RAISECOM

www.raisecom.com

ISCOM6820 (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: Raisecom Building, No. 11, East Area, No. 10 Block, East Xibeiwang Road, Haidian District, Beijing, P.R.China

Postal code: 100094

Notice

Preface

Objectives

This document describes how to configure features and services supported by the ISCOM6820-GP, such as basic configurations, configuring xPON services, configuring multicast services, configuring CATV services, configuring MAC address, configuring VLAN, configuring spanning tree, configuring routing, configuring DHCP, configuring QoS, configuring OAM, configuring system security, configuring link security, and configuring system management, and provides related configuration examples. The appendix lists terms, acronyms, and abbreviations involved in this document.

This document helps you master basic principles and configurations of the ISCOM6820-GP, and how to use the ISCOM6820-GP for networking.

Versions

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

Product name	Hardware version	Software version
ISCOM6820	A	V3.23

Related manuals

The following table lists manuals and their contents related to the ISCOM6820-GP.

Name	Description
ISCOM6820-GP (A) Hardware Description	This document describes the hardware structure and card of the ISCOM6820-GP, including product overview, chassis, fan, cards, cables, pluggable optical modules, lookup table of LEDs, and lookup table of weight and power consumption.

Name	Description
ISCOM6820-GP (A) Configuration Guide	This document mainly describes services supported by the ISCOM6820-GP, and introduce configuration methods and procedures of these services in terms of service overview, default configurations, configuration methods, and configuration examples, including basic configurations, EPON service configurations, xPON service configurations, multicast service configurations, VoIP service configurations, CATV service configurations, TDMoP service configurations, MAC address table configurations, VLAN configurations, Spanning Tree configurations, routing configurations, DHCP configurations, QoS configurations, system security configurations, link security configurations, and system management configurations.
ISCOM6820-GP (A) Quick Installation Guide	This document mainly describes the installation procedures after unpacking the device, including the installation tools, precautions, installation scenarios, installation conditions, and installation steps.
ISCOM6820 (A) Installation Guide	This document mainly describes precaution before installation, installation methods, and verification after installation, including safety information, installation description, installing the chassis, installing the fan, installing cards, wiring cables, hardware installation verification, power-on verification, device initialization, and installation reference.

Conventions

Symbol conventions

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

Symbol	Description
	Indicate a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.
	Indicate a potentially hazardous situation that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.
	Provide additional information to emphasize or supplement important points of the main text.
	Indicate 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	Buttons and navigation path are in **Boldface**.
Italic	Book titles are in *italics*.
Lucida Console	Terminal display is in `Lucida Console`.
Book Antiqua	Heading 1, Heading 2, Heading 3, and Block are in Book Antiqua.

Special conventions

Convention	Description
/:*	Indicate the serial number of the ONU interface. The value of * depends on the actual configurations.
:	Indicate the serial number of the PON interface. The value of * depends on the actual configurations.
//*:*	Indicate the serial number of the ONU UNI. The value of * depends on the actual configurations.

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. Only 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.

Convention	Description
[x | y | .] *	Optional alternative items are grouped in square brackets and separated by vertical bars. A minimum of none or a maximum of all can be selected.

Change history

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

Issue 03 (2024-04-03)

Third commercial release

- Added LLDP.
- Added the function of the unknown multicast traffic to use the broadcast channel.
- Added the ISCOM6800-XGHA.
- Added mOLT remote management.

Issue 02 (2023-08-03)

Second commercial release

- Added the ISCOM6800-GPHA and ISCOM6800-XCHA.
- Upgraded the system software to V3.21.

Issue 01 (2023-03-30)

Initial commercial release

Contents

Figures

Tables

1 Basic configurations

This chapter describes basic configurations and configuration process of the ISCOM6820, including the following sections:

- CLI
- Accessing device
- Managing users
- Managing cards
- Managing interfaces
- Managing time
- Upgrade and backup
- Configuration examples

1.1 CLI

1.1.1 Overview

Command Line Interface (CLI) is the path for communication between users and the device. You can configure, monitor, and manage the device by executing related commands.

You can log in to the Device through a PC that runs the terminal emulation program or the CPE device. You can enter CLI once the command prompt appears.

The features of CLI:

- Local configuration through the Console interface is available.
- Local or remote configuration through Telnet or Secure Shell v2 (SSHv2) is available.
- Provide protection for different command levels. Users in different levels can only execute commands in corresponding levels.
- Different command types belong to different command modes. You can only execute a type of configuration in its related command mode.
- Shortcut keys can be used to execute commands.
- Check a history command by checking command history. The last 5000 history commands can be saved on the device.
- Online help is available by typing "?" at any time.

- Support smart analysis methods, such as incomplete matching and context association, to facilitate user input.

1.1.2 Levels and privileges

CLI levels

The ISCOM6820 use hierarchical protection methods to divide command line into 4 levels from low to high:

- Visitor: you can execute the **ping**, **clear**, and **history** commands in this level.
- Monitor: you can execute the **show** command and so on.
- Operator: you can execute commands for different services like Virtual Local Area Network (VLAN), IP routing, and so on Most service configuration commands can be executed in this level.
- Administrator: you can execute file system commands (saving, deleting, uploading, and downloading files), user management commands (user authorization and management), FTP commands, and TFTP commands.

User levels

Corresponding to the CLI levels, users are divided into 16 levels from low to high. Users in different levels can execute commands in related CLI levels.

- 1–4: you can execute commands in visitor level.
- 5–9: you can execute commands in monitor level or lower.
- 10–14: you can execute commands in operator level or lower.
- 15: you can execute commands in administrator level or lower.

Privilege management

Table 1-1 lists the corresponding relationship between the CLI level and user level.

Table 1-1 Corresponding relationship between the CLI level and user level

Levels	Visitor	Monitor	Operator	Administrator
administrator	Permitted	Permitted	Permitted	Permitted
operator	Permitted	Permitted	Permitted	Forbidden
monitor	Permitted	Permitted	Forbidden	Forbidden
visitor	Permitted	Forbidden	Forbidden	Forbidden

1.1.3 Modes

Overview

Command mode is the CLI environment. All system commands are registered in one (or some) command line mode, and the command can only run in the corresponding mode.

Establish a connection with the device. If the device is in default configuration, it will enter user EXEC mode, and the screen will display:

```
Raisecom>
```

Input the **enable** command and correct password, and press **Enter** to enter privileged EXEC mode. The default password is raisecom.

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

In privileged EXEC mode, input the **config** command to enter global configuration mode.

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

Note

- Command line prompt "Raisecom" is the default host name. You can use the **hostname** *string* command to modify the host name in privileged EXEC mode.
- Some commands can be used both in global configuration mode and other modes, but the accomplished functions are closely related to command line modes.
- Generally, in a command line mode, you can return to the upper command line mode by using the **quit** or **exit** command, but in the privileged EXEC mode, you need to use the **quit**, **exit**, or **disable** command to return to user EXEC mode.
- You can use the **end** command to return to privileged EXEC mode from any command line mode except the user EXEC mode or privileged EXEC mode.

CLI modes

The ISCOM6820 supports the following CLI modes:

Mode	Enter method	Description
User EXEC	Log in to the ISCOM6820, input correct username and password	`Raisecom>`
Privileged EXEC	In user EXEC mode, enter the **enable** command and correct password. **Note** The user with the level 11 or higher can enter this mode.	`Raisecom#`

Mode	Enter method	Description
Global configuration	In privileged EXEC mode, enter the **config** command.	`Raisecom(config)#`
Aggregation group interface configuration	In global configuration mode, enter the **interface port-channel** *port-channel-id* command.	`Raisecom(config-port-channel-id)#`
VLAN interface configuration	In global configuration mode, enter the **interface vlanif** *vlan-id* command.	`Raisecom(config-vlanif-num)#`
VLAN configuration	In global configuration mode, enter the **vlan** *vlan-id* command.	`Raisecom(config-vlan-id)#`
GPON interface configuration	In global configuration mode, enter the **interface gpon-olt** *slot-id/port-id* command.	`Raisecom(config-if-gpon-olt-slot-id:port-id)#`
GPON interface batch configuration	In global configuration mode, enter the **interface range gpon-olt** *slot-id/port-list* command.	`Raisecom(config-if-gpon-olt-range)#`
GPON ONU remote management configuration	In global configuration mode, enter the **gpon-onu uni ethernet range** *slot-id/olt-id/onu-id* command.	`Raisecom(config-gpon-onu-slot-id/port-id:onu-id)#`
GPON ONU remote management batch configuration	In global configuration mode, enter the **gpon-onu range** *slot-id/olt-id/onu-list* command.	`Raisecom(config-gpon-onu-range)#`
GPON ONU UNI configuration	In global configuration mode, input the **gpon-onu uni ethernet** *slot-id/olt-id/onu-id/uni-id* command.	`Raisecom(config-gpon-onu-ethernet-slot-id/port-id/onu-id:uni-id)#`
GPON ONU UNI batch configuration	In global configuration mode, input the **gpon-onu uni ethernet range** *slot-id/olt-id/onu-id/uni-list* command.	`Raisecom(config-gpon-onu-ethernet-range)#`
GPON OLT alarm profile configuration	In global configuration mode, input the **snmp-trap-gpon-olt-profile** *profile-id* command.	`Raisecom(config-snmp-trap-gpon-olt-profile:profile-id)#`
GPON OLT line profile configuration	In global configuration mode, input the **gpon-onu-line-profile** *profile-id* command.	`Raisecom(config-gpon-onu-line-profile:profile-id)#`
EPON ONU service profile configuration	In global configuration mode, enter the **gpon-onu-service-profile** *profile-id* command.	`Raisecom(config-gpon-onu-service-profile:profile-id )#`

Mode	Enter method	Description
GPON automatic authentication rule configuration	In global configuration mode, enter the **gpon-auto-authentication-rule** *profile-id* command.	`Raisecom(config-gpon-auto-auth-rule:1)#`
L2 ACL configuration	In global configuration mode, enter the **l2-access-list** *acl-id* command.	`Raisecom(config-l2-acl-acl-id)#`
L2 ACL sub-rule configuration	In L2 ACL configuration mode, enter the **rule** *rule-id* command.	`Raisecom(config-l2-acl-acl-id-rule-rule-id)#`
IPv4 ACL configuration	In global configuration mode, enter the **ip-access-list** *acl-id* command.	`Raisecom(config-ip-acl-acl-id)#`
IPv4 ACL sub-rule configuration	In IPv4 ACL configuration mode, enter the **rule** *rule-id* command.	`Raisecom(config-ip-acl-acl-id-rule-rule-id)#`
Hybrid ACL configuration	In global configuration mode, enter the **hybrid-access-list** *acl-id* command.	`Raisecom(config-hybrid-acl-acl-id)#`
Hybrid ACL sub-rule configuration	In Hybrid ACL configuration mode, enter the **rule** *rule-id* command.	`Raisecom(config-hybrid-acl-acl-id-rule-rule-id)#`
VLAN ACL rule configuration	In global configuration mode, enter the **vlan-access-list** *acl-id* command.	`Raisecom(config-qinq-acl-1)#`

1.1.4 Shortcut keys

The ISCOM6820 supports following shortcut keys.

Shortcut key	Description
Up Arrow (↑)	Show the previous command if there is any command entered earlier; the displayed command does not change if the current command is the earliest one in history records.
Down Arrow (↓)	Show the next command if there is any newer command. The displayed command does not change if the current command is the newest one in history records.
Left Arrow (←)	Move the cursor leftward by one character. The displayed command does not change if the cursor is already at the beginning of the command.
Right Arrow (→)	Move the cursor rightward by one character. The displayed command does not change if the cursor is already at the end of the command.

Shortcut key	Description
Backspace	Delete the character before the cursor. The displayed command does not change if the cursor is already at the beginning of the command.
Tab	Press **Tab** after entering a complete keyword, and the cursor will automatically appear a space to the end. Press **Tab** again, and the system will show the follow-up available keywords. Press **Tab** after entering an incomplete keyword, and the system automatically executes partial helps: • When only one keyword matches the entered incomplete keyword, the system takes the complete keyword to replace the entered incomplete keyword and leaves one space between the cursor and end of the keyword. • When no keyword or multiple keywords match the entered incomplete keyword, the system displays the prefix, and you can press **Tab** to check words circularly. In this case, there is no space from the cursor to the end of the keyword. Press **Space bar** to enter the next word. • If you enter an incorrect keyword, pressing **Tab** will move the cursor to the next line and the system will prompt an error. In this case, the entered keyword does not change.
Ctrl+A	Move the cursor to the beginning of the command.
Ctrl+B	Identical to the **Left Arrow** key.
Ctrl+C	Interrupt the ongoing command, such as **ping** and **traceroute**.
Ctrl+D	Return to the previous mode.
Ctrl+E	Move the cursor to the end of the command.
Ctrl+F	Identical to the Right Arrow key
Ctrl+G	Delete the entire line.
Ctrl+K	Delete all characters from the cursor to the end of the command.
Ctrl+L	Clear screen information.
Ctrl+S	Identical to the **Down Arrow** key
Ctrl+X	Delete all characters before the cursor (except the cursor location).
Ctrl+Y	Show history commands.
Ctrl+Z	Return to privileged EXEC mode from the current mode (except user EXEC mode).
Space bar or **Y**	Scroll down one screen.
Enter	Scroll down one line.

1.1.5 Display information

Display features

The CLI provides the following display features:

- The help information and prompt messages displayed at the CLI are in English.
- When messages are displayed at more than one screen, you can suspend displaying them with one of the following operations, as listed in Table 1-2.

Table 1-2 Shortcut keys about display features

Function key	Description
Press **Space bar** or **Y**	Scroll down one screen.
Press **Enter**	Scroll down one line.
Press any letter key (except **Y**)	Stop displaying and executing commands.

Filtering display information

The ISCOM6820 supports a series of commands starting with **show**, to check device configurations, operation and diagnostic information. Generally, these commands can output more information, and then user needs to add filtering rules to filter out unnecessary information.

For common **show** commands on the ISCOM6820, see its maintenance guide.

The **show** command of the ISCOM6820 supports four kinds of filtering modes:

- | **begin** *string*: show all lines starting from the assigned string.
- | end *string*: show all lines ending at the assigned string.
- | **exclude** *string*: show all lines mismatching the assigned string.
- | **include** *string*: show all lines only matching the assigned string.

Page-break

Page-break is used to suspend displaying messages when they are displayed at more than one screen. After page-break is enabled, you can use shortcut keys listed in Table 1-2. If page-break is disabled, all messages are displayed when they are displayed at more than one screen.

Step	Command	Description
1	`Raisecom#terminal page-break enable`	Enable page-break. By default, it is enabled. You can use the **terminal page-break disable** command to restore default status.

1.1.6 Showing history commands

The history commands can be automatically saved at the CLI. You can use the up arrow (↑) or down arrow (↓) to schedule history commands and use them repeatedly.

Step	Command	Description
1	Raisecom>**terminal history** *number*	Configure the number of history commands saved in the system. By default, it is 20.

The ISCOM6820 supports checking or executing some history command by using the **history** command in any command line mode.

```
Raisecom>history
   Maximum number of Terminal history commands :1000
    cmdExtTime    cmdExtResult  user            cmd
-------------------------------------------------------------------------
    0000:00:26:51  success      raisecom        ena
    0000:00:21:05  success      raisecom        config
    0000:00:20:53  success      raisecom        interface gpon-onu 3/1/1
    0000:00:20:41  success      raisecom        ex
    0000:00:20:09  success      raisecom        epon-onu uni ethernet
3/1/1/1
    0000:00:17:20  success      raisecom        language chinese
    0000:00:08:38  success      raisecom        language english
    0000:00:08:20  success      raisecom        ex
    0000:00:08:19  success      raisecom        exit
    0000:00:07:14  success      raisecom        show gpon-onu 3/1/1 uni
ethernet snmp trap
    0000:00:06:08  success      raisecom        config
    0000:00:05:24  success      raisecom        gpon-onu uni ethernet
3/1/1/1
    0000:00:00:52  success      raisecom        ex
    0000:00:00:51  success      raisecom        exit
```

1.1.7 Acquiring help

Complete help

You can acquire complete help under following three conditions:

- You can enter a question mark (?) at the system prompt to display a list of commands and brief descriptions in any command line mode.

```
Raisecom>?
```

The command output is as below:

```
clear  Clear screen
enable  Turn on privileged mode command
exit  Exit current mode and down to previous mode
help  Message about help
history  Most recent history command
language Language of help message
list  List command
quit  Exit current mode and down to previous mode
terminal Configure terminal
```

- After you enter a keyword, press the **Space bar** and enter a question mark (?), all related commands and their brief descriptions are displayed if the question mark (?) matches another keyword.

```
Raisecom#clock ?
```

The command output is as below:

```
 set    Set system time and date
 summer-time Enable summer time
 timezone  Set system timezone offset
```

- After you enter a parameter, press the **Space bar** and enter a question mark (?), all related parameters and descriptions are displayed if the question mark (?) matches a parameter.

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

The command output is as below:

```
<1-4094> VLAN ID
```

Partial help

You can acquire partial help under following three conditions:

- After you enter a particular character string and a question mark (?), a list of key words that begin with the particular character string is displayed.

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

The command output is as below:

```
clear   Clear screen
  cpu    CPU monitor
  create  Create operation
```

- After you enter a command, press **Space bar**, and enter a particular character string and a question mark (?), a list of commands that begin with a particular character string is displayed.

```
Raisecom#show c?
```

The command output is as below:

```
 card      Card
 card-power    card power information
 card-temperature card temperature information
 clock      System date and time
 command_set    command set config information
 cpu-utilization  CPU utilization
```

- After you enter a partial command name and press **Tab**, the full form of the keyword is displayed if there is a unique match command. Otherwise, press **Tab** continuously to display different keywords and then you can select the required one.

Error message

The ISCOM6820 print out the following error messages according to the error type when you input incorrect commands.

Error message	Description
% " * " Incomplete command.	The input command is incomplete.
% Invalid input at '^' marked.	The keyword marked with "^" is invalid or does not exist.
% Ambiguous input at '^' marked, follow keywords match it.	The keyword marked with "^" is unclear.
% " * " Unconfirmed command.	The input command is not unique.
% " * " Unknown command.	The input command does not exist.
% You Need higher priority!	You need more authority to execute the command.

1.2 Accessing device

1.2.1 Accessing through Console interface

The Console interface is the control interface for local management.

Note

- You must use the dedicated configuration cable for Raisecom devices when logging into the device through the Console interface.
- For technical specifications of the Console interface and model of the configuration cable, see *ISCOM6820 (A) Hardware Description*.

If you want to access the device through the Console interface, connect the Console interface and RS-232 serial interface of the PC, as shown in Figure 1-1; then run the terminal emulation program such as Windows XP Hyper Terminal program in the PC to configure communication parameters as shown in Figure 1-2, and then log in to the device.

Figure 1-1 Accessing the device through a PC connected with Console interface

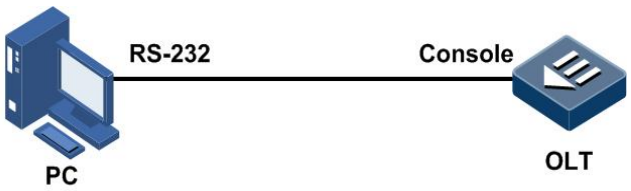
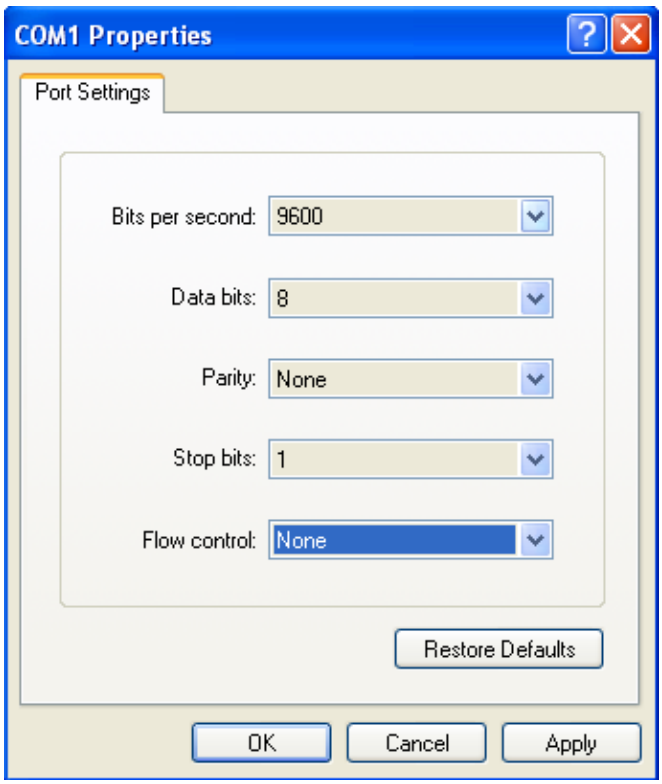


Figure 1-2 Communication parameters in Hyper Terminal



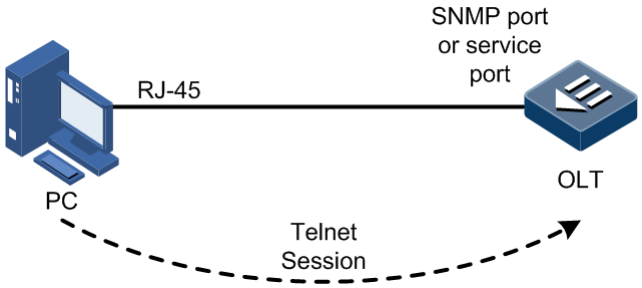
1.2.2 Accessing through Telnet

To use a PC to log in to the device remotely through Telnet, log in to a device from the PC at first, and then Telnet other ISCOM6820 devices on the network. Thus, you do not need to connect a PC to each device. Moreover, you need to ensure that the device can ping through the PC.

The OLT provides the following Telnet services:

- Telnet Server: run the Telnet client program on a PC to log in to the device, and then configure and manage it. As shown in Figure 1-3, the OLT works as the Telnet server.

Figure 1-3 Networking with the OLT as the Telnet server

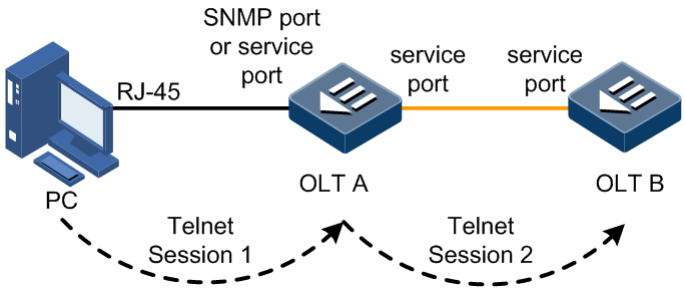


Before accessing the device through Telnet, you need to log in to the device through the Console interface and enable Telnet services. Configure the device as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface vlanif` *vlan-id*	Enter VLAN interface configuration mode.
3	`Raisecom(config-vlanif-*)#ip address` *ip-address* `[` *ip-mask* `] [ sub ]` `Raisecom(config-vlanif-*)#exit`	Configure the IP address and mask of the device, and bind the IP address to the VLAN. The VLAN is the one in which the interface which needs to enable Telnet services is.
4	`Raisecom(config)#telnet-server close terminal-telnet` *session-number*	(Optional) disconnect a specified Telnet session connected to the device.
5	`Raisecom(config)#telnet-server port close`	Configure the disconnection of Telnet.

- Telnet Client: after you log in to OLT A through the PC terminal emulation program or Telnet client program on a PC, then log in to OLT B using the **telnet** command to configure and manage it. As shown in Figure 1-4, OLT A works as the Telnet server as well as the Telnet client.

Figure 1-4 Networking with the OLT as the Telnet client



Configure the device working as the Telnet client as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#telnet` *ipv4-address* `[ port` *port-id* `]`	Log into other devices through Telnet.

1.2.3 Accessing through SSHv2

Telnet transmits data in plaintext. The user name, password, and configurations are easy to be intercepted by other users, which brings potential security hazards. Therefore, Telnet is mainly used to manage devices inside a network.

SSHv2 is a secure data transmission protocol, which can effectively prevent disclosure of information in remote management through data encryption, and provide greater security for remote login and other network services.

Before accessing the device through SSHv2, you must log in to the device through the Console interface and enable the SSHv2 service.

Default configurations of the SSHv2 service on the ISCOM6820 are as below.

Function	Default value
SSHv2 server status	Disable
RSA public key	N/A
SSHv2 key pair length	512 bit
Authentication mode	Local user-password
SSHv2 authentication timeout	600s
Allowable times of SSHv2 authentication failure	20
SSHv2 interception interface ID	22
SSHv2 session status	Enable

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**generate ssh-key** [*key-length*]	Generate local SSHv2 secret key.
3	Raisecom(config)#**ssh2 server**	Start the SSHv2 server. You can use the **no ssh2 server** command to disable SSHv2 Server.
4	Raisecom(config)#**ssh2 server authentication password**	Configure the SSHv2 authentication mode to local password. You can use the **no ssh2 server authentication** command to restore default configurations.
	Raisecom(config)#**ssh2 server authentication rsa-key**	Configure the the SSHv2 authentication mode to RSA key. You can use the **no ssh2 server authentication** command to restore default configurations.
	Raisecom(config)#**ssh2 server authentication public-key** (Ctrl+r) for save input and return (Ctrl+z) for discard input and return.	Configure the the SSHv2 authentication mode to public key. You can use the **no ssh2 server authentication** command to restore default configurations.
5	Raisecom(config)#**ssh2 server authentication-timeout** *timeout*	(Optional) configure SSHv2 authentication timeout. When the client authentication time exceeds this limit, the device will refuse to continue authentication and disconnect. You can use the **no ssh2 server authentication-timeout** command to restore default configurations.
6	Raisecom(config)#**ssh2 server authentication-retries** *count*	(Optional) configure the number of failed SSHv2 authentication attempts. When the number of client authentication failures exceeds this limit, the device will refuse to continue authentication and disconnect.
7	Raisecom(config)#**ssh2 server port** *port-id*	Configure SSHv2 listening port number. You can use the **no ssh2 server port** command to restore default configurations. **Note** When you configure the SSHv2 listening port number of a device, the parameters entered do not take effect immediately. Instead, they only take effect until the SSHv2 server is restarted.
8	Raisecom(config)#**ssh2 server session** *session-list* { **enable** | **disable** }	Enable/Disable the specified SSHv2 sessions.

1.2.4 Configuring Console terminal

If the user enters the login password incorrectly more than three times, the terminal will prohibit the user from continuing the operation. In this case, the user needs to wait for a certain period of time before login again.

The device supports timeout disconnection for all user interfaces. If the user does not perform any operation within the specified time, the user will be automatically disconnected. After the timeout expires, the user needs to log in to the device through the console terminal again.

The Console terminal configuration is the basic configuration for the user to log in to the device and perform device operations. You can configure the Console terminal based on the actual condition.

Configure the device as below.

Step	Command	Description
1	Raisecom>**terminal time-out** { *period* | **disable** }	Configure timeout exit time of the Console terminal.
2	Raisecom>**enable**	Enter privileged EXEC mode.
3	Raisecom#**logout**	Log out the device.
4	RaisecomRaisecom#**show terminal**	Show configurations of the terminal user.

1.2.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show telnet-server**	Show Telnet configurations.
2	Raisecom#**show ssh2 server**	Show the SSHv2 server.
3	Raisecom#**show ssh2 public-key**	Show the public key used for SSHv2 authentication on the device and clietn.
4	Raisecom#**show interface vlanif** [{ *vlan-list* | **detail** }]	Show configurations of the VLAN interface.
5	Raisecom#**show telnet-server port status**	Show configurations and status of the Telnet interface on the Telnet server.

1.3 Managing users

1.3.1 Default configurations

Default user configurations of the device are as below.

Function	Default value
Default user	• User name: raisecom • Password: raisecom • User privilege: 15 (Administrator)
New user privilege	15 (Administrator)

We recommend modifying the default user name and password to prevent illegal visits from breaking down the device.

1.3.2 Creating or deleting users

Configure the device as below.

Step	Command	Description
1	Raisecom#**user name** *username* **password** *password*	Create a user, or modify the user name and password.
2	Raisecom#**password** please input password: please input again:	Modify the current password.
3	Raisecom#**no username** *username*	Delete a user.  Online users cannot be deleted.

When modifying the password, you should input the same password for two times. Otherwise, the modification fails.

1.3.3 Managing user privileges

Configure the device as below.

Step	Command	Description
1	Raisecom#**user name** *username* **privilege** *level*	(Optional) configure the user level and privilege.
2	Raisecom#**enable password**	(Optional) modify the password in privilege EXEC mode.
3	Raisecom#**user login**{ **local-radius** | **local-tacacs** | **local-user** | **radius-local** | **radius-user** | **tacacs-local** | **tacacs-user** }	(Optional) configure the authentication mode for user login.

Step	Command	Description
4	Raisecom#**enable login** { **local-radius** | **local-tacacs** | **local-user** | **radius-local** | **radius-user** | **tacacs-local** | **tacacs-user** }	(Optional) configure the authentication mode for login in privilege EXEC mode.
5	Raisecom#**enable auth bypass**	(Optional) bypass password authentication when entering the privileged EXEC mode to user EXEC mode. Use the **no enable auth bypass** command to restore the default password authentication mode.
6	Raisecom#**user** *user-name* { **allow-exeset** | **disallow-exeset** } *commandset*	Configure the name of the command set to be executed.

Note

The user under privilege 11 can enter privileged EXEC mode without the password.

1.3.4 Refining user privileges

User privilege refining provides the concept of command set and enhances users' executive capability of commands. You can flexibly define a command set as needed by arranging commands of different levels into a set, and specifying to allow or forbid users from executing the command set. Thus, it facilitates you to manage user privileges flexibly according to actual conditions.

The system supports 10 command sets. One command set contains 50 commands. The administrator can control the command set configuration for some common users. In this case, the common users are allowed or forbidden to execute commands in the command set.

Note

User privilege refining cannot be operated on the administrator.

Configure the device as below.

Step	Command	Description
1	Raisecom#**command-set** *cmdsetname* Raisecom(command-set:*)#	Create a command set.
2	Raisecom(command-set:*)#**command** "*cmdkeylist*" Raisecom(command-set:*)#exit Raisecom#	Create a command in the command set.
3	Raisecom#**user** *user-name* { **allow-exeset** | **disallow-exeset** } *commandset*	Configure the name of the command set to be executed.

1.3.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show user** [**detail**]	Show information about login users.
3	Raisecom#**show command-set detail** [*cmdsetname*]	Show details of the command set.

1.4 Managing cards

1.4.1 Default configurations

Default configurations of cards on the device are as below.

Function	Default value
Created type	• Slots 1–12: SMUA • Slot 3: XCOA, GPHA, or XCHA • Slot 4: XCOA, GPHA, or XCHA • Slots 6–7: power supply cards, unmanageable • Slot 5: fan card, unmanageable
Actual type	N/A
Creation type	N/A
Serial number	N/A
Card status	Not-used
Card power status	off
Fan management mode	auto
Fan gear	5, namely, working at the maximum rotational speed

1.4.2 Creating cards

The ISCOM6820 do not support creating cards. The system defines the card status through the following two types:

- Created type: the card type specified by users using the **create card** command.
- Actual type: the card type detected by the system automatically when the card is inserted into the slot.

