config)#truck group 1 1-2 lacp-static
```

Step 2 Configure port 1 priority to make port 1 as master link and port 2 as standby link.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#lacp port-priority 10000
Raisecom(config-port)#exit
```

Step 3 Enable static LACP function.

```
Raisecom(config)#trunk enable
```

Checking results

Use the command of **show trunk** to shoe static LACP link aggregation global configuration.

```
Raisecom#show trunk
Trunk: Enable
Loading sharing mode:SXORDMAC
Trunk Group Mode   Member Ports        Efficient Ports
-----------------------------------------------------------
1         static 2,3               --
```

Use the command of **show lacp internal** to show opposite system LACP protocol port status, mark, port priority, management key, operation key and port status host status configuration.

```
Raisecom(config)#show lacp internal
Flags:
       S - Device is requesting Slow LACPDUs
       F - Device is requesting Fast LACPDUs
       A - Device is in Active mode
       P - Device is in Passive mode
Port State     Flags Port-Pri   Admin-key Oper-key Port-State
-------------------------------------------------------------------------
1     down       SA    10000       0x1       0x1      0x4D
2     down       SA    32768       0x1       0x1      0x4D
```

Use the command of **show lacp neighbor** to show opposite system LACP protocol port status, mark, port priority, management key, operation key and port status host status configuration.

15.16.8 Examples for configuring failover

Networking requirements

As the figure shows below, as one of the OLT A dual-adscription devices, user needs to configure failover function on ISCOM5508 to ensure that OLT A can detect link failure quickly and switch to standby link when ISCOM5508 uplink line disconnects.

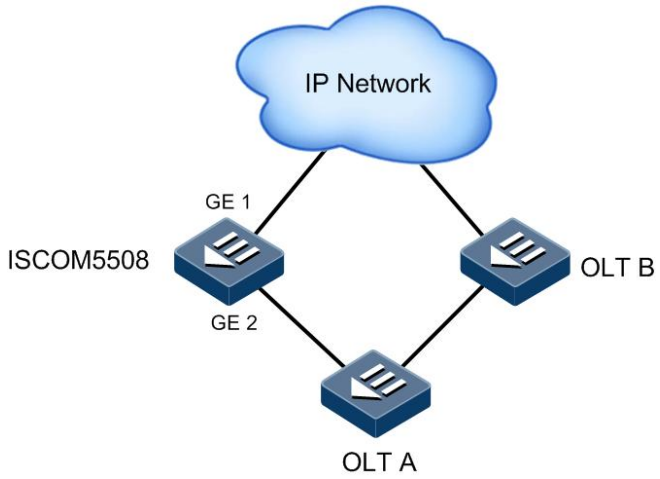

Figure 15-8 Failover networking

Configuration steps

Step 1 Create and enable failover function group.

```
Raisecom#config
Raisecom(config)#link-state-tracking group 1
```

Step 2 Configure failover function group uplink port.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#link-state-tracking group 1 upstream
Raisecom(config-port)#exit
```

Step 3 Configure failover function group downlink port.

```
Raisecom(config)#interface port 2
Raisecom(config-port)#link-state-tracking group 1 downstream
```

Checking results

Use the command of **show link-state-tracking group** to show device failover function configuration.

```
Raisecom#show link-state-tracking group 1
Link State Tracking Group: 1 (Enable)
Status:  Failover
Upstream Interfaces:
```

```
   Port 1(up)
Downstream Interfaces:
   Port 2(up)
```

Use the command of **show link-admin-status port** to show device port management information.

Raisecom# **show link-admin-status port 1-2**

```
Port      module          admin
-------------------------------------
1         shutdown         Up
          linkStateTrack   Up
          SecurityMac      Up
          EthRing          Up
2         shutdown         Up
          linkStateTrack   Up
          SecurityMac      Up
          EthRing          Up
```

15.16.9 Examples for configuring Ethernet ring

Networking requirements

As the figure shows below, four ISCOM5508 devices take ring networking, configure Ethernet ring function to achieve the elimination of ring network loopback, fault protection switching and auto fault recovery functions. Therein, ISCOM5508 A is the master node.

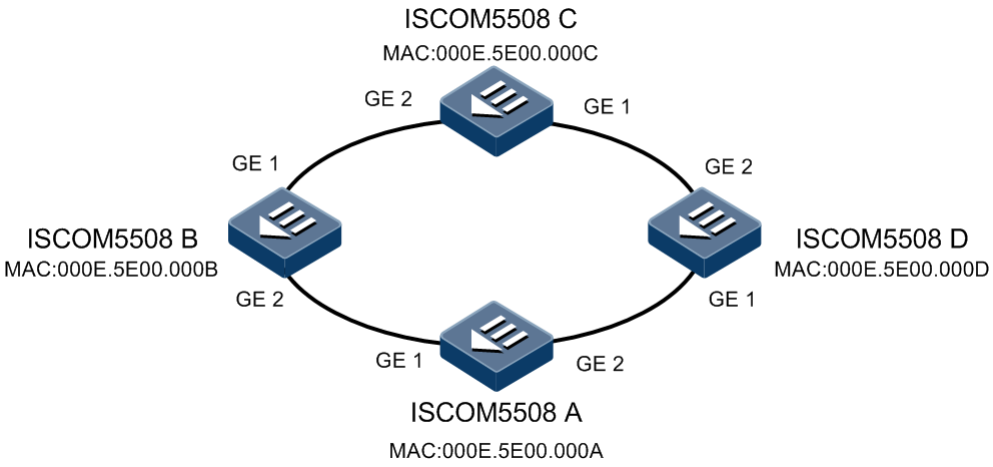

Figure 15-9 Ethernet ring networking

Configuration steps

Four ISCOM5508 devices have the same configuration method; here just take ISCOM5508 A as an example.

Step 1 Configure ISCOM5508 A Ethernet ring function.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)#ethernet ring 1 2
Raisecom(config-port)#exit
Raisecom(config)#ethernet ring enable
```

Step 2 Configure ISCOM5508 A port mode and allow Ethernet ring protocol through.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 2
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 2
Raisecom(config-port)#exit
```

Checking results

Use the command of **show ethernet ring** to show Ethernet ring configuration.

```
Raisecom#show ethernet ring
Ethernet Ring Upstream-Group:--
Ethernet Ring 1:
Ring Admin:         Enable
Ring State:         Unenclosed
Bridge State:       Block
Ring state duration:  0 days, 0 hours, 0 minutes, 55 seconds
Bridge Priority:     1
Bridge MAC:         000E.5E00.000A
Ring DB State:       Block
Ring DB Priority:    1
Ring DB:            000E.5E00.000A
Hello Time:         1
Restore delay:       5
Hold Time:          15
Protocol Vlan:       2
```

Use the command of **show ethernet ring port** to show Ethernet ring port status.

```
Raisecom#show ethernet ring port
Ethernet Ring 1:
```

```
Primary Port:         1
Port Active State:     Active
State:               Block
Peer State:           None
Switch counts:         5
Current state duration: 0 days, 0 hours, 2 minutes, 28 seconds
Peer Ring Node:
--1:000E.5E00.000B:1–
--2:000E.5E00.000B:1–
--3:000E.5E00.000B:1--
Secondary Port:       2
Port Active State:     Active
State:               Forward
Peer State:           None
Switch counts:         6
Current state duration: 0 days, 0 hours, 2 minutes, 28 seconds
Peer Ring Node:
--1:000E.5E00.000B:2–
--2:000E.5E00.000B:2–
--3:000E.5E00.000B:2--
```

15.16.10 Examples for configuring loopback detection

Networking requirements

As the figure shows below, OLT 1/1 of ISCOM5508 connects ONU through POS, UNI1 and UNI 2 of ONU connect user network. User can enable loopback detection function on ONU through ISCOM5508 remote management ONU so as to detect the loopback in user VLAN100.

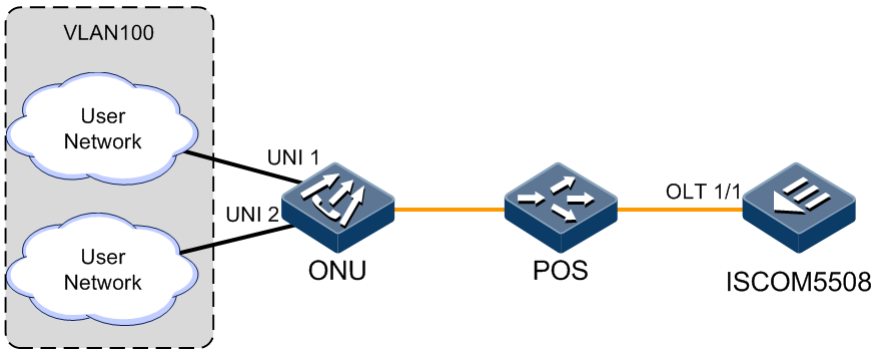

Figure 15-10 Loopback detection networking

Configuration steps

Step 1 Configure loopback detection VLAN to enable.

```
Raisecom#fttx
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#loopback-detection vlan 100
```

Step 2 Configure port detection UNI port to enable.

```
Raisecom(fttx-onu1/1:1)#uni ethernet 1
Raisecom(fttx-onu-uni1/1/1:1)#loopback-detection enable
Raisecom(fttx-onu-uni1/1/1:1)#exit
Raisecom(fttx-onu1/1:1)#uni ethernet 2
Raisecom(fttx-onu-uni1/1/1:2)#loopback-detection enable
```

Checking results

Use the command of **show interface onu** *slot-id/olt-id/onu-id* **loopback-detection** to show loopback detection configure.