Only when the created type and actual type are consistent can the card work properly.

Note

Values of the card status indicate as below:
- not-used: the card is not created nor inserted into the slot.
- offline: the card is created but is not inserted into the slot.
- non-provisioned: the card is not created but is inserted into the slot.

- type-mismatched: the card is created and inserted into the slot, but the created type and actual type are inconsistent.
- version-mismatched: the card is created and inserted into the slot, and the created type and actual type are consistent, but the versions do not match.
- disable: the card is created and inserted into the slot, and the created type and actual type are consistent, but communication fails.
- loading-config: the card is created and inserted into the slot, the created type and actual type are consistent, communication runs properly, and configuration files are being loaded.
- loading-config-failed: configuration files fail to be loaded.
- inservice: configuration files are loaded successfully and the card works properly.

After the card is inserted into the slot, you need to create the card in the system to configure and manage the card. When creating the card, you need to specify the slot ID and card type.

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**create card slot** *slot-id* **type** { **auto** | **xcoa** | **gpha** | **xcha** | **xgha** }	Create a card on the device. You can use the **no create card slot** *slot-id* [**now**] command to delete the card.
3	Raisecom(config)#**device description** *description*	(Optional) configure the description of the device to identify different devices. You can use the **no device description** command to delete the descriptions.
4	Raisecom(config)#**slot** *slot-id* **description** *description*	(Optional) configure the description of the slot to identify different slots. You can use the **no slot** *slot-id* **description** command to delete the description.

1.4.3 Restarting cards

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**reboot** { **slot** { *slot-id* | **all** }| **gpon-onu** *slot-id/olt-id/onu-list* } [**now**]	Restart the specified card.
2	Raisecom#**config**	Enter global configuration mode.
3	Raisecom(config)#**power** { **on** | **off** } **slot** *slot-id*	Turning on/off the card power.

1.4.4 Fan management

The ISCOM6820 supports smart fans of which the gear position and rotational speed can be automatically or manually adjusted.

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**fan speed mode** { **auto** | **manual** }	Configure the fan management mode. You can use the **no fan speed mode** command to restore default configurations.
3	Raisecom(config)#**fan speed manual** *level*	Configure the fan gear. You can use the **no fan manual** command to restore default configurations.

1.4.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show card**	Show information about all cards.
2	Raisecom#**show card-temperature management information**	Show the current temperature, temperature alarm threshold, temperature management status, temperature management status, and other information.
3	Raisecom#**show cpu-utilization** [**slot** *slot-list*]	Show the CPU utilization rate of the card.
4	Raisecom#**show device** [**location**]	Show information about the OLT device, including the type, MAC address, serial number, and slots on the main control card.
5	Raisecom#**show version slot** *slot-id*	Show version information about the card in a specified slot, including card type, card hardware version, system software version, bootrom version, firmware version, and CPLD version.
6	Raisecom#**show slot** *slot-id*	Show information about the specified slot, including the type of the card supported by the slot, description of the slot, the available status of the slot, the slot ID, the actual card type of the slot, and the type of card that should be installed. It will display null if the type of card is not specified and the actual card is not in place.
7	Raisecom#**show fan**	Show fan status.

1.5 Managing interfaces

1.5.1 Default configurations of the OLT 10GE interface

Default configurations of the OLT 10GE interface on the ISCOM6820 are as below.

Function	Default value
Status	Enable
Rate and duplex mode	10G/1G configurable rate
Flow control	Disable
MTU	1600 Bytes
Refresh frequency of interface dynamic statistics	2s

Default configurations of the ONU interface

Default configurations of the Ethernet interface on the Raisecom ONU are as below.

Function	Default value
Interface status	Enable
Interface rate	Auto (auto-negotiation)
Interface duplex mode	Auto (auto-negotiation)
Interface flow control	Disable
Interface MTU	1518 bytes

1.5.2 Enabling/Disabling interfaces

Enabling/Disabling the OLT interface

Configure the ISCOM6820 as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface { ten-gigabitethernet | gpon-olt } slot-id/port-id`	Enter physical interface configuration mode.
3	`Raisecom(config-if-*-*:*)#shutdown`	Disable the interface. You can use the **no shutdown** command to enable the interface.

Enabling/Disabling the ONU interface

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#{ **gpon-onu** } **uni ethernet** *slot-id/olt-id/onu-id/uni-id*	Enter PON ONU UNI interface configuration mode.
3	Raisecom(config-*-onu-ethernet-*/*/*:*)#**shutdown**	Disable the interface. You can use the **no shutdown** command to enable the interface. **Note** When you use this command to shut down the ONU UNI, no Trap is reported in the command mode. To show Trap, enable the alarm Trap. For details, see section 13.10 Configuring alarm and event management.

1.5.3 Configuring basic properties of interfaces

Configuring basic properties of the OLT interface

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**system mtu** *size*	Configure the global MTU. You can use the **no system mtu** command to restore default configurations.
3	Raisecom(config)#**interface ten-gigabitethernet** *slot-id/port-id*	Enter 10GE interface configuration mode.
4	Raisecom(config-if-ten-gigabitethernet-*:*)#**speed** { **10000** | **1000** }	Configure the interface rate.
5	Raisecom(config-if-ten-gigabitethernet-*:*)#**description** *word*	Configure interface description. You can use the **no description** command to restore default configurations.

Configuring basic properties of the ONU interface

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#{ **gpon-onu** } **uni ethernet** *slot-id/olt-id/onu-id/uni-id*	Enter PON ONU UNI interface configuration mode.

Step	Command	Description
3	Raisecom(config-*-onu-ethernet-*/*/*:*)#**speed** { **10** | **100** | **1000** } **duplex** { **half** | **full** }	Configure the rate and duplex mode of the ONU Ethernet interface.
4	Raisecom(config-*-onu-ethernet-*/*/*:*)#**speed auto**	Configure auto-neogitation for the rate and duplex mode of the ONU Ethernet interface.
5	Raisecom(config-*-onu-ethernet-*/*/*:*)#**uni name** *name*	Configure the description of the physical interface.

1.5.4 Configuring interface statistics

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**dynamic statistics time** *period*	Configure the interval of dynamic statistics on the interface. You can use the **no dynamic statistics time** command to restore default configurations.
3	Raisecom(config)#**clear interface** { **gpon-olt** |**ten-gigabitethernet** } *slot-id/port-id* **statistics**	Clear interface statistics saved on the device.

1.5.5 Configuring flow control on interfaces

Configuring flow control on the OLT interface

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface ten-gigabitethernet** *slot-id/port-id*	Enter physical interface configuration mode.
3	Raisecom(config-if-ten-gigabitethernet-*-*:*)#**flowcontrol** { **receive** | **send** }	Configure flow control on the interface. You can use the **no flowcontrol** { **receive** | **send** } command to restore default configurations.

Configuring flow control on the ONU interface

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#{ **gpon-onu** } **uni ethernet** *slot-id/olt-id/onu-id/uni-id*	Enter PON ONU UNI interface configuration mode.
3	Raisecom(config-*-onu-ethernet-*/*/*:*)#**flowcontrol** { **enable** | **disable** }	Enable/Disable flow control on the physical interface. You can use the **no flowcontrol** { **receive** | **send** } command to restore default configurations.

1.5.6 Configuring the IP interface

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface vlanif** *vlan-id*	Enter VLAN interface configuration mode.
3	Raisecom(config-vlanif-*)#**ip address** *ip-address* [*ip-mask*] [**sub**]	(Optional) configure the IP address of the VLAN interface. You can use the **no ip address** *ip-address* command to delete the configuration.
4	Raisecom(config-vlanif-*)#**ipv6 address** *A:B::C:D/M* [**eui-64**] Raisecom(config-vlanif-*)#**ipv6 address** *A:B::C:D* **link-local**	(Optional) configure the IPv6 address of the Layer 3 interface. You can use the **no ipv6 address** *A:B::C:D* **link-local** command or **no ipv6 address** *A:B::C:D/M* [**eui-64**] command to delete the configuration.
5	Raisecom(config-vlanif-*)#**description** *word*	Configure the interface description. You can use the **no description** command to restore to default values.

Note

- Each VLAN interface supports 4 IPv4 addresses.
- Each VLAN interface supports 4 IPv6 addresses.

1.5.7 Configuring out-of-band network management interface

The SNMP interface on the MCC is used for out-of-band network management.

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**management-port ip address** *ip-address* [*mask*]	Configure the IPv4 address for the out-of-band management interface.

Step	Command	Description
	Raisecom(config)#management-port ipv6 address *ip-address* [link-local]	Configure the IPv6 address for the out-of-band management interface.

- The IP address of the out-of-band management interface cannot be in the same network segment as that of the Layer 3 IP interface.
- The IP address of the out-of-band management interface is 192.168.1.100.

1.5.8 Checking configurations

Checking configurations of the OLT interface

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show interface** { **gpon-olt** | **ten-gigabitethernet** } *slot-id/olt-id*	Show interface configurations, including the interface status, rate, duplex mode, and forwarding mode.
2	Raisecom#**show interface** { **gpon-olt** | **ten-gigabitethernet** } *slot-id/olt-id* **description**	Show the description of the specified physical interface.
3	Raisecom#**show interface** { **gpon-olt** | **ten-gigabitethernet** } *slot-id/olt-id* **statistics**	Show interface statistics.
4	Raisecom#**show interface** { **ten-gigabitethernet** } *slot-id/olt-id* **flowcontrol**	Show flow control information about the interface.
5	Raisecom#**show system mtu**	Show the system MTU.
6	Raisecom#**show management-port** [**ip-address**]	Show the IPv4 address of the out-of-band management interface.
7	Raisecom#**show interface vlanif [{** *vlan-list* **| detail }]**	Show configurations of the VLAN interface.
8	Raisecom#**show interface vlanif** *if-id* **description**	Show the description of the VLAN interface.
9	Raisecom#**show interface vlanif brief**	Show parameter information about the VLAN interface.

Checking configurations of the ONU interface

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show interface** { **gpon-onu** } [*slot-id/olt-id/onu-id*] **creation-information**	Show information about created ONUs.

No.	Command	Description
2	Raisecom#**show interface** { | **gpon-onu** } [*slot-id/olt-id/onu-id*] **online-information**	Show online information about ONUs.
3	Raisecom#**show** { | **gpon-onu** } *slot-id/olt-id/onu-id* **information**	Show information about ONUs.
4	Raisecom#**show** { **gpon-onu** } *slot-id/olt-id/onu-id* **uni ethernet** *uni-id* **information**	Show the rate, duplex mode, flow control, and connection status of the ONU UNI.
5	Raisecom#**show** { **gpon-onu** } *slot-id/olt-id/onu-id* **uni ethernet** *uni-id* **statistic**	Show statistics on ONU UNIs.

1.5.9 Maintenance

You can use the following commands to maintain the running and configuration of the port management feature.

No.	Command	Description
1	Raisecom#**clear interface** { **gpon-olt** | **ten-gigabitethernet**} *slot-id/port-id* **statistics**	Clear interface statistics.

1.6 Managing time

1.6.1 Default configurations

Default configurations of time management on the ISCOM6820 are as below.

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	Disable

1.6.2 Configuring time and time zone

Configuring time

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**clock set** hour minute second year month day	Configure the system time, including hour, minute, second, year, month, and day.

Configuring time zone

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**clock timezone** { + | - } *hour minute*	Configure the time zone. You can use the **clock timezone** command to restore default configurations.

1.6.3 Configuring DST

DST (DST) is a local time regulation for saving energy. At present, there are nearly 110 countries using DST every summer around the world, but different countries have different stipulations for DST. Thus, you should consider the local conditions when configuring DST.

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**clock summer-time**	Enable the device DST. You can use the **no clock summer-time** command to disable DST.
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 the calculating period of the system DST. You can use the **no clock summer-time recurring** command to restore default configurations.

Note

- When you configure the system time manually, if the system uses DST, such as DST from 2 A.M. on the second Sunday, April to 2 a.m. on the second Sunday, September every year, you have to adjust the clock one hour forward during this period, that is, set the time offset as 60min. So the period from 2 a.m. to 3 a.m. on the second Sunday, April each year is inexistent. Configuring time manually in this period will fail.
- The DST in southern hemisphere is opposite to the northern hemisphere, which is from September to April next year. If the start time is later than end time, the system will suppose that it is in the southern hemisphere. That is to say, the DST is the period from the start time this year to the end time next year.

1.6.4 Configuring NTP

Network Time Protocol (NTP) is a time synchronization protocol defined by RFC1305, used to synchronize time between distributed time servers and clients. NTP transportation is based on UDP, using port 123.

The purpose of NTP is to synchronize all clocks in a network quickly and then the device can provide different applications over a unified time. Meanwhile, NTP can ensure very high accuracy, with accuracy of 10ms around.

The device in support of NTP cannot only accept synchronization from other clock source, but also synchronize other devices as a clock source.

The device adopts multiple NTP working modes for time synchronization:

- Server mode

In this mode, the device works as the NTP server. The client sends the clock synchronization request packet to the NTP server. The server sends a response after receiving the request. Then the client performs clock synchronization after receiving the response packet.

- Client mode

In this mode, the device works as the NTP client. You should specify the IP address of the NTP server for the client to realize clock synchronization.

- Symmetric peer mode

In this mode, the symmetric active peer sends the clock synchronization packet to the symmetric passive peer. The symmetric passive peer works in passive mode automatically after receiving the packet, and sends the response packet. The symmetric active peer and symmetric passive peer in this mode can synchronize with each other.

By default, the IP address of the NTP server is not configured. If the version is not configured when you configure the NTP server, the version No. is 3.

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ntp server** { *ip-address* | *ipv6-address* } [**version** *version-number*]	(Client mode) configure the IP address of the NTP server. You can use the **no ntp server** { *ip-address* | *ipv6-address* } command to restore default configurations.
3	Raisecom(config)#**ntp peer** { *ip-address* | *ipv6-address* } [**version** *version-number*]	(Symmetric peer mode) configure the IP address of the NTP symmetric peer. You can use the **no ntp peer** { *ip-address* | *ipv6-address* } command to restore default configurations.
4	Raisecom(config)#**ntp refclock-master** [*stratum*]	(Server mode) configure the local clock as the NTP reference clock source. You can use the **no ntp refclock-master** command to delete the configuration.

Note

If the device is configured as the NTP reference clock source (server mode), it cannot be configured as the NTP server (client mode) or NTP symmetric peer; and vice versa.

1.6.5 Configuring SNTP

Simple Network Time Protocol (SNTP) is used to synchronize the system time with the time of the SNTP server. You can specify the IP address of the SNTP server on the device to synchronize its system time with the SNTP server, thus implementing time synchronization on the whole network. The ISCOM6820 can act as SNTP clients only.

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sntp-client**	Enable SNTP Client. You can use the **no sntp client** command to disable this function.
3	Raisecom(config)#**sntp-client server** { *ip-address* | *ipv6-address* }	Configure the IP address of the SNTP client. You can use the **no sntp-client server** command to restore default configurations.

Note

SNTP and NTP are mutually exclusive. Therefore, they cannot be used at the same time.

1.6.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show ntp status**	Show the NTP status.
2	Raisecom#**show ntp associations**	Show information about the NTP connection.
3	Raisecom#**show clock**	Show configurations of the system time and time zone.
4	Raisecom#**show sntp-client**	Show configurations of the SNTP client.

1.7 Upgrade and backup

1.7.1 Introduction

The device supports two system extended boot files and two system startup files, and provides 1:1 backup and protection for system files. Thus, it decreases faults and service interruption caused by corrupted system files and system upgrade.

- When loading of the system file fails, the system will automatically switch to load the backup file. You can troubleshoot the primary file after starting the system using the backup file.

- When upgrading the system file, you can upgrade the backup file first, and switch the system to the backup file, and then upgrade the primary file. In this way, you can decrease the service interruption caused by system upgrade.
- When upgrading the system file, you can upgrade the primary file and back up the original system file. When the network fails due to the upgrade, you can switch to the original file immediately to ensure the normal service.

1.7.2 Upgrading OLT system files

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**download** { **mainrom1** | **system1** | **system2** | **cpld1** | **cpld2** |**startup-config** | **fpga** } **ftp** *ip-address username password filename* **slot** *slot-id*	(Optional) upgrade the system boot file or system startup file through FTP. **Note** • Before selecting system1 or system2 file, use the show version command to show whether the current system is active. If yes, it cannot be upgraded; in this case, you can choose to upgrade the other system. • The mainrom1, system1, and system2 can be upgraded in slots 3 and 4. • The startup-config file can be upgrade in slot 3 only. • The cpld file can be upgrade in slots 1–4. • For other commands, see command reference.
	Raisecom#**download** { **mainrom1** | **system1** | **system2** | **cpld1** | **cpld2** |**startup-config** | **fpga** } **tftp** *ip-address filename* **slot** *slot-id*	(Optional) upgrade the system boot file or system startup file through TFTP. **Note** • Before selecting system1 or system2 file, use the show version command to show whether the current system is active. If yes, it cannot be upgraded; in this case, you can choose to upgrade the other system. • The mainrom1 and system1can be upgraded in slots 3 and 4. • The startup-config or system 2 file can be upgrade in slot 3 only. • The cpld file can be upgrade in slots 1–4. • For other commands, see command reference.
	Raisecom#**download** { **mainrom1** | **system1** | **system2** | **cpld1** | **cpld2** | | **startup-config** | **fpga** } **sftp** *ip-address username password filename* **slot** *slot-id*	(Optional) upgrade the system boot file or system startup file through SFTP. **Note** • Before selecting system1 or system2 file, use the show version command to show whether the current system is active. If yes, it cannot be upgraded; in this case, you can choose to upgrade the other system. • The mainrom1 and system1can be upgraded in slots 3 and 4. • The startup-config or system 2 file can be upgrade in slot 3 only. • The cpld file can be upgrade in slots 1–4. • For other commands, see command reference.

Step	Command	Description
2	Raisecom#**commit** { **system1** | **system2** } **gpon-onu** *slot-id/olt-id/onu-id*]	Specify the version of the system software to be loaded. **Note** After specifying the version, you need to restart the device to switch to the specified version.
3	Raisecom#**write startup-config**	Save current configurations.
4	Raisecom#**erase startup-config**	(Optional) clear the configuration file of the current system. **Caution** This command will clear the configuration file in the system and cause service interruption. Use it with caution.

1.7.3 Backing up OLT system files

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**upload startup-config** { **ftp** *ip-address username password filename* | **sftp** *ip-address username password filename* | **tftp** *ip-address filename* } **slot 3**	(Optional) back up the system startup file through FTP/SFTP/TFTP.

1.7.4 Upgrading ONU system files

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**download system1 ftp** *ip-address username password filename* **gpon-onu** { *slot-id/olt-id/onu-list* | **all** | **slot** *slot-id* } [**device-type** *onu-type* [**version** *version*]] [**commit**]	(Optional) upgrade ONU system files through FTP.
	Raisecom#**download system1 tftp** *ip-address filename* **gpon-onu** { *slot-id/olt-id/onu-list* | **all** | **slot** *slot-id* } [**device-type** *onu-type* [**version** *version*]] [**commit**]	(Optional) upgrade ONU system files through TFTP.
2	Raisecom#**download** { **ftp**| **sftp** } *ip-address username password filename* **gpon-onu** *slot-id/olt-id/onu-id* [**auto-commit**]	(Optional) upgrade ONU system files through FTP/SFTP.

Step	Command	Description
3	Raisecom#**commit** { **system1** | **system2** } **gpon-onu** *slot-id/olt-id/onu-id*]	Specify the version of the system software to be loaded. **Note** After specifying the version, you need to restart the device to switch to the specified version.

1.7.5 Configuring auto-saving

The ISCOM6820 supports the auto-saving feature. This feature can avoid loss of system configurations due to human carelessness, such as forgetting to save the configurations.

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**auto-write** { **enable** | **disable** }	Enable/Disable the auto-saving feature.
3	Raisecom(config)#**auto-write time** *time*	(Optional) configure the time for auto-saving.

1.7.6 Configuring FTP/TFTP/SFTP parameters

Configure the ISCOM6820 as below.

Step	Command	Description
1	Raisecom#**ftp** *ip-address username password* Raisecom#**ftp** *ipv6-address* [**scopeid** *scope-id*] *username password*	Configure FTP parameters.
2	Raisecom#**sftp ip-address username password** Raisecom#**sftp** *ipv6-address* [**scopeid** *scope-id*] *username password*	Configure TFTP parameters.
3	Raisecom#**sftp** *ip-address username password* Raisecom#**sftp** *ipv6-address* [**scopeid** *scope-id*] *username password*	Configure SFTP parameters.

1.7.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show** { **ftp** | **tftp** | **sftp** }	Show configuration parameters of the FTP, TFTP, and SFTP.
2	Raisecom#**show startup-config**	Show configurations loaded when the device starts.

No.	Command	Description
3	Raisecom#**show running-config**	Show current configurations of the device.
4	Raisecom#**show version**	Show the system version.
5	Raisecom#**show version** [**slot** *slot-id* | **gpon-onu** *slot-id/olt-id/onu-list*]	Show the version in the specified slot or of the ONU.
6	Raisecom#**show auto-write**	Show the auto-saving time.

1.7.8 Maintenance

You can use the following commands to maintain the running and configuration of the port management feature.

No.	Command	Description
1	Raisecom(config)#**clear interface gpon-olt***slot-id/port-id* **statistics**	Clear statistics on Ethernet interfaces.

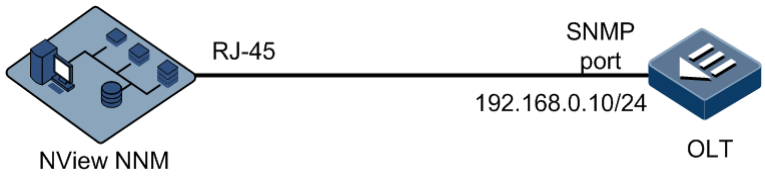
1.8 Configuration examples

1.8.1 Example for configuring out-of-band network management

Networking requirements

As shown in Figure 1-5, the NView NNM system manages the OLT through out-of-band network management. The IP address of the out-of-band management interface is 192.168.0.10.

Figure 1-5 Configuring out-of-band network management



Configuration steps

Configure the IP address of the out-of-band management interface.

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

Checking results

Show the IP address of the out-of-band management interface.

```
Raisecom#show management-port ip-address
Prifix IF    Address        NetMask        Source     Catagory
-------------------------------------------------------------
OB     0     192.168.0.10   255.255.255.0  assigned   primary
```

1.8.2 Example for configuring in-band network management

Networking requirements

As shown in Figure 1-6, the NView NNM system manages the OLT through in-band network management. The IP address of the VLAN interface is 192.168.0.1. The mask is 255.255.255.0. The VLAN ID is 2.

Figure 1-6 Configuring in-band network management

Configuration steps

Step 1 Create a VLAN and configure properties of the interface.

```
Raisecom#config
Raisecom(config)#create vlan 2 active
Raisecom(config)#interface ten-gigabitethernet 1/1
Raisecom(config-if-ten-gigabitethernet-1:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-1:1)#switchport trunk allowed vlan
2
Raisecom(config-if-ten-gigabitethernet-1:1)#exit
```

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

```
Raisecom(config)#interface vlanif 2
Raisecom(config- vlanif-0)#ip address 192.168.0.1 255.255.255.0 2
```

Checking results

Show the IP address of the VLAN interface.

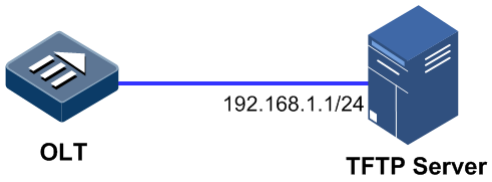
```
Raisecom#show interface vlanif
IF                          Address        NetMask        Catagory
------------------------------------------------------------------------------
-----
vlan2                        10.11.51.123    255.255.254.0   primary
```

1.8.3 Example for upgrading OLT through TFTP

Networking requirements

As shown in Figure 1-7, the TFTP server is connected to the OLT. Configure the system startup file to upgrade the OLT as system1. The IP address of the TFTP server is 192.168.1.1. The system file to be upgraded is ISCOM6820-ROAP_2.2.2_20130607.

Figure 1-7 Upgrading OLT through TFTP



Configuration steps

Step 1 Download the system startup file through TFTP.

```
Raisecom#download system1 tftp 192.168.1.1 ISCOM6820-roap_2.2.2_20130607
slot 3
```

Step 2 Write the configured file into the memory.

```
Raisecom#write startup-config
```

Step 3 Start the system1 file.

```
Raisecom#commit system1
```

Step 4 Restart the device and the device will automatically load the downloaded system startup file.

```
Raisecom#reboot
```

Checking results

Show OLT versions.

```
Raisecom#show version
   Product Name     : ISCOM6820
   Product Version  : P300R003C00
   ROAP Version     : 1.3
   System MAC Address: 000e.5e03.0158

   Slot ID: 3
      Card Type        : ISCOM6820EPSC
      Product  Version  : --
      System1  Version  : ISCOM6820EPSC_ROAP_2.2.2_20130607  (active)
(committed)
      System2  Version  : ISCOM6820EPSC_ROAP_2.2.2_20130607
      Bootrom  Version  : ISCOM6820EPSC_FLASH_BOOTROM_2.0.2_20130607
      CPLD     Version  : V1.0
      Mainrom1 Version  : ISCOM682EP0SC _FLASH_BOOTROM_2.0.2_20130607
   System   Uptime   : 0 days, 9 hours, 57 minutes
```

2 Configuring xGPON services

This chapter describes xGPON services and the configuration process of the device, and provides related configurations examples, including the following sections:

- Introduction
- Registration and deregistration
- Configuring xGPON interface
- Configuring key update
- Configuring ONU mirroring
- Configuring the adjustment value of Rx optical power
- Configuring alarm profile
- Configuring DBA profile
- Configuring line profile
- Configuring service profile
- Configuring rate limit profile
- Configuring TR069 management profile
- Managing laser-always-on ONUs
- Configuration examples

2.1 Introduction

2.1.1 Structure of the xGPON system

The Gigabit capable Passive Optical Network (GPON) system adopts the point-to-multipoint network topology structure, and uses fibers to implement full access high-speed transmission of data, voice, and video services.

A typical GPON network consists of three parts:

- Optical Line Terminal (OLT): the OLT is not only a switch or router, but also a multi-service provider platform. It provides optical interfaces for the Passive Optical Network (PON). It is the core component of the entire GPON system.

- Optical Network Unit (ONU) or Optical Network Termination (ONT): it is a user-side device in the PON system and provides users with various physical interfaces and bandwidth services.
- Optical Distribution Netwrok (ODN): it is composed of the Passive Optical Splitter (POS) and fibers. The POS is a passive device that connects the OLTs and ONUs, and its function is to distribute downstream data and centralize upstream data.

The GPON is a Gigabit Passive Optical Network (GPON) complying with ITU-T G.984.x series standards and specifications. The downlink rate can reach 1.2 or 2.4 Gbit/s, and the uplink rate can reach 155 Mbit/s, 622 Mbit/s, 1.2 Gbit/s, or 2.4 Gbit/s.

The XG(S)-Combo PON supports the ITU-T G.987.x standard XG-PON and the ITU-T G.9807.x standard XGS-PON. Each interface provides an uplink rate of 9.953 or 2.488 Gbit/s and a downlink rate of 9.953 Gbit/s.

2.1.2 Principles of the xGPON

The GPON adopts a single-fiber Wavelength Division Multiplexing (WDM) optical transmission method, following the wavelength allocation of 1310 nm for uplink and 1490 nm for downlink specified in ITU-T G.984.2. The XG(S)-Combo PON follows the XG-PON and XGS-PON of ITU-T G.987.x standards, with wavelength allocation of 1260–1280 nm for uplink and 1575–1580 for downlink. It transmits single-fiber bidirectional data with ONUs.

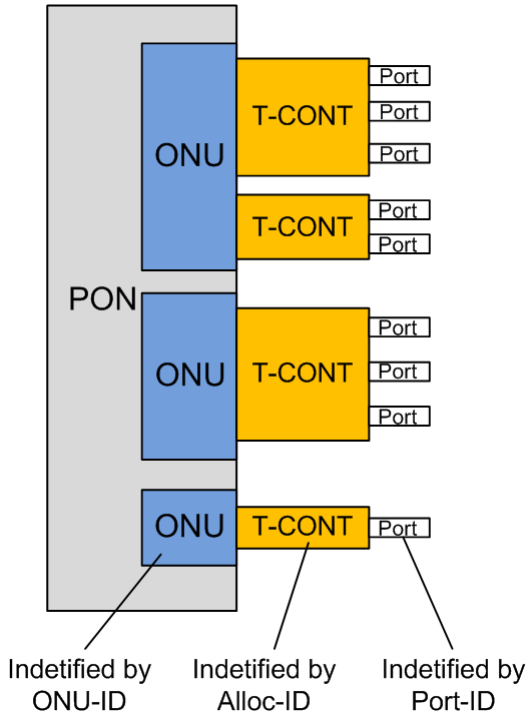
To separate signals from multiple users in the same fiber, the following two multiplexing techniques are used:

- The downlink data stream adopts the broadcast technology, and each ONU receives its own data, with a transmission rate of 2.4 Gbit/s.
- The uplink data stream adopts the TDMA technology, and each ONU sends data within a specific allocated timeslot, with a transmission rate of 1.2 Gbit/s.

2.1.3 Basic principles

The ISCOM6820 serves as an xGPON OLT, connected downstream to xGPON ONUs. It transmits GPON Encapsulation Method (GEM) frames with ONUs. GEM frames are identified by the GEM Port-ID, and are carried by the T-CONT in the uplink direction, as shown in Figure 2-1.

Figure 2-1 Multiplexing structure of the xGPON (GEM mode)



T-CONT

The XGPON uses T-CONT, which is the most basic control unit for upstream service flow in the xGPON system, to implement service aggregation. A T-CONT corresponds to a bandwidth type of the service flow. Each bandwidth type has its own QoS characteristics, which are mainly reflected in bandwidth guarantee. They are divided into fixed bandwidth, guaranteed bandwidth, guaranteed/non-guaranteed bandwidth, best effort forwarding, and hybrid methods (corresponding to type 1 to type 5 in Table 2-1).

Table 2-1 Available T-CONT types

Bandwidth type	Delaying sensitivity	Aoolcoation mode	T-CONT type				
			Type 1	Type 2	Type 3	Type 4	Type 5
Fixed	Yes	Provisioned	Yes	No	No	No	Yes
Assure	No	Provisioned	No	Yes	Yes	No	Yes
Non-assure	No	Dynamic	No	No	Yes	No	Yes
Best-effort	Yes	Dynamic	No	No	No	No	Yes

Each T-CONT is uniquely identified by Alloc-ID, with values ranging from 0 to 4095. The Alloc-ID is globally allocated by the OLT; in other words, each ONU under the OLT cannot use two T-CONTs of the same Alloc-ID.

GEM Port

Each T-CONT is composed of one or more GEM ports, and each GEM port carries a type of service flows. A T-CONT can carry different service flows of one or more GEM ports.

Each GEM port is identified by a unique Port ID, which ranges from 0 to 4095 and is globally allocated by the OLT. GEM ports with duplicate Port IDs cannot be used under the same PON interface.

The GEM port identifies the service virtual channel between the OLT and ONUs, which is the channel carrying service flows and is similar to the VPI/VCI ID in ATM virtual connections.

2.1.4 IPHOST functions

The IPhost interface configured on the ONU is equivalent to the upstream sub-interface on the ONU. It can be configured with IP-based services. The same IPhost interface can be configured with one or more services, such as broadband, IPTV, and voice. Its application scenarios include FTTH and FTTB.

2.2 Registration and deregistration

2.2.1 Default configurations

Default configurations of registration and deregistration on the ISCOM6820 are as below.

Function	Default value
ONU auto-discovery period	5s
ONU registration mode	SN

2.2.2 Registering ONU

Configuring ONU registration distance

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gpon-olt** *slot-id/olt-id*	Enter GPON interface configuration mode.
3	Raisecom(config-if-gpon-olt-*:*)#**distance min** *min-distance* **max** *max-distance*	Configure the range of ONU registration distance.

Configuring ONU auto-registration

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)#**interface gpon-olt** *slot-id/olt-id*	Enter GPON interface configuration mode.
3	Raisecom(config-if-gpon-olt-*:*)#**authorization mode none**	Configure the ONU to work in the auto-registration mode.

Creating ONU manually

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gpon-olt** *slot-id/olt-id*	Enter GPON interface mode.
3	Raisecom(config-if-gpon-olt-*:*)#**authorization mode** { **loid** | **loid-checkcode** | **sn** | **sn-password** | **password** | **hybrid** }	Configure the ONU registration mode. You can use the **no authorization mode** command to restore default configuration.
4	Raisecom(config-if-gpon-olt-*:*)# **create gpon-onu** [*onu-id*] **sn** *snstring* [**password** *password*] [**suspend**] { **line-profile-id** *line-profile-id* | **line-profile-name** *line-profile-name* } { **service-profile-id** *service-profile-id* | **service-profile-name** *service-profile-name* } [**onu_type** { **auto** | **xgpon** | **xgspon** | **gpon** }]	(Optional) create the ONU registered based on the SN or SN+password, and bind the corresponding line profile and service profile. You can use the **no create gpon-onu** *onu-id* command to delete the ONU.
	Raisecom(config-if-gpon-olt-*:*)# **create gpon-onu** [*onu-id*] **password** *password* [**suspend**] { **line-profile-id** *line-profile-id* | **line-profile-name** *line-profile-name* } { **service-profile-id** *service-profile-id* | **service-profile-name** *service-profile-name* } [**onu_type** { **auto** | **xgpon** | **xgspon** | **gpon** }]	(Optional) create the ONU registered based on the password, and bind the corresponding line profile and service profile. You can use the **no create gpon-onu** *onu-id* command to delete the ONU.
	Raisecom(config-if-gpon-olt-*:*)# **create gpon-onu** [*onu-id*] **loid** *loid* [**checkcode** *checkcode*] [**suspend**] { **line-profile-id** *line-profile-id* | **line-profile-name** *line-profile-name* } { **service-profile-id** *service-profile-id* | **service-profile-name** *service-profile-name* } [**onu_type** { **auto** | **xgpon** | **xgspon** | **gpon** }]	(Optional) create the ONU registered based LOID or LOID+checkcode, and bind the corresponding line profile and service profile. You can use the **no create gpon-onu** *onu-id* command to delete the ONU.
	Raisecom(config-if-gpon-olt-*:*)#**create gpon-onu** [*onu-id*] **sn** *snstring*	(Optional) create an ONU based on SN or ID.

2.2.3 Deregistering ONU

You can enable the ONU to resend the registration request by deregistering it, which is usually used in engineering maintenance. If you suspect the logical link of an ONU working improperly, you can resume it through deregistration.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface gpon-onu` *slot-id/olt-id/onu-id*	Enter GPON ONU virtual interface configuration mode.
3	`Raisecom(config-if-gpon-onu-*/*:*)#deregister`	Configure ONU deregistration.

2.2.4 Activating ONUs

Activating all ONUs

You can activate all ONUs at a time under a PON interface on the OLT.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface gpon-olt` *slot-id/olt-id*	Enter GPON interface configuration mode.
3	`Raisecom(config-if-gpon-olt-*:*)#active all-suspend-onu`	Activate all ONUs which are in suspended status. **Note** After the ONU is activated, it will restart the registration process.

Activating single ONU

You can activate or suspend a single ONU on the OLT.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface gpon-onu` *slot-id/olt-id/onu-id*	Enter GPON ONU virtual interface configuration mode.
3	`Raisecom(config-if-gpon-onu-*/*:*)#state { active | suspend }`	Activate or suspend the ONU.

2.2.5 Clearing information about the illegal ONU

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gpon-olt** *slot-id/olt-id*	Enter GPON interface configuration mode.
3	Raisecom(config-if-gpon-olt-*:*)#**clear illegal-onu**	Clear information about illegal ONUs.

2.2.6 Configuring key words for ONU registration

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gpon-onu** *slot-id/olt-id/onu-id*	Enter GPON ONU virtual interface configuration mode.
3	Raisecom(config-if-gpon-onu-*/*:*)#**rebind sn** *sn*	(Optional) configure the key word for registering ONUs based on SN.
4	Raisecom(config-if-gpon-onu-*/*:*)#**password** *password*	(Optional) configure the key word for registering ONUs based on password.
5	Raisecom(config-if-gpon-onu-*/*:*)#**loid checkcode** *checkcode*	(Optional) configure the key word for registering ONUs based on LOID.
6	Raisecom(config-if-gpon-onu-*/*:*)#**mng-mode omci**	(Optional) configure the mode for managing ONUs.

2.2.7 Checking configurations

No.	Command	Description
1	Raisecom#**show interface gpon-olt** *slot-id/olt-id* **auth information**	Show information about ONU registration under a GPON interface.
2	Raisecom#**show interface gpon-onu** *slot-id/olt-id/onu-id* **sn**	Show information about SN-based ONU registration.
3	Raisecom#**show interface gpon-onu** *slot-id/olt-id/onu-id* **loid**	Show information about LOID-based ONU registration.
4	Raisecom#**show interface gpon-onu** *slot-id/olt-id/onu-id* **creation-information**	Show ONU registration information.
5	Raisecom#**show interface gpon-onu** *slot-id/olt-id/onu-id* **online-information**	Show ONU online information.
6	Raisecom#**show interface gpon-olt** *slot-id/olt-id* **illegal-onu**	Show information about illegally registered ONUs under the OLT GPON interface.

No.	Command	Description
7	Raisecom#**show interface gpon-onu** [*slot-id/olt-id/onu-list*] **description-information**	Show the ONU description.
8	Raisecom#**show interface gpon-onu** [*slot-id/olt-id/onu-list*] **download-information**	Show the loaded configurations of the ONU.

2.3 Configuring xGPON interface

2.3.1 Default configurations

Default configurations of the xGPON interface on the ISCOM6820 are as below.

Function	Default value
FEC in downstream direction	• GPON interface: disable • XGPON/XGSPON interface: enable
xGPON interface bound alarm profile	1
GEM port used by broadcast, unknown multicast, and unknown unicast packets	• Braodcast packets on the GPON interface: 4095 • Braodcast packets on the XGSPON interface: 5119
GEM port used by multicast packets	• Multicast packets on the GPON interface: 4094 • Multicast packets on the XGSPON interface: 5118
GPON interface end-to-end access	Disable

2.3.2 Configuring interfaces

Configure the GPON interface as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gpon-olt** *slot-id/olt-id*	Enter GPON interface configuration mode.
3	Raisecom(config-if-gpon-olt-*:*)#**fec** { **enable** | **disable** }	(Optional) enable/disable FEC on the GPON interface in downlink direction.

Configure the GPON ONU interface as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gpon-onu** *slot-id/olt-id/onu-id*	Enter GPON ONU virtual interface configuration mode.
3	Raisecom(config-if-gpon-onu-*/*:*)#**vlan dot1q-tunnel broadcast gemport** *gemport-id*	Configure the GEM interface used by broadcast packets of the GPON interface.
4	Raisecom(config-if-gpon-onu-*/*:*)# **multicast gemport** *port-id*	Configure the GEM interface used by multicast packets of the GPON interface.
5	Raisecom(config-if-gpon-onu-*/*:*)# **dba-mode** { **normal** | **extended** }	Configure the DBA mode of the GPON interface.

2.3.3 Checking configurations

No.	Command	Description
1	Raisecom#**show interface gpon-olt** *slot-id/olt-id* **basic information**	Show configurations of the GPON interface.
2	Raisecom#**show interface gpon-onu** *slot-id/olt-id/onu-id* **gemport** *gem* **vlan**	Show configurations of the GEM VLAN on the ONU.
3	Raisecom#**show interface gpon-olt** *slot-id/olt-id* { **upstream** | **downstream** } **ni statistics**	Show statistics on traffic of uplink interfaces and downlink interfaces of the chip.
4	Raisecom#**show gemport-tcont current-use-count**	Show the number of GEM interfaces and the number of TCONT used by the entire device.

2.4 Configuring key update

2.4.1 Default configurations

Default configurations of the OLT alarm profile with a default ID of 1 on the ISCOM6820 are as below.

Function	Default value
Key update	Disable
Key update period	30s

2.4.2 Configuring key update

No.	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**encryption gpon-slot** *slot-id* **key-update** { **enable** | **disable** }	Enable/Disable key update.
3	Raisecom(config)#**encryption gpon-slot** *slot-id* **key-update-period** *time*	(Optional) configure the period for updating the key.

2.4.3 Checking configurations

No.	Command	Description
1	Raisecom#**show gpon-slot** *slot-id* **encryption key-update**	Show configurations of key update.

2.5 Configuring ONU mirroring

2.5.1 Configuring ONU mirroring

No.	Command	Description
1	Raisecom#active { **system1** | **system2** } **gpon-onu** *slot-id/olt-id/onu-list*	Activate ONU mirroring.
2	Raisecom#**commit** { **system1** | **system2** } **gpon-onu** *slot-id/olt-id/onu-list*	Configure the ONU system as the major system.

2.6 Configuring the adjustment value of Rx optical power

2.6.1 Configuring the adjustment value of Rx optical power

No.	Command	Description
1	Raisecom#**gpon-onu** *slot-id/olt-id/onu-id* { **onu-rx-olt-power** | **olt-rx-onu-power** } { **decrease** | **increase** } *value* [**decimal** *decimal-value*]	Configure the adjustment value of Rx optical power.

2.6.2 Checking configurations

No.	Command	Description
1	Raisecom#**show gpon-onu** { **olt-rx-onu-power** | **onu-rx-olt-power** }	Show the adjustment value of Rx optical power.

2.7 Configuring alarm profile

2.7.1 Default configurations

Default configurations of the OLT alarm profile with a default ID of 1 on the ISCOM6820 are as below.

Function	Default value
Alarm profile ID	1
Alarm profile name	profile-1
All alarm	Enable
PON interface LOF alarm	Disable
ONU LOF alarm	Disable
ONU LOS alarm	Disable
ONU window drift alarm	Disable
ONU remote indication alarm	Disable
ONU Ploam loss alarm	Disable
ONU GEM delineation loss alarm	Disable
ONU acknowledgement loss alarm	Disable
ONU signal degradation alarm	Disable
ONU signal degradation alarm threshold	5
ONU signal failure alarm	Disable
ONU signal failure alarm threshold	4
ONU physical equipment error alarm	Disable
ONU key update error alarm	Disable
ONU transmission layer warning	Disable
ONU transmission layer alarm	Disable
ONU registration failure alarm	Enable

Function	Default value
ONU laser-always-on alarm	Disable
ONU laser-always-on alarm threshold	12

2.7.2 Configuring OLT alarm profile

Configuring OLT alarm profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-trap-gpon-olt-profile** *profile-id*	Create the OLT alarm profile and enter OLT alarm profile configuration mode. You can use the **no snmp-trap-gpon-olt-profile** *profile-id* command to delete the profile. **Note** • If the profile exists, enter profile configuration mode directly. • If the profile does not exist, you need to create the profile first, and then enter profile configuration mode.
3	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**name** *profile-name*	(Optional) configure the name of the OLT alarm profile.
4	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**all-trap** { **enable** | **disable** }	(Optional) enable/disable all alarms.
5	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**pon-upstream-frame-loss** { **enable** | **disable** }	(Optional) enable/disable uplink LOF alarm on the PON interface.
6	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**onu-upstream-frame-loss** { **enable** | **disable** }	(Optional) enable/disable uplink LOF alarm on the ONU.
7	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**onu-signal-loss** { **enable** | **disable** }	(Optional) enable/disable ONU LOS alarm.
8	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**onu-window-drift** { **enable** | **disable** }	(Optional) enable/disable ONU window drift alarm.
9	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**onu-remote-defect-indication** { **enable** | **disable** }	(Optional) enable/disable ONU remote indication alarm.

Step	Command	Description
10	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**onu-ploam-loss** { **enable** | **disable** }	(Optional) enable/disable ONU Ploam loss alarm.
11	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**onu-gem-channel-delineatin-loss** { **enable** | **disable** }	(Optional) enable/disable ONU GEM delineation loss alarm.
12	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**onu-acknowledge-loss** { **enable** | **disable** }	(Optional) enable/disable ONU acknowledgement loss alarm.
13	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**onu-signal-degraded** { **enable** | **disable** }	(Optional) enable/disable ONU signal degradation alarm.
14	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**onu-signal-degraded threshold** *value*	(Optional) configure ONU signal degradation alarm threshold.
15	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**onu-signal-failure** { **enable** | **disable** }	(Optional) enable/disable ONU signal failure alarm.
16	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**onu-signal-failure threshold** *value*	(Optional) configure ONU signal failure alarm threshold.
17	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**onu-physical-quipment-error** { **enable** | **disable** }	(Optional) enable/disable ONU physical equipment error alarm.
18	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**onu-key-loss** { **enable** | **disable** }	(Optional) enable/disable ONU key update error alarm.
19	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**onu-transmission-interference-warning** { **enable** | **disable** }	(Optional) enable/disable ONU transmission layer warning.
20	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**onu-transmission-interference-alarm** { **enable** | **disable** }	(Optional) enable/disable ONU transmission layer alarm.
21	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**onu-auth-failed** { **enable** | **disable** }	(Optional) enable/disable ONU registration failure alarm.
22	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**onu-laster-always-on** { **enable** | **disable** }	(Optional) enable/disable ONU laser-always-on alarm.
23	Raisecom(config-snmp-trap-gpon-olt-profile:*)#**onu-laster-always-on threshold** *value*	(Optional) configure ONU laser-always-on alarm threshold.

Binding profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gpon-olt** *slot-id/olt-id*	Enter GPON interface configuration mode.
3	Raisecom(config-if-gpon-olt-*:*)#**snmp-trap-gpon-olt-profile** *profile-id*	Configure the GPON interface bound alarm profile.

2.7.3 Configuring ONU profile

Configuring ONU profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-trap-gpon-onu-profile** *profile-id*	Create the ONU alarm profile and enter ONU alarm profile configuration mode.
3	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**name** *profile-name*	(Optional) configure the name of the ONU alarm profile.
4	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**gemport-lost-packets threshold** *value*	(Optional) configure GEM port packet loss alarm threshold.
5	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**gemport-misinserted-packets threshold** *value*	(Optional) configure GEM port packet mis-transmission alarm threshold.
6	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**gemport-impaired-blocks threshold** *value*	(Optional) configure GEM port impaired data block alarm threshold.
7	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**ethernet-fcs-error-packets threshold** *value*	(Optional) configure FCS error frame alarm threshold.
8	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**ethernet-excessive-collision-packets threshold** *value*	(Optional) configure excessive collision frame alarm threshold.
9	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**ethernet-late-collision-counter threshold** *value*	(Optional) configure Tx delay collision alarm threshold.
10	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**ethernet-too-long-packets threshold** *value*	(Optional) configure oversized frame alarm threshold.
11	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**ethernet-rx-buffer-overflow-counter threshold** *value*	(Optional) configure Rx buffer overflow alarm threshold.
12	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**ethernet-tx-buffer-overflow-counter threshold** *value*	(Optional) configure Tx buffer overflow alarm threshold.

Step	Command	Description
13	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**ethernet-single-collision-packets threshold** *value*	(Optional) configure single-collision Tx frame alarm threshold.
14	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**ethernet-multiple-collision-packets threshold** *value*	(Optional) configure multi-collision Tx frame alarm threshold.
15	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**ethernet-sqe-counter threshold** *value*	(Optional) configure synchronous queue element test error alarm threshold.
16	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**ethernet-deferred-transmission-packets threshold** *value*	(Optional) configure delay frame alarm threshold.
17	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**ethernet-internal-mac-tx-error-packets threshold** *value*	(Optional) configure alarm threshold of Tx failure frame due to MAC sub-layer transmission error.
18	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**ethernet-carrier-sense-error-counter threshold** *value*	(Optional) configure carrier sense loss error alarm threshold.
19	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**ethernet-alignment-error-packets threshold** *value*	(Optional) configure unaligned frame alarm threshold.
20	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**ethernet-internal-mac-rx-error-packets threshold** *value*	(Optional) configure alarm threshold of Rx failure frame due to MAC sub-layer receiving error.
21	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**ethernet-pppoe-filter-packets threshold** *value*	(Optional) configure alarm threshold of discarded frame due to PPPoE frame filtering.
22	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**ethernet-drop-event-counter threshold** *value*	(Optional) configure alarm threshold of discarded frame event due to resource shortage.
23	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**ethernet-undersize-packets threshold** *value*	(Optional) configure undersized frame alarm threshold.
24	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**ethernet-fragments-packets threshold** *value*	(Optional) configure fragment alarm threshold.
25	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**ethernet-jabbers-packets threshold** *value*	(Optional) configure Jabber frame alarm threshold.
26	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**mac-bridge-port-delay-exceeded-discard-packets threshold** *value*	(Optional) configure alarm threshold of discarded frame due to timeout.
27	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**mac-bridge-port-mtu-exceeded-discard-packets threshold** *value*	(Optional) configure alarm threshold of discarded frame due to oversized MTU.
28	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**mac-bridge-port-rx-error-discard-packets threshold** *value*	(Optional) configure Rx error frame alarm threshold.

Step	Command	Description
29	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**fec-corrected-bytes threshold** *value*	(Optional) configure FEC corrected byte alarm threshold.
30	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**fec-corrected-code-words threshold** *value*	(Optional) configure FEC corrected code word alarm threshold.
31	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**fec-uncorrected-code-words threshold** *value*	(Optional) configure FEC corrected code word alarm threshold.
32	Raisecom(config-gpon-onu-snmp-trap-profile:*)#**fec-seconds threshold** *value*	(Optional) configure FEC duration alarm threshold.

Binding ONU profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu** *slot-id/olt-id/onu-id*	Enter GPON ONU remote management configuration mode.
3	Raisecom(config-gpon-onu-*/*:*)#**snmp-trap-gpon-onu-profile** *profile-id*	Configure the ONU bound alarm profile.

2.7.4 Checking configurations

No.	Command	Description
1	Raisecom#**show snmp-trap-gpon-olt-profile** *profile-id*	Show OLT alarm profile configurations.
2	Raisecom#**show interface gpon-olt** *slot-id/olt-list* **basic information**	Show binding relationship between the OLT GPON interface and alarm profile.
3	Raisecom#**show snmp-trap-gpon-onu-profile** { **all** | *profile-list* }	Show ONU alarm profile configurations.
4	Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **snmp-trap-profile**	Show binding relationship between the ONU and alarm profile.

2.8 Configuring DBA profile

2.8.1 Default configurations

Default configurations of the DBA profile with a default ID of 1 on the ISCOM6820 are as below.

Function	Default value
DBA profile ID	1
DBA profile name	Profile-1
DBA profile type	Type 3
Fixed bandwidth	0 kbit/s
Assured bandwidth	1024 kbit/s
Maximum bandwidth	1024000 kbit/s

2.8.2 Creating DBA profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**create dba-profile** *profile-id* **name** *profile-name* **type1 fix** *fix-bandwidth*	Create the DBA profile of the fixed bandwidth type. You can use the **no create dba-profile** *profile-id* command to delete the profile.
	Raisecom(config)#**create dba-profile** *profile-id* **name** *profile-name* **type2 assure** *assure-bandwidth*	Create the DBA profile of the assured bandwidth type. You can use the **no create dba-profile** *profile-id* command to delete the profile.
	Raisecom(config)#**create dba-profile** *profile-id* **name** *profile-name* **type3 assure** *assure-bandwidth* **max** *max-bandwidth*	Create the DBA profile of the assured bandwidth+maximum bandwidth type. You can use the **no create dba-profile** *profile-id* command to delete the profile.
	Raisecom(config)#**create dba-profile** *profile-id* **name** *profile-name* **type4 max** *max-bandwidth*	Create the DBA profile of the maximum bandwidth type. You can use the **no create dba-profile** *profile-id* command to delete the profile.
	Raisecom(config)#**create dba-profile** profile-id **name** profile-name **type5 fix** fix-bandwidth **assure** assure-bandwidth **max** max-bandwidth	Create the DBA profile of the fixed bandwidth+assured bandwidth+maximum bandwidth type. You can use the **no create dba-profile** *profile-id* command to delete the profile.

Note

The profile in use cannot be deleted.

2.8.3 Modifying DBA profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)#**dba-profile** *profile-id* **name** *profile-name*	Modify the name of the DBA profile.
	Raisecom(config)#**dba-profile** *profile-id* **type1 fix** *fix-bandwidth*	Modify the DBA profile of the fixed bandwidth type.
	Raisecom(config)#**dba-profile** *profile-id* **type2 assure** *assure-bandwidth*	Modify the DBA profile of the assured bandwidth type.
	Raisecom(config)#**dba-profile** *profile-id* **type3 assure** *assure-bandwidth* **max** *max-bandwidth*	Modify the DBA profile of the assured bandwidth+maximum bandwidth type.
	Raisecom(config)#**dba-profile** *profile-id* **type4 max** *max-bandwidth*	Modify the DBA profile of the maximum bandwidth type.
	Raisecom(config)#**dba-profile** *profile-id* **type5 fix** *fix-bandwidth* **assure** *assure-bandwidth* **max** *max-bandwidth*	Modify the DBA profile of the fixed bandwidth+assured bandwidth+maximum bandwidth type.

Note

- The profile to be modified must exist.
- The profile in use cannot be modified.

2.8.4 Checking configurations

No.	Command	Description
1	Raisecom#**show dba-profile** { **all** | *profile-list* }	Show DBA profile configurations.

2.9 Configuring line profile

2.9.1 Default configurations

N/A

2.9.2 Configuring line profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)#**gpon-onu-line-profile** *profile-id*	Create the line profile and enter line profile configuration mode. You can use the **no gpon-onu-line-profile** *profile-id* command to delete the profile. **Note** • If the profile exists, enter profile configuration mode directly. • If the profile does not exist, you need to create the profile first, and then enter profile configuration mode.
3	Raisecom(config-gpon-onu-line-profile:*)#**name** *profile-name*	(Optional) configure the profile name.
4	Raisecom(config-gpon-onu-line-profile:*)#**omcc encryption** { **enable** | **disable** }	(Optional) enable/disable OMCC encryption.
5	Raisecom(config-gpon-onu-line-profile:*)#**fec upstream** { **enable** | **disable** }	(Optional) enable FEC on the uplink channel.
6	Raisecom(config-gpon-onu-line-profile:*)#**create gem** *gem-index* **tcont** *tcont-id*	(Optional) create a GEM port, and configure its binding relation with T-CONT. You can use the **no create gem** *gem-index* command to delete the configuration.
7	Raisecom(config-gpon-onu-line-profile:*)#**mapping mode** { **vlan** | **vlan-pri** | **pri** | **port** | **port-vlan** | **port-pri** | **port-vlan-pri** }	(Optional) configure the mapping between the GEM port and services.
8	Raisecom(config-gpon-onu-line-profile:*)#**gem** *gem-index* **mapping** *mapping-index* { **vlan** *vlan-id* [**priority** *pri*] } | **priority** *pri* | **ethernet** *port-id* | **ip-host** *port-id* | **ethernet** *port-id* **vlan** *vlan-id* [**priority** *pri*] | **ethernet** *port-id* **priority** *pri* }	(Optional) configure the mapping between the GEM port and ONU-side services. You can use the **no gem** *gem-index* **mapping** *mapping-index* command to delete the mapping.
9	Raisecom(config-gpon-onu-line-profile:*)#**gem** *gem-index* **mac-address-learning limit** *count*	(Optional) configure MAC address learning limit on the GEM port. You can use the **no gem** *gem-index* **mac-address-learning limit** command to restore default configuration.
10	Raisecom(config-gpon-onu-line-profile:*)#**create tcont** *tcont-id* **dba-profile** *profile-id*	(Optional) create a T-CONT, and configure its binding relationship with the DBA profile. You can use the **no create tcont** *tcont-id* command to delete the configuration.
11	Raisecom(config-gpon-onu-line-profile:*)#**tcont** *tcont-id* **dba-profile** *profile-id*	(Optional) modify the DBA profile bound to TCONT.

Step	Command	Description
12	Raisecom(config-gpon-onu-line-profile:*)# **gem** *gem-index* **encryption** { **enable** | **disable** } **encryption-us** { **enable** | **disable** }	(Optional) enable/disable GEM port encryption.
13	Raisecom(config-gpon-onu-line-profile:*)#**gem** *gem-index* { **upstream** | **downstream** } **policing-profile** *profile-id* Raisecom(config-gpon-onu-line-profile:*)#**gem** *gem-index* { **upstream** | **downstream** } **policing-profile-name** *profile-name*	(Optional) bind the GEM port with the rate limiting profile to limit the rate of the GEM port.
14	Raisecom(config-gpon-onu-line-profile:*)#**gem** *gem-index* **priority-queue** *priority-queue-id*	(Optional) modify the priority queue of the GEM port.

Configure the device that needs to enter the line profile with the template name as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu-line-profile name** *profile-name* Raisecom(config-gpon-onu-line-profile:*)#	Enter line profile configuration mode through the profile name.

2.9.3 Binding line profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gpon-onu** *slot-id/olt-id/onu-id*	Enter GPON ONU virtual interface mode.
3	Raisecom(config-if-gpon-onu-*/*:*)#**line-profile-id** *profile-id*	(Optional) change the line profile configured on the ONU by modifying the line profile ID.
	Raisecom(config-if-gpon-onu-*/*:*)#**line-profile-name** *profile-name*	(Optional) change the line profile configured on the ONU by modifying the line profile name.

Note

- When you change the line profile configured on the ONU by modifying the line profile ID, the system will automatically update the profile name to make it consistent with the new profile.

- When you change the line profile configured on the ONU by modifying the line profile name, the system will automatically update the profile ID to make it consistent with the new profile.

2.9.4 Checking configurations

No.	Command	Description
1	Raisecom#**show gpon-onu-line-profile** { **all** | *profile-list* }	Show configurations of the line profile.

2.10 Configuring service profile

2.10.1 Default configurations

N/A

2.10.2 Configuring profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu-service-profile** *profile-id*	Create a service profile and enter service profile configuration mode. You can use the **no gpon-onu-service-profile** *profile-id* command to delete the template. **Note** • If the template exists, the system will directly enter template configuration mode. • If the template does not exist, the system will create a template before entering template configuration mode.
3	Raisecom(config-gpon-onu-service-profile:*)#**name** *profile-name*	(Optional) configure the name of the service profile.
4	Raisecom(config-gpon-onu-service-profile:*)#**port-num** { **ethernet** *eth-id* [**pots** *pots-id*] | **pots** *pots-id* | **veip** *veip-id* }	(Optional) configure the number of ONU interfaces.
5	Raisecom(config-gpon-onu-service-profile:*)#**mac-address-table learning** { **enable** | **disable** }	(Optional) enable/disable dynamic MAC address learning on the ONU.
6	Raisecom(config-gpon-onu-service-profile:*)#**mac-address-table learning aging-time** *time*	(Optional) configure the aging time of the dynamic MAC addresses on the ONU.

Step	Command	Description
7	Raisecom(config-gpon-onu-service-profile:*)#**switchport isolation** { **enable** | **disable** }	(Optional) enable/disable ONU UNI isolation.
8	Raisecom(config-gpon-onu-service-profile:*)#**mac-address-table dlf discard** { **enable** | **disable** }	(Optional) enable/disable ONU DLF packet discarding.
9	Raisecom(config-gpon-onu-service-profile:*)#**mac-address-table aging-time** *aging-time*	(Optional) configure the aging time of the service profile MAC address table.
10	Raisecom(config-gpon-onu-service-profile:*)#{ **uni ethernet** *uni-list* | **veip** *id* } **immediate-leave enable**	(Optional) enable immediate leave on the ONU Ethernet interface or VEIP interface. You can use the **disable** form to disable this function.
11	Raisecom(config-gpon-onu-service-profile:*)#{ **uni ethernet** *uni-list* | **veip** *id* } **unauth-join enable**	(Optional) configure unauthenticated join of the ONU Ethernet interface or VEIP interface. You can use the **disable** form to disable this function.
12	Raisecom(config-gpon-onu-service-profile:*)#**multicast vlan translation** *vlan-id*	(Optional) configure the destination VLAN ID for the ONU to translate downlink multicast VLAN.
13	Raisecom(config-gpon-onu-service-profile:*)#**uni ethernet** *uni-id* **vlan mode** { **transparent** | **tagged** | **translation** | **aggregation** | **trunk** }	(Optional) configure the VLAN mode of the ONU UNI. You can use the **no uni ethernet uni-id vlan mode** command to restore default configuration.
14	Raisecom(config-gpon-onu-service-profile:*)#**uni ethernet** *uni-id* **native vlan** *vlan-id* [*priority*]	(Optional) configure the default VLAN ID of the ONU UNI. You can use the **no uni ethernet uni-id native vlan** command to restore default configuration.
15	Raisecom(config-gpon-onu-service-profile:*)#**uni ethernet** *uni-id* **vlan translation-rule** *rule-id*	(Optional) configure the VLAN mapping rule of the ONU UNI. You can use the **no uni ethernet uni-id vlan translation-rule** command to restore default configuration.
16	Raisecom(config-gpon-onu-service-profile:*)#**uni ethernet** *uni-id* **vlan aggregation-rule** *rule-id*	(Optional) configure the VLAN aggregation rule of the ONU UNI. You can use the **no uni ethernet uni-id vlan aggregation-rule** command to restore default configuration.
17	Raisecom(config-gpon-onu-service-profile:*)#**uni ethernet** *uni-id* **vlan trunk allowed** *vlan-list*	(Optional) configure the list of VLANs allowed to pass by the ONU UNI in Trunk mode. You can use the **no uni ethernet uni-id vlan trunk allowed** command to restore default configuration.
18	Raisecom(config-gpon-onu-service-profile:*)#**uni ethernet** *uni-id* **mac-address-table threshold** { *value* | **unlimited** }	(Optional) configure the MAC address limit on the ONU UNI. You can use the **no uni ethernet uni-id mac-address-table threshold** command to restore default configuration.