```
Raisecom#show interface onu 1/1/1 loopback-detection
ONU ID: 1/1/1
   Period: 4s
   VLAN  : 100
   PORT ID  State    Loop Flag  State/Time    Source Port
   ------------------------------------------------------
   1       enable   no        --/infinite   0
   2       enable   no        --/infinite   0
   3       disable  no        --/infinite   0
   4       disable  no        --/infinite   0
```

15.16.11 Examples for configuring layer-2 protocol transparent transmission

Networking requirements

As the figure shows below, ISCOM5508 connects VLAN 100 and VLAN 200 network through POS and ONU. To achieve the same user network in different regions unified operating STP protocol, user needs to configure STP protocol transparent transmission function on ISCOM5508.

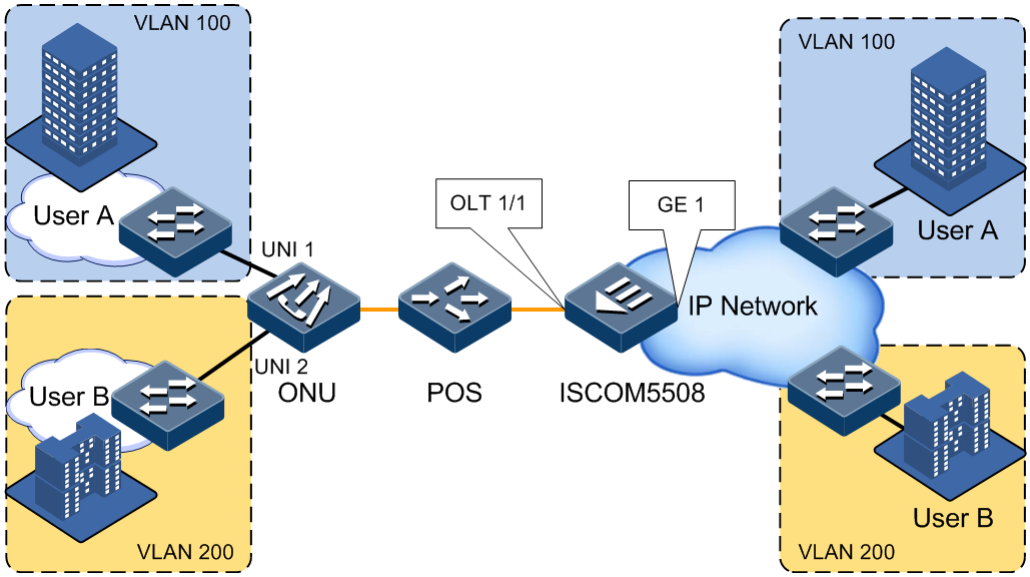

Figure 15-11 Layer-2 protocol transparent transmission networking

Configuration steps

- Configure OLT.

Step 1 Create VLAN 100 and VLAN 200 on ISCOM5508 and activate them.

```
Raisecom#config
Raisecom(config)#create vlan 100,200 active
```

Step 2 Configure port mode for ISCOM5508 uplink port and PON port.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 100,200
Raisecom(config-port)#exit
Raisecom(config)#interface port 7
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 100,200
Raisecom(config-port)#end
```

- Configure ONU.

Step 3 Configure port attributes for ONU uplink port and UNI port.

```
Raisecom#fttx
Raisecom(fttx)#interface onu 1/1/1
Raisecom(fttx-onu1/1:1)#uni ethernet 1
Raisecom(fttx-onu-uni1/1/1:1)#vlan mode transparent
```

```
Raisecom(fttx-onu-uni1/1/1:1)#exit
Raisecom(fttx-onu1/1:1)#uplink
Raisecom(fttx-onu1/1:1)#uni ethernet 2
Raisecom(fttx-onu-uni1/1/1:2)#vlan mode transparent
Raisecom(fttx-onu-uni1/1/1:2)#exit
Raisecom(fttx-onu1/1:1)#uplink
Raisecom(fttx-onu-uplink1/1/1:1)#vlan mode transparent
```

Checking results

Use the command of **show relay** to show layer-2 protocol transparent transmission information.

```
Raisecom#show relay
COS for Encapsulated Packets: 5
Destination MAC Address for Encapsulated Packets: 010E.5E00.0003
Port          vlan  Egress-Port   Protocol      Drop-Threshold
Shutdown-Threshold
------------------------------------------------------------------------
----------------
1(up)         --    --         stp(enable)   1500             --
                               dot1x         --               --
                               lacp          --               --
                               gvrp          --               --

2(up)         --    --          stp           --              --
                               dot1x         --               --
                               lacp          --               --
                               gvrp          --               --

3(up)         --    --          stp           --              --
                               dot1x         --               --
                               lacp          --               --
                               gvrp          --               --

4(up)         --    --          stp           --              --
                               dot1x         --               --
                               lacp          --               --
                               gvrp          --               --
5(up)         --    --          stp           --              --
                               dot1x         --               --
                               lacp          --               --
                               gvrp          --               --
6(up)         --   --           stp           --              --
                               dot1x         --               --
                               lacp          --               --
                               gvrp          --               --
7(up)         --     1         stp(enable) 1500               --
                               dot1x         --               --
                               lacp          --               --
                               gvrp          --               --
```

15.16.12 Examples for configuring ELPS protection application in 1:1 mode

Networking requirements

As the figure shows below, to improve link reliability between ISCOM5508 A and ISCOM5508 B, configure 1:1 ELPS on the two devices and detect fault over physical port status. GE 1 and GE 2 VLAN range is 100–200.

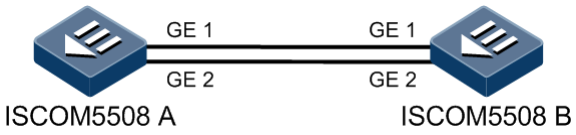

Figure 15-12 ELSP networking in 1:1 mode

Configuration steps

Step 1 Create VLAN 100–VLAN 200 and add port into VLAN 100–VLAN 200.

- Configure ISCOM5508 A.

```
Raisecom#config
Raisecom(config)#create vlan 100-200 active
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 100-200 confirm
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 100-200 confirm
Raisecom(config-port)#exit
```

- Configure ISCOM5508 B.

```
Raisecom#config
Raisecom(config)#create vlan 100-200 active
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 100-200 confirm
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 100-200 confirm
Raisecom(config-port)#exit
```

Step 2 Create ELSP protection line in 1:1 mode.

- Configure ISCOM5508 A.

```
Raisecom(config)#ethernet line-protection 1 working port 1 100-200
protection port 2 100-200 one-to-one
```

- Configure ISCOM5508 B.

```
Raisecom(config)#ethernet line-protection 1 working port 1 100-200
protection port 2 100-200 one-to-one
```

Step 3 Configure fault detection mode.

- Configure ISCOM5508 A.

```
Raisecom(config)#ethernet line-protection 1 working failure-detect
physical-link
Raisecom(config)#ethernet line-protection 1 protection failure-detect
physical-link
```

- Configure ISCOM5508 B.

```
Raisecom(config)#ethernet line-protection 1 working failure-detect
physical-link
Raisecom(config)#ethernet line-protection 1 protection failure-detect
physical-link
```

Checking results

Use the command of **show ethernet line-protection** to show ELSP configuration in 1:1 mode.

Take ISCOM5508 A as an example:

```
Raisecom#show ethernet line-protection 1
Id:1
Name:
ProtocolVlan:100-200
Working(Port-Vlanlist-FaiureDetect-MAID-LocalMep-RemoteMep)(State/LCK):
port1-100-200-physical--0-0-0(Active/N)
Protection(Port-Vlanlist-FaiureDetect-MAID-LocalMep-RemoteMep)(State/F/M):
port2-100-200-physical--0-0-0(Standby/N/N)
Wtr(m):5
Holdoff(100ms):0
```

Use the command of **show ethernet line-protection aps** to show ELSP APS protocol information in 1:1 mode.

Take OLT A as an example:

```
Raisecom#show ethernet line-protection 1 aps
Id      Type    Direction Revert Aps State Signal(Requested/Bridged)
-------------------------------------------------------------------------
1-Local  1:1     bi       yes    yes NR-W  null/null
1-Remote 1:1     bi       yes    yes NR-W  null/null
```

15.16.13 Examples for configuring ELPS protection application in 1+1 mode

Networking requirements

As the figure shows below, to improve link reliability between ISCOM5508 A and ISCOM5508 B, configure 1+1 one-way ELPS on the two devices and detect fault over CFM. GE 1 and GE 2 VLAN range is 100–200.

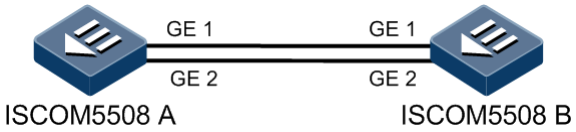

Figure 15-13 ELSP networking in 1+1 mode

Configuration steps

Step 1 Create VLAN 100–VLAN 200 and add port into VLAN 100–VLAN 200.

- Configure ISCOM5508 A.

```
Raisecom#config
Raisecom(config)#create vlan 100-200 active
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 100-200 confirm
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 100-200 confirm
Raisecom(config-port)#exit
```

- Configure ISCOM5508 B.

```
Raisecom#config
Raisecom(config)#create vlan 100-200 active
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
```

```
Raisecom(config-port)#switchport trunk allowed vlan 100-200 confirm
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 100-200 confirm
Raisecom(config-port)#exit
```

Step 2 Configure CFM.

- Configure ISCOM5508 A.

```
Raisecom(config)#ethernet cfm domain md-name md1 level 7
Raisecom(config)#service ma1 level 7
Raisecom(config-service)#service vlan-list 100
Raisecom(config-service)#service mep down mpid 1 port 1
Raisecom(config-service)#service mep down mpid 2 port 2
Raisecom(config-service)#service remote-mep 3
Raisecom(config-service)#service remote-mep 4
Raisecom(config-service)#service cc enable mep 1
Raisecom(config-service)#service cc enable mep 2
Raisecom(config-service)#exit
Raisecom(config)#ethernet cfm enable
```

- Configure ISCOM5508 B.

```
Raisecom(config)#ethernet cfm domain md-name md1 level 7
Raisecom(config)#service ma1 level 7
Raisecom(config-service)#service vlan-list 100
Raisecom(config-service)#service mep down mpid 3 port 1
Raisecom(config-service)#service mep down mpid 4 port 2
Raisecom(config-service)#service remote-mep 1
Raisecom(config-service)#service remote-mep 2
Raisecom(config-service)#service cc enable mep 3
Raisecom(config-service)#service cc enable mep 4
Raisecom(config-service)#exit
Raisecom(config)#ethernet cfm enable
```

Step 3 Create 1+1 one-way ELSP protection line.

- Configure ISCOM5508 A.

```
Raisecom(config)#ethernet line-protection 1 working port 1 100-200
protection port 2 100-200 one-plus-one-uni
```

- Configure ISCOM5508 B.

```
Raisecom(config)#ethernet line-protection 1 working port 1 100-200
protection port 2 100-200 one-plus-one-uni
```

Step 4 Configure fault detection mode.

- Configure ISCOM5508 A.

```
Raisecom(config)#ethernet line-protection 1 working failure-detect cc md
md1 ma ma1 level 7 mep 1 3
Raisecom(config)#ethernet line-protection 1 protection failure-detect cc
md md1 ma ma1 level 7 mep 2 4
```

- Configure ISCOM5508 B.

```
Raisecom(config)#ethernet line-protection 1 working failure-detect cc md
md1 ma ma1 level 7 mep 3 1
Raisecom(config)#ethernet line-protection 1 protection failure-detect cc
md md1 ma ma1 level 7 mep 4 2
```

Checking results

Use the command of **show ethernet line-protection** to show ELSP configuration in 1+1 mode.