Step	Command	Description
19	Raisecom(config-gpon-onu-service-profile:*)#**uni ethernet** *uni-id* **max-frame-size** *size*	(Optional) configure the maximum frame size allowed to pass by the ONU UNI. You can use the **no uni ethernet uni-id max-frame-size** command to restore default configuration.
20	Raisecom(config-gpon-onu-service-profile:*)#**uni ethernet** *uni-id* { **ingress** | **egress** } **policing-profile** *profile-id*	(Optional) bind a rate limiting profile with the ONU UNI. You can use the **no uni ethernet uni-id** { **ingress** | **egress** } **policing-profile** command to restore default configuration.
21	Raisecom(config-gpon-onu-service-profile:*)#**uni ethernet** *id* **vlan drop-untagged enable**	(Optional) enable the VLAN of the ONU Ethernet interface to discard untagged packets. You can use the **disable** form to disable this function.
22	Raisecom(config-gpon-onu-service-profile:*)#**uni ethernet** *id* **vlan dot1q-tunnel enable**	(Optional) enable Tunnel on the ONU Ethernet interface. You can use the **disable** form to disable this function.
23	Raisecom(config-gpon-onu-service-profile:*)#**uni ethernet vlan dot1q-tunnel enable**	(Optional) enable the service profile to enable Tunnel on the Ethernet interface. You can use the **disable** form of this command to disable this function.
24	Raisecom(config-gpon-onu-service-profile:*)#**uni ethernet** *uni-list* **pre-alloc-vlan-num** *vlan-num*	(Optional) configure the number of pre-assigned VLANs on the ONU UNI.
25	Raisecom(config-gpon-onu-service-profile:*)#**veip** *veip-id* **tr-069-profile** *profile-id*	(Optional) bind the service profile with the TR069 template.
26	Raisecom(config-gpon-onu-service-profile:*)#**veip** *veip-id* **iphost** *iphost-id*	(Optional) bind the service profile with the specified IPHost interface.
27	Raisecom(config-gpon-onu-service-profile:*)#**iphost-num** *iphost-num*	(Optional) configure the maximum number of IPHost interfaces.
28	Raisecom(config-gpon-onu-service-profile:*)#**iphost index mode** { **dhcp** | **pppoe** | **static** }	(Optional) configure the internet access mode of the IPHost interface.
29	Raisecom(config-gpon-onu-service-profile:*)#**iphost** *index* **native vlan** *id* [*priority*]	(Optional) configure the local VLAN of the IPHost interface.
30	Raisecom(config-gpon-onu-service-profile:*)#**iphost** *index* **pre-alloc-vlan-num** *num*	(Optional) configure the number of pre-assigned VLANs on the IPHost interface.
31	Raisecom(config-gpon-onu-service-profile:*)#**iphost** *index* **service** { **internet** | **iptv** | **voip-sinalling** | **voip-media** | **management** }*	(Optional) configure the service type of the IPHost interface.
32	Raisecom(config-gpon-onu-service-profile:*)#**voip-protocol** { **sip** | **h248** }	(Optional) configure the voice protocol type of the service profile.

Step	Command	Description
33	Raisecom(config-gpon-onu-service-profile:*)#**country-code** { *num* | **china** | **undefine** }	(Optional) configure the country code of the service profile.
34	Raisecom(config-gpon-onu-service-profile:*)#**time-zone** { *num* | **beijing** | **undefine** }	(Optional) configure the time zone code of the service profile.
35	Raisecom(config-gpon-onu-service-profile:*)# **iphost** *index* **access-control** { **http**| **https** | **ping** | **telnet** } { **enable** | **disable** }	Configure the access control mode of the IPHost interface based on WAN connection.
36	Raisecom(config-gpon-onu-service-profile:*)# **iphost** *index* **service mode bridge cos** *cos* **portlist** *list* **ssidlist** *list* Raisecom(config-gpon-onu-service-profile:*)#**iphost** *index* **service mode hybrid [nat { enable | disable }] cos** *cos* **portlist** *list* **ssidlist** *list* Raisecom(config-gpon-onu-service-profile:*)#**iphost** *index* **service mode route [nat { enable | disable }] cos** *cos* **portlist** *list* **ssidlist** *list*	Configure the service working mode of the IPHost interface.
37	Raisecom(config-gpon-onu-service-profile:*)#**iphost** *index* **type** { **ipv4** | **ipv6** | **both** }	Configure the IP address type of the IPHost.
38	Raisecom(config-gpon-onu-service-profile:*)#**domain** *bakname*] Raisecom(config-gpon-onu-service-profile:*)#**manage-server iphost** *index* **no primary-domain** [**no backup-domain** | **backup-domain** *bakname*]	(Optional) configure the master/slave domain name of the IPHost interface on the management server.

2.10.3 Configuring multicast services in service profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu-service-profile** *profile-id*	Enter service profile configuration mode.
3	Raisecom(config-gpon-onu-service-profile:*)#{ **uni ethernet** *uni-list* | **veip** *id* } **work-mode** { **multicast-ctrl** | **normal** }	(Optional) enable the working mode of the ONU Ethernet interface or VEIP interface.

Step	Command	Description
4	Raisecom(config-gpon-onu-service-profile:*)#{ **uni ethernet** *uni-list* | **veip** *id* } **igmp-forward** { **translation** *vlan-id* [*priority*] | **transparent** | **tag** *vlan-id* [*priority*] }	(Optional) configure the policy for the ONU Ethernet interface or VEIP interface to process packets of the uplink multicast VLAN.
5	Raisecom(config-gpon-onu-service-profile:*)#{ **uni ethernet** *uni-list* | **veip** *id* } **multicast vlan** { **strip** | **transparent** | **translation** *vlan-id* }	(Optional) configure the policy for the ONU Ethernet interface or VEIP interface to process packets of the downlink multicast VLAN. You can use the **no { uni ethernet uni-list | veip id }multicast vlan** command to restore default configuration.
6	Raisecom(config-gpon-onu-service-profile:*)#{ **uni ethernet** *uni-list* | **veip** *id* } **igmp-version** { **v2** | **v3** }	(Optional) configure the IGMP version of the ONU Ethernet interface or VEIP interface.
7	Raisecom(config-gpon-onu-service-profile:*)#{ **uni ethernet** *uni-list* | **veip** *id* } **mcast-vlan** *vlan-list*	(Optional) configure the controllable multicast VLAN list of the ONU Ethernet interface or VEIP interface.
8	Raisecom(config-g pon-onu-service-profile:*)#**uni ethernet** *uni-list* **mctrl package** *package-list*	(Optional) configure controllable multicast package binding of the ONU UNI.
9	Raisecom(config-gpon-onu-service-profile:*)#{ **uni ethernet** *uni-list* | **veip** *id* } **unauth-join** { **enable** | **disable** }	(Optional) configure unauthenticated join of the ONU Ethernet interface or VEIP interface.

2.10.4 Entering profile with profile name

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu-service-profile** *profile-id*	Create a service profile and enter service profile configuration mode. You can use the **no gpon-onu-service-profile** *profile-id* command to delete this template.
3	Raisecom(config-gpon-onu-service-profile:*)#**name** *profile-name*	Configure the profile name.
4	Raisecom(config-gpon-onu-service-profile:*)#**exit** Raisecom(config)#**gpon-onu-service-profile name** *profile-name*	Enter service profile configuration mode through the profile name.

2.10.5 Binding service profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)#**interface gpon-onu** *slot-id/olt-id/onu-id*	Enter GPON ONU virtual interface mode.
3	Raisecom(config-if-gpon-onu-*/*:*)#**service-profile-id** *profile-id*	(Optional) change the service profile configured on the ONU by modifying the service profile ID.
	Raisecom(config-if-gpon-onu-*/*:*)#**service-profile-name** *profile-name*	(Optional) change the service profile configured on the ONU by modifying the service profile name.

Note

- When you change the service profile configured on the ONU by modifying the service profile ID, the system will automatically update the profile name to make it consistent with the new profile.
- When you change the service profile configured on the ONU by modifying the service profile name, the system will automatically update the profile ID to make it consistent with the new profile.

2.10.6 Checking configurations

No.	Command	Description
1	Raisecom#**show gpon-onu-service-profile** { **all** | *profile-list* }	Show configurations of the service profile.

2.11 Configuring rate limit profile

2.11.1 Default configuration

N/A

2.11.2 Configuring profile

No.	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**create policing-profile** *profile-id* **name** *profile-name*	Create a rate limit profile. You can use the **no create policing-profile** *profile-id* command to delete the profile.
3	Raisecom(config)#**policing-profile** *profile-id* **name** *profile-name*	(Optional) modify the name of the rate limit profile.

No.	Command	Description
4	Raisecom(config)#**policing-profile** *profile-id* **cir** *cir* **pir** *pir* **cbs** *cbs* **pbs** *pbs*	Configure the parameters of the rate limit profile.

To enter GPON ONU UNI configuration mode, create a GPON service profile, configure the number of Ethernet interfaces, and bound them with the ONU.

2.11.3 Binding profile

No.	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu uni ethernet** *slot-id/olt-id/onu-id/uni-id*	Enter GPON ONU UNI configuration mode.
3	Raisecom(config-if-gpon-onu-ethernet-*/*/*:*)#**policing-profile** { **ingress** | **egress** } *profile-id*	Bind a rate limit profile to the ONU UNI. You can use the **no policing-profile** { **ingress** | **egress** } command to delete the binding relation.

2.11.4 Checking configurations

No.	Command	Description
1	Raisecom#**show policing-profile** { **all** | *profile-list* }	Show configurations of the rate limit profile.

2.12 Configuring TR069 management profile

The device can manage the GPON HGU remotely through the Automatic Configuration Server by using TR-069.
The TR069 management profile is a sub-profile of service profile. By configuring the profile ID, you can associate the sub-profile with the service profile. For the association method, see section 2.10 Configuring service profile. When the service profile is bound to the ONU, so will be the sub-profile.

2.12.1 Default configurations

N/A

2.12.2 Creating template

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**create tr069-mng-profile** *profile-id*	Create a TR069 management profile. You can use the **no create tr069-mng-profile** *profile-id* command to delete the template.

2.12.3 Configuring template

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**tr069-mng-profile** *profile-id* **enable**	Enable TR069 management profile. You can use the **tr069-mng-profile** *profile-id* **disable** command to disable this template.
3	Raisecom(config)#**tr069-mng-profile** *profile-id* **acs-addr** *address*	Configure the ACS address of the TR069 management profile.
4	Raisecom(config)#**tr069-mng-profile** *profile-id* **acs-cpe-username** *name* **acs-cpe-password** *password*	Configure the ACS user name and ACS password of the TR069 management profile.
5	Raisecom(config)#**tr069-mng-profile** *profile-id* **vlan** *vlan-id* **priority** *priority*	(Optional) configure the VLAN and priority of the TR069 management profile.
6	Raisecom(config)#**tr069-mng-profile** *profile-id* **acs-cpe-username** *name* **acs-cpe-password** *password*	Configure the ACS CPE user name and password of the TR069 management profile.
7	Raisecom(config)#**tr069-mng-profile** *profile-id* **acs-inform** { **enable** | **disable** }	(Optional) enable ACS notification of the TR069 management profile.

Note

Do not delete the template in use.

2.12.4 Checking configurations

No.	Command	Description
1	Raisecom#**show tr069-mng-profile** { **all** | *profile-list* }	Show the TR069 management profile.

2.13 Managing laser-always-on ONUs

Step	Command	Description
1	Raisecom# **show interface gpon-olt** [*slot-id/olt-list*] **onu-laser-always-on history** [**sn** *sn-num*]	Show all records about laser-always-on ONUs or show records by the specified interface or SN.
2	Raisecom#**config**	Enter global configuration mode.
3	Raisecom(config)# **clear interface gpon-olt** [*slot-id/olt-list*] **onu-laser-always-on history** [**onu** *onu-id*]	Clear all records about laser-always-on ONUs or clear records by the specified PON interface or ONU ID.

2.14 Configuring VLAN

2.14.1 Default configurations

N/A

2.14.2 Configuring VLAN

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gpon-onu** *slot-id/olt-id/onu-id*	Enter GPON ONU virtual interface mode.
3	Raisecom(config-if-gpon-onu-*/*:*)#**vlan-access-list** *list* **gemport** *port*	(Optional) configure the VLAN ACL on the GEM interface.
4	Raisecom(config-if-gpon-onu-*/*:*)#**vlan-mapping outer** *vlan-list* **aggregate outer** *vlan-id* **inner** { **add** *vlan-list* | **unchange** } **gemport** *port-id*	(Optional) configure inner and outer VLAN mapping of the VLAN aggregation group.
5	Raisecom(config-if-gpon-onu-*/*:*)#**native vlan** *vlan-id* **gemport** *port-list*	(Optional) configure local VLAN of the GEM interface.
6	Raisecom(config-if-gpon-onu-*/*:*)#**vlan upstream gem** *gem-id* **vlan** *vlan-id* **mode** { **replace replace-vlan** *vlan-id* | **replace-stacking replace-vlan** *vlan-id* **stacking-vlan** *vlan-id* | **stacking stacking-vlan** *vlan-id* }	(Optional) configure the replacement and adding of VLAN for the uplink traffic of the GEM interface.
7	Raisecom(config-if-gpon-onu-*/*:*)#**vlan mode** { **transparent** | **trunk** } **gemport** *port-list*	(Optional) configure the VLAN mode of the GEM interface.

2.14.3 Configuring VLAN mapping based on GEM

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gpon-onu** *slot-id/olt-id/onu-id*	Enter GPON ONU virtual interface mode.
3	Raisecom(config-if-gpon-onu-*/*:*)#**vlan-mapping egress outer** *vlan-id* **translate outer** *vlan-id* **gemport** *port-id*	(Optional) configure VLAN mapping in the egress direction of the interface.
4	Raisecom(config-if-gpon-onu-*/*:*)#**vlan-mapping ingress outer** *vlan-id* **translate outer** *vlan-id* **inner** { **add** *vlan-id* | **unchange** } **gemport** *port-id*	(Optional) configure VLAN mapping in the ingress direction of the interface.
5	Raisecom(config-if-gpon-onu-*/*:*)#**vlan-mapping both outer** *outer-vlan-id* **translate outer** *outer-vlan-id* **inner** { *inner-vlan-id* | **add** *inner-vlan-id* | **copy-from-outer** | **remove** | **unchange** } **gemport** *port* Raisecom(config-if-gpon-onu-*/*:*)#**vlan-mapping both outer** *outer-vlan-id* **inner** *inner-vlan-id* **translate outer** *outer-vlan-id* **inner** { *inner-vlan-id* | **remove** | **copy-from-outer** } **gemport** *port*	(Optional) configure the 1:1 VLAN mapping rule based on GEM interface. Use the **no vlan-mapping both outer** *outer-vlan-id* to delete the configuration.
6	Raisecom(config-if-gpon-onu-*/*:*)#**vlan-mapping both outer** *outer-vlan-list* **aggregate outer** *outer-vlan-id* **inner { add** *inner-vlan-id* | **unchange } gemport** *port*	(Optional) configure the VLAN aggregation mapping rule based on GEM interface. Use the **no** form of this command to delete the configuration.
7	Raisecom(config-if-gpon-onu-*/*:*)#**vlan-mapping both cos-aware outer** *before-outer before-cos* **translate outer** *after-outer* [*after-cos*] **inner** { *inner-vlan-id* | **add** *inner-vlan-id* | **copy-from-outer** | **remove** | **unchange** } **gemport** *port*	(Optional) configure the VLAN+CoS VLAN mappig rule based on GEM interface. Use the **no** form of this command to delete the configuration.

2.14.4 Checking configurations

Showing ONU configurations

No.	Command	Description
1	Raisecom#**show interface gpon-onu** *slot-id/olt-id/onu-id* **gemport port** { **vlan** | **vlan-access-list** }	Show VLAN configurations of the ONU GEM interface.
2	Raisecom#**show interface gpon-onu** *slot-id/olt-id/onu-id* **gemport port vlan-mapping** { **aggregate** | **egress translate** | **ingress translate** }	Show ONU GEM interface aggregation and ingress/egress VLAN mapping.
3	Raisecom#**show interface gpon-onu** *slot-id/olt-id/onu-list* **vlan upstream**	Show configurations of the GEM VLAN of the specified ONU.

No.	Command	Description
4	Raisecom#**show interface gpon-onu** *slot-id/olt-id/onu-list* **gemport** *port* **vlan-mapping both translate**	Show the 1:1 VLAN mapping rule in both directions of the GEM interface.
5	Raisecom#**show interface gpon-onu** *slot-id/olt-id/onu-list* **gemport** *port* **vlan-mapping both aggregate**	Show the VLAN aggregation mapping rule in both directions of the GEM interface.
6	Raisecom#**show interface gpon-onu** *slot-id/olt-id/onu-list* **gemport** *port* **vlan-mapping both cos-aware translate**	Show the VLAN+CoS VLAN mapping ruel based on GEM interface.

2.15 Configuring auto-authentication rule profile

2.15.1 Default configuration

N/A

2.15.2 Creating and configuring auto-authentication rule profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-auto-authentication-rule** rule-id	Create a ONU auto-authentication rule profile, and enter it. You can use the **no gpon-auto-authentication-rule** command to delete the profile.
3	Raisecom(config-gpon-auto-auth-rule:*)#**match port** slot-id/olt-list	Configure the matching interface in the auto-authentication rule. You can use the **no** form of this command to delete the configuration.
4	Raisecom(config-gpon-auto-auth-rule:*)#**match port add** slot-id/olt-list	Add the matching condition for interfaces in the auto-authentication rule.
5	Raisecom(config-gpon-auto-auth-rule:*)#**match port remove** slot-id/olt-list	Delete the matching condition for interfaces in the auto-authentication rule.
6	Raisecom(config-gpon-auto-auth-rule:*)#**match onu-device-type** device-type	Configure the matching condition for ONU device type in the auto-authentication rule. You can use the **no** form of this command to disable this function.
7	Raisecom(config-gpon-auto-auth-rule:*)#**match ethernet port-num** port-num	Configure the matching condition for the number of ONU Ethernet interfaces in the auto-authentication rule. You can use the **no** form of this command to disable this function.

8	Raisecom(config-gpon-auto-auth-rule:*)#**match wlan port-num** port-num	Configure the matching condition for the number of ONU WLAN interfaces in the auto-authentication rule. You can use the **no** form of this command to disable this function.
9	Raisecom(config-gpon-auto-auth-rule:*)#**match catv port-num** port-num	Configure the matching condition for the number of ONU CATV interfaces in the auto-authentication rule. You can use the **no** form of this command to disable this function.
10	Raisecom(config-gpon-auto-auth-rule:*)#**match veip port-num** port-num	Configure the matching condition for the number of ONU VEIP interfaces in the auto-authentication rule. You can use the **no** form of this command to disable this function.
11	Raisecom(config-gpon-auto-auth-rule:*)#**match pots port-num** port-num	Configure the matching condition for the number of ONU voice interfaces in the auto-authentication rule. You can use the **no** form of this command to disable this function.

2.15.3 Binding profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-auto-authentication-rule** *template-id*	Enter the ONU auto-authentication rule profile.
3	Raisecom(config-gpon-auto-auth-rule:*)#**service-profile-id** { **auto** | *profile-id* }	Configure the service profile used when the ONU is online in the auto-authentication rule.
4	Raisecom(config-gpon-auto-auth-rule:*)#**line-profile-id** { **auto** | *profile-id* }	Configure the line profile used when the ONU is online in the auto-authentication rule.

2.15.4 Checking configurations

No.	Command	Description
1	Raisecom#**show gpon-auto-authentication-rule** { **all** | *rule-id* }	Show configurations of the auto-authentication rule profile.
2	Raisecom#**show interface gpon-olt** [*slot-id/olt-list*] **auto-authentication rule**	Show configurations of the interface and its associated auto-authentication rules.

2.16 Configuration examples

2.16.1 Example for configuring ONU auto-registration

Networking requirements

As shown in Figure 2-2, when you configure the ONU authentication mode to none on OLT interface 3/1, the ONU will be added to the OLT through auto-registration.

Figure 2-2 ONU auto-registration

Configuration steps

Configure the ONU authentication mode to none.

```
Raisecom#config
Raisecom(config)#interface gpon-olt 3/1
Raisecom(config-if-gpon-olt-3:1)#authorization mode none
```

Checking results

Show the ONU authentication mode.

```
Raisecom#show interface gpon-olt 3/1 auth information
    Distance(m)   onu-auto  onu-auto-find  Authorization Created
Registered
OLT ID  min   max   find    Period(s)    Mode     Onus   Onus
-------------------------------------------------------------------------
-----------------
3/1   1    60000  enable   5       none     2    2
```

Show information about the ONU registered on the OLT.

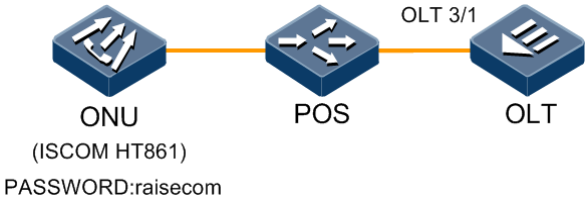
```
ONU ID    SN               Device Type         Creation Date        State
Line Profile       Service Profile      Description

ID     name        ID     name
-------------------------------------------------------------------------
-----------------------------------------------------
3/1/1    RCMG12344444       GS8104-4G           2020-12-25,05:00:28
active         1024    Def_P_all    1018    Def_4E       --
```

2.16.2 Configuring ONU registration based on password authentication mode

Networking requirements

As shown in Figure 2-3, enable password authentication mode on OLT interface 3/1 to register ONU. The model of the ONU to be registered is HT861 and the password is raisecom.

Figure 2-3 ONU registration based on password authentication mode



Configuration steps

Step 1 Configure the ONU authentication mode to password.

```
Raisecom#config
Raisecom(config)#interface gpon-olt 3/1
Raisecom(config-if-gpon-olt-3:1)#authorization mode password
```

Step 2 Create the ONU authorization entry based on password.

```
Raisecom(config-if-gpon-olt-3:1)#create gpon-onu password raisecom line-
profile-id 9 servicservice-profile-id 8
```

Checking results

Show ONU authentication mode.

```
Raisecom#show interface gpon-olt 3/1 auth information

    Distance(m)   onu-auto  onu-auto-find  Authorization Created
Registered

OLT ID  min   max   find    Period(s)    Mode      Onus   Onus

-------------------------------------------------------------------------
-----------------

3/1   1    60000  enable   5       password    2    2
```

Show information about the ONU registered on the OLT.

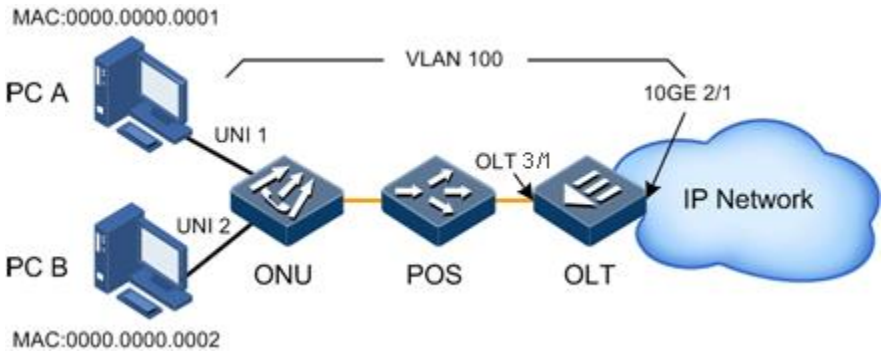
```
Raisecom#show interface gpon-onu creation-information

ONU ID   SN              Device Type         Creation Date        State
Line Profile       Service Profile      Description

ID     name       ID     name

------------------------------------------------------------------------
------------------------------------------------------

3/1/1    RCMG12344444      HT861          2020-12-25,05:00:28   active
9   profile-9   8   profile-8       --
```

2.16.3 Configuring Ethernet data services

Networking requirements

As shown in Figure 2-4, PC A connects UNI 1 on the ONU. The user VLAN is 100. PON interface 3/1 on the device is connected downstream to the ONU while the 10GE interface 2/1 is connected upstream to the IP network. In such case, you can activate the data services.

Figure 2-4 Data service networking



Configuration steps

- Configure the OLT.

Step 1 Configure a line profile.

```
Raisecom#config
Raisecom(config)#gpon-onu-line-profile 100
Raisecom(config-gpon-onu-line-profile:100)#mapping-mode port
Raisecom(config-gpon-onu-line-profile:100)#create tcont 1 dba-profile 1
Raisecom(config-gpon-onu-line-profile:100)#create gem 1 tcont 1
Raisecom(config-gpon-onu-line-profile:100)#gem 1 mapping 1 ethernet 1
Raisecom(config-gpon-onu-line-profile:100)#exit
```

Step 2 Configure a service profile.

```
Raisecom(config)#gpon-onu-service-profile 200
Raisecom(config-gpon-onu-service-profile:200)#port-num ethernet 4
Raisecom(config-gpon-onu-service-profile:200)#uni ethernet 1 vlan trunk
allowed 100
Raisecom(config-gpon-onu-service-profile:200)#exit
```

Step 3 Configure the GPON downlink interface.

```
Raisecom(config)#interface gpon-olt 3/1
Raisecom(config-if-gpon-olt-3:1)#authorization mode none
Raisecom(config-if-gpon-olt-3:1)#exit
Raisecom(config)#gpon-auto-authentication-rule 1
Raisecom (config-gpon-auto-auth-rule:1)#service-profile-id 200
Raisecom (config-gpon-auto-auth-rule:1)# line-profile-id 100
Raisecom(config-if-gpon-olt-3:1)#switchport trunk allowed vlan 100
Trunk allow vlan will be reconfiged,please input 'yes' to confirm set
allowed vlan:[yes]yes
Raisecom(config-if-gpon-olt-3:1)#switchport trunk untagged vlan remove 1
Raisecom(config-if-gpon-olt-3:1)#switchport mode trunk
Raisecom(config-if-gpon-olt-3:1)#quit
```

Step 4 Configure the uplink interface.

```
Raisecom#config
Raisecom(config)#create vlan 100 active
Raisecom(config)#interface ten-gigabitethernet 2/1
Raisecom(config-if-ten-gigabitethernet-2:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-2:1)#switchport trunk allowed vlan
100
Raisecom(config-if-ten-gigabitethernet-2:1)#exit
```

- Configure the ONU.

```
Raisecom(config)#interface gpon-onu 3/1/1
Raisecom(config-if-gpon-onu-3/1:1)#service-profile-id 200
Raisecom(config-if-gpon-onu-3/1:1)#line-profile-id 100
Raisecom(config-if-gpon-onu-3/1:1)#end
```

Checking results

Show information about the ONU created on the OLT.

```
Raisecom#show interface gpon-onu creation-information

ONU ID   SN              Device Type         Creation Date        State
Line Profile       Service Profile      Description


ID     name       ID     name

------------------------------------------------------------------------
------------------------------------------------------

3/1/1    RCMG12344444      GS8104-4G          2020-12-25,05:00:28
active        100   profile-100   200   profile-200       --
```

Show ONU online information.

```
Raisecom#show interface gpon-onu online-information

ONU ID  State   Distance(m)  Login Date     Logout Date    Logout Reason

------------------------------------------------------------------------
-----------------------------------

3/1/1  online  46      2000-08-10,22:09:55 2000-08-10,22:09:49 Branch
fiber cut
```

Show VLAN configurations on the ONU Ethernet interface.

```
Raisecom#show gpon-onu 3/1/1 uni ethernet vlan

 UNI Ethernet ID: 1
  Work Mode       : normal
  VLAN mode       : transparent
  Native VLAN(pri)    : 1 (0)
  Trunk Allowed VLAN   : 100
  Translation-rule    : n/a
  Aggregation-rule    : n/a
  MAC Address Threshold  : 0
  Max Frame Size     : 1522
  Ingress Policing-profile: 0
  Egress Policing-profile: 0
  Drop Untagged     : disable
Dot1q-tunnel     : disable
```

Show the status of the Ethernet interface on the ONU.

```
Raisecom#show gpon-onu 3/1/1 uni ethernet information            US-
policing DS-policing     PPPoE
```

```
Port ID   Speed(actual)     Admin  Link Profile   Profile   Loopback
filter  PoE   alarm-ctrl   FlowControl

-------------------------------------------------------------------------
-------------------------------------------------------------

3/1/1/1   auto/auto(unknown)   enable  down 0     0     disable  disable
disable disable    disable
```

3 Configuring ONU remote management services

This chapter describes the ONU management and Wi-Fi functions of the ISCOM6820, including the following sections:

- Configuring remote management of xGPON ONU
- Configuring Wi-Fi (GPON)

3.1 Configuring remote management of xGPON ONUs

3.1.1 Default configurations

Note

Raisecom has various types of xGPON ONUs which have different features and default configurations. The following table lists common features and default configurations for reference.

Function	Default values
UNI alarm suppression	Disable
UNI flow control	Disable
ONU UNI interface loopback	Disable
Default VLAN ID of the ONU UNI	VLAN 1
ONU Rx optical power	The high alarm threshold is 0. The low alarm threshold is -80 (namely, -80 ×0.5 dBm).
ONU Tx optical power	The high alarm threshold is 12 (namely, 12 ×0.5 dBm). The low alarm threshold is 0.
UNI PSE	Enable
UNI interface	Enable

Function	Default values
UNI rate and duplex mode	Auto-negotiation

3.1.2 Basic configurations

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu** *slot-id/olt-id/onu-id*	Enter GPON ONU remote management configuration mode.
3	Raisecom(config-gpon-onu-*/*:*)#**reboot** [**now**]	(Optional) restart the GPON ONU. **Note** The system also supports rebooting the ONU using the **reboot gpon-onu** [**all** | *slot-id/olt-id/onu-id*] [**now**] command in privileged mode.

3.1.3 Configuring management parameters

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu** *slot-id/olt-id/onu-id*	Enter GPON ONU remote management configuration mode.
3	Raisecom(config-gpon-onu-*/*:*)#**onu-rx-power high-threshold** *value* **low-threshold** *value*	(Optional) configure the alarm threshold of the Rx optical power of the GPON ONU.
4	Raisecom(config-gpon-onu-*/*:*)#**onu-tx-power high-threshold** *high-value* **low-threshold** *low-value*	(Optional) configure the alarm threshold of the Tx optical power of the GPON ONU.

3.1.4 Configuring user interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu uni ethernet** *slot-id/olt-id/onu-id/uni-id*	Enter GPON ONU UNI configuration mode.
3	Raisecom(config-gpon-onu-ethernet-*/*/*:*)#**shutdown**	(Optional) shut down the interface.
4	Raisecom(config-gpon-onu-ethernet-*/*/*:*)#**native vlan** *vlan-id*	(Optional) configure the Native VLAN.

Step	Command	Description
5	Raisecom(config-gpon-onu-ethernet-*/*/*:*)#**speed auto** Raisecom(config-gpon-onu-ethernet-*/*/*:*)#**speed** { **10** | **100** | **1000** } **duplex** { **half** | **full** }	(Optional) configure the interface rate and duplex mode.
6	Raisecom(config-gpon-onu-ethernet-*/*/*:*)#**loopback** { **enable** | **disable** }	(Optional) enable/disable interface loopback.
7	Raisecom(config-gpon-onu-ethernet-*/*/*:*)#**flowcontrol** { **enable** | **disable** }	(Optional) enable/disable interface flow control.
8	Raisecom(config-gpon-onu-ethernet-*/*/*:*)#**alarm-control** { **enable interval** *time* | **disable** }	(Optional) enable/disable interface alarm suppression.
9	Raisecom(config-gpon-onu-ethernet-*/*/*:*)#**pppoe-filter** { **enable** | **disable** }	(Optional) enable/disable PPPoE packet suppression on the interface. **Note** When this function is enabled, the interface only allows PPPoE packets to pass.
10	Raisecom(config-gpon-onu-ethernet-*/*/*:*)#**poe pse** { **enable** | **disable** }	(Optional) enable/disable interface PPPoE.

3.1.5 Configuring voice functions

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu uni pots** *slot-id/olt-id/onu-id/pots-id*	Enter GPON ONU POTS interface configuration mode.
3	Raisecom(config-gpon-onu-pots-*/*/*:*)#**sip-agent sip-proxy** *name* **outbound** *name* **sip-registrar** *name* **primary-dns** *ip-address* **secondary-dns** *ip-address*	(Optional) configure the SIP proxy server.
4	Raisecom(config-gpon-onu-pots-*/*/*:*)#**sip-user aor** *user-aor* **username** *name* **password** *password*	(Optional) configure the registration address of SIP users.

3.1.6 Configuring PPPoE Agent

PPoE Proxy is mainly used to process a specific tag in a PPPoE packet. The tag contains two fields: Circuit ID and Remote ID.

- The circuit ID is filled with the VLAN ID, interface number, and host name information of the interface that receives the client request packet.
- The remote ID is filled with the MAC address of the client or the MAC address of the ONU.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu** *slot-id/olt-id/onu-id*	Enter GPON ONU management configuration mode.
3	Raisecom(config-gpon-onu-*/*:*)#**pppoe-agent** { **enable** | **disable** }	Enable/Disable PPPoE Agent.
4	Raisecom(config-gpon-onu-*/*:*)#**pppoe-agent circuit-id string** *string*	Configure the customized value of PPPoE Agent Circuit_ID Option. You can use the **no pppoe-agent circuit-id string** command to restore to the default condition. of the interface customized value.
5	Raisecom(config-gpon-onu-*/*:*)#**pppoe-agent circuit-id mode** { **onu-eth-id** | **onu-mac** | **client-mac** | **user-define** }	Configure the padding mode of PPPoE Agent Circuit_ID. You can use the **no pppoe-agent circuit-id mode** command to restore the Remote_ID to the default value.
6	Raisecom(config-gpon-onu-*/*:*)#**pppoe-agent remote-id string** *string*	Configure the user-defined value of PPPoE Agent Remote_ID.
7	Raisecom(config-gpon-onu-*/*:*)#**pppoe-agent remote-id mode** { **onu-eth-id** | **onu-mac** | **client-mac** | **user-define** }	Configure the padding mode of PPPoE Agent Remote_ID.

3.1.7 Configuring rate-limit profile on ETH interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu uni ethernet** *slot-id/olt-id/onu-id/uni-id*	Enter GPON ONU UNI configuration mode.
3	Raisecom(config-gpon-onu-ethernet-*/*/*:*)#**policing-profile-name** { **ingress** | **egress** } *name*	Configure rate limiting in the uplink and downlink of the ETH interface based on rate-limit profile name.

3.1.8 Configuring ONU access control mode

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu** *slot-id/olt-id/onu-id*	Enter GPON ONU management configuration mode.
3	Raisecom(config-gpon-onu-*/*:*)#**access-control** { **http** | **telnet** | **ping** | **https** } **mode** { **blockall** | **allowwan** | **allowlan** | **allowall** }	Configure the ONU access control mode.

3.1.9 Configuring ONU IPHost interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu** *slot-id/olt-id/onu-id*	Enter GPON ONU management configuration mode.
3	Raisecom(config-gpon-onu-*/*:*)#**iphost** *iphost-id* **dhcp**	(Optional) configure the uplink IPHost interface mode to DHCP.
	Raisecom(config-gpon-onu-*/*:*)#**iphost** *iphost-id* **pppoe username** *name* **password** *password*	(Optional) configure the uplink IPHost interface mode to PPPoE and configure the user name and password.
	Raisecom(config-gpon-onu-*/*:*)#**iphost** *iphost-id* **static address** *ip-address* [**mask** *ip-address*] **default-gw** *ip-address* { **primary-dns** *ip-address* | **secondary-dns** *ip-address* }*	(Optional) configure the static IP address, gateway, and DNS server IP address of the uplink IPHost interface.
4	Raisecom(config-gpon-onu-*/*:*)#**iphost** *iphost-id* **service** { **internet** | **iptv** | **voip-sinalling** | **voip-media** | **management** }*	(Optional) configure the service type of IPHost interface.
5	Raisecom(config-gpon-onu-*/*:*)#**iphost** *iphost-id* **service mode** { **bridge** | **hybrid** | **route** } **cos** *cos* [**portlist** *list*] [**ssidlist** *list*]	(Optional) configure ONU IPHost interface mode.
6	Raisecom(config-gpon-onu-*/*:*)#**iphost** *iphost-id* **service mode** { **hybrid** | **route** } **nat enable**	(Optional) enable NAT on ONU IPHost interface
7	Raisecom(config-gpon-onu-*/*:*)#**iphost** *iphost-id* **vlan** *vlan-id* [**priority** *priority*]	(Optional) configure VLAN partitions based on IPHost interface and configure the priority of the partitioned VLAN.

Note

- The WAN interface in Internet Management mode can generate static routes and polity routes automatically.
- The WAN interface in Manangement mode can only generate policy routes automatically.
- The WAN interface in Internet mode can only generate static routes automatically.
- The Voip-sinalling Management, Voip-media Management, Voip-media, Voip-sinalling, Voip-sinalling Internet, and Voip-media Internet are supported by devices that support VoIP only. Devices in these modes can automatically generate policy routes.

3.1.10 Checking configurations

No.	Command	Description
1	Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **information**	Show basic information about the ONU.
2	Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **detail-information**	Show details of the ONU.
3	Raisecom#**show version gpon-onu** [*slot-id/olt-id/onu-id list*] Raisecom#**show version gpon-onu slot** *slot-list* Raisecom#**show version gpon-onu gpon-olt** *slot-id/olt-list* Raisecom#**show version gpon-onu xgspon-olt** *slot-id/olt-list*	Show the ONU version.
4	Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **capability**	Show ONU capability.
5	Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **uni ethernet** [*uni-id*] **information**	Show ONU UNI configurations.
6	Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **spanning-tree**	Show global spanning tree configurations of the ONU.
7	Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **uni ethernet** [*uni-id*] **spanning-tree**	Show spanning tree configurations on the ONU UNI.
8	Raisecom#**show onu-remote vlan translation-rule-gpon**	Show configurations of VLAN mapping created on the ONU.
9	Raisecom#**show onu-remote vlan aggregation-rule-gpon**	Show configurations of VLAN aggregation created on the ONU.
10	Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **uni ethernet** [*uni-id*] { **statistics** | **statistics-15min** }	Show ONU UNI statistics.
11	Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **gemindex** [*gem-index*] **statistics-15min**	Show ONU GEM Port statistics.
12	Raisecom#**show interface gpon-olt** [*slot-id/olt-list*] **transceiver rx-onu-power**	Show the Rx optical power of the OLT PON interface.
13	Raisecom#**show gpon-onu** [*slot-id/olt-id*] **device statistics**	Show statistics on ONU types.
14	Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **pppoe-agent**	Show PPPoE configurations of the ONU.
15	Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **access-control-mode**	Show the ONU access control mode.
16	Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **iphost** [*iphost-id*] [**service**]	Show ONU IPHost port configurations.
17	Raisecom#**show interface gpon-onu** *slot-id/olt-id/onu-list* **tcont** [*tcont-id*] **information**	Show TCONT information about the GPON ONU.
18	Raisecom#**show gpon-onu** *slot-id/olt-id/onu-list* **iphost** [*iphost-id*] [**access-control-mode**]	Show the access control mode of the ONU IPhost interface.

3.2 Configuring Wi-Fi (GPON)

3.2.1 Default configurations

N/A

3.2.2 Configuring Wi-Fi

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu** *slot-id/olt-id/onu-id*	Enter GPON ONU management configuration mode.
3	Raisecom(config-gpon-onu-*/*:*)#**wifi admin enable**	Enable Wi-Fi management status. You can use the **wifi admin disable** command to disable this function.
4	Raisecom(config-gpon-onu-*/*:*)#**wifi country code** *id*	Configure the Wi-Fi country code.
5	Raisecom(config-gpon-onu-*/*:*)#**wifi standard** { **802.11b** | **802.11bg** | **802.11bgn** | **802.11g** | **802.11n** | **802.11gn**| **802.11gna** }	Configure the Wi-Fi standard.

3.2.3 Configuring 5G Wi-Fi

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu** *slot-id/olt-id/onu-id*	Enter GPON ONU remote management configuration mode.
3	Raisecom(config-gpon-onu-*/*:*)#**wifi-5g admin enable**	Enable Wi-Fi administrative status. You can use the **wifi-5g admin disable** command to disable this function.
4	Raisecom(config-gpon-onu-*/*:*)#**wifi-5g country code** *id*	Configure the 5G Wi-Fi country code.
5	Raisecom(config-gpon-onu-*/*:*)# **wifi-5g standard** { **802.11a** | **802.11ac** | **802.11na** | **802.11acana** | **802.11acna** | **802.11nacax** }	Configure the 5G Wi-Fi standard.

3.2.4 Configuring Wi-Fi access point

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu** *slot-id/olt-id/onu-id*	Enter GPON ONU remote management configuration mode.

Step	Command	Description
3	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap** *id* **admin enable**	Enable Wi-Fi access point management. You can use the **wifi-ap** *id* **admin disable** command to disable this function.
4	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap** *id* **auth mode** { **unauth** | **wep-open** | **wep-share** | **wpa** | **wpa2** | **wpa2-mixed** }	Configure the authentication mode of the Wi-Fi access point.
5	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap** *id* **client isolate enable**	Enable Wi-Fi access point user isolation. You can use the **wifi-ap** *id* **client isolate disable** command to disable this function.
6	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap** *id* **client max** *num*	Configure the maximum access clients of the Wi-Fi access point.
7	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap** *id* **hidden enable**	Configure the Wi-Fi access point to hidden status. You can use the **wifi-ap** *id* **hidden disable** command to disable this function.
8	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap** *id* **ssid-name** *name*	Configure the SSID name of the Wi-Fi access point.
9	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap** *id* **wep key** *key*	(Optional) configure the authentication mode of the Wi-Fi access point to WEP and configure its secret key node.
10	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap** *id* **wepdefkey** *key* { **key** *key* | **keyformat** { **ascii** | **hex** } | **keylength** { **128bit** | **64bit** } }	(Optional) configure the default key of the WEP authentication mode of the Wi-Fi access point.
11	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap** *id* **wpa encryptionmode** { **aes** | **mixed** | **tkip** }	(Optional) configure the WPA authentication mode of the Wi-Fi access point.
12	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap** *id* **wpa key** *key*	(Optional) configure the WPA secret key of the Wi-Fi access point.
13	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap** *id* **workrate** { **11m** | **12m** | **18m** | **1m** | **24m** | **2m** | **36m** | **48m** | **5.5m** | **54m** | **6m** | **9m** | **auto** | **mcs0** | **mcs1** | **mcs10** | **mcs11** | **mcs12** | **mcs13** | **mcs14** | **mcs15** | **mcs2** | **mcs3** | **mcs4** | **mcs5** | **mcs6** | **mcs7** | **mcs8** | **mcs9** }	(Optional) configure the working rate of the Wi-Fi access node.

3.2.5 Configuring 5G Wi-Fi access point

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu** *slot-id/olt-id/onu-id*	Enter GPON ONU remote management configuration mode.

Step	Command	Description
3	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap-5g** *id* **admin enable**	Enable the administrative status of the 5G Wi-Fi access point. You can use the **wifi-ap-5g** *id* **admin disable** command to disable this function.
4	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap-5g** *id* **auth mode** { **unauth** | **wep-open** | **wep-share** | **wpa** | **wpa2** | **wpa2-mixed** }	Configure the authentication mode of the 5G-Wi-Fi access point.
5	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap-5g** *id* **client isolate enable**	Enable user isolation of the 5G Wi-Fi access point. You can use the **wifi-ap-5g** *id* **client isolate disable** command to disable this function.
6	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap-5g** *id* **client max** *num*	Configure the maximum client accesses to the 5G Wi-Fi access point.
7	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap-5g** *id* **hidden enable**	Enable the hidden status of the 5G Wi-Fi access point. You can use the **wifi-ap** *id* **hidden disable** command to disable this function.
8	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap-5g** *id* **ssid-name** *name*	Configure the SSID name of the 5G Wi-Fi access point.
9	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap-5g** *id* **wep key** *key*	(Optional) configure the 5G Wi-Fi access point authentication mode to WEP and configure its key node.
10	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap-5g** *id* **wepdefkey** *key* { **key** *key* | **keyformat** { **ascii** | **hex** } | **keylength** { **128bit** | **64bit** } }	(Optional) configure the default key for the WEP authentication mode of the 5G Wi-Fi access point.
11	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap-5g** *id* **wpa encryptionmode** { **aes** | **mixed** | **tkip** }	(Optional) configure the WPA authentication mode of the 5G Wi-Fi access point.
12	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap-5g** *id* **wpa key** *key*	(Optional) configure the WPA key of the 5G Wi-Fi access point.
13	Raisecom(config-gpon-onu-*/*:*)#**wifi-ap-5g** *id* **workrate** { **12m** | **18m** | **24m** | **36m** | **48m** | **54m** | **6m** | **9m** | **auto** | **mcs0** | **mcs0-nss1** | **mcs0-nss2** | **mcs1** | **mcs1-nss1** | **mcs2-nss2** | **mcs2** | **mcs2-nss1** | **mcs2-nss2** |**mcs3** | **mcs3-nss1** | **mcs3-nss2** | **mcs4**| **mcs4-nss1** | **mcs4-nss2** | **mcs5** | **mcs5-nss1** | **mcs5-nss2** | **mcs6** | **mcs6-nss1** | **mcs6-nss2** | **mcs7** | **mcs7-nss1** | **mcs7-nss2** | **mcs8-nss1** | **mcs8-nss2** | **mcs9-nss1** | **mcs9-nss2** }	(Optional) configure the working rate of the 5G Wi-Fi access point.

3.2.6 Checking configurations

No.	Command	Description
1	Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **wifi information**	Show configurations of GPON ONU Wi-Fi.
2	Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **wifi-5g information**	Show configurations of GPON ONU 5G Wi-Fi.

4 Configuring multicast services

This chapter describes multicast services and configuration process of the device, including the following sections:

- Introduction
- Quick configurations of multicast services
- Configuring static multicast
- Configuring IGMP Snooping
- Configuring IGMP Proxy
- Configuring MVR
- Configuring dynamic controllable multicast
- Configuring MLD Proxy
- Configuring multicast VLAN
- Configuring the selection of the unknown multicast channel
- Maintenance

4.1 Introduction

4.1.1 Multicast

Multicast is a point to multipoint data transmission method. The method can effectively solve the single point sending and multipoint receiving problems. During the network packet transmission, it can save network resources and improve information security.

Comparisons among unicast, broadcast, and multicast

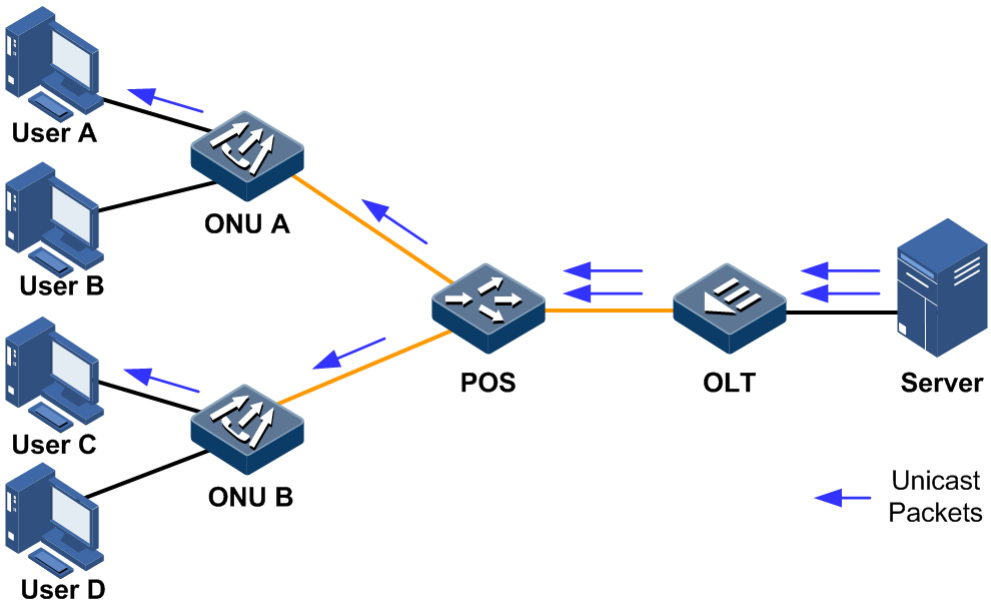
In Ethernet network, packets are transmitted in forms of unicast, broadcast, and multicast.

- Unicast: the system establishes a packet transmission path for each user who needs this packet and sends an independent copy of the packet to the user.

As shown in Figure 4-1, assume that User A and User C need a certain type of packets. In the unicast transmission mode, the Server establishes a transmission path with User A and User C respectively. Because the number of transmitted packets depends on the number of users, when there are more users need a certain packet, multiple identical packet flows will be

transmitted through the network. Therefore, the bandwidth hits a bottleneck. In the unicast transmission mode, packets cannot be transmitted in a large scale.

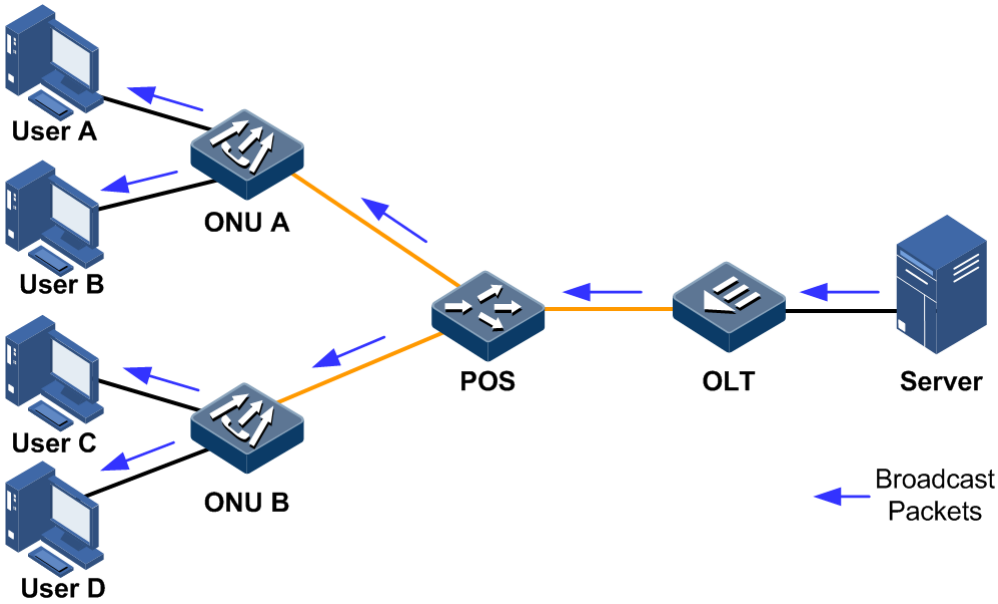
Figure 4-1 Unicast transmission mode



- Broadcast: the system sends a packet to all users in the network, regardless whether they need it or not. All users will receive a broadcast packet.

As shown in Figure 4-2, assume that User A and User C need a certain type of packets. In the broadcast transmission mode, the Server floods this type of packets through a router and all users (including User B) will also receive these packet. The security and non-gratuitousness of the packets cannot be ensured. In addition, network resources cannot be well utilized when few users need this type of packets.

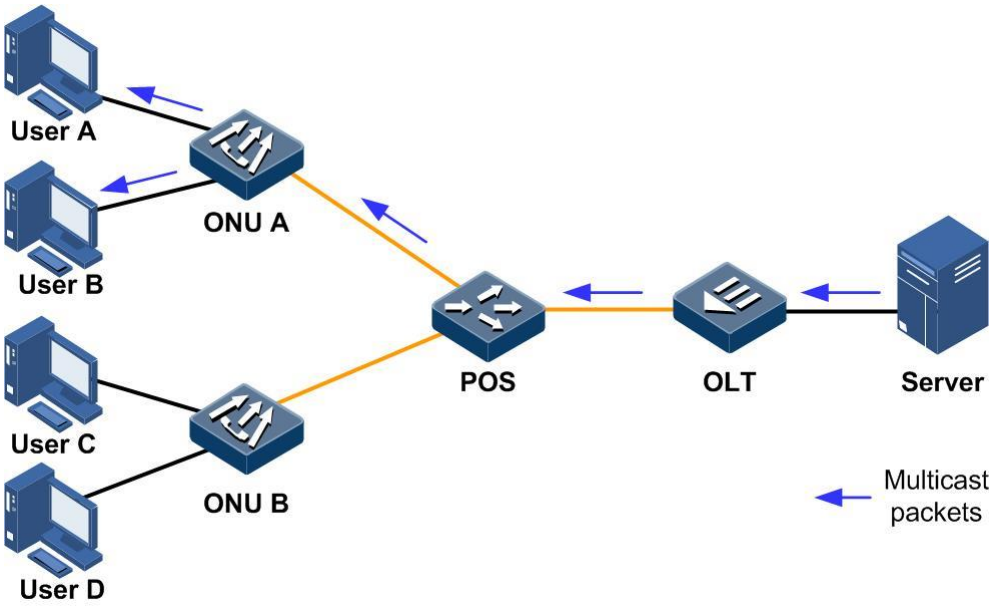
Figure 4-2 Broadcast transmission mode



- Multicast: when some users need a specified packet, the multicast packet sender (multicast source) sends this packet once. This packet is copied and forwarded at the furthest port.

As shown in Figure 4-3, assume that User A and User C need a certain packet. In the multicast transmission mode, User A and User C makes up a group. The ISCOM6820 and ONU devices in the network establish a multicast forwarding table based on its own Internet Group Management Protocol (IGMP) packet. Therefore, the packet is transmitted to receivers who need it.

Figure 4-3 Multicast transmission mode



As described above, the unicast transmission mode fits for a network with few users while the broadcast transmission mode fits for a network with many users. Both the unicast and the broadcast transmission modes work inefficiently when the number of users in a network is not confirmed. In the multicast mode, when the number of users increases exponentially, packets can be transmitted to the specific user without increasing the backbone bandwidth. This makes multicast become one research hotspot of the current network technologies.

Basic concepts

Basic concepts involved in the multicast service are shown as below.

- Multicast source: the device used to send multicast packets. It is the server that sends packets by taking the multicast address as the destination address. A multicast source can send packets to multiple multicast groups simultaneously. In addition, multiple multicast sources can send packets to a multicast group.
- Multicast group: the device used to receive multicast packets. The device uses a multicast IP address to identify a multicast group. A user host (or other receiving devices) becomes a member of a multicast group once it is added to the group. And then the host can recognize and receive packets with the specified IP multicast address. Hosts in a multicast group can be located in any place.
- Multicast router: the router supporting multicast in a network. The multicast router locates at the end network segment that is connected with the user host, to manage multicast members, implement multicast routing, and to conduct forwarding multicast packets.

- Router interface: an interface on the device, which is used to connect the multicast router and the user host. The interface is used to connect the multicast router and receive IGMP packets.
- Member interface: an interface on the device. The interface is used to connect to the user host and send multicast packets.

You must note that the multicast source may (or may not) belong to a multicast group. In addition, multiple multicast sources may send identical packets to a multicast group.

Multicast address

To make the multicast source and the multicast group communicate with each other across the Internet, you must provide a network-layer multicast, using IP multicast addresses.

To make multicast packets transmitted across the local physical network properly, you must provide a link-layer multicast (hardware cast). When the link layer adopts Ethernet technologies, the hardware multicast uses multicast MAC addresses.

To make multicast packet traverse the network layer and the link layer properly, there must be a technology used to map IP multicast addresses to multicast MAC addresses.

- IP multicast address

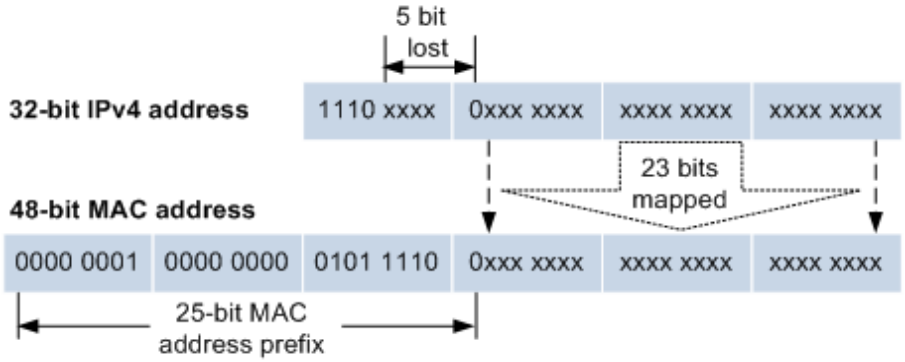
Internet Assigned Numbers Authority (IANA) takes Class D IPv4 addresses as multicast addresses. The IPv4 multicast address ranges from 224.0.0.0 to 239.255.255.255.

- Multicast MAC address

When a unicast packet is transmitted through Ethernet network, the MAC address of the receiver is used. However, when a multicast packet is transmitted, the destination is not a specified receiver but a group with multiple members. Therefore, a multicast MAC address must be adopted.

As formulated by IANA, the first 24 bits of a multicast MAC address is fixed to 0x01005E; the twenty fifth bit is set to 0. The last 23 bits are related to the last 23 bits of an IPv4 multicast address. Figure 4-4 shows the mapping between an IPv4 multicast address and a multicast MAC address.

Figure 4-4 Mapping between an IPv4 multicast address and a multicast MAC address



Because the first 4 bits of an IP multicast address is 1110, and only the last 23 bits of the IP multicast address is mapped to a multicast MAC address. The lost 5 bits will make 32 IP multicast addresses mapped to an identical MAC address. Therefore, during Layer 2 processing, besides the related IPv4 multicast, the device will receive other multicast data. These redundant multicast data will be filtered on the upper layer of the device.

Advantages and applications of multicast

Compared with the unicast and broadcast transmission modes, the multicast transmission mode has the following advantages:

- Improve efficiency, reduce network traffic, and reduce server and CPU load.
- Optimize performance and reduce redundant traffic.
- Make multipoint application available with distribution applications.

With increasingly development of Internet, more and more data, voice, and video information are exchanged in the Internet. Emerging services, such as electronic commerce, online conference, online auction, Video on Demand (VOD), and remote education, are become more popular. These services bring requirements on information security and non-gratuitousness. However, traditional unicast and broadcast transmission modes cannot meet these requirements.

Supported Multicast features

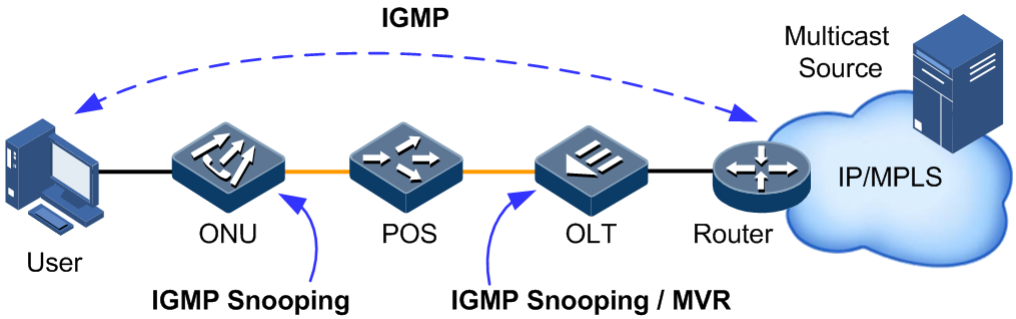
For a network that needs to implement multicast services, you need to deploy various multicast protocols at different nodes of the network. These multicast protocols cooperate with each other to implement network-based multicast services.

In general, based on layers of the Open System Interconnect (OSI), multicast is divided into 2 types:

- Layer 3 multicast: IP multicast working in the network layer. And related multicast protocols are called Layer 3 multicast protocols, such as IGMP.
- Layer 2 multicast: IP multicast working in the data link layer. And related multicast protocols are called Layer 3 multicast protocols, including Internet Group Management Protocol Snooping (IGMP Snooping), Multicast VLAN Registration (MVR), and so on.

Figure 4-5 shows operating positions of the IGMP and Layer 2 multicast protocols.

Figure 4-5 Operating positions of the IGMP and Layer 2 multicast protocols



IGMP is an integrated part of the TCP/IP protocol suite, used for managing IPv4 multicast members. It is a communications protocol used by hosts and adjacent routers on IP networks to establish and maintain multicast group memberships. IGMP manages multicast groups by sending and receiving IGMP packets between the host and the multicast router. IGMP packets are encapsulated in IP packets. IGMP packets are in a form of Query packet, Report packet, or a Leave packet.

The implementation process of the IGMP is shown as below:

- A host is added to a multicast group by sending a Report packet to the multicast router and leave from the multicast group by sending a Leave packet. The host can decide which packets to receive.
- The multicast router sends Query packets periodically and receives Report packets and Leave packets sent by hosts to learns multicast groups in a network segment. If a multicast group is in a network segment, the multicast router forwards multicast data to the network segment. Otherwise, no multicast data is forwarded to the network segment.

At present, there are 3 IGMP versions, IGMPv1, IGMPv2, and IGMPv3. The new version is compatible to old versions. Currently, IGMPv2 is the most commonly-used version. The Leave packet fits for IMGPv2 and IMGPv3 only.

4.1.2 IGMP Snooping

IGMP Snooping is a Layer 2 multicast function. It maintain port information of multicast packets, manage and control forwarding multicast packets by listening multicast packets between multicast groups and hosts.

When the device listens to an IGMP Report packet sent to a multicast group by a host, the device will add the interface, which is connected to the host, to the forwarding table of the multicast group. Similarly, when the device is enabled with immediate-leave, it will delete the interface from the forwarding table of the multicast group after it listens to an IGMP Leave packet. If no packet of a multicast group is listened, the device will delete the interface from the multicast group.

IGMP Snooping forwards multicast data through Layer 2 multicast forwarding table. When the device receives multicast data, it forwards the multicast data to related Tx interface based on the multicast forwarding table instead of flooding the data to all interfaces. Therefore, it helps save bandwidth efficiently.

IGMP Snooping can establish the Layer 2 multicast forwarding table through dynamic learning or manual configuration.

4.1.3 IGMP Proxy

IGMP Proxy is an IGMP agent mechanism, which runs on a Layer 2 device to help manage and control multicast groups. IGMP Proxy processes IGMP packets. For multicast sources, it acts as a host; while for the downlink network, it acts as a multicast router.