Take ISCOM5508 A as an example:

```
Raisecom#show ethernet line-protection 1
Id:1
Name:
MEL:7
ProtocolVlan:100-200
Working(Port-Vlanlist-FaiureDetect-MAID-LocalMep-RemoteMep)(State/LCK):
port1-100-200-cc-md1ma1-1-3(Active/N)
Protection(Port-Vlanlist-FaiureDetect-MAID-LocalMep-RemoteMep)(State/F/M):
port2-100-200-cc-md1ma1-2-4(Standby/N/N)
Wtr(m):5
Holdoff(100ms):0
```

Use the command of **show ethernet line-protection aps** to show ELSP APS protocol information in 1+1 mode.

Take ISCOM5508 A as an example:

```
Raisecom#show ethernet line-protection 1 aps
Id      Type    Direction Revert Aps State Signal(Requested/Bridged)
```

```
------------------------------------------------------------------------------
1-Local  1+1     uni      yes    yes NR-W  null/normal
```

15.16.14 Examples for configuring single ring ERPS protection

Networking requirements

As the figure shows below, to improve Ethernet reliability, the four devices ISCOM5508 A, ISCOM5508 B, ISCOM5508 C and ISCOM5508 D build up an ERPS single ring.

ISCOM5508 A device is RPLOwner, ISCOM5508 B is RPLNeighbour; the RPL link between ISCOM5508 A and ISCOM5508 B is blocked.

The fault detection mode between ISCOM5508 A and ISCOM5508 D is physical-link-or-cc, other links adopt default fault detection mode (physical-link).

By default, VLAN is 1, and the congested VLAN range is 1–4094.

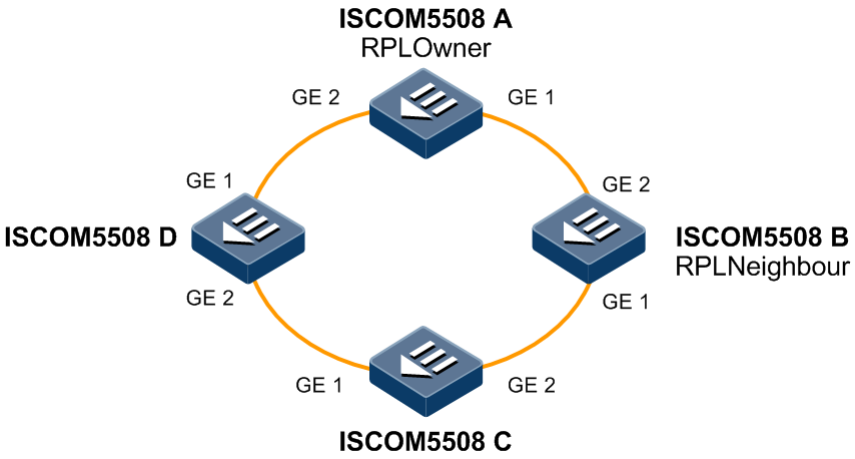

Figure 15-14 Single ring ERPS networking

Configuration steps

Step 1 Add port into VLAN 1–VLAN 4094.

- Configure ISCOM5508 A.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
```

- Configure ISCOM5508 B.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
```

- Configure ISCOM5508 C.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
```

- Configure ISCOM5508 D.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
```

Step 2 Configure CFM.

- Configure ISCOM5508 A.

```
Raisecom(config)#ethernet cfm domain md-name md1 level 7
Raisecom(config)#service ma1 level 7
Raisecom(config-service)#service vlan-list 1
Raisecom(config-service)#service mep down mpid 1 port 2
Raisecom(config-service)#service remote-mep 2
Raisecom(config-service)#service cc enable mep 1
Raisecom(config-service)#exit
Raisecom(config)#ethernet cfm enable
```

- Configure ISCOM5508 D.

```
Raisecom(config)#ethernet cfm domain md-name md1 level 7
Raisecom(config)#service ma1 level 7
```

```
Raisecom(config-service)#service vlan-list 1
Raisecom(config-service)#service mep down mpid 2 port 1
Raisecom(config-service)#service remote-mep 1
Raisecom(config-service)#service cc enable mep 2
Raisecom(config-service)#exit
Raisecom(config)#ethernet cfm enable
```

Step 3 Create ERPS protection ring.

- Configure ISCOM5508 A.

```
Raisecom(config)#ethernet ring-protection 1 east port 1 west port 2 node-
type rpl-owner rpl east
```

- Configure ISCOM5508 B.

```
Raisecom(config)#ethernet ring-protection 1 east port 1 west port 2 node-
type rpl-neighbour rpl west
```

- Configure ISCOM5508 C.

```
Raisecom(config)#ethernet ring-protection 1 east port 1 west port 2
```

- Configure ISCOM5508 D.

```
Raisecom(config)#ethernet ring-protection 1 east port 1 west port 2
```

Step 4 Configure fault detection mode.

- Configure ISCOM5508 A.

```
Raisecom(config)#ethernet ring-protection 1 west failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 1 2
```

- Configure ISCOM5508 D.

```
Raisecom(config)#ethernet ring-protection 1 east failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 2 1
```

Checking results

Use the command of **show ethernet ring-protection status** to show ERPS protection ring.

Take ISCOM5508 A for example, RPL link is congested to avoid loopback:

```
Raisecom#show ethernet ring-protection status
Id/Name  Status   Last Occur(ago)   East-State West-State sc Traffic-
vlanlist
-------------------------------------------------------------------------
1       idle   0 day 0:0:50:750   block      forwarding   1   1-4094
```

Cut off link between ISCOM5508 B and ISCOM5508 C by manual to simulate fault, use command again on ISCOM5508 A to show ERPS protection ring status and RPL link switches to forwarding status.

```
Raisecom#show ethernet ring-protection status
Id/Name  Status   Last Occur(ago)   East-State West-State sc Traffic-
vlanlist
-------------------------------------------------------------------------
1       Protection  0 day 0:0:55:950  forwarding forwarding   1   1-4094
```

15.16.15 Examples for configuring cross ring ERPS protection

Networking requirements

As the figure shows below, to improve Ethernet reliability, the devices ISCOM5508 A, ISCOM5508 B, ISCOM5508 C, ISCOM5508 D, ISCOM5508 E and ISCOM5508 F build up cross ring ERPS network.

ISCOM5508 A, ISCOM5508 B, ISCOM5508 C and ISCOM5508 D build up the master ring, ISCOM5508 D is master ring RPLOwner, ISCOM5508 C is master ring RPLNeighbour, congest port is ISCOM5508 D Port 1, protocol VLAN adopts default value 1.

ISCOM5508 A, ISCOM5508 B, ISCOM5508 E and ISCOM5508 F build up secondary ring, ISCOM5508F is secondary ring RPLOwner, ISCOM5508 A is secondary ring RPLNeighbour, congest port is ISCOM5508 F Port 1, protocol VLAN is 4094. By default, virtual path mode of secondary ring is with mode.

By default, the congestion VLAN range of master and secondary ring is 1–4094.

All master ring devices adopt physical-link-or-cc mode to detect fault, while secondary ring adopts defaulted fault detection mode (physical-link).

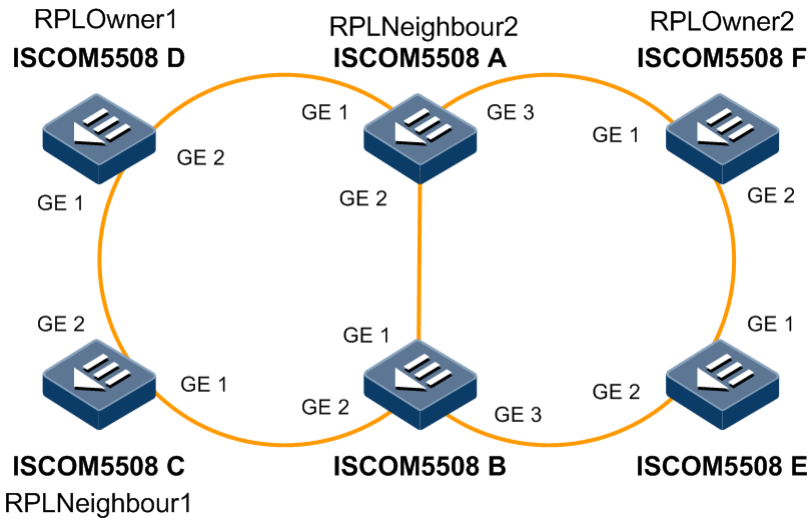

Figure 15-15 Cross ring ERPS networking

Configuration steps

Step 1 Add port into VLAN 1–VLAN 4094.

- Configure ISCOM5508 A.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 3
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
```

- Configure ISCOM5508 B.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 3
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
```

- Configure ISCOM5508 C.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
```

- Configure ISCOM5508 D.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
```

- Configure ISCOM5508 E.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
```

- Configure ISCOM5508 F.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#exit
```

Step 2 Configure master ring CFM detection.

- Configure ISCOM5508 A.

```
Raisecom(config)#ethernet cfm domain md-name md1 level 7
Raisecom(config)#service ma1 level 7
Raisecom(config-service)#service vlan-list 1
Raisecom(config-service)#service mep down mpid 1 port 1
Raisecom(config-service)#service mep down mpid 2 port 2
Raisecom(config-service)#service cc enable mep 1
Raisecom(config-service)#service cc enable mep 2
Raisecom(config-service)#exit
Raisecom(config)#ethernet cfm enable
```

- Configure ISCOM5508 B.

```
Raisecom(config)#ethernet cfm domain md-name md1 level 7
Raisecom(config)#service ma1 level 7
Raisecom(config-service)#service vlan-list 1
Raisecom(config-service)#service mep down mpid 3 port 1
Raisecom(config-service)#service mep down mpid 4 port 2
Raisecom(config-service)#service cc enable mep 3
Raisecom(config-service)#service cc enable mep 4
Raisecom(config-service)#exit
Raisecom(config)#ethernet cfm enable
```

- Configure ISCOM5508 C.

```
Raisecom(config)#ethernet cfm domain md-name md1 level 7
Raisecom(config)#service ma1 level 7
Raisecom(config-service)#service vlan-list 1
Raisecom(config-service)#service mep down mpid 5 port 1
Raisecom(config-service)#service mep down mpid 6 port 2
Raisecom(config-service)#service cc enable mep 5
Raisecom(config-service)#service cc enable mep 6
Raisecom(config-service)#exit
Raisecom(config)#ethernet cfm enable
```

- Configure ISCOM5508 D.

```
Raisecom(config)#ethernet cfm domain md-name md1 level 7
Raisecom(config)#service ma1 level 7
Raisecom(config-service)#service vlan-list 1
Raisecom(config-service)#service mep down mpid 7 port 1
Raisecom(config-service)#service mep down mpid 8 port 2
Raisecom(config-service)#service cc enable mep 7
Raisecom(config-service)#service cc enable mep 8
Raisecom(config-service)#exit
Raisecom(config)#ethernet cfm enable
```

Step 3 Create ERPS protection ring master ring.

- Configure ISCOM5508 A.

```
Raisecom(config)#ethernet ring-protection 1 east port 1 west port 2
```

- Configure ISCOM5508 B.

```
Raisecom(config)#ethernet ring-protection 1 east port 1 west port 2
```

- Configure ISCOM5508 C.

```
Raisecom(config)#ethernet ring-protection 1 east port 1 west port 2 node-
type rpl-neighbour rpl west
```

- Configure ISCOM5508 D.

```
Raisecom(config)#ethernet ring-protection 1 east port 1 west port 2 node-
type rpl-owner rpl east
```

Step 4 Configure master ring detection mode.

- Configure ISCOM5508 A.

```
Raisecom(config)#ethernet ring-protection 1 east failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 1 8
Raisecom(config)#ethernet ring-protection 1 west failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 2 3
```

- Configure ISCOM5508 B.

```
Raisecom(config)#ethernet ring-protection 1 east failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 3 2
Raisecom(config)#ethernet ring-protection 1 west failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 4 5
```

- Configure ISCOM5508 C.

```
Raisecom(config)#ethernet ring-protection 1 east failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 5 4
Raisecom(config)#ethernet ring-protection 1 west failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 6 7
```

- Configure ISCOM5508 D.

```
Raisecom(config)#ethernet ring-protection 1 east failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 7 6
Raisecom(config)#ethernet ring-protection 1 west failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 8 1
```

Step 5 Configure ERPS protection ring secondary ring.

- Configure ISCOM5508 A.

```
Raisecom(config)#ethernet ring-protection 2 east port 3 node-type rpl-
neighbour protocol-vlan 4094
Raisecom(config)#ethernet ring-protection 2 propagate enable
```

- Configure ISCOM5508 B.

```
Raisecom(config)#ethernet ring-protection 2 east port 3 protocol-vlan
4094
Raisecom(config)#ethernet ring-protection 2 propagate enable
```

- Configure ISCOM5508 E.

```
Raisecom(config)#ethernet ring-protection 2 east port 3 west port 2
protocol-vlan 4094
```

- Configure ISCOM5508 F.

```
Raisecom(config)#ethernet ring-protection 2 east port 3 west port 2 node-
type rpl-owner rpl east protocol-vlan 4094
```

Checking results

Use the command of **show ethernet ring-protection status** to show ERPS protection ring.

Check configuration on ISCOM5508 A:

```
Raisecom#show ethernet ring-protection status
Id/Name  Status   Last Occur(ago)East-State West-State sc   Traffic-
vlanlist
-------------------------------------------------------------------------
1       idle   0 day 0:0:50:750  forwarding  forwarding 1     1-4094
Id/Name  Status   Last Occur(ago)East-State West-State sc   Traffic-
vlanlist
-------------------------------------------------------------------------
2       idle   0 day 0:0:50:750  forwarding  forwarding 1     1-4094
```

Check configuration on ISCOM5508 D:

```
Raisecom#show ethernet ring-protection status
Id/Name  Status   Last Occur(ago)   East-State West-State sc Traffic-
vlanlist
-------------------------------------------------------------------------
1       idle   0 day 0:0:50:750  block      forwarding  1   1-4094
```

Check configuration on ISCOM5508 F:

```
Raisecom#show ethernet ring-protection status
Id/Name  Status   Last Occur(ago)   East-State West-State sc Traffic-
vlanlist
-------------------------------------------------------------------------
2       idle   0 day 0:0:50:750  block      forwarding  1   1-4094
```

15.16.16 Examples for configuring port backup

Networking requirements

As the figure shows below, to ensure link security of ISCOM5508 uplink port, user needs to configure port backup on ISCOM5508 to achieve port link protection and load-sharing, the requirements are as follows:

- GE 1 is the master port of VLAN 100–VLAN 150 and GE 2 is the secondary port of VLAN 100–VLAN 150.
- GE 2 is the master port of VLAN 151–VLAN 200, and GE 1 is the secondary port of VLAN 151–VLAN 200.

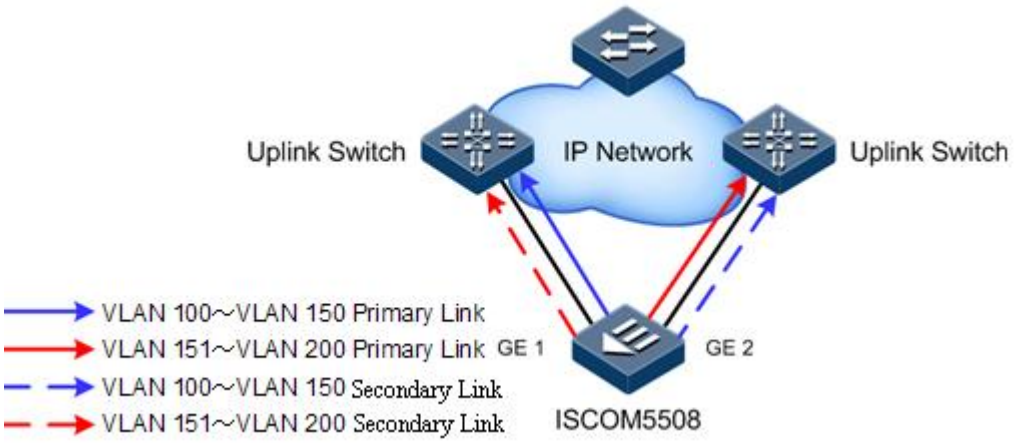

Figure 15-16 Port backup networking

Configuration steps

Step 1 Configure VLAN 100–VLAN 150 port backup.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport backup port 2 vlanlist 100-150
Raisecom(config-port)#exit
```

Step 2 Configure VLAN 151–VLAN 200 port backup.

```
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport backup port 1 vlanlist 151-200
Raisecom(config-port)#exit
```

Checking results

Use the command of **show switchport backup** to show port backup configuration.