A Layer 2 device, where IGMP Proxy is enabled, has 2 roles:

- Querier: at the user side, it acts as a server. It queries user information by sending Query packets periodically and processes Report and Leave packets sent by users.
- Host: at the network router side, it acts as a client. It responds Query packets sent by multicast routers, sends Report and Leave packets, and sends current user information to the network as required.

This agent mechanism can efficiently obtain and control user information. In addition, it helps to reduce number of protocol packets at the network side and network load.

IGMP Proxy establishes the multicast forwarding table by intercepts IGMP packets between users and multicast rooters.

Note

IGMP Proxy can work with MVR.

Concepts related to IGMP Proxy are as below.

- IGMP Querier

If the multicast mode is configured to IGMP Proxy, the device periodically sends IGMP query packets to query information about multicast members on the interface.

- Query interval

After you configure the interval for general query packets in IGMP Proxy mode, IGMP Proxy query timeout will be recounted, and TTL of all online member interfaces in this mode will be reset to "general query interval+maximum response time". By default, the query interval is set to 125s.

- Maximum response time of Query packets

The maximum response time for query packets is used to control the deadline for reporting member relations by a host. When the host receives query packets, it starts a timer for each multicast group. The value of the timer is between 0 and maximum response time. When the timer expires, the host sends the Report packet to the multicast group.

- Interval for last member to respond

The device sends Query packets continuously to a specified multicast group after it receives IGMP Leave packets of the specified multicast group.

The query packet for the specified multicast group is sent to query whether the group has members on the interface. If yes, the members must send Report packets within the maximum response time; after the device receives Report packets in a specie period, it continues to maintain multicast forwarding entries of the group. If the members fail to send Report packets within the maximum response time, it is believed that the last member of the multicast group has left, and multicast forwarding entries of the multicast group will be deleted.

4.1.4 MVR

MVR is a multicast restriction mechanism running on Layer 2 devices. It is used to manage and control multicast groups, and implement Layer 2 multicast.

By configuring multicast VLANs, MVR adds member ports of different Customer VLAN (CVLAN) of the device to multicast VLANs. Therefore, users in different VLANs can share the same multicast VLAN. Multicast flows are transmitted across a multicast VLAN. You do not need to copy multicast flows for each VLAN. In this way, bandwidth is saved. In addition, security is enhanced by isolating multicast VLANs and CVLANs.

The differences of MVR and IGMP Snooping are as below.

- Multicast VLANs and CVLANs in IGMP Snooping are identical.
- Multicast VLANs and CVLANs in MVR are different.

4.1.5 Dynamic controllable multicast

In the PON system, dynamic controllable multicasts forward multicast services in a form of SCB+IGMP. The ISCOM6820 supports CTC OAM-based dynamic controllable multicast.

Dynamic controllable multicast refers than an Optical Line Terminal (OLT) identifies a user based on the IGMP control packet carried by the user, and then controls Optical Network Units (ONUs) to forward multicast data by extending Operation Administration, and Maintenance (OAM) information. The main process is shown as below.

- OLT process
  - At the OLT side, you should maintain a user multicast service authority control table, facilitating centralized management users' multicast service access authorities.
  - The OLT uses the Logical Link Identifiers (LLID) and the VLAN IDs carried by uplink the IGMP Report packets to identify ports (users).
  - Based on the multicast service authority control list, the OLT judges whether a port (user) has the access authority and its parameters of the related multicast services. The OLT uses extended multicast control OAM packets to send access authority of a port (user) to ONUs. And then ONUs decides to forward or discard multicast services from the port (user).
- ONU process
  - The ONU maintains a multicast address filtering table and a multicast forwarding table. The ONU dynamically refreshes these 2 tables based on multicast control OAM packets sent by the OLT.
  - The ONU adds a VLAN tag of the port (user) to received IGMP Report/Leave packets and then sends them to the OLT.
  - After receiving multicast control OAM packets sent by the OLT, the ONU adds or deletes ONU local multicast filtering entries and multicast forwarding entries based on the contents of the packets. And then the ONU decides to forward or discard related multicast traffic.
  - The ONU supports removing VLAN IDs for downlink multicast traffic.

4.2 Quick configurations of multicast services

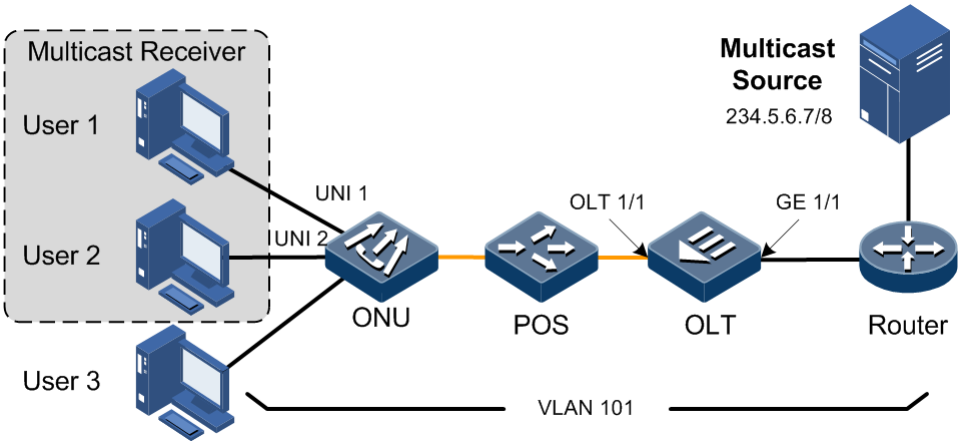
The configuration of multicast services is complex and involves many configuration items. This section provides configuration examples for several typical applications to facilitate users quickly provisioning multicast services.

4.2.1 Example for configuring IGMP Snooping

Networking requirements

As shown in Figure 4-6, the uplink port 10GE 1/1 of the OLT device is connected to the multicast router, and the PON port OLT 3/1 is connected to the ONU. The two Ethernet ports UNI 1 and UNI 2 on the ONU are connected to two users. All multicast users belong to the same VLAN 101. You need to configure IGMP Snooping and immediate leave on the OLT and the ONU respectively to enable the suer to receive multicast data.

Figure 4-6 IGMP Snooping networking



Configuration steps

- Configure the OLT.

Step 1 Create a multicast VLAN and configure the interface attribute.

```
Raisecom#config
Raisecom(config)#create vlan 101 active
Raisecom(config)#multicast-vlan 101
Raisecom(config)#interface ten-gigabitethernet 1/1
Raisecom(config-if-ten-gigabitetherne-1:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitetherne-1:1)#switchport trunk allowed vlan
101
Raisecom(config-if-ten-gigabitetherne-1:1)#exit
Raisecom(config)#interface gpon-olt 3/1
Raisecom(config-if-gpon-olt-3:1)#switchport mode trunk
Raisecom(config-if-gpon-olt-3:1)#switchport trunk allowed vlan 101
Raisecom(config-if-gpon-olt-3:1)#exit
```

Step 2 Configure the role of the multicast VLAN interface and enable immediate leave.

```
Raisecom#config
Raisecom(config)#interface ten-gigabitethernet 1/1
Raisecom(config-if-ten-gigabitethernet-1:1)#multicast-vlan 101 router
Raisecom(config-if-ten-gigabitethernet-1:1)#exit
Raisecom(config)#interface gpon-olt 3/1
Raisecom(config-if-gpon-olt-3:1)#multicast-vlan 101 member
Raisecom(config-if-gpon-olt-3:1)#igmp snooping immediate-leave multicast-
vlan 101
```

Step 3 Enable global IGMP.

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

- Configure the ONU.

Step 4 Create a multicast VLAN and configure the interface attribute.

```
Raisecom#config
Raisecom(config)#gpon-onu-service-profile 1
Raisecom(config-gpon-onu-service-profile:1)#port-num ethernet 4
Raisecom(config-gpon-onu-service-profile:1)#uni ethernet 1 vlan mode
tagged
Raisecom(config-gpon-onu-service-profile:1)#uni ethernet 1 native vlan
101
Raisecom(config-gpon-onu-service-profile:1)#uni ethernet 1 mcast-vlan 101
Raisecom(config-gpon-onu-service-profile:1)#uni ethernet 1 multicast vlan
strip
Raisecom(config-gpon-onu-service-profile:1)#uni ethernet 2 vlan mode
tagged
Raisecom(config-gpon-onu-service-profile:1)#uni ethernet 2 native vlan
101
Raisecom(config-gpon-onu-service-profile:1)#uni ethernet 2 mcast-vlan 101
Raisecom(config-gpon-onu-service-profile:1)#uni ethernet 2 multicast vlan
strip
```

Step 5 Enable IGMP Snooping and configure immediate leave.

```
Raisecom(config-gpon-onu-service-profile:1)#uni ethernet 1 multicast mode
snooping
Raisecom(config-gpon-onu-service-profile:1)#uni ethernet 1 immediate-
leave enable
Raisecom(config-gpon-onu-service-profile:1)#exit
```

Step 6 Bind the service profile with ONUinterface 3/1/1.

```
Raisecom#config
Raisecom(config)#interface gpon-onu 3/1/1
Raisecom(config-if-gpon-onu-3/1:1)#service-profile-id 1
```

Checking results

- Check OLT configurations.

Check whether IGMP configurations on the OLT are correct.

```
Raisecom#show igmp
igmp: enable
igmp snooping timeout: 300s
igmp proxy version: v3
```

```
igmp proxy query interval: 125s
igmp proxy query max response: 5s
igmp proxy last query interval: 1s
igmp proxy last query count: 2
igmp proxy source-ip: 192.168.1.100
```

Check whether multicast VLAN configurations on the ONU are correct.

```
Raisecom#show multicast-vlan
multicast-vlan mode     cvlan forward  upstream-priority  downstream-
priority
-------------------------------------------------------------------------
-----
101          snooping  disable      keep            keep
```

Check whether routing interface configurations of IGMP multicast VLAN are correct.

```
Raisecom#show multicast-vlan 101 router
Multicast vlan         Router
-----------------------------------------------------
101                   ten-gigabitethernet1/1
```

Check whether member interface configurations of IGMP multicast VLAN are correct.

```
Raisecom#show multicast-vlan 101 member
Multicast vlan         Router               Static
-----------------------------------------------------------
  101                  ten-gigabitethernet1/1   static
```

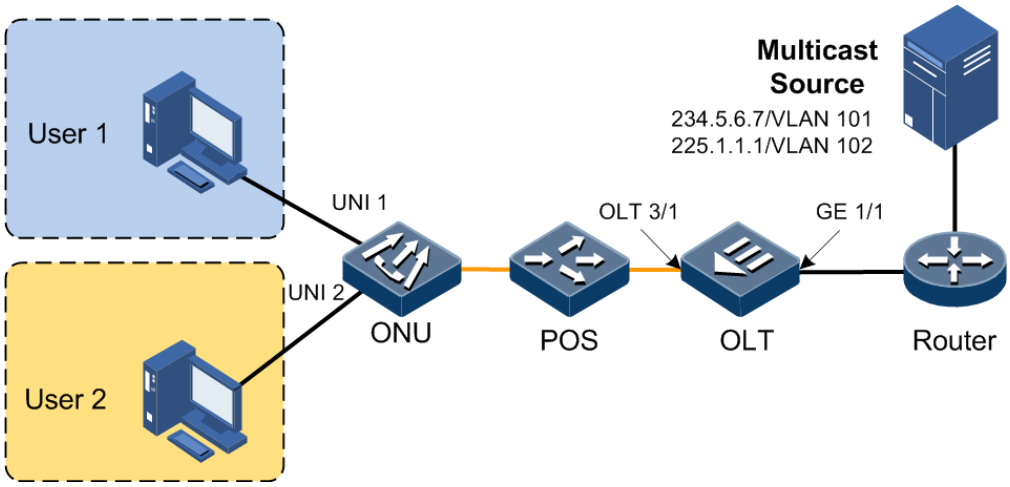
4.2.2 Example for configuring dynamic controllable multicast

Networking requirements

As shown in Figure 4-7, port 10GE 1/1 of the OLT device is connected to the multicast router, and PON port OLT 3/1 is connected to the user through the ONU. By configuring the dynamic controllable multicast, you can enable User 1 and User 2 with different access rights to channel 1 (234.5.6.7) and channel 2 (225.1.1.1).

- User 1: it is allowed to watch channel 1 and has 10 minutes of preview permission for channel 2.
- User 2: it is allowed to watch channel 2 but not channel 1.

Figure 4-7 Dynamic controllable multicast networking



Configuration steps

- Configuring the OLT.

Step 1 Create a multicast VLAN and configure unknown multicast filtering.

```
Raisecom#config
Raisecom(config)#creat vlan 1,2,101,102 active
Raisecom(config)#multicast-vlan 101
Raisecom(config)#multicast-vlan 102
Raisecom(config)#multicast-vlan 1
Raisecom(config)#multicast-vlan 2
Raisecom(config)#mac-address-table unknown-multicast filter vlanlist
1,2,101,102
Raisecom(config)#exit
```

Step 2 Enable IGMP.

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

Step 3 Create a multicast channel.

```
Raisecom(config)#multicast-ctrl
Raisecom(config)#multicast-ctrl channel id 1 name channel1 group-ip
234.5.6.7
Raisecom(config)#multicast-ctrl package package1
Raisecom(config)#multicast-ctrl package package1 channel channel1 permit
Raisecom(config)#multicast-ctrl package package1 channel channel2 preview
peview-profile profile1
Raisecom(config)#multicast-ctrl channel id 2 name channel2 group-ip
225.1.1.1
```

```
Raisecom(config)#multicast-ctrl package package2
Raisecom(config)#multicast-ctrl package package2 channel channel2 permit
Raisecom(config)#multicast-ctrl package package2 channel channel1 deny
```

Step 4 Enable global preview and configure a preview template.

```
Raisecom(config)#multicast-ctrl preview
Raisecom(config)#multicast-ctrl peview-profile profile1
Raisecom(config)#multicast-ctrl peview-profile profile1 duration 10
```

Step 5 Create a dynamic controllable multicast user and specify the channel package of the user.

```
Raisecom(config)#multicast-ctrl user user1 source 3/1/1 cvlan 1
Raisecom(config)#multicast-ctrl user user1 package package1
Raisecom(config)#multicast-ctrl user user2 source 3/1/2 cvlan 2
Raisecom(config)#multicast-ctrl user user2 package package2
```

Step 6 Configure multicast VLAN and MVR.

```
Raisecom(config)#mvr
Raisecom(config)#multicast-vlan 101 group 234.5.6.7
Raisecom(config)#multicast-vlan 102 group 225.1.1.1
Raisecom(config)#interface epon-olt 3/1
Raisecom(config-if-gpon-olt-3:1)#multicast-vlan 101 member
Raisecom(config-if-gpon-olt-3:1)#multicast-vlan 102 member
Raisecom(config-if-gpon-olt-3:1)#exit
```

Step 7 Configure information about the OLT interface.

```
Raisecom(config)#interface gpon-olt 3/1
Raisecom(config-if-gpon-olt-3:1)#switchport mode trunk
Raisecom(config-if-gpon-olt-3:1)#switchport trunk allowed vlan
1,2,101,102
Raisecom(config-if-gpon-olt-3:1)#exit
Raisecom(config)#interface ten-gigabitethernet 1/1
Raisecom(config-if-ten-gigabitethernet-1:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-1:1)#switchport trunk allowed vlan
101,102
Raisecom(config-if-ten-gigabitethernet-1:1)#end
```

- Configure the ONU.

Step 8 Configure the ONU multicast mode to dynamic controllable multicast.

```
Raisecom#config
Raisecom(config)#gpon-onu 3/1/1
Raisecom(config-gpon-onu-3/1:1)#ip igmp mode ctrl-multicast
Raisecom(config-gpon-onu-3/1:1)#exit
```

Step 9 Configure information about the ONU interface.

```
Raisecom(config)#gpon-onu uni ethernet 3/1/1/1
Raisecom(config-gpon-onu-ethernet-3/1/1:1)#multicat vlan stripped
Raisecom(config-gpon-onu-ethernet-3/1/1:1)#exit
Raisecom(config)#gpon-onu uni ethernet 3/1/1/2
Raisecom(config-gpon-onu-ethernet-3/1/1:2)#multicat vlan stripped
```

Checking results

- Check OLT configurations.

Check configurations of the dynamic controllable multicast channel.

```
Raisecom#show multicast-ctrl channel

ID     Channel         cdr     group ip
-----------------------------------------
1      RaisecomChenable   255.1.1.1-255.1.1.1
2     RaisecomChenable   234.5.6.7-234.5.6.7
```

Show user configurations.

```
Raisecom#show multicast-ctrl user
Total user number: 2
User source cvlan package state
-------------------------------------------------------------------------------
user1vport 3/1/11 package1 online
User2vport 3/1/22 package1 online
```

- Show ONU configurations.

Show the processing mode of ONU IGMP packets.

```
Raisecom#show gpon-onu 3/1/1 ip igmp
ONU ID: 3/1/1
   IGMP Mode                  : ctrl-multicast
   Last Member Query Count      : 2
   Last Member Query Interval    : 2s
   Aging Time                 : 300s
```

```
Immediate-leave Administrative : enable
```

4.3 Configuring static multicast

4.3.1 Preparing for configurations

Scenario

The device support static multicast, permitting you to configure the static multicast group, specify the corresponding relationship among the multicast MAC address, multicast VLAN, and multicast interface, and add/remove a specify interface to/from a static multicast group.

If the multicast members and corresponding interfaces are fixed, you can configure static multicast to lower performance waste caused by monitoring multicast packets.

Prerequisite

N/A

4.3.2 Default configurations

N/A

4.3.3 Configuring static multicast

The device adds the member interface to the multicast routing table by identifying the IGMP packet sent by the host automatically. You can manually configure the device to add member interfaces for a specified multicast routing table.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mac-address-table static multicast** *mac-address* **vlan** *vlan-id* **interface** {**gpon-olt** *slot-id/olt-id* |**ten-gigabitethernet** *slot-id/olt-id* | **port-channel** *group-id* }	Configure static Layer 2 multicast MAC address entries.
3	Raisecom(config)#**mac-address-table static multicast** *mac-address* **vlan** *vlan-id* { **add** | **remove** } **interface** { **epon-olt** *slot-id/olt-id* | **gpon-olt** *slot-id/olt-id* | **ten-gigabitethernet** *slot-id/olt-id* | **port-channel** *group-id* }	(Optional) configure the add/remove L2 multicast address of the interface.

4.3.4 Configuring static multicast

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)#**mac-address-table unknown-multicast filter vlanlist** *vlan-list*	(Optional) configure the VLAN list for unknown multicast filtering.

4.3.5 Checking configurations

No.	Command	Description
1	Raisecom#**show mac-address-table multicast** [**statistics**]	Show configurations of the multicast MAC address forwarding table.

4.4 Configuring IGMP Snooping

4.4.1 Preparing for configurations

Scenario

If multiple ONU users need to receive data from the multicast source, you can enable IGMP Snooping on the device or ONU, and create and maintain multicast forwarding tables by monitoring multicast packets between the router and host, to achieve Layer 2 multicast.

- Create a multicast forwarding table recording the corresponding relationship between the multicast packet and PON interface on the device to achieve multicast information distribution based on PON interface.
- Create a multicast forwarding table recording the corresponding relationship between the multicast packet and UNI on the ONU to achieve multicast information distribution based on UNI.

Prerequisite

Create and configure the related VLAN.

4.4.2 Default configurations

Default configurations of IGMP Snooping on the device are as below.

Function	Default value
Global multicast VLAN mode	IGMP Snooping
Global IGMP Snooping	Disable
IGMP Snooping under VLAN	Disable
Aging time of multicast routing entries	300s
Multicast router interface	N/A

Function	Default value
Immediate-leave	Disable
Static multicast routing table	N/A

Default configurations of IGMP Snooping on the ONU devices are as below.

Function	Default value
IGMP mode	IGMP Snooping
Timeout times for the last member to send IGMP query packets	2
Interval for the last member to send IGMP query packets	2s
Aging time of multicast route entries	300s
Forwarding mode of multicast service traffic	VLAN+MAC
Immediate leave	disable

The single-interface ONU ISCOM6101 does not support being configured with the forwarding mode of multicast service traffic and cannot identify VLANs. It forwards packets according to the MAC address by default.

4.4.3 Configuring IGMP Snooping

Configuring IGMP on OLT

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#igmp`	Enable global IGMP Snooping. You can use the **no igmp** command to disable this function.

If the current multicast VLAN mode is IGMP Snooping, you can use the **igmp** command to enable global IGMP features; if the current multicast VLAN mode is IGMP Proxy, you need to use the **multicast-vlan mode** command to switch the multicast VLAN mode to IGMP Snooping, and then use the **igmp** command to enable global IGMP features.

4.4.4 (Optional) configuring aging time of multicast routing entries

In IGMP Snooping, when the device does not receive the IGMP packet about Layer 2 multicast routing in a period of time, maybe the relevant host or router has left from the multicast group without sending the leave packet. You can configure the aging time of multicast routing entries to delete these entries from the multicast routing table automatically when the aging time expires.

Configuring aging time of OLT multicast routes

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#igmp snooping timeout { period | infinite }`	Configure the aging time of multicast routing entries. You can use the **no igmp snooping timeout** command to restore default configuration.

4.4.5 (Optional) configuring immediate leave

When the user host sends the IGMP leave packet, the device does not immediately delete multicast route, but wait for a while before deletion. When there are a lot of downstream users, and the operation of adding or leaving is frequent, you can configure the immediate-leave feature. Then multicast route will be deleted immediately when the user host sends the IGMP leave packet.

This function is only applied to IGMPv2/v3.

Configuring OLT immediate leave

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface { gpon-olt slot-id/olt-id | | gigabitethernet slot-id/olt-id | port-channel group-id }`	Enter physical interface configuration mode. Enter interface configuration mode.
3	`Raisecom(config-if-*-*:*)#igmp-mld snooping immediate-leave multicast-vlan vlan-list`	Configure immedate leave based on interface or interface + VLAN. You can use the **no igmp snooping immediate-leave multicast-vlan** *vlan-list* command to disable this function.

4.4.6 Checking configurations

Checking configurations of OLT

No.	Command	Description
1	Raisecom#**show igmp**	Show IGMP global configurations.
2	Raisecom#**show igmp statistics**	Show statistics on IGMP packets.
3	Raisecom#**show interface** { **gpon-olt** *slot-id/olt-id* | **ten-gigabitethernet** *slot-id/olt-id* | **port-channel** *group-id* } **igmp statistics**	Show statistics on IGMP packets on a specified interface.

4.5 Configuring IGMP Proxy

4.5.1 Preparing for configurations

Scenario

In a network where the multicast routing protocol is widely applied, there are multiple hosts or client subnets receiving multicast information. Configure IGMP Proxy on a multicast router and device connected to the host to block IGMP packets between the host and router to reduce the network load.

IGMP Proxy can reduce the task of configuring and managing the client subnet through a multicast router and achieve client subnet multicast connection at the same time.

IGMP Proxy and IGMP Snooping cannot be used concurrently in the same multicast VLAN.

Prerequisite

Create a VLAN and add related interfaces to the VLAN.

4.5.2 Default configurations

Default configurations of IGMP Proxy on the ISCOM6820 are as below.

Function	Default value
IGMP version	v2
IGMP query interval	125s
Maximum response time of Tx Query packets	10s
Query interval of the last member	2s
Query times of the last member	2
Source IP address of IGMP Proxy packet sent by IGMP querier	192.168.1.100
IGMP Proxy robustness coefficient	2

4.5.3 Configuring IGMP Proxy

Configuring OLT IGMP Proxy

When you use the **igmp** command to enable global IGMP features, the default working mode of the multicast VLAN is IGMP Snooping. If you need to enable IGMP Proxy, use the **multicast-vlan mode** command to switch the multicast VLAN mode to IGMP Proxy.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#igmp proxy query-interval` *seconds*	(Optional) configure the IGMP query interval. You can use the **no igmp proxy query-interval** command to restore default configuration.
3	`Raisecom(config)#igmp proxy query-max-response` *seconds*	(Optional) configure the maximum response time of IGMP query. You can use the **no igmp proxy query-max-response** command to restore default configuration.
4	`Raisecom(config)#igmp proxy last-query-interval` *seconds*	(Optional) configure the query interval of the last member in the multicast group. You can use the **no igmp proxy last-query-interval** command to restore default configuration.
5	`Raisecom(config)#igmp proxy last-query-count` *count*	(Optional) configure the query times of the last member in the multicast group. You can use the **no igmp proxy last-query-count** command to restore default configuration.
6	`Raisecom(config)#igmp proxy source-ip` *ip-address*	(Optional) configure the source IP address of the IGMP Proxy packet sent by the IGMP querier. You can use the **no igmp proxy source-ip** command to restore default configuration.
7	`Raisecom(config)#igmp proxy robustness` *robustness*	Configure the IGMP Proxy robustness coefficient. You can use the **no igmp proxy robustness** command to restore default configuration.

Checking configurations

No.	Command	Description
1	`Raisecom#show igmp`	Show configurations of IGMP Proxy on the OLT.

4.6 Configuring MVR

4.6.1 Preparing for configurations

Scenario

When multiple user hosts need to receive data from the multicast source, and different user hosts, host and multicast router belong to different VLANs, you can configure MVR on the multicast router and the device connected to the user host, to enable users in different VLANs to receive the same multicast packet and reduce bandwidth waste.

Prerequisite

Create a VLAN and add related interfaces to the VLAN.

4.6.2 Default configurations

Default configurations of MVR on the ISCOM6820 are as below.

Function	Default value
Global MVR	Disable

4.6.3 Configuring basic MVR

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#mvr`	Enable global MVR. You can use the **no mvr** command to disable this function.

4.6.4 Checking configurations

No.	Command	Description
1	`Raisecom#show mvr`	Show MVR configurations.

4.7 Configuring dynamic controllable multicast

4.7.1 Preparing for configurations

Scenario

Multicast data features heavy traffic and numerous receivers. So you must strictly manage the multicast source and receivers, and control the transmission direction and range of multicast data, in order to implement transmission of multicast services on the IP network.

Otherwise, operating multicast services not only affects the current IP network but also fails to provide services of the expected quality for receivers.

Prerequisite

You must configure the dynamic controllable multicast feature on the OLT and ONU simultaneously to implement this function in the EPON system.

4.7.2 Default configurations

Default configurations of dynamic controllable multicast on the ISCOM6820 are as below.

Function	Default value
Dynamic controllable multicast	Disable
Channel preview	Enable
Auto-reset period of preview	weekly
Aware time of preview	4s
CDR	Enable
IP address of CDR Rx server	0.0.0.0
Maximum number of CDR	65535
Maximum duration when there is no on-demand packet	5min

4.7.3 Configuring global parameters

4.7.4 Parameters

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#multicast-ctrl`	Enable global dynamic controllable multicast.

Step	Command	Description
3	Raisecom(config)#**multicast-ctrl max-non-igmp-report-duration** *time*	(Optional) configure the maximum duration when there is no on-demand packet. You can use the **no multicast-ctrl max-non-igmp-report-duration** command to restore default configuration.

4.7.5 Configuring user management

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**multicast-ctrl user** *username* **source** *slot-id/port-id/vport-id* **cvlan** *vlan-id*	Create a dynamic controllable multicast user.
3	Raisecom(config)#**multicast-ctrl user** *username* **package** *packagename*	Configure the channel package for the specified user.
4	Raisecom(config)#**multicast-ctrl user** s*lot-id/port-id/vport-id* **cvlan** *cvlan* **package id** { **add** | **remove** } *id*	(GPON) configure the CVLAN, and modify the channel package.

4.7.6 Configuring channel management

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**multicast-ctrl channel id** *channel-id* **name** *channel-name* **vlan** *vlan-id* **group-ip{** *ip-addre s* | *ipv6-addre s* }[*end-ip-address* | *end- ipv6-addre s*]	Create a multicast channel. You can use the **no multicast-ctrl channel name** command to delete the configuration.
3	Raisecom(config)#**multicast-ctrl channel** *channelname* **cdr**	(Optional) enable channel CDR. You can use the **no multicast-ctrl channel** *channelname* **cdr** command to disable this function.
4	Raisecom(config)#**multicast-ctrl package** *packagename*	Create a channel package. You can use the **no multicast-ctrl package** *packagename* command to delete the channel.
5	Raisecom(config)#**multicast-ctrl package** *packagename* **channel** *channelname* { **deny** | **permit** | **preview** } [**peview-profile** *profile*]	Add channels to the package. You can use the **no multicast-ctrl package** *packagename* **channel** *channelname* command to restore default configuration.

4.7.7 Configuring preview rules

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**multicast-ctrl preview**	Enable the preview function. You can use the **no multicast-ctrlp review** command to disable this function.
3	Raisecom(config)#**multicast-ctrl preview reset**	Configure manual preview reset.
4	Raisecom(config)#**multicast-ctrl preview auto-reset-period** { **daily** | **weekly** | **monthly** | **custom** }	Configure the auto-reset period of preview. You can use the **no multicast-ctrl preview auto-reset-period** command to restore default configuration.
5	Raisecom(config)#**multicast-ctrl preview auto-reset-time** *time*	Configure the auto-reset time of preview. You can use the **no multicast-ctrl preview auto-reset** command to restore default configuration.
6	Raisecom(config)#**multicast-ctrl preview aware-time** *time*	Configure the aware time of preview. You can use the **no multicast-ctrl preview aware-time** command to restore default configuration.
7	Raisecom(config)#**multicast-ctrl preview-profile** *profile*	Create a preview profile. You can use the **nomulticast-ctrl preview-profile** *profile* command to delete the profile.
8	Raisecom(config)#**multicast-ctrl preview-profile** *profile* **total-time** *time*	Configure the total time for previewing a profile. You can use the **no multicast-ctrl preview-profile** *profile* **total-time** command to restore default configuration.
9	Raisecom(config)#**multicast-ctrl preview-profile** *profile* **count** *count*	Configure the maximum times for previewing a profile. You can use the **no multicast-ctrl preview-profile** *profile* **count** command to restore default configuration.
10	Raisecom(config)#**multicast-ctrl preview-profile** *profile* **duration** *time*	Configure the maximum duration for previewing a profile at one time. You can use the **no multicast-ctrl preview-profile** *profile* **duration** command to restore default configuration.
11	Raisecom(config)#**multicast-ctrl preview-profile** *profile* **interval** *time*	Configure the interval for previewing a profile for a second time. You can use the **no multicast-ctrl preview-profile** *profile* **interval** command to restore default configuration.

4.7.8 Configuring CDR

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)#**multicast-ctrl cdr**	Enable CDR management. You can use the **no multicast-ctrl cdr** command to disable this function.
3	Raisecom(config)#**multicast-ctrl cdr max-records** *number*	Configure the maximum number of CDR. You can use the **no multicast-ctrl cdr max-records** command to restore default configuration.
4	Raisecom(config)#**multicast-ctrl cdr report**	Configure manual CDR reporting.
5	Raisecom(config)#**multicast-ctrl cdr report-interval** *report-interval*	Configure the interval for reporting CDR manually. You can use the **no multicast-ctrl cdr report-interval** command to restore default configuration.
6	Raisecom(config)#**multicast-ctrl cdr report-threshold** *value*	Configure the threshold for reporting CDR manually. You can use the **no multicast-ctrl cdr report-threshold** command to restore default configuration.
7	Raisecom(config)#**multicast-ctrl cdr aware-time** *value*	Configure the CDR awaring time.

4.7.9 Checking configurations

No.	Command	Description
1	Raisecom#**show multicast-ctrl**	Show configurations of dynamic controllable multicast.
2	Raisecom#**show multicast-ctrl channel** [*channelname*] **online-user**	Show channel online users.
3	Raisecom#**show multicast-ctrl channel** [*channelname*]	Show channel configurations.
4	Raisecom#**show multicast-ctrl user** [*username*]	Show user configurations.
5	Raisecom#**show multicast-ctrl user** [*username*] **online-channel**	Show the channel package of the user.
6	Raisecom#**show multicast-ctrl package** [*package-name*]	Show information about the channel package.
7	Raisecom#**show multicast-ctrl cdr**	Show CDR configurations.
8	Raisecom#**show multicast-ctrl cdr-content**	Show the current CDR.
9	Raisecom#**show multicast-ctrl preview**	Show preview configurations.
10	Raisecom#**show multicast-ctrl preview-profile** [*profile*]	Show preview profile configurations.

4.8 Configuring MLD Proxy

4.8.1 Preparing for configurations

Scenario

Multicast Listener Discover (MLD) is a network protocol used by multicast technology. It is used to discover multicast listeners for the IPv6 device in its directly-connected network segment, namely the host nodes that expect to receive multicast data.

To implement the multicast function in an IPv6 network, you need to configure the MLD multicast function.

Prerequisite

N/A

4.8.2 Default configurations

Default configurations of MLD Proxy on the ISCOM6820 are as below.

Function	Default value
Global MLD multicast	Disable
MLD multicast IP address	Local link address, namely, the address generated by the local MAC address and starting with FE80, such as fe80::2a0:1eff:fea0:aaa0
MLD Proxy query interval	125s
Maximum response time of MLD Proxy query	10s
Query interval of MLD Proxy last member	2s
Number of query packets of MLD Proxy last member	2
MLD Proxy robustness coefficient	2
MLD Proxy version	V1

4.8.3 Configuring MLD Proxy

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#mld`	Enable MLD Proxy. You can use the **no mld** command to disable this function.

Step	Command	Description
3	Raisecom(config)#**mld proxy source-ip** *ipv6-address*	(Optional) configure the source IPv6 address of the query packet sent by the MLD Proxy querier. You can use the **no mld proxy source-ip** command to restore default configurations.
4	Raisecom(config)#**mld proxy query-interval** *period*	(Optional) configure the MLD Proxy query interval. You can use the **no mld proxy query-interval** command to restore default configurations.
5	Raisecom(config)#**mld proxy query-max-response-time** *period*	(Optional) configure the maximum response time of MLD Proxy query. You can use the **no mld proxy query-max-response** command to restore default configurations.
6	Raisecom(config)#**mld proxy last-query-interval** *period*	(Optional) configure the query interval of MLD Proxy last member. You can use the **no mld proxy last-query-interval** command to restore default configurations.
7	Raisecom(config)#**mld proxy last-query-count** *count*	(Optional) configure the times to query the MLD Proxy last member. You can use the **no mld proxy last-query-count** command to restore default configurations.
9	Raisecom(config)#**mld proxy robustness** *robustness*	(Optional) configure the robustness coefficient of MLD Proxy. You can use the **no mld proxy robustness** command to restore default configurations.

4.8.4 Checking configurations

No.	Command	Description
1	Raisecom#**show mld statistics**	Show MLD configurations.
2	Raisecom#**show interface** { **gpon-olt** *slot-id/olt-id* | **ten-gigabitethernet** *slot-id/port-id* | **port-channel** *group-id* } **mld statistics**	Show statistics on MLD packets on a specified interface.

4.9 Configuring multicast VLAN

4.9.1 Preparing for configurations

Scenario

In the traditional on-demand multicast mode, when hosts in different VLANs request the same multicast group at the same time, Layer 3 devices need to copy multicast data to each VLAN. This not only wastes the bandwidth, but also increases the burden of the Layer 3 device.

You can use the multicast VLAN to solve the problem. After you configure the multicast VLAN on the Layer 2 device, the Layer 3 device only needs to make a copy of multicast data in the multicast VLAN and sent it to the Layer 2 device, without making a copy in each VLAN. In this case, it saves the network bandwidth and reduces the burden of the Layer 3 device.

Prerequisite

N/A

4.9.2 Default configurations

Default configurations of multicast VLAN on the ISCOM6820 are as below.

Function	Default value
Multicast VLAN	Disable
Working mode of multicast VLAN	Snooping
CVLAN transparent transmission	Disable
Priority of multicast VLAN uplink protocol packets	keep
Priority of multicast VLAN downlink protocol packets	keep

4.9.3 Configuring multicast VLAN

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**multicast-vlan** *vlan-id*	Create a multicast VLAN.
3	Raisecom(config)#**multicast-vlan** *vlan-id* **mode** { **snooping** | **proxy** }	Configure the working mode of the multicast VLAN.
4	Raisecom(config)#**multicast-vlan** *vlan-id* **group** { *group-address* [*count*] | **any** }	Configure binding the multicast VLAN with the group address. You can use the **no multicast-vlan** *vlan-id* **group** { *group-address* [*count*] | **any** } command to restore default configuration.
5	Raisecom(config)#**multicast-vlan** *vlan-id* **cvlan-forward**	Configure CVLAN transparent transmission.
6	Raisecom(config)#**multicast-vlan** *vlan-id* **upstream-priority** *pri*	Configure the priority of multicast VLAN uplink protocol packets.
7	Raisecom(config)#**multicast-vlan** *vlan-id* **downstream-priority** *pri*	Configure the priority of multicast VLAN downlink protocol packets.
8	Raisecom(config)#**interface** { **gpon-olt** *slot-id/olt-id* | **ten-gigabitethernet** *slot-id/olt-id* | **port-channel** *group-id* }	Enter physical interface configuration mode.

Step	Command	Description
9	Raisecom(config-if-*-*:*)#**multicast-vlan** *vlan-id* **router**	Configure the interface as the multicast VLAN router interface. **Note** When the multicast VLAN router interface is not configured through this comman, the device supports dynamically learning the interface role.
10	Raisecom(config-if-*-*:*)#**multicast-vlan** *vlan-id* **member**	Configure the interface as the multicast VLAN member interface. Configure the interface as the multicast VLAN router interface. **Note** When the multicast VLAN router interface is not configured through this comman, the device supports dynamically learning the interface role.

4.9.4 Checking configurations

No.	Command	Description
1	Raisecom#**show multicast-vlan** *vlan-id*	Show configurations of the multicast VLAN.
2	Raisecom#**show multicast-vlan** *vlan-id* **group**	Show multicast VLAN group addresses.
3	Raisecom#**show multicast-vlan** *vlan-id* **router**	Show the multicast VLAN router interface.
4	Raisecom#**show multicast-vlan** *vlan-id* **member**	Show the member interfaces of a specified IGMP multicast VLAN.

4.10 Configuring the selection of the unknown multicast channel

4.10.1 Preparing for configurations

Scenario

Configure the unknown multicast packets to use the broadcast channel so as to reduce the impact of unknown multicast packets on the multicast channel. After this function is enabled, unknown multicast packets are bound to the unknown multicast flooding group.

Prerequisites

N/A

4.10.2 Default configurations

Default configurations of the unknown multicast packets to use the broadcast channel are as below.

Function	Default value
Unknown multicast packets to use the broadcast channel	Unknown multicast packets use the broadcast channel.

4.10.3 Enabling unknown multicast packets to use the broadcast channel

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)# **pon detach unknown-mcast enable**	Unknown multicast packets use the broadcast channel.

4.11 Maintenance

No.	Command	Description
1	Raisecom(config)#**clear igmp statistics**	Clear IGMP packet statistics.
2	Raisecom(config)#**clear interface** { **gpon-olt** *slot-id/olt-id*| **ten-gigabitethernet** *slot-id/olt-id*| **port-channel** *group-id* } **igmp statistics**	Clear IGMP packet statistics on a specified interface.
3	Raisecom(config)#**clear mld statistics**	Clear MLD packet statistics.
4	Raisecom(config)#**clear interface** { **gpon-olt** *slot-id/olt-id* | **ten-gigabitethernet** *slot-id/olt-id* | **port-channel** *group-id* } **mld statistics**	Clear MLD packet statistics on a specified interface.
5	Raisecom(config)#**multicast-ctrl cdr clear**	Clear CDR information.

4.12 Configuration examples

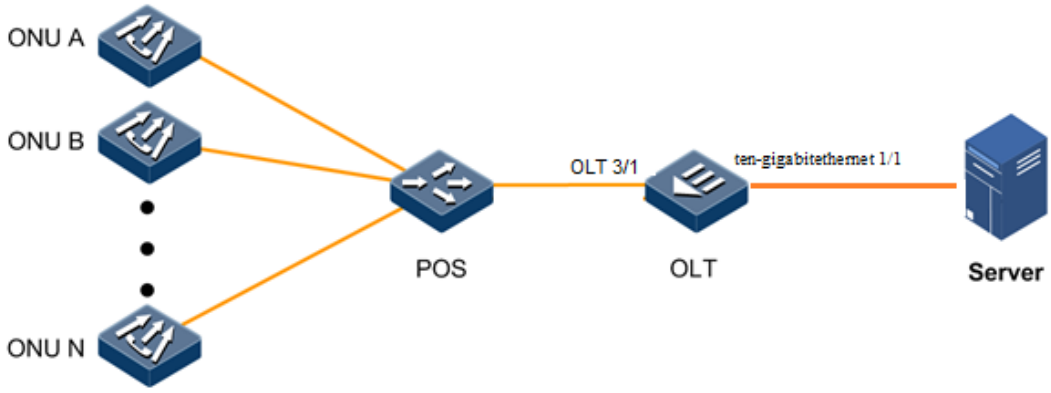
4.12.1 Example for configuring IGMP Snooping

Networking requirements

As shown in Figure 4-8, the OLT is connected by ten-gigabitethernet interface 1/1 to the multicast source and by interface 3/1 to ONUs. Enable IGMP Snooping on the OLT.

Through configurations, the ONUs can receive multicast data of multicast VLAN 200 only and discard unknown multicast data directly to avoid broadcasting them in its VLAN.

Figure 4-8 IGMP Snooping application



Configuration steps

Step 1 Create VLANs.

```
Raisecom#config
Raisecom(config)#create vlan 100,200 active
```

Step 2 Configure multicast VLAN and IGMP Snooping.

```
Raisecom(config)#multicast-vlan 200
Raisecom(config)#multicast-vlan 200 mode proxy
Raisecom(config)#multicast-vlan 200 group any
Raisecom(config)#mvr
Raisecom(config)#igmp
```

Step 3 Configure the uplink interface on the OLT.

```
Raisecom(config)#interface ten-gigabitethernet 1/1
```

```
Raisecom(config-if-ten-gigabitethernet-1:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-1:1)#switchport trunk allowed vlan
100,200 confirm
Raisecom(config-if-ten-gigabitethernet-1:1)#multicast-vlan 200  router
Raisecom(config-if-ten-gigabitethernet-1:1)#quit
```

Step 4 Configure the PON interface.

- Configure the ONU service profile, making interfaces 1 and 2 as Internet access interfaces and interfaces 3 and 4 as multicast interfaces.

```
Raisecom(config)#gpon-onu-service-profile 6
Raisecom(config-gpon-onu-service-profile:6)#name 4_portos
Raisecom(config-gpon-onu-service-profile:6)#port-num ethernet 4
Raisecom(config-gpon-onu-service-profile:6)#uni ethernet 1 vlan mode
tagged
Raisecom(config-gpon-onu-service-profile:6)#uni ethernet 1 native vlan
100
Raisecom(config-gpon-onu-service-profile:6)#uni ethernet 2 vlan mode
tagged
Raisecom(config-gpon-onu-service-profile:6)#uni ethernet 2 native vlan
100
Raisecom(config-gpon-onu-service-profile:6)#uni ethernet 3 vlan mode
tagged
Raisecom(config-gpon-onu-service-profile:6)#uni ethernet 3 native vlan
2501
Raisecom(config-gpon-onu-service-profile:6)#uni  ethernet 3multicast vlan
strip
Raisecom(config-gpon-onu-service-profile:6)#uni  ethernet 3 immediate-
leave enable
Raisecom(config-gpon-onu-service-profile:6)#uni  ethernet 3 uni ethernet
1-4 mcast-vlan 200
Raisecom(config-gpon-onu-service-profile:6)#uni ethernet 4 vlan mode
tagged
Raisecom(config-gpon-onu-service-profile:6)#uni ethernet 4 native vlan
2501
Raisecom(config-gpon-onu-service-profile:6)#uni ethernet 4multicast vlan
strip
Raisecom(config-gpon-onu-service-profile:6)#uni ethernet 4 immediate-
leave enable
Raisecom(config-gpon-onu-service-profile:6)#uni ethernet 4 uni ethernet
1-4 mcast-vlan 200
Raisecom(config-gpon-onu-service-profile:6)#quit
```

- Create ONUs.

```
Raisecom(config)#interface gpon-olt 3/1
Raisecom(config-if-gpon-olt-3:1)#create gpon-onu 1 sn RCMG18B0A1F1 line-
profile-id 1024 service-profile-id 6
Raisecom(config-if-gpon-olt-3:1)#switchport mode trunk
```

```
Raisecom(config-if-gpon-olt-3:1)#switchport trunk allowed vlan 100,200
confirm
Raisecom(config-if-gpon-olt-3:1)#multicast-vlan 200 member
```

Checking results

Use the **show igmp** command on the OLT to show global IGMP configurations.

```
Raisecom#show igmp
igmp:enable
igmp snooping timeout(s):30
igmp proxy version:v2
igmp proxy query interval(s):10
igmp proxy query max response(s):10
igmp proxy last query interval(s):2
igmp proxy last query count:2
igmp proxy robustness:2
igmp proxy source-ip:192.168.1.100
igmp require-router-alert:disable
igmp ssdp enable slot:
```

5 Configuring MAC address

This chapter describes basic principles and configuration process of the MAC address table for the device, and provides related configuration examples, including the following sections:

- Introduction
- Configuring dynamic MAC address
- Configuring static MAC address
- Maintenance and search

5.1 Introduction

The ISCOM6820 supports forwarding packets at the data link layer. It forwards packets to related interfaces based on destination MAC addresses of these packets. The MAC address is a Layer 2 forwarding table that records the relationship between MAC addresses and forwarding interfaces. The MAC address table is the basis for the ISCOM6820 to quickly forward Layer 2 packets.

MAC address entries in the MAC address table consist of following information:

- Destination MAC address
- Interface ID corresponding to the destination MAC address
- VLAN ID to which an interface belongs
- Static/Dynamic flags

The MAC address table on the ISCOM6820 consists of two kinds of address entries:

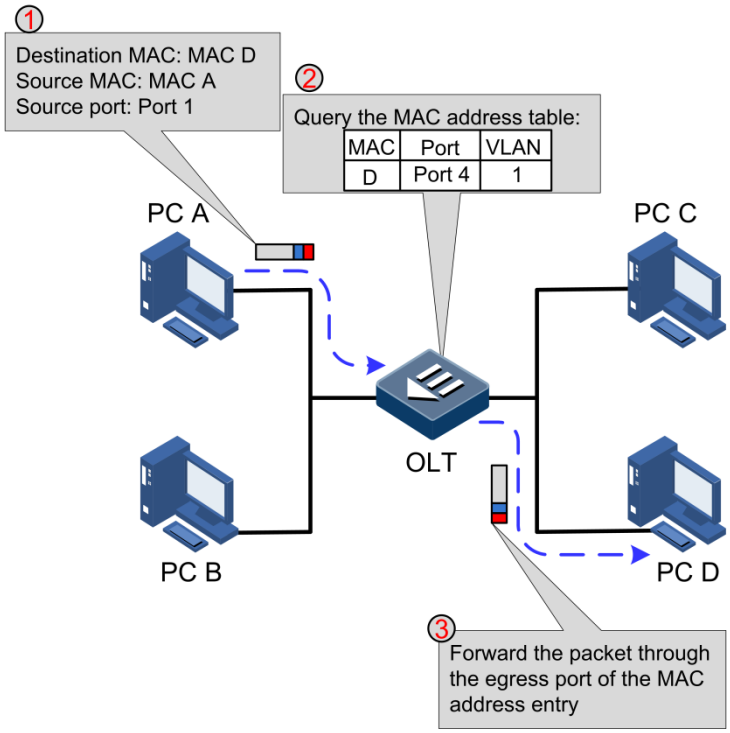
- Static MAC address entries: also termed as permanent addresses, you can add and remove them manually. It does not age with time. For a small network, by manually adding static addresses, you can reduce the broadcast traffic across the network.
- Dynamic MAC address entries: refers to MAC addresses that can be added through MAC address learning mechanism. Dynamic MAC addresses can be deleted when the configured aging time expires.

When forwarding packets, based on the information about MAC address entries, the ISCOM6820 adopts the following modes:

- Unicast: when a MAC address entry, which is related to the destination MAC address of a packet, is listed in the MAC address table, the device will directly forward the packet

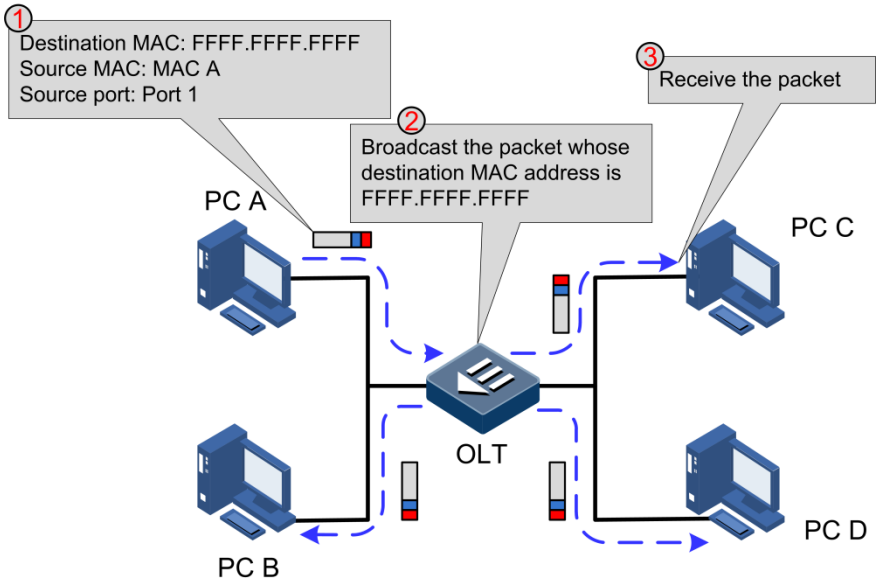
through the egress interface. Otherwise, the device will broadcast the packet, as shown in Figure 5-1.

Figure 5-1 Unicast forwarding mode of MAC address



- Multicast: when the device receives a packet whose destination address is a multicast MAC address, if the MAC address table contains an entry that is related to the destination MAC address of the packet, the device will forward the packet through the egress interface. Otherwise, the device will broadcast this packet.
- Broadcast: when the device receives an all-F packet, or when the device receives a packet whose MAC address is not listed in the MAC address table, it will flood the packet to all interfaces in the same VLAN except for the interface that receives this packet, as shown in Figure 5-2.

Figure 5-2 Broadcast forwarding mode of MAC address



5.2 Configuring dynamic MAC address

5.2.1 Preparing for configurations

Scenario

Dynamic MAC address entries can be added through the MAC address learning mechanism. You can limit the number of MAC addresses to be learnt. Dynamic MAC address entries will be deleted when the configured aging time expires, and can also be deleted manually. Dynamic MAC address entries will be cleared when the device is restarted.

Prerequisite

N/A

5.2.2 Default configurations

Default configurations of dynamic MAC address entries on the ISCOM6820 are as below.

Function	Default value
MAC address learning	Enable
Aging time of MAC address	300s
MAC address limit	Unlimited

Default configurations of dynamic MAC address entries on the Raisecom ONU devices are as below.

Function	Default value
MAC address learning	Enable
Aging time of MAC address	300s
MAC address limit	Unlimited

5.2.3 Configuring MAC address learning

When the network scale is large or positions of hosts change frequently, using static MAC addresses will increase maintenance workload. Thus, you need to configure MAC address learning to make the device learn MAC address dynamically to implement Layer 2 forwarding.

Configuring MAC address learning of OLT

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface { gpon-olt | ten-gigabitethernet} slot-id/olt-id`	Enter interface configuration mode.
3	`Raisecom(config-if-*-*:*)#mac-address-table learning`	Enable MAC address learning. You can use the **no mac-address-table learning** command to disable this function.

5.2.4 (Optional) configuring aging time of MAC address

To avoid explosive increase of the MAC address table, you need to configure the aging time for the dynamic MAC address table. The timer starts when a MAC address is added to the MAC address table, if no interface receives the frame whose source address is the MAC address in the aging time, the MAC address will be deleted from the dynamic MAC address table. Otherwise, the aging time timer will be updated and start timing again.

Configuring MAC address aging time of OLT

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#mac-address-table aging-time { 0 | period }`	Configure the aging time of dynamic MAC addresses. You can use the **no mac-address-table aging-time** command to restore default configuration. **Note** The value 0 refers to that the dynamic MAC address is not aged.

5.2.5 Checking configurations

Checking OLT configurations

No.	Command	Description
1	Raisecom#**show interface ten-gigabitethernet** *slot-id/port-list* **mac-address-table**	Show configurations of the MAC address on the OLT interface.
2	Raisecom#**show mac-address-table l2-address** [**vlan** *vlan-id* | **interface** { **gpon-olt** *slot-id/port-id* | **ten-gigabitethernet** *slot-id/port-id* | **port-channel** *group-id* }]	Show MAC address entries on the OLT interface.
3	Raisecom#**show mac aging-time**	Show the aging time of MAC addresses on the OLT.

Checking ONU configurations

No.	Command	Description
1	Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **mac-address-table l2-address** [**uni ethernet** *uni-id*] { **all** | **dynamic** | **static** } [**count**]	Show configurations of MAC address table on the ONU Ethernet interface.

5.3 Configuring static MAC address

5.3.1 Preparing for configurations

Scenario

Static MAC address entries, also termed as permanent addresses, can be added or removed manually, and do not age with time. For a network with small changes of devices, you can add static MAC address entries manually to decrease broadcast traffic on the network.

Prerequisite

N/A

5.3.2 Default configurations

N/A

5.3.3 Configuring static unicast MAC address

Static MAC address can be set for fixed servers, special persons (manager, financial staff, and so on) fixed and important hosts to make sure all data traffic to the MAC address are forwarded from the interface related to the static MAC address related preferentially.

Configuring static unicast MAC addresses of OLT

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mac-address-table static unicast** *mac-address* **vlan** *vlan-id* **interface** { **gpon-onu** *slot-id/port-id* | **ten-gigabitethernet** *slot-id/port-id* | **port-channel** *group-id* }	Configure static unicast MAC address entries on the OLT. You can use the **no mac-address-table static unicast** *mac-address* **vlan** *vlan-id* command to delete the configuration.

5.3.4 Configuring static multicast MAC address

Configuring static multicast MAC addresses on the OLT

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mac-address-table static multicast** *mac-address* **vlan** *vlan-id* { **add** | **remove** } **interface** { **epon-olt** *slot-id/port-id* | **gpon-olt** *slot-id/port-id* | **ten-gigabitethernet** *slot-id/port-id* | **port-channel** *group-id* }	Configure static multicast MAC addresses. You can use the **no mac-address-table static multicast** *mac-address* **vlan** *vlan-id* **port-list** *port-list* command to delete the configuration.

5.3.5 Configuring MAC address flapping

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** {**ten-gigabitethernet** } *slot-id/olt-id*	Enter physical interface configuration mode.
3	Raisecom(config-if-*-*:*)#**mac-address-table station move**	Configure MAC address flapping.

5.3.6 Checking configurations

Checking OLT configurations

No.	Command	Description
1	Raisecom#**show mac-address-table static unicast** [**vlan** *vlan-id* | **interface** { **gpon-olt** *slot-id/port-id* | **ten-gigabitethernet** *slot-id/port-id* | **port-channel** *group-id* }]	Show static unicast MAC addresses on the OLT.

No.	Command	Description
2	Raisecom#**show mac-address-table statistics unicast** [**vlan** *vlan-id* | **interface** { **gpon-olt** *slot-id/port-id* | **ten-gigabitethernet** *slot-id/port-id* | **port-channel** *group-id* }]	Show statistics on static unicast MAC addresses on the OLT.
3	Raisecom#**show mac-address-table multicast** [**statistics**]	Show static multicast MAC addresses on the OLT.

5.4 Maintenance and search

5.4.1 Preparing for configurations

Scenario

The ISCOM6820 supports clearing the Layer 2 MAC address table, including:

- Clear all MAC address entries.
- Clear dynamically-learnt MAC address entries.
- Clear statically-configured MAC address entries.

You can use the **search** command to search for the content of the MAC address entry and related information of the OLT or ONU.

Prerequisite

N/A

5.4.2 Default configurations

N/A

5.4.3 Clearing MAC addresses

Clearing MAC addresses on the OLT

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**clear** [**interface** { **gpon-olt** | **ten-gigabitethernet** } *slot-id/port-id*] **mac-address-table unicast** [**dynamic** | **static**] [**vlan** *vlan-id*]	Clear unicast MAC address entries on the OLT.

5.4.4 Searching MAC address

Searching MAC addresses on the OLT

Step	Command	Description
1	Raisecom#**search mac-address** *mac-address*	Search for a MAC address entry on the OLT.

5.4.5 Tracing MAC address

Step	Command	Description
1	Raisecom#**trace mac-address** *mac-address*	Trace a specified MAC address.

5.4.6 Checking configurations

Checking OLT configurations

No.	Command	Description
1	Raisecom#**show interface ten-gigabitethernet** *slot-id/port-list* **mac-address-table**	Show configurations of the MAC address table on the OLT.
2	Raisecom#**show mac-address-table l2-address** [**vlan** *vlan-id* | **interface** { **gpon-olt** *slot-id/port-id* | **ten-gigabitethernet** *slot-id/port-id* | **port-channel** *group-id* }]	Show information about the MAC address table on the OLT interface.
3	Raisecom#**show mac-address-table multicast** [**statistics**]	Show multicast MAC address entries on the OLT.
4	Raisecom#**show mac-address-table static unicast** [**vlan** *vlan-id* | **interface** { **gpon-olt** *slot-id/port-id* | **ten-gigabitethernet** *slot-id/port-id* | **port-channel** *group-id* }]	Show static unicast MAC address entries on the OLT.
5	Raisecom#**show mac-address-table statistics unicast** [**vlan** *vlan-id* / **interface** { **gpon-olt** *slot-id/port-id* | **ten-gigabitethernet** *slot-id/port-id* | **port-channel** *group-id* }]	Show statistics on static unicast MAC addresses on the OLT.

Checking ONU configurations

No.	Command	Description
1	Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **mac-address-table l2-address** [**uni ethernet** *uni-id*] { **all** | **dynamic** | **static** } [**count**]	Show MAC address entries on the ONU or specified ONU UNI.

6 Configuring VLAN

This chapter describes the VLAN features and configuration process of the device, and provides related configuration examples, including the following sections:

- Introduction
- Configuring VLAN
- Configuring QinQ
- Configuring VLAN ACL
- Configuring VLAN mapping
- Configuring VLAN partitioning
- Configuration examples

6.1 Introduction

6.1.1 VLAN

Overview

When too many PCs work in a network, a number of broadcast traffic will be generated. This will reduce network performance, even worse, making the network collapsed. To ensure PCs work at a high speed in the network, you must partition broadcast domains to reduce broadcast traffic. That is why Virtual Local Area Network (VLAN) technology is introduced.

VLAN is a Layer 2 isolation technology that is used to partition devices in a Local Area Network (LAN) logically instead of physically to network segments. Therefore multiple distinct virtual broadcast domains are created. By partitioning the VLAN, you can isolate hosts that do not need to communicate with others. Therefore, the broadcast traffic is reduced and fewer broadcast storms are generated.

A VLAN is a logical subnet or a broadcast domain. PCs in a VLAN can be located at different places. You can add any PC to a VLAN as required.

Hosts in a VLAN can receive data frames sent by other hosts in the same VLAN. However, they cannot receive data frames sent by hosts in other VLANs. Hosts in different VLANs can communicate through a router or a Layer 3 switch.

Note

Broadcast domain refers to a collection of devices that can receive broadcast packets sent by any device in a network. If the broadcast domain and broadcast traffic are over great, network performance will be reduced. What's worse, the network will collapse. Therefore, you must partition broadcast domain to improve network performance when establishing a network. You can partition a broadcast domain either by routers or by partitioning VLANs on a switch.

Advantages of VLAN

By partitioning VLANs, you can realize:

- Portioning broadcast domains and reducing broadcast storms
- Improving network security
- Simplifying network management

Working principle of VLAN

After you partition VLANs on a switching device, the device will be virtualized as multiple switching devices. The switching devices learn MAC addresses and forwarding packets based on VLAN. Each VLAN has an independent MAC address table.

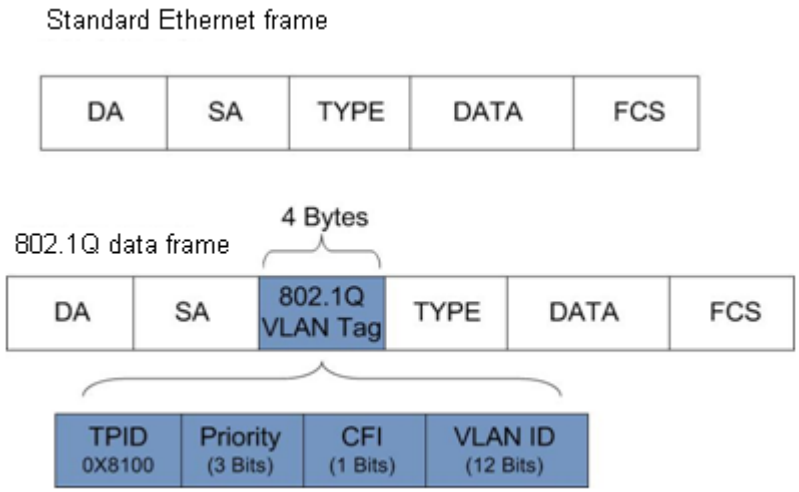
When a frame is sent to the ingress interface of a device, the device will query the VLAN where the ingress interface is and then query the MAC address table to which the VLAN is related. If the destination MAC address of the frame is listed in the MAC address table, the frame will be forwarded. Otherwise, the frame is discarded.

802.1Q protocol and VLAN Tag

After partitioning VLANs, to identify frames from different VLANs, you can use 802.1Q protocol to add VLAN Tags to them.

The 802.1Q protocol defines a new Ethernet field. Compared with the Ethernet frame, 802.1Q frame has a 4-Byte 802.1Q VLAN Tag field, which is added after the SA field. Figure 6-1 shows structures of Ethernet frame and 802.1Q frame.