```
Raisecom#show switchport backup
Restore delay: 15s
Restore mode: port-up
Active Port(State)   Backup Port(State)   Vlanlist
-----------------------------------------------------------
1         (up)            2      (up)      100-150
2         (up)            1      (up)      151-200
```

16 Configuring system management

This chapter introduces basic principle and configuration of system management and provides related configuration applications.

- SNMP
- RMON
- Optical module digital diagnostics
- System log
- Alarm management
- Performance management
- System monitoring
- Ping
- Traceroute
- LLDP
- Watchdog
- Keepalive
- Tx and Rx packets statistics
- Maintenance
- Configuring examples

16.1 SNMP

16.1.1 Default configuration of SNMP

The default configuration of SNMP is as below:

Function	Default value
SNMP view	By default: system, internet view

Function	Default value
SNMP community	By default: public, private community Index CommunityName ViewName Permission 1 public internet ro 2 private internet rw
SNMP access group	By default: initialnone, initial group
SNMP user	By default: none, md5nopriv, shanopriv user
Mapping relation between SNMP user and access group	Index GroupName UserName SecModel 1 initialnone raisecomnone usm 2 initial raisecommd5nopriv usm 3 initial raisecomshanopriv usm
Logo and the contact method of administrator	support@Raisecom.com
Device physical location	world china raisecom
Trap status	Enable
SNMP target host address	N/A

16.1.2 Configuring basic function for SNMP v1/v2c

In order to protect itself and prevent its MIB from unauthorized access, SNMP Agent proposes the concept of community. The management station in the same community must use the community name in all Agents operating, or their requests will not be accepted.

Community name refers to use different SNMP string to identify different group. Different community can have read-only or read-write access permission. Groups with read-only permission can only query the device information, while groups with read-write authority can configure the device in addition to query the device information.

SNMP v1/v2c uses the community name authentication scheme, and the SNMP packets which are inconsistent to the community name will be discarded.

Please configure SNMP v1, v2c on the device as below.

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#snmp-server view` *view-name oid-tree* [*mask*] { `included` | `excluded` }	(Optional) Create SNMP view and configure MIB variable range.
3	`Raisecom(config)#snmp-server community` *com-name* [`view` *view-name*] { `ro` | `rw` }	Create community name and configure the corresponding view and access permission.

16.1.3 Configuring basic function for SNMP v3

SNMPv3 uses USM over user authentication mechanism. USM comes up with the concept of access group: one or more users correspond to one access group, each access group sets the related read, write and announce view; users in access group have access permission in this view. User access group dent Get and Set request must have permission corresponding to the request, or the request will not be accepted.

As the Figure below shows, network management station uses the normal access from SNMP v3 to ISCOM5508 and the configuration is as below:

- Configure user.
- Check which access group the user belongs to.
- Configure view permission for access group.
- Create view.

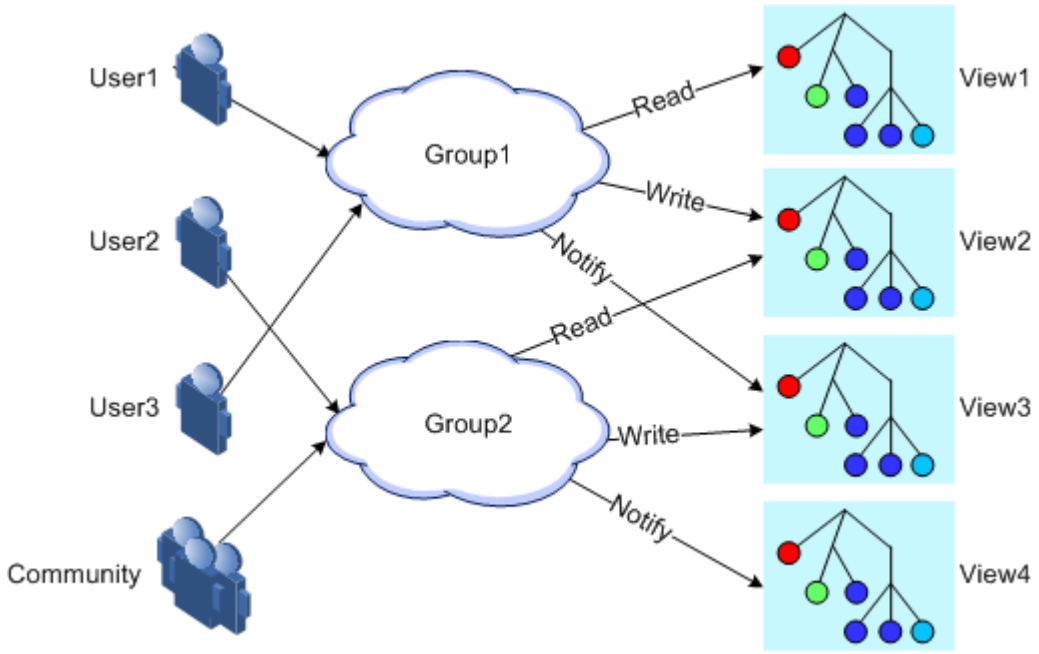

Figure 16-1 Sketch map of SNMP v3 authentication mechanism

Please configure SNMP v3 on the device as below:

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#snmp-server view` *view-name oid-tree* [*mask*] { `included` | `excluded` }	Create SNMP view and configure MIB variable range.
3	`Raisecom(config)#snmp-server user` *username* [`remote` *engineid*] `authentication` { `md5` | `sha` } *authpassword*	Create user and configure authentication mode.
4	`Raisecom(config)#snmp-server access` *group-name* [`read` *view-name*] [`write` *view-name*] [`notify` *view-name*] [`context` *context-name*{ `exact` | `prefix` }] `usm` { `noauthnopriv` | `authnopriv` }	Create and configure SNMP v3 access group.

Step	Configuration	Description
5	Raisecom(config)#**snmp-server group** *group-name* **user** *username* { **v1sm** | **v2csm** | **usm** }	Configure the mapping relation between user and access group.

16.1.4 Configuring other information of SNMP

Configure other information of SNMP, including:

- Logo and contact method of administrators
- Physical location of ISCOM5508

All SNMP v1, v2c and v3 are in support of the above configuration.

Please configure other information of SNMP on the device as below.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server contact** *contact*	(Optional) Configure logo and contact method of administrators. **Note** For example: use E-mail as logo and contact method of administrators.
3	Raisecom(config)#**snmp-server location** *location*	(Optional) assign the physical location of device.

16.1.5 Configuring Trap

Note

Except for target host configuration, Trap configuration of SNMP v1, v2c and v3 are identical.

Trap means the device sends unrequested information to NMS automatically, which is used to report some critical events.

Finish the following tasks before configuring Trap function:

- Configure SNMP basic function. SNMP v1 and v2c versions need to configure community name; SNMP v3 needs to configure username and SNMP view.
- Configure routing protocol, and make sure routing between ISCOM5508 and NMS is available.

Please configure SNMP Trap on the device as below.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.

Step	Configuration	Description
2	Raisecom(config)#**interface ip** *if-number*	Enter Layer-3 interface configuration mode.
3	Raisecom(config-ip)#**ip address** *ip-address* [*ip-mask*] *vlan-id*	Configure device IP address.
4	Raisecom(config-ip)#**snmp-server host** *ip-address* **version 3** { **noauthnopriv** | **authnopriv** } *name* [**udpport** *value*]	(Optional) Configure Trap/Notification target host over SNMP v3.
5	Raisecom(config-ip)#**snmp-server host** *ip-address* **version** { **1** | **2c** |**3** } *community-name* [**udpport** *value*]	(Optional) Configure Trap target host over SNMP v1, SNMP v2c and SNMP v3.
6	Raisecom(config-ip)#**snmp-server enable traps**	Enable OLT sending Trap function. The command of no snmp-server enable traps can be used to disable this function.

16.1.6 Checking configuration

Check the result by the commands below after configuration:

No.	Item	Description
1	Raisecom#**show snmp access**	Show the attributions of all access group names and groups.
2	Raisecom#**show snmp community**	Show configuration information of SNMP community.
3	Raisecom#**show snmp config**	Show basic configuration information of SNMP.
4	Raisecom#**show snmp group**	Show mapping relationship between SNMP user and access group.
5	Raisecom#**show snmp host**	Show SNMP target host information.
6	Raisecom#**show snmp statistics**	Show SNMP statistics.
7	Raisecom#**show snmp user**	Show SNMP user information.
8	Raisecom#**show snmp view**	Show SNMP view information.

16.2 RMON

16.2.1 Default configuration of RMON

The default configuration of RMON is as below:

Function	Default value
Statistics group	Enable all interfaces statistics function (including layer-3 interface and physical port)
History statistics group	Disable
Alarm group	N/A
Event group	N/A

16.2.2 Configuring RMON statistics

RMON statistics function can set the interface statistics, including interface sending and receiving packet, too small or too large packets, conflict, cyclic redundancy check and error count, packet loss, length of received packet, fragment, broadcast, multicast, and unicast news, etc.

Please configure RMON statistics function on the device as below.

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#rmon statistics { ip` *`if-number`* `| port-list` *`port-list`* `} [ owner` *`owner-name`* `]`	Enable interface RMON statistics function and configure related parameters.

16.2.3 Configuring RMON history statistics

Please configure RMON history statistics function on the device as below.

Step	Configuration	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#rmon history { ip` *`if-number`* `| port-list` *`port-list`* `} [ shortinterval` *`period`* `] [ longinterval` *`period`* `] [ buckets` *`number`* `] [ owner` *`owner-name`* `]`	Enable interface RMON history statistics function and configure related parameters. Short interval of history sampling is 1-600s; long interval is 600-3600s; save the cycle queue size of port history data with the range of 10-1000. The command of **no rmon history** {**ip** *if-number* | **port-list** *port-list*} can be used to disable history statistics group. When closing port history group function, the port will not take data collection statistics, and will clear all the history data collected previously.

16.2.4 Configuring RMON alarm group

Set one RMON alarm group instance (alarm-id) to monitor one MIB variable (mibvar). When the value of monitoring data exceeds the defined threshold, alarm event will generate. Record the log to send Trap to network management station according to the definition of alarm event.

- The monitored MIB variable must be real, and the data value type is correct. If the setting variable does not exist or value type variable is incorrect, return error. In the successfully setting alarm, if the variable cannot be collected later, close the alarm; reset if you want to monitor the variable again.
- When closing a port statistics functions, it doesn't mean no data statistics, but user cannot continue to have access to the port statistics data.

By default, the triggered event number is 0, refers to no triggered event. If the number is not zero, and there is no corresponding configuration in event group, when the control variable is abnormal, it cannot trigger the event successfully until the event is established.

Alarm will be triggered as long as matching the condition when configuring the upper or lower limits for one of the events in the event table. If there is no configuration for the upper and lower limits related alarm event (rising-event-id, falling-event-id) in the event table, alarm will not generate even meeting the alarm conditions.

Please configure RMON alarm group on the device as below.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**rmon alarm** *alarm-id mibvar* [**interval** *period*] { **delta** | **absolute** } **rising-threshold** *value* [*event*] **falling-threshold** *value* [*event*] [**owner** *owner-name*]	Add alarm instance to RMON alarm group and configure related parameters. The command of **no rmon alarm** *alarm-id* can be used to delete alarm group.

16.2.5 Configuring RMON event group

Please configure RMON event group on the device as below.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**rmon event** *event-id* [**log**] [**trap**] [**description** *string*] [**owner** *owner-name*]	Add event to RMON event group and configure related event processing mode. The command of **no rmon event** *event-id* can be used to delete alarm group.

16.2.6 Checking configuration

Check the result by the commands below after configuration:

No.	Item	Description
1	Raisecom#**show rmon**	Show RMON configuration information.
2	Raisecom#**show rmon alarms**	Show RMON alarm group information.
3	Raisecom#**show rmon events**	Show RMON event group information.
4	Raisecom#**show rmon statisttics**	Show RMON statistics group information.
5	Raisecom#**show rmon history** { **ip** *if-number* | **port** *port-id* }	Show RMON history statistics group information.

16.3 Optical module digital diagnostics

16.3.1 Default configuration of optical module digital diagnostics

The default configuration of optical module digital diagnostics is as below:

Function	Default value
Global monitoring to optical module digital diagnostics	Enable (cannot be configured)
Global Trap to optical module abnormal operation alarm	Enable (cannot be configured)
Port monitoring to optical module digital diagnostics	Disable
Port Trap to optical module abnormal operation alarm	Enable

16.3.2 Configuring port monitoring to optical module digital diagnostics

Please configure port monitoring to optical module digital diagnostics on the device as below.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter EPON system global configuration mode.
2	Raisecom(fttx)#**interface** [**range**] **transceiver** *slot-id/olt-id*	Enable transceiver configuration mode.
3	Raisecom(fttx-transceiver*:*)#**transceiver ddm** { **enable** | **disable** }	Enable/Disable port optical module digital diagnostics.

16.3.3 Configuring port Trap to optical module abnormal operation alarm

Please configure port Trap to optical module abnormal operation alarm on the device as below.

Step	Configuration	Description
1	Raisecom#**fttx**	Enter EPON system global configuration mode.
2	Raisecom(fttx)#**interface** [**range**] **transceiver** *slot-id/olt-id*	Enable transceiver configuration mode.
3	Raisecom(fttx-transceiver)#**transceiver trap** { **enable** | **disable** }	Enable/Disable optical module parameters abnormal alarm.

16.3.4 Checking configuration

Check the result on the device as below after configuration.

No.	Item	Description
1	Raisecom#**show transceiver**	Show global switch status and interface switch status of optical module measurement and diagnostics functions.
2	Raisecom#**show interface transceiver** *slot-id/port-id* **ddm** [**detail** | **information** | **threshold-violation**]	Show optical module digital diagnostics information.
3	Raisecom#**show interface transceiver** *slot-id/port-id* **ddm history** [**15m** | **24h**]	Show history information of optical module performance parameter.

16.4 System log

16.4.1 Default configuration of system log

The default configuration of system log is as below:

Function	Default value
Enable/disable system log	Enable
Output log information to console	Enable, the output level is information.
Output log information to file	Enable, the output module is config.
Set log host	N/A

Function	Default value
Output log to monitor	Disable
Configure log speed	N/A
Set log information timestamp	Standard time

16.4.2 Configuring basic information for system log

Please configure basic information for the system log as below:

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**logging on**	Enable system log function.
3	Raisecom(config)#**logging time-stamp** { **date-time** | **relative-start** | **null** }	Configure timestamp.
4	Raisecom(config)#**logging rate** *rate*	Configure transmitting rate for system log.

16.4.3 Configuring system log output direction

Please configure system log output on the device as below.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**logging console** { *severity-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** }	(Optional) Configure system log output direction as Console interface.
3	Raisecom(config)# **logging host** *ip-address* { **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** } { *severity-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** }	(Optional) Configure system log output direction as log host.
4	Raisecom(config)#**logging monitor** { *severity-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** }	(Optional) Configure system log output direction as monitor console.

16.4.4 Checking configuration

Check the result by the commands below after configuration:

No.	Item	Description
1	`Raisecom#show logging`	Show related system log configuration information.

16.5 Alarm management

Logical link alarm statistics function is used to monitor the logical link between OLT and ONU. The main logical link monitoring alarm event supported by ISCOM5508 is as follows:

Alarm event	Description
ONU register event	The event generates after registering some ONU successfully.
ONU deregister event	The event generates after deregistering some ONU. Common reasons: • ONU reset. • Severe failure between main fiber and branch fiber connected with ONU. • Severe error code.
ONU illegal register event	The event generates when the unauthorized ONU tries to apply for registration. Common reason: OLT port is non-auto authentication mode and the ONU device hasn't been installed.
Uplink/downlink BER threshold crossing alarm	The alarm generates when uplink/downlink BER of logical link exceeds 10^{-9}, which often caused by the poor optical signal quality.
Uplink/downlink FER threshold crossing alarm	The alarm generates when uplink/downlink FER of logical link exceeds 10^{-9}, which often caused by the poor optical signal quality.

16.5.1 Default configuration of alarm management

Please configure alarm management on the device as below:

Function	Default value
Illegal ONU register alarm switch	Enable
ONU register failure alarm switch	Enable
Uplink/downlink FER threshold crossing alarm switch	Disable
LLID mismatch threshold crossing alarm switch	Disable
LLID mismatch threshold crossing alarm threshold	5000 frames/s
Key update failure alarm switch	Disable

Function	Default value
Uplink/downlink BER threshold crossing alarm switch	Disable

16.5.2 Configuring OLT alarm management

OLT alarm configuration mainly refers to alarm switch control; alarm switch can be controlled separately on each OLT port. Each alarm switch consists of a master switch and a group of specific type alarm switches. Some serious alarms will be reported fixedly and cannot be configured to disable.

Please configure OLT alarm management:

Step	Configuration	Description
1	Raisecom#**fttx**	Enter EPON system global configuration mode.
2	Raisecom(fttx)#**interface olt** *slot-id/olt-id*	Enter OLT configuration mode.
3	Raisecom(fttx-olt*:*)#**snmp trap** { **enable** | **disable** }	(Optional) Enable/disable alarm reporting switch
4	Raisecom(fttx-olt*:*)#**snmp trap encryption-key-update-failure** { **enable** | **disable** }	(Optional) Enable/disable key update failure alarm switch.
5	Raisecom(fttx-olt*:*)#**snmp trap ber-threshold-crossing downstream** { **enable** | **disable** }	(Optional) Enable/disable downlink BER threshold crossing alarm switch.
6	Raisecom(fttx-olt*:*)#**snmp trap ber-threshold-crossing upstream** { **enable** | **disable** }	(Optional) Enable/disable uplink BER threshold crossing alarm switch.
7	Raisecom(fttx-olt*:*)#**snmp trap fer-threshold-crossing downstream** { **enable** | **disable** }	(Optional) Enable/disable downlink FER alarm switch.
8	Raisecom(fttx-olt*:*)#**snmp trap fer-threshold-crossing upstream** {**enable** | **disable** }	(Optional) Enable/disable uplink FER alarm switch.
9	Raisecom(fttx-olt*:*)#**snmp trap llid-mismatch-threshold-crossing** {**enable** | **disable** }	(Optional) Enable/disable LLID mismatch threshold crossing alarm switch.
10	Raisecom(fttx-olt*:*)#**snmp trap llid-mismatch-threshold-crossing threshold** *rate*	(Optional) Configure LLID mismatch threshold crossing alarm threshold.
11	Raisecom(fttx-olt*:*)#**snmp trap onu-registration-unauthorized** { **enable** | **disable** }	(Optional) Enable/disable illegal ONU register alarm switch.
12	Raisecom(fttx-olt*:*)#**snmp trap onu-registration-failure** {**enable** | **disable** }	(Optional) Enable/disable ONU register failure alarm switch.
13	Raisecom(fttx-olt*:*)#**snmp trap onu-laser-always-on** {**enable** | **disable** }	(Optional) Enable/disable ONU laser-always-on alarm detection.

Step	Configuration	Description
14	Raisecom(fttx-olt*:*)#**snmp trap onu-laser-always-on threshold** *power*	(Optional) Configure ONU laser-always-on alarm detection threshold.
15	Raisecom(fttx-olt*:*)#**snmp trap errored-frame** {**enable** | **disable** }	(Optional) Enable/disable DOT3OAM errored-frame alarm.
16	Raisecom(fttx-olt*:*)#**snmp trap errored-frame threshold** *value*	(Optional) Configure DOT3OAM errored-frame alarm detection threshold.
17	Raisecom(fttx-olt*:*)#**snmp trap errored-frame-period** {**enable** | **disable** }	(Optional) Enable/disable DOT3OAM errored-frame-period alarm.
18	Raisecom(fttx-olt*:*)#**snmp trap errored-frame-period threshold** *value*	(Optional) Configure DOT3OAM errored-frame-period alarm detection threshold.
19	Raisecom(fttx-olt*:*)#**snmp trap errored-frame-seconds-summary** {**enable** | **disable** }	(Optional) Enable/disable DOT3OAM errored-frame-seconds-summary alarm.
20	Raisecom(fttx-olt*:*)#**snmp trap errored-symbol-period** { **enable** | **disable** }	(Optional) Enable/disable DOT3OAM errored-symbol-period alarm.
21	Raisecom(fttx-olt*:*)#**snmp trap port-ber** { **enable** | **disable** }	(Optional) Enable/disable OLT port BER alarm.

16.5.3 Configuring ONU alarm management

ONU alarm management has a global enable switch; when the switch is disabled, any alarms from ONU cannot be reported to the NMS; and when this switch is enabled, the various types of alarms control switches will determine whether the related alarms can be reported to NMS.

Please configure ONU alarm management:

Step	Configuration	Description
1	Raisecom#**fttx**	Enter EPON system global configuration mode.
2	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode.
3	Raisecom(fttx-onu*/*:*)#**alarm** { **temperature-high** | **power** }	Enable ONU alarm switch.

Note

"Power-down alarm" is non-maskable serious alarm.

16.5.4 Checking configuration

Checking OLT alarm management configuration information

Check the configuration result by the commands below:

Step	Item	Description
1	Raisecom#**show interface olt** *slot-id/olt-id* **snmp trap**	Show OLT alarm management configuration information.

Checking ONU alarm management configuration information

Check the configuration result by the commands below:

Step	Item	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **alarm**	Show ONU alarm management configuration information.

16.6 Performance management

Performance management can be divided into PON performance management, ONU UNI port performance management and PON port performance management.

- PON performance management: contains PON statistics information query and clear function; statistics point includes ONU logical link (unicast/broadcast link) and ONU PON chip UNI port.
- UNI port performance management: contains Ethernet port performance data query and clear function.
- PON port performance management: contains PON port performance data query and clear function.

16.6.1 OLT performance management

OLT performance management contains PON statistics information query and clear function; statistics point includes OLT CNI port, OLT and ONU logical link, ONU UNI port.

Please configure OLT performance management:

No.	Item	Description
1	Raisecom#**fttx**	Enter EPON system global configuration mode.
2	Raisecom#**show interface olt** *slot-id/olt-id* { **upstream** | **downstream** | **all** } **statistics** [**pon** | **cni**]	Show OLT specified statistics point in the selected direction or PON statistics information on all statistics point.
3	Raisecom(fttx)#**clear interface olt-onu** *slot-id/olt-id* **statistics**	Clear all PON statistics information, including OLT/ONU PON MAC chip CNI/UNI port statistics information.
4	Raisecom(fttx)#**clear interface onu** *slot-id/olt-id/onu-id* **statistics** { **fec** | **mpcp** | **omp-emulation** | **basic** | **link-quality** }	Clear the selected ONU PON statistics information.

16.6.2 ONU performance management

Please configure OLT performance management:

No.	Item	Description
1	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* { **upstream** | **downstream** | **all** } **statistics** [**olt-onu** | **pon** | **uni**]	Show ONU specified statistics points in selected direction or PON statistics information on all statistics points.
2	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **statistics** { **basic** | **link-quality** | **fec** | **mpcp** | **omp-emulation** }	Show the selected ONU PON statistics information.
3	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **voice statistics sip**	Show ONU SIP message statistics information. SIP message is aimed at the overall ONU device statistics.
4	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **voice statistics rtp**	Show ONU RTP media package statistics information. RTP media package is aimed at the overall ONU device statistics.
5	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **voice statistics call pots** [*pots-id*]	Show ONU POTS port calling statistics information. Call statistics are aimed at the single POTS port statistics.
6	Raisecom#**show interface onu** *slot-id/olt-id/onu-id* **voice statistics error-code**	Show ONU error code statistics information.
7	Raisecom#**fttx**	Enter EPON system global configuration mode.
8	Raisecom(fttx)#**interface onu** *slot-id/olt-id/onu-id*	Enter ONU configuration mode.
9	Raisecom(fttx-onu*/*:*)#**clear interface onu** *slot-id/olt-id/onu-id* **voice statistics sip**	Clear ONU SIP message statistics information.
10	Raisecom(fttx-onu*/*:*)#**clear interface onu** *slot-id/olt-id/onu-id* **voice statistics rtp**	Clear ONU RTP media package statistics information.
11	Raisecom(fttx-onu*/*:*)#**clear interface onu** *slot-id/olt-id/ onu-id* **voice statistics call pots** { **all** | pots-id }	Clear ONU POTS port calling statistics information.