Figure 6-1 Structures of Ethernet frame and 802.1Q frame



- Tag Protocol Identifier (TPID): a new type defined by IEEE to identify the frame as an IEEE 802.1Q-tagged frame. The 802.1Q TPID is 0x8100.
- VLAN Identifier (VID): a 12-bit field specifying the VLAN to which the frame belongs. The value ranges from 0 to 4095. VLAN 0 and VLAN 4095 are reserved VLANs. So the general range is 1 to 4094.
- Canonical Format Indicator (CFI): a 1-bit field used for compatibility among bus Ethernet, FDDI, and Token Ring networks.
- Priority Code Point (PCP): a 3-bit field which indicates the frame priority. Values are from 0 (best effort) to 7 (highest). The bigger the number is, the higher the priority is. When the network is congested, the device sends packets with higher priorities first.

VLAN mode of OLT interface

The interface on the ISCOM6820 supports two modes: Access mode and Trunk mode.

Table 6-1 lists compassion of interface modes and packet processing modes.

Table 6-1 VLAN modes and packet processing modes

Interface type	Processing ingress packets		Processing egress packets
	Untagged packet	Tagged packet	
Access	Add the Tag of the Access VLAN to the packet.	• If the VLAN ID for a packet is identical to the Access VLAN, receive the packet. • If the VLAN ID for a packet is not identical to the Access VLAN, discard the packet.	If the VLAN ID for a packet is identical to the Access VLAN ID, send the packet after removing the Tag.

Interface type	Processing ingress packets		Processing egress packets
	Untagged packet	Tagged packet	
Trunk	If the Native VLAN is in the VLAN ID list on an interface, receive the packet after adding the Tag of the Native VLAN to the packet.	• If the VLAN ID for a packet is in the VLAN ID list on an interface, receive the packet. • If the VLAN ID for a packet is not in the VLAN ID list on an interface, discard the packet.	• If the VLAN ID for a packet is identical to the Native VLAN ID, send the packet after removing the Tag. • If the VLAN ID for a packet is not identical to the Native VLAN ID, send the packet with its original Tag. Otherwise, discard the packet.

VLAN modes of ONU interface

Raisecom ONUs supports the following VLAN modes:

- VLAN Transparent mode
- VLAN Tagged mode
- VLAN Translation mode
- VLAN Trunk mode

Specific behaviours of various VLAN modes are shown as below.

Table 6-2 lists how ONU interfaces to process Ethernet frames in VLAN Transparent mode.

Table 6-2 Processing modes of Ethernet frames in VLAN Transparent mode

Direction	With/Without Tag	Processing mode
Uplink	With VLAN Tag	Forward Ethernet packets without any change (reserve the original VLAN Tag).
	Without VLAN Tag	Forward Ethernet packets without any change.
Downlink	With VLAN Tag	Forward Ethernet packets without any change (reserve the original VLAN Tag).
	Without VLAN Tag	Forward Ethernet packets without any change.

Table 6-3 lists how ONU interfaces to process Ethernet frames in VLAN Tagged mode.

Table 6-3 Processing modes of Ethernet frames in VLAN Tagged mode

Direction	With/Without Tag	Processing mode
Uplink	With VLAN Tag	Discard Ethernet packets.
	Without VLAN Tag	Forward Ethernet packets by adding new VLAN Tags (Native VLAN of the interface).

Direction	With/Without Tag	Processing mode
Downlink	With VLAN Tag	Forward Ethernet packets to related UNI based on VID and remove their VLAN Tags. If VLAN IDs of downlink Tagged packets are not identical to the configured ones, these packets are discarded.
	Without VLAN Tag	Discard Ethernet packets.

Table 6-4 lists the mode used by the ONU to process Ethernet frames in VLAN Translation mode.

Table 6-4 Processing modes of Ethernet frames in VLAN Translation mode

Direction	With/Without Tag	Processing mode
Uplink	With VLAN Tag	If VIDs of the original Tags have related entries (input VIDs) in VLAN Translation list of the related interface, forward Ethernet packets after translating VIDs into related VIDs (output VIDs). Otherwise, Ethernet packets are discarded.
	Without VLAN Tag	Forward Ethernet packets by adding native VLANs to Untagged packets.
Downlink	With VLAN Tag	If VIDs of the original Tags have related entries (input VIDs) in VLAN Translation list of the related interface, forward Ethernet packets after translating VIDs into related VIDs (output VIDs). Otherwise, Ethernet packets are discarded. If VIDs of the original Tags are native VIDs, forward Ethernet packets after removing their Tags.
	Without VLAN Tag	Discard Ethernet packets.

Table 6-5 lists the mode used by the ONU to process Ethernet frames in VLAN Trunk mode.

Table 6-5 Processing modes of Ethernet frames in VLAN Trunk mode

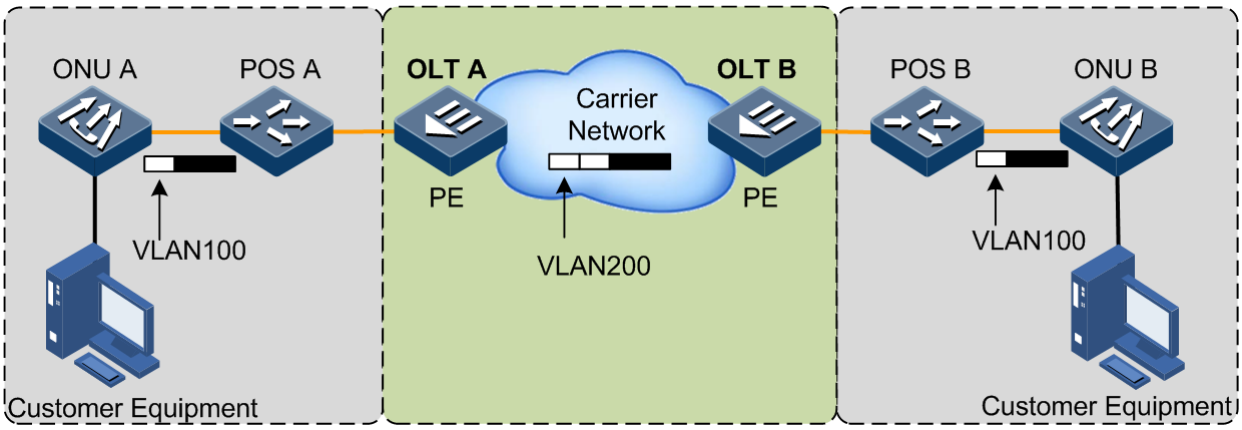
Direction	With/Without Tag	Processing mode
Uplink	With VLAN Tag	If VLANs carried by Ethernet packets are in allowed VLAN list of the interface, forward these Ethernet packets. Otherwise, discard these Ethernet packets.
	Without VLAN Tag	Forward Ethernet packets by adding native VLANs to Untagged packets.
Downlink	With VLAN Tag	If VLANs carried by Ethernet packets are in allowed VLAN list of the interface, forward these Ethernet packets. Otherwise, discard these Ethernet packets. If VLAN IDs carried by Ethernet packets are native VLANs, forward these Ethernet packets.
	Without VLAN Tag	Discard Ethernet packets.

6.1.2 QinQ

QinQ technology is an extension of 802.1Q, which is defined in the 802.1ad standard defined by the IEEE.

Basic QinQ is a simple Layer 2 VPN tunnel technique, which encapsulates outer VLAN Tag for user private network packet at the carrier access end. The packet takes double VLAN Tag to transmit through backbone network (public network) of carrier. In the public network, the packet is transmitted according to the outer VLAN Tag (public VLAN Tag). And the private VLAN Tag is transmitted as the data in the packet.

Figure 6-2 Basic QinQ networking



As shown in Figure 6-2, the OLT is the Provider Edge (PE). Its uplink interface is connected to the Carrier network and the PON interface is connected to the user network through ONUs.

A packet is sent to the PE by a customer equipment, carrying a Tag VLAN 100. When passing through the uplink interface of the PE, the packet is added with an outer Tag VLAN 200. And then the packet is sent to the Carrier network through the uplink interface of the PE.

When the packet with the outer Tag is sent to the peer PE, this PE will remove the outer Tag of the packet and then send the packet to the customer equipment. In this case, the packet only carries the Tag VLAN 100.

6.1.3 VLAN mapping

VLAN mapping is mainly used to replace the private VLAN Tags of Ethernet packets with Carrier's VLAN Tags, so that packets will be transmitted according to Carrier's VLAN forwarding rules. When packets are sent to the peer private network from the Carrier network, these VLAN Tags recover to the original private VLAN Tags, according to the same VLAN forwarding rules. Therefore, packets are correctly sent to the destination.

When two or more user networks, which connect the Carrier network, communicate with each other, these user networks define different service access requirements and various VLAN Tags for all packets. When the Carrier network performs Layer 2 switching on packets, with VLAN mapping, the Carrier's access device will replace VLAN Tags of these packets with VLAN Tags defined by the Carrier. According to the switching mode and route defined by the Carrier, packets are forwarded to the destination. When packets are sent to the peer user network from the Carrier network, the Carrier defined VLAN Tags are replaced with VLAN Tags that can be recognized by the user network. Then the peer user network performs the Layer 2 addressing among the VLAN Tags to access to destination hosts.

When the OLT receives packets with private VLAN Tags, it will match the private VLAN Tags according to configured VLAN mapping rules. If success, the private VLAN Tags are replaced according to configured VLAN mapping rules. VLAN mapping provides the following modes:

- 1:1 VLAN mapping: the VLAN Tag carried by a packet from a specified VLAN is replaced with a new VLAN Tag.
- N:1 VLAN mapping: different VLAN Tags carried by packets from two or more VLANs are replaced with the same VLAN Tag

6.2 Configuring VLAN

6.2.1 Preparing for configurations

Scenario

The main function of VLAN is to divide logic network segments. There are 2 typical application modes:

- In a small-scale LAN, you can partition multiple VLANs on a Layer 2 device, separating hosts logically. In this case, hosts in the same VLAN can communicate with each other, while hosts in different VLANs cannot.
- In a large-scale LAN or enterprise network, there are many hosts. The hosts in the same department are located at different places but they need to communicate with each other. You can configure VLANs on multiple interconnected Layer 2 devices to make hosts in the same VLAN communicate with each other and hosts in different VLANs unable to communicate. If hosts in different VLANs need to communicate, use a Layer 3 device, such as a router.

Prerequisite

N/A

6.2.2 Default configurations

Default configurations of VLAN on the ISCOM6820 are as below.

Function	Default value
Interface TPID	0x8100
Filter type of uplink data packets on interface	All (allow all packets to pass)
VLAN processing mode on interface	• Uplink: Access • Downlink: Access
New priority used by the interface to add VLAN Tag to data	• Uplink: 0 • Downlink: 0
Enable/Disable the interface to use a new priority when adding VLAN Tag to data	• Uplink: disable • Downlink: disable

Function	Default value
VLAN ID used by the interface to add VLAN Tag to data	• Uplink: 1 • Downlink: 1

Default configurations of VLAN on the ISCOM6820 are as below.

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

6.2.3 Configuring OLT interface VLAN

Creating VLAN

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#create vlan` *vlan-id* { **active** | **suspend** }	Create a VLAN. You can use the **no vlan** { **all** | *vlan-id* } command to delete the VLAN.
3	`Raisecom(config)#vlan` *vlan-id*	Enter VLAN configuration mode. **Note** If the VLAN has not been created, the system creates a VLAN automatically when you use this command, and the VLAN is in suspended status.
4	`Raisecom(config-vlan-*)#name` *name*	(Optional) configure the VLAN name. You can use the **no name** command to restore default configuration.
5	`Raisecom(config-vlan-*)#state` { **active** | **suspend** }	(Optional) configure the VLAN status.
6	`Raisecom(config-vlan-*)#p2p` { **enable** | **disable** }	(Optional) enable/disable VLAN intercommunication.

Note

- VLAN 1 is the default VLAN. All interfaces in Access mode belong to the default VLAN. VLAN 1 cannot be created and deleted.

- By default, VLANs are named by "VLAN + 4-digit VLAN ID". For example, VLAN 1 is named VLAN 0001 by default, and VLAN 4094 is named as VLAN 4094 by default.
- All configurations of VLAN are not effective until the VLAN is activated. When the VLAN is in suspended status, you can configure the VLAN, such as deleting/adding interfaces and setting VLAN name. The configurations will be saved by the system. Once the VLAN is activated, the configurations will take effect in the system.

Configuring interface VLAN mode

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** { **ten-gigabitethernet** | **gpon-olt** } *slot-id/port-id*	Enter physical interface configuration mode.
3	Raisecom(config-if-*-*:*)#**switchport mode** { **access** | **trunk** }	Configure the interface mode to Access or Trunk. You can use the **no switchport mode** command to restore default configurations.

Configuring interface VLAN of Access mode

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** { **ten-gigabitethernet** | **gpon-olt** } *slot-id/port-id*	Enter physical interface configuration mode.
3	Raisecom(config-if-*-*:*)#**switchport mode access**	Configure the VLAN mode of the interface to Access.
4	Raisecom(config-if-*-*:*)#**switchport access vlan** *vlan-id*	Configure the default VLAN for the interface in Access mode. You can use the **no switchport access vlan** command to restore default configuration.
5	Raisecom(config-if-*-*:*)#**vlan drop-untagged**	(Optional) configure the interface to discard the untagged packet. You can use the **no vlan drop-untagged** command to restore default configuration.
6	Raisecom(config-if-*-*:*)#**exit**	Return global configuration mode.
7	Raisecom(config)#**interface ten-gigabitethernet** *slot-id/port-id*	Enter 10GE physical interface configuration mode.
8	Raisecom(config-if-ten-gigabitethernet-*:*)#**switchport down-hold-time** *time*	(Optional) configure the the delay time for the uplink interface being Down.

Note

- If the VLAN is not created and activated when you configure the default VLAN for the Access interface, the system will create and activate the VLAN automatically.
- If the Access VLAN is deleted or suspended by users manually, the system will configure the Access VLAN of the interface as default VLAN 1 automatically.
- The Access interface-allowed VLAN list is only effective to the static VLAN.

Configuring interface VLAN of Trunk mode

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** { **ten-gigabitethernet** | **gpon-olt** } *slot-id/port-id*	Enter physical interface configuration mode.
3	Raisecom(config-if-*-*:*)#**switchport mode trunk**	Configure the VLAN mode of the interface to Trunk.
4	Raisecom(config-if-*-*:*)#**switchport trunk native vlan** *vlan-id*	Configure the Native VLAN of the interface. You can use the **no switchport trunk native vlan** command to restore default configuration.
5	Raisecom(config-if-*-*:*)#**switchport trunk allowed vlan** { **all** | [**add** | **remove**] *vlan-list* } [**confirm**]	Configure the VLAN allowed to pass by the Trunk interface. You can use the **no switchport trunk allowed vlan** command to restore default configuration. **Note** By default, the Trunk interface allows all VLANs to pass.
6	Raisecom(config-if-*-*:*)#**switchport trunk untagged vlan** { **all** | [**add** | **remove**] *vlan-list* } [**confirm**]	(Optional) configure the VLAN of which the Tag is removed by the Trunk egress interface. You can use the **no switchport trunk untagged vlan** command to restore default configuration.
7	Raisecom(config-if-*-*:*)#vlan drop-untagged	(Optional) configure the interface to discard the untagged packet. You can use the **no vlan drop-untagged** command to restore default configuration.
8	Raisecom(config-if-*-*:*)#**exit**	Return global configuration mode.
9	Raisecom(config)#**interface ten-gigabitethernet** *slot-id/port-id*	Enter 10GE physical interface configuration mode.
10	Raisecom(config-if-ten-gigabitethernet-*:*)#**switchport down-hold-time** *time*	(Optional) configure the the delay time for the uplink interface being Down.

Note

- The Trunk interface allows Native VLAN packets to pass regardless of configurations on Trunk interface allowed VLAN list and Untagged VLAN list. The forwarded packets do not carry VLAN TAG.
- When you configure the Native VLAN, the system will create and activate the VLAN automatically if the VLAN is not created and activated in advance.
- The system will configure the Trunk Native VLAN as the default VLAN if the Native VLAN is deleted or blocked manually.
- The Trunk interface allowed VLAN list and Trunk Untagged VLAN list are only effective to the static VLAN.

Configuring VLAN ACL

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface { ten-gigabitethernet | gpon-olt } slot-id/port-id`	Enter physical interface configuration mode.
3	`Raisecom(config-if-*-*:*)#switchport vlan-access-list list rule rule-id add { inner | outer } vlan-id`	Add the VLAN to the VLAN ACL.
4	`Raisecom(config-if-*-*:*)#switchport vlan-access-list list rule rule-id remove inner`	Delete the external VLAN ID from the VLAN ACL.
5	`Raisecom(config-if-*-*:*)#switchport vlan-access-list list rule rule-id translate { inner | outer } vlan to vlan-id`	Translate the VLAN ID in the VLAN ACL.

6.2.4 Configuring VLAN on ONU UNI

Configuring VLAN mode

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)# gpon-olt uni ethernet slot-id/olt-id/onu-id/uni-id`	Enter ONU UNI Ethernet interface configuration mode.
3	`Raisecom(config-*-onu-ethernet-*/*/*:*)#vlan mode { tagged | translation | transparent | trunk | aggregation }`	Configure the VLAN mode of the ONU UNI. You can use the **no vlan mode** command to restore default configurations.

Configuring VLAN translation rules

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**vlan translation-rule** *rule-id* **old** *vlan-id priority* **new** *vlan-id priority*	Create a VLAN translation rule. You can use the **no vlan translation-rule** { *rule-id* | **all** } command to delete the VLAN translation rule.
3	Raisecom(config)#{ **gpon-olt** } **uni ethernet** *slot-id/olt-id/onu-id/uni-id*	Enter ONU UNI Ethernet interface configuration mode.
4	Raisecom(config-*-onu-ethernet-*/*/*:*)#**vlan translation-rule** *rule-list*	Apply the VLAN translation rule to the ONU UNI. You can use the **no vlan translation-rule** command to restore default configurations.

Note

- The rule ID created and the rule contents must be unique.
- The rule after being created cannot be modified. If you need to modify it, you have to delete it and recreate one.
- The rule which is referenced by the UNI cannot be deleted. If you need to delete it, you should cancel the reference relationship first.

Configuring VLAN aggregation rules

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**vlan aggregation-rule** *rule-id* [**name** *name*] **vlan-list** *vlan-list* **target** *vlan-id*	Create a VLAN aggregation rule. You can use the **no vlan aggregation-rule** { **all** | *rule-list* } command to delete the configurations.
3	Raisecom(config)#**vlan aggregation-rule** *rule-id* **name** *name* [**vlan-list** *vlan-lilst* **target** *vlan-id*]	Configure the VLAN aggregation rule name. You can use the **no vlan aggregation-rule** { **all** | *rule-list* } command to delete the configurations.
4	Raisecom(config)#{ **gpon-olt** } **uni ethernet** *slot-id/olt-id/onu-id/uni-id*	Enter ONU UNI Ethernet interface configuration mode.
5	Raisecom(config-*-onu-ethernet-*/*/*:*)#**vlan aggregation-rule** *rule-list*	Apply VLAN aggregation rules to the ONU UNI. You can use the **no vlan aggregation-rule** command to restore default configurations.

Note

- The rule ID created and the rule contents must be unique.
- The rule after being created cannot be modified. If you need to modify it, you have to delete it and recreate one.

- The rule which is referenced by the UNI cannot be deleted. If you need to delete it, you should cancel the reference relationship first.

Configuring default VLAN on UNI

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#{ **gpon-olt** } **uni ethernet** *slot-id/olt-id/onu-id/uni-id*	Enter ONU UNI Ethernet interface configuration mode.
3	Raisecom(config-*-onu-ethernet-*/*/*:*)#**native vlan** *vlan-id* [*priority*]	Configure the default VLAN and priority of the ONU UNI. You can use the **no native vlan** command to restore default configurations. **Note** This command takes effect only in Tag, Trunk, and Translation VLAN modes.

Configuring Trunk VLAN

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#{ **gpon-olt** } **uni ethernet** *slot-id/olt-id/onu-id/uni-id*	Enter ONU UNI Ethernet interface configuration mode.
3	Raisecom(config-*-onu-ethernet-*/*/*:*)#**vlan trunk allowed** *vlan-list*	Configure the VLAN list allowed to pass by the ONU UNI in Trunk mode. You can use the **no vlan tunkd allowed** command to restore default configurations.

6.2.5 Checking configurations

No.	Command	Description
1	Raisecom#**show vlan** [*vlan-list* | **static** | **dynamic**]	Show VLAN configurations.
2	Raisecom#**show vlan** [*vlan-list*] **member-port**	Show information about the VLAN member interface and untagged interface.
3	Raisecom#**show onu-remote vlan translation-rule** [*rule-list*]	Show the created VLAN translation rules of the ONU.
4	Raisecom#**show onu-remote vlan aggregation-rule** [*rule-list*]	Show the created VLAN aggregation rules of the ONU.
5	Raisecom#**show epon-onu** *slot-id/olt-id/onu-id* **uni ethernet** [*uni-id*] **vlan**	Show VLAN configurations of the ONU Ethenet interface.

No.	Command	Description
6	Raisecom#**show interface** { **gpon-olt** *slot-id/olt-id* | **ten-gigabitethernet** *slot-id/olt-id* } **switchport vlan-access-list**	Show configurations of the VLAN ACL on the physical interface.
7	Raisecom#**show interface** { **gpon-olt** *slot-id/port-list* / **gpon-onu** *slot-id/olt-id/onu-list* / **gigabitethernet** *slot-id/port-list* / **ten-gigabitethernet** *slot-id/port-list* / **ten-giga-epon-olt** *slot-id/port-list* }**vlan**	Show configurations of the VLAN on the interface.

6.3 Configuring QinQ

6.3.1 Preparing for configurations

Scenario

With application of basic QinQ, you can add outer VLAN Tag to plan the VLAN ID freely for the private network so as to make the data at both ends of carrier network transmitted transparently without conflicting with the VLAN ID in the Internet Service Provider's (ISP) network.

Prerequisite

N/A

6.3.2 Default configurations

Default configurations of QinQ on the ISCOM6820 are as below.

Function	Default value
TPID of outer Tag	0x8100
Basic QinQ	Disable

6.3.3 Configuring basic QinQ

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** { **ten-gigabitethernet** |**gpon-olt** } *slot-id/port-id*	Enter physical interface configuration mode.
3	Raisecom(config-if-*-*:*)#**vlan dot1q-tunnel**	Enable basic QinQ on the interface. You can use the **no vlan dot1q-tunnel** to disable this function.

Step	Command	Description
4	Raisecom(config-if-*-*:*)#**vlan tpid** *tpid*	Configure the outer VLAN TPID. You can use the **no vlan tpid** command to restore default configuration.

Note

- After QinQ is enabled, the interface processes the received tagged packets as untagged packets, namely, adding outer VLAN Tags to original packets.
- After QinQ is enabled, configurations for the outer VLAN are the same with those for the general VLAN. For details, refer to section 6.2.3 Configuring OLT interface VLAN.

6.3.4 Checking configurations

No.	Command	Description
1	Raisecom#**show interface** [**ten-gigabitethernet** | **gpon-olt**] *slot-id/olt-id* **vlan-mapping**	Show QinQ configurations on the interface.

6.4 Configuring VLAN ACL

6.4.1 Preparing for configurations

Scenario

With VLAN ACL, you can flexibly match the source MAC address, SVLAN, CVLAN, CoS, and Ethernet type in Layer 2 packets, and the source IPv4 address, destination IPv4 address and IP type in Layer 3 packets by configuring matching rules, and configure actions on different packets according to the matching situation, such as adding outer VLANs, modifying inner VLANs, and so on.

Prerequisite

N/A

6.4.2 Default configurations

N/A

6.4.3 Creating ACL

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)#**vlan-access-list** *list-number*	Create a VLAN ACL and enter the VLAN ACL configuration mode. You can use the **no vlan-access-list** *acl-numb*er command to delete the ACL.
3	Raisecom(config-vlan-acl)#**description** *desc-string*	(Optional) configure the VLAN ACL description. You can use the **no description** command to restore to the default condition.
4	Raisecom(config-vlan-acl)#**rule** *rule-number*	Create a VLAN ACL sub-rule and enter sub-rule configuration mode. You can use the **no rule** *rule-number* command to delete the sub-rule.
5	Raisecom(config-vlan-acl-*-rule-*)#**access-type** { **permit** | **deny** }	Configure the access type of the sub-rule.

6.4.4 Configuring matching contents

Configuring IPv4 matching contents

Step	Command	Description
1	Raisecom(config-vlan-acl-*-rule-*)#**match mac source** *mac-address* [*mask*]	(Optional) match the source MAC address.
2	Raisecom(config-vlan-acl-*-rule-*)#**match** { **svlan** *vlan-id* | **svlan-cos** *cos* }	(Optional) match the SVLAN ID and CoS.
3	Raisecom(config-vlan-acl-*-rule-*)#**match** { **cvlan** *vlan-id* | **cvlan-cos** *cos* }	(Optional) match the CVLAN ID and CoS.
4	Raisecom(config-vlan-acl-*-rule-*)#**match ethertype** { *frame-type frame-type-mask* | **arp** | **eapol** | **flowcontrol** | **ip** | **loopback** | **mpls** | **mpls-mcast** | **pppoe** | **pppoedisc** | **x25** | **x75** }	(Optional) match the protocol type in the Layer 2 frame header.
5	Raisecom(config-vlan-acl-*-rule-*)#**match ip** { **destination-address** | **source-address** } *ip-address* [*mask*]	(Optional) match the source and destination IP address.
6	Raisecom(config-vlan-acl-*-rule-*)#**match ip protocol** { *protocol-num* | **ahp** | **esp** | **gre** | **icmp** | **igmp** | **igrp** |**ipinip** | **ospf** | **pcp** | **pim** | **tcp** | **udp** }	(Optional) match the IP upper-layer protocol type.
7	Raisecom(config-vlan-acl-*-rule-*)#**match ip tcp** { **destination-port** | **source-port** } { *port-id* | **bgp** | **domain** | **echo** | **exec** | **finger** | **ftp** | **ftp-data** | **gopher** | **hostname** | **ident** | **irc** | **klogin** | **kshell** | **login** | **lpd** | **nntp** | **pim-auto-rp** | **pop2** | **pop3** | **smtp** | **sunrpc** | **tacacs** | **talk** | **telnet** | **time** | **uucp** | **whois** | **www** }	(Optional) match the destination or source port ID of TCP packets. You can use the **no match ip tcp** { **destination-port** | **source-port** } command to delete the configuration.

Step	Command	Description
8	Raisecom(config-vlan-acl-*-rule-*)#**match ip udp** { **destination-port** | **source-port** } { *port-id* | **biff** | **bootpc** | **bootps** | **domain** | **echo** | **mobile-ip** | **netbios-dgm** | **netbios-ns** | **netbios-ss** | **ntp** | **pim-auto-rp** | **rip** | **smtp** | **snmptrap** | **sunrpc** | **syslog** | **tacacs** | **talk** | **tftp** | **time** | **who** }	(Optional) match the destination or source port ID of UDP packets. You can use the **no match ip udp** { **destination-port** | **source-port** } command to delete the configuration.

Configuring IPv6 matching contents

Step	Command	Description
1	Raisecom(config-vlan-acl-*-rule-*)#**match ipv6** { **destination-address** *ipv6-address/prexfix* | **source-address** *ipv6-address/prexfix* }	(Optional) match the source and destination IPv6 addresses.
2	Raisecom(config-vlan-acl-*-rule-*)#**match ipv6 protocol** *protocol-num*	(Optional) match the IPv6 ID.
3	Raisecom(config-vlan-acl-*-rule-*)#**match ipv6 traffic-class** *class-value*	(Optional) define ACL matching rules. Match the IPv6 Traffic-class. If the attribute of the packet is the same as the defined rule, the packet will be processed (permit or deny). You can use the **no match ipv6 traffic-class** command to delete the rule.

6.4.5 Configuring actions for matched packets

Step	Command	Description
1	Raisecom(config-vlan-acl-*-rule-*)#**add** { **outer** | **inner** } *vlan-id*	(Optional) add a VLAN. You can use the **no add** { **outer** | **inner** } command to delete the configuration.
2	Raisecom(config-vlan-acl-*-rule-*)#**remove inner**	(Optional) remove the VLAN. You can use the **no remove inner** command to delete the configuration.
3	Raisecom(config-vlan-acl-*-rule-*)#**translate** { **outer** | **inner** } **vlan to** *vlan-id*	(Optional) configure VLAN mapping. You can use the **no translate** { **outer** | **inner** } **vlan** command to delete the configuration.
4	Raisecom(config-vlan-acl-*-rule-*)#**translate outer cos to** *cos*	(Optional) modify the CoS value. You can use the **no translate outer cos** command to delete the configuration.

6.4.6 Applying VLAN-ACL

Step	Command	Description
1	Raisecom(config)#**interface** { **ten-gigabitethernet** | **gpon-olt** } *slot-id/port-id*	Enter physical interface configuration mode.
2	Raisecom(config-if-*-*:*)#**vlan-access-list** *list-num*	Apply VLAN ACL rules to the interface. You can use the **no vlan-access-list** *list-num* command to delete VLAN ACL rules. **Note** Applying a VLAN ACL to an interface actually only processes incoming interface packets and has no effect on outgoing interface packets.
3	Raisecom(config-if-*-*:*)#**switchport vlan-access-list** *access-list* **rule** *rule-number* **add outer** *vlan-id* Raisecom(config-if-*-*:*)#**switchport vlan-access-list** *access-list* **rule** *rule-number* **translate outer vlan to** *vlan-id* Raisecom(config-if-*-*:*)#**switchport vlan-access-list** *access-list* **rule** <1-256> **add inner** *vlan-id* Raisecom(config-if-*-*:*)#**switchport vlan-access-list** *access-list* **rule** <1-256> **translate inner vlan to** *vlan-id* Raisecom(config-if-*-*:*)#**switchport vlan-access-list** *access-list* **rule** <1-256> **remove inner**	Apply the VLAN ACL subrules in the ingress direction of the interface. This application matches the contents to be matched defined in the corresponding VLAN ACL subrule and defines the action for packets.

6.4.7 Checking configurations

No.	Command	Description
1	Raisecom#**show vlan-access-list** { **all** | *acl-num* }	Show VLAN ACL configurations.
2	Raisecom#**show interface** [**ten-gigabitethernet** | **gpon-olt**] *slot-id/olt-id* **vlan-access-list**	Show VLAN ACL rules applied to the interface.

6.5 Configuring VLAN mapping

6.5.1 Preparing for configurations

Scenario

Different from QinQ, VLAN mapping changes the VLAN Tag without encapsulating multilayer VLAN Tags so that packets are transmitted according to the carrier's VLAN forwarding rules. VLAN mapping does not increase the length of the original packet. It can be used in the following scenarios:

- Translate the VLAN ID of user service to the VLAN ID of the carrier.
- Translate VLAN IDs of multiple user services to the VLAN ID of the carrier.

Prerequisite

- Connect the interface, configure its physical parameters, and make it Up at the physical layer.
- Create a VLAN.

6.5.2 Default configurations

Default configurations of VLAN mapping on the ISCOM6820 are as below.

Function	Default value
VLAN mapping	Enable

6.5.3 Configuring VLAN mapping mode

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface { ten-gigabitethernet | gpon-olt } slot-id/port-id`	Enter physical interface configuration mode.
3	`Raisecom(config-if-*-*:*)#vlan-mapping cos-aware`	Configure CoS-aware VLAN mapping, that