12	Raisecom(fttx-onu*/*:*)#**clear interface onu** *slot-id/olt-id/onu-id* **voice statistics error-code**	Clear ONU error code statistics information.
13	Raisecom(fttx-onu*/*:*)#**clear interface onu** *slot-id/olt-id/onu-id* **voice statistics sdp**	Clear ONU SDP performance statistics information.

16.7 System monitoring

ISCOM5508 is in support of ONU system monitoring functions, including:

- Temperature monitoring

- Power monitoring
- Fan monitoring

16.7.1 Default configuration of system monitoring

The Raisecom ONU device system monitoring default configuration is as follows:

Function	Default value
Temperature monitoring	Enable
Power monitoring	Enable
Fan monitoring	Enable

16.7.2 Configuring temperature monitoring

Please configure temperature monitoring function:

Step	Configuration	Description
1	`Raisecom#fttx`	Enter EPON system global configuration mode.
2	`Raisecom(fttx)#interface onu` *`slot-id/olt-id/onu-id`*	Enter ONU configuration mode.
3	`Raisecom(fttx-onu*/*:*)#alarm temperature-high`	Configure to enable ONU temperature monitoring.

16.7.3 Configuring power monitoring

Please configure power monitoring function:

Step	Configuration	Description
1	`Raisecom#fttx`	Enter EPON system global configuration mode.
2	`Raisecom(fttx)#interface onu` *`slot-id/olt-id/onu-id`*	Enter ONU configuration mode.
3	`Raisecom(fttx-onu*/*:*)#alarm power`	Configure to enable ONU power monitoring.

16.7.4 Configuring fan monitoring

Please configure fan monitoring function:

Step	Configuration	Description
1	Raisecom#**fttx**	Enter EPON system global configuration mode.
2	Raisecom(fttx)#**fan speed mode** {**auto** | **manual** }	Configure fan control mode.
3	Raisecom(fttx)#**fan speed manual** *grade*	(Optional) Configure fan speed grade.
4	Raisecom(fttx)#**fan speed min** *min-speed* **max** *max-speed*	(Optional) Configure fan speed. The configured minimum speed is less than the maximum speed.

Note

User needs to specify the fan control mode as manual mode before configuring fan speed grade manually.

16.7.5 Checking configuration

Check the configuration result by the commands below:

No.	Item	Description
1	Raisecom#**show fan**	Show fan status and configuration information.

16.8 Ping

Please take the following configuration to test remote host through PING function:

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface ip** *if-number*	Enter layer-3 interface configuration mode.
3	Raisecom(config-ip)#**ip address** *ip-address* [*ip-mask*] *vlan-id*	Configure device IP address
4	Raisecom(config-ip)#**end**	Return to privileged EXEC mode.
5	Raisecom#**ping** *ip-address* [**count** *NumPktsRe*] [**size** *SizeofIcmpEchPkt*][**waittime** *PktTimOut*]	Test whether the remote host is reachable.

Note

Users cannot execute other operations to the device in the process of **Ping**. They can execute other operations after **Ping** or interrupt **Ping** by **Ctrl**+**C**.

16.9 Traceroute

Configure IP address and default gateway for ISCOM5508 device before using Traceroute function.

Please configure Traceroute function on the device as below:

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface ip** *if-number*	Enter layer-3 interface configuration mode.
3	Raisecom(config-ip)#**ip address** *ip-address* [*ip-mask*] *vlan-id*	Configure port IP address.
4	Raisecom(config-ip)#**exit**	Exit from port configuration mode and enter global configuration mode.
5	Raisecom(config)#**ip default-gateway** *ip-address*	Configure default gateway.
6	Raisecom(config)#**exit**	Exit from global configuration mode and enter privileged EXEC mode.
7	Raisecom#**traceroute** *ip-address* [**firstttl** *fitst-ttl*] [**maxttl** *max-ttl*] [**port** *port-id*] [**waittime** *period*] [**count** *count*]	Test network connection by traceroute command and check packet passed network nodes.

16.10 LLDP

16.10.1 LLDP default configuration

LLDP default configuration on ISCOM5508 device:

Function	Default value
LLDP global function	Disable
LLDP port function	Enable
Delay sending timer	2s
Period sending timer	30s
Aging coefficient	4

Function	Default value
Restart timer	2s
LLDP alarm function	Enable
Alarm notification timer	5s

16.10.2 Configuring global LLDP

Caution

The global LLDP function cannot be enabled instantly after disabling; it can enable again after restarting timer timeout. Because disable or enable operations are equal to the receiving and transmitting packets logout and login; when disabling LLDP function, the device will send protocol ShutDown message; LLDP can be logged out after finishing messages transmission of each ports, that is to say, the LLDP logout needs a delay. If enabling LLDP again before delayed logout, LLDP will be logged out in delayed logout, which will make the configuration different from actual situation.

Please configure to enable global LLDP function on the device as below:

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**lldp** { **enable** | **disable** }	Configure to enable/disable global LLDP function.

16.10.3 Enabling port LLDP

Please configure to enable port LLDP function on the device as below:

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port-list** *port-list*	Enter physical layer port configuration mode.
3	Raisecom(config-port)#**lldp** { **enable** | **disable** }	Configure to enable/disable port LLDP function.

16.10.4 Configuring basic LLDP

Caution

When configuring delay sending timer and period sending timer, the value of delay sending timer must be less than or equal to one quarter of period sending timer value.

Please configure to basic LLDP function on the device as below:

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**lldp message-transmission interval** *period*	(Optional) Configure period sending timer for LLDP packet.
3	Raisecom(config)#**lldp message-transmission delay** *period*	(Optional) Configure delay sending timer for LLDP packet.
4	Raisecom(config)#**lldp message-transmission hold-multiplier** *hold-multiplier*	(Optional) Configure LLDP packets aging coefficient.
5	Raisecom(config)#**lldp restart-delay** *period*	(Optional) Configure restart timer. The device can enable global LLDP function again after restart time when disabling global LLDP function.

16.10.5 Configuring LLDP alarm

Enable LLDP alarm notification function to send topology information update alarm to Nview NNM system when the network changes.

Please configure LLDP alarm function on the device as below:

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server lldp-trap** { **enable** | **disable** }	Enable/disable LLDP alarm function.
3	Raisecom(config)#**lldp trap-interval** *period*	(Optional) Configure LLDP alarm Trap period sending timer.

Note

After enabling LLDP alarm function, the device will send alarm Trap when it detects neighbor aging, new neighbor, and neighbor information changes.

16.10.6 Checking configuration

Check the configuration result by the commands below:

No.	Item	Description
1	Raisecom#**show lldp local config**	Show LLDP local configuration.
2	Raisecom#**show lldp local system-data** [**port-list** *port-list*]	Show LLDP local system information.
3	Raisecom#**show lldp remote** [**port-list** *port-list*][**detail**]	Show LLDP neighbor information.
4	Raisecom#**show ldp statistic** [**port-list** *port-list*]	Show LLDP message statistics information.

16.11 Watchdog

The watchdog function can prevent the system program from dead circulation caused by uncertain fault so as to improve the stability of system.

Please configure watchdog for the device as below:

Step	Configuration	Description
1	Raisecom#**watchdog** { **enable** | **disable** }	Enable/disable watchdog function.
2	Raisecom#**show watchdog**	(Optional) Check watchdog function status. By default, enable watchdog function.

16.12 Keepalive

16.12.1 Preparing for configuration

Networking situation

ISCOM5508 sends KeepAlive Trap packet to make NMS discover NE in a short time, improve NMS working efficiency and reduce the working load of administrators. User can configure to enable or disable the KeepAlive Trap transmission and its period. When enabling KeepAlive Trap switch, if setting snmp enable traps and layer-3 IP address, ISCOM5508 will send a KeepAlive Trap to all target hosts with Bridge Trap every KeepAlive Trap Interval.

Preconditions

- Configure SNMP port IP address.
- Configure basic function of SNMP: SNMP v1 and v2c versions need to configure community name; SNMP v3 needs to configure username and SNMP view.
- Configure routing protocol: make sure routing between ISCOM5508 and NMS is reachable.

16.12.2 Default configuration of KeepAlive Trap

The default configuration of KeepAlive Trap:

Function	Default value
KeepAlive Trap function	Disable
KeepAlive Trap period	300s

16.12.3 Configuring to send KeepAlive Trap

Please configure KeepAlive Trap function as below:

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server keepalive-trap** { **enable** | **disable** | **pause** }	Enable/disable/pause to send KeepAlive Trap.
3	Raisecom(config)#**snmp-server keepalive-trap interval** *period*	(Optional) Configure KeepAlive Trap transmission period.

Caution

To avoid multiple devices sending KeepAlive Trap in the same time according to the same period and causing heavy network management load, the actual transmission period of KeepAlive Trap is timed as period+5s random transmission.

16.12.4 Checking configuration

Check the configuration result by the commands below:

No.	Item	Description
1	Raisecom#**show keepalive**	Show KeepAlive configuration.

16.13 Tx and Rx packets statistics

16.13.1 Enabling/Disabling Tx and Rx packets statistics of specified type messages

Please configure to enable/disable Tx and Rx packets statistics of specified type messages:

Step	Configuration	Description
1	Raisecom#**debug driver**	Enable Tx and Rx packets statistics function.
2	Raisecom#**config**	Enter global configuration mode.
3	Raisecom(config)#**logging console debugging**	Configure Console Logging level as Debugging.
4	Raisecom(config)#**driver** { **receive-packet** | **send-packet** } **ethertype-classify** { **arp** | **dhcpsnooping** | **Ethernet-ring** | **igmpsnooping**| **ip** | **lacp** | **mstp** | **other** | **relay-dot1x** | **relay-gmrp** | **relay-gvrp** | **relay-lacp** | **relay-stp** } **syslog** { **enable** | **disable** } [**port** *port-id*]	Configure to enable/disable Tx and Rx packets statistics function.

16.13.2 Discarding/Recovering specified types of messages

Please configure to discard/recover specified types of messages:

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**driver** { **receive-packet** | **send-packet** } [**ethertype-classify** { **arp** | **dhcpsnooping** | **ethernet-ring** | **igmpsnooping**| **ip** | **lacp** | **mstp** | **other** | **relay-dot1x** | **relay-gmrp** | **relay-gvrp** | **relay-lacp** | **relay-stp** }] **discard** { **enable** | **disable** } [**port** *port-id*]	Configure to discard/recover specified types of messages.

16.13.3 Checking configuration

Check the configuration result by the commands below:

No.	Item	Description
1	Raisecom#**show device statistics**	Show Tx and Rx packets statistics configurations.

16.14 Maintenance

User can maintain system features by the following commands.

Command	Description
Raisecom(config)#**clear lldp statistic** [**port-list** *port-list*]	Clear LLDP statistics information.
Raisecom(config)#**clear lldp remote-table** [**port-list** *port-list*]	Clear LLDP neighbor information.
Raisecom(config)#**clear device statistics** [**arp** | **dhcpsnooping** | **ethernet-ring** | **igmpsnooping** | **ip** | **lacp** | **mstp** | **other** | **relay-dot1x** | **relay-gmrp** | **relay-gvrp** | **relay-lacp** | **relay-stp**] { **receive** | **send** }	Clear Tx and Rx packets statistics information.

16.15 Configuring examples

16.15.1 Examples for configuring SNMP

Networking requirements

As shown in the Figure below, ISCOM5508 IP address is 192.168.0.10, User 1, md5 authentication algorithm; authentication password is raisecom, access mib2 view with all MIB variables under 1.3.6.1.2.1, create guestgroup access group; security mode is usm, security level is authentication without encryption; readable view name is mib2, complete security level is usm user 1 mapped to guestgroup access group, and show the results.

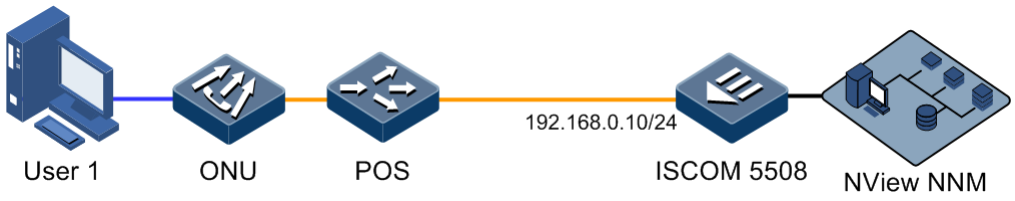

Figure 16-2 SNMP v3 configuration application networking

Configuration steps

Step 1 Configure IP address.

```
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address 192.168.0.10 10
Raisecom(config-ip)#exit
```

Step 2 Configure view and its OID tree range.

```
Raisecom(config)#snmp-server view mib2 1.3.6.1.2.1 1.1.1.1.0.1 included
```

Step 3 Configure SNMP user.

```
Raisecom(config)#snmp-server user guestuser1 authentication md5 raisecom
```

Step 4 Configure SNMP access group.

```
Raisecom(config)#snmp-server access guestgroup read mib2 usm authnopriv
```

Step 5 Configure user belonging to specified access group.

```
Raisecom(config)#snmp-server group guestgroup user user1 usm
```

Checking results

Show all access group names and attributes.

```
Raisecom#show snmp access
Index:  0
Group:  initial
Security Model: usm
Security Level: authnopriv
Context Prefix: --
Context Match: exact
Read View: internet
Write View: internet
Notify View:  internet

Index:  1
Group:  guestgroup
Security Model: usm
Security Level: authnopriv
Context Prefix: --
Context Match: exact
Read View: mib2
Write View: --
Notify View:  internet

Index:  2
Group:  initialnone
Security Model: usm
Security Level: noauthnopriv
Context Prefix: --
Context Match: exact
Read View: system
Write View: --
Notify View:  internet
```

Show all access group names and mapping information.

```
Raisecom#show snmp group
Index   GroupName         UserName          SecModel
-----------------------------------------------------------
  0     initialnone        none               usm
  1     initial            md5nopriv          usm
  2     initial            shanopriv          usm
  3     guestgroup         guestuser1         usm
```

16.15.2 Examples for configuring system log output to log host

Networking requirements

As the Figure shows below, configure system log function, output device log information to log host for user to check.

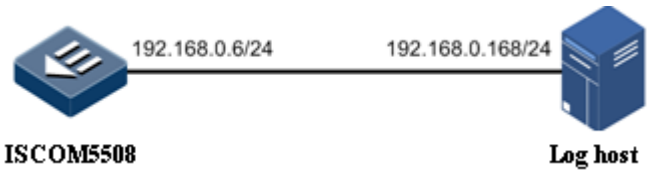

Figure 16-3 System log output to log host networking

Configuration steps

Step 1 Configure ISCOM5508 device IP address.

```
Raisecom#config
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address 192.168.0.6 255.255.255.0 1
Raisecom(config-ip)#exit
```

Step 2 Configure system log output to log host PC.

```
Raisecom(config)#logging on
Raisecom(config)#logging time-stamp datetime
Raisecom(config)#logging rate 10
Raisecom(config)#logging host 192.168.0.168 local0 warnings
```

Checking results

Show system log configuration by the command of **show logging**.

```
Raisecom#show logging
Syslog logging:Enable, 0 messages dropped, messages rate-limited 10 per
second
Console logging:Enable, level=informational, 30 Messages logged
Monitor logging:Disable, level=informational, 0 Messages logged
Time-stamp logging messages: date-time

Log host information:
Target Address    Level      Facility   Sent     Drop
------------------------------------------------------------
192.168.0.168     warnings   local0       0        0
```

16.15.3 Examples for configuring KeepAlive Trap

Networking requirements

As the Figure shows below, the IP address of ISCOM5508 is 192.168.1.2, SNMP v2c Trap target host address is 192.168.1.1, read and write community name is public, SNMP version is v2c. Configure time interval sending KeepAlive Trap from ISCOM5508 to SNMP network management station as 120s and enable KeepAlive Trap function.

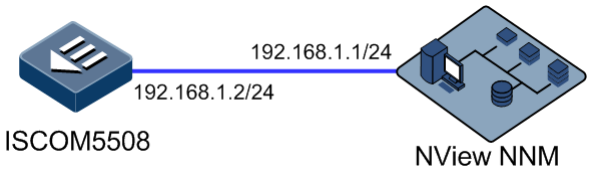

Figure 16-4 KeepAlive application networking

Configuration steps

Step 1 Configure ISCOM5508 management IP address.

```
Raisecom#config
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address 192.168.1.2 255.255.255.0 1
Raisecom(config-ip)#exit
```

Step 2 Configure Trap target host IP address for SNMP.

```
Raisecom(config)#snmp-server host 192.168.1.1 version 2c public
```

Step 3 Configure KeepAlive Trap function.

```
Raisecom(config)#snmp-server keepalive-trap enable
Raisecom(config)#snmp-server keepalive-trap interval 120
```

Checking results

Check KeepAlive configuration information by the command of **show keepalive**.

```
Raisecom#show keepalive
Keepalive Admin State:Enable
Keepalive trap interval:120s
Keepalive trap count:1
```

17 Appendix

17.1 Port Table of Comparisons

The corresponding relationship of ISCOM5508 device physical port and switch port is as below:

Physical port	Switch port
GE1	Port 1
GE2	Port 2
GE3	Port 3
GE4	Port 4
GE5	Port 5
GE6	Port 6
OLT 1/1	Port 7
OLT 1/2	Port 8
OLT 1/3	Port 9
OLT 1/4	Port 10
OLT 2/1	Port 11
OLT 2/2	Port 12
OLT 2/3	Port 13
OLT 2/4	Port 14
OLT 3/1	Port 15
OLT 3/2	Port 16
OLT 3/3	Port 17
OLT 3/4	Port 18

17.2 Terms

Connectivity Fault Management (CFM)	A standard defined by IEEE. It defines protocols and practices for OAM (Operations, Administration, and Maintenance) for paths through 802.1 bridges and local area networks (LANs). Used to diagnose fault for EVC (Ethernet Virtual Connection). Cost-effective by fault management function and improve Ethernet maintenance.
Ethernet Linear Protection Switching (ELPS)	A protocol based on ITU-T G.8031 APS (Automatic Protection Switching) to protect an Ethernet connection. It is a kind of end-to-end protection technology. Including two linear protection modes: linear 1:1 protection switching and linear 1+1 protection switching.
Ethernet Ring Protection Switching (ERPS)	An APS (Automatic Protection Switching) protocol based on ITU-T G.8032 Recommendation to provide backup link protection and recovery switching for Ethernet traffic in a ring topology and at the same time ensuring that there are no loops formed at the Ethernet layer.
Failover	Provide a port association solution, extending link backup range. Transport fault of upper layer device quickly to downstream device by monitoring upstream link and synchronize downstream link, then trigger switching between master and standby device and avoid traffic loss.
Link Aggregation	A computer networking term which describes using multiple network cables/ports in parallel to increase the link speed beyond the limits of any one single cable or port, and to increase the redundancy for higher availability.
Mobile Backhaul	Solve communication problem from BTS to BSC for 2G, NodeB to RNC for 3G. Mobile backhaul for 2G focuses on voice service, not request high bandwidth, implemented by TDM microwave or SDH/PDH device. In 3G times, lots of data service as HSPA, HSPA+, etc concerning to IP service, voice is changing to IP as well, namely IP RAN, to solve problem of IP RAN mobile backhaul is solving whole network backhaul, satisfying both data backhaul and voice transportation over IP (clock synchronization).
Precision Time Protocol(PTP)	IEEE 1588 v2 protocol is also called PTP (Precision Time Protocol), a high-precision time protocol for synchronization used in measurement and control systems residing on a local area network. Accuracy in the sub-microsecond range may be achieved with low-cost implementations.
QinQ	QinQ is (also called Stacked VLAN or Double VLAN) extended from 802.1Q, defined by IEEE 802.1ad recommendation. Basic QinQ is a simple layer-2 VPN tunnel technology, encapsulating outer VLAN Tag for client private packets at carrier access end, the packets take double VLAN Tag passing through trunk network (public network). In public network, packets only transmit according to outer VLAN Tag, the private VLAN Tag are transmitted as data in packets.

SyncE	A technology adopts Ethernet link codes recover clock, similar to SDH clock synchronization quality, SyncE provides frequency synchronization of high precision. Unlike traditional Ethernet just synchronize data packets at receiving node, SyncE implements real-time synchronization system for inner clock.

17.3 Abbreviations

Numerics

A

ACL	Access Control List
APS	Automatic Protection Switching

B

BC	Boundary Clock

C

CCM	Continuity Check Message
CDMA2000	Code Division Multiple Access 2000
CFM	Connectivity Fault Management
CoS	Class of Service
CDR	Calling Detail Records

D

DoS	Deny of Service
DRR	Deficit Round Robin
DSCP	Differentiated Services Code Point

E

EFM	Ethernet in the First Mile
ELPS	Ethernet Linear Protection Switching
ERPS	Ethernet Ring Protection Switching
EVC	Ethernet Virtual Connection

F

FIB	Forwarding Information Base
FTP	File Transfer Protocol

G

GARP	Generic Attribute Registration Protocol
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GVRP	GARP VLAN Registration Protocol

I

IANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGMP Snooping	Internet Group Management Protocol Snooping
IP	Internet Protocol
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector

L

LACP	Link Aggregation Control Protocol
LBM	LoopBack Message
LBR	LoopBack Reply
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
LTM	LinkTrace Message
LTR	LinkTrace Reply

M

MA	Maintenance Association
MAC	Medium Access Control
MD	Maintenance Domain

MEG	Maintenance Entity Group
MEP	Maintenance associations End Point
MIB	Management Information Base
MIP	Maintenance association Intermediate Point
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transfered Unit
MVR	Multicast VLAN Registration

N

NNM	Network Node Management

O

OAM	Operation, Administration and Management
OC	Ordinary Clock

P

PC	Personal Computer
PPP	Point to Point Protocol
PTP	Precision Time Protocol

Q

QoS	Quality of Service

R

RADIUS	Remote Authentication Dial In User Service
RMON	Remote Network Monitoring
RMEP	Remote Maintenance association End Point
RNC	Radio Network Controller
RSTP	Rapid Spanning Tree Protocol

S

SFP	Small Form-factor Pluggables

SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict-Priority
SSHv2	Secure Shell v2
STP	Spanning Tree Protocol

T

TACACS+	Terminal Access Controller Access Control System
TC	Transparent Clock
TCP	Transmission Control Protocol
TD-SCDMA	Time Division-Synchronous Code Division Multiple Access
TDM	Time Division Multiplex
TFTP	Trivial File Transfer Protocol
TLV	Type Length Value
ToS	Type of Service

V

VLAN	Virtual Local Area Network

W

WCDMA	Wideband Code Division Multiple Access
WRR	Weight Round Robin

瑞斯康达科技发展股份有限公司
RAISECOM TECHNOLOGY CO.,LTD.

Address: Building 2, No. 28, Shangdi 6th Street, Haidian District, Beijing, P.R.China.
Postal code: 100085 Tel: +86-10-82883305
Fax: 8610-82883056 http://www.raisecom.com Email: export@raisecom.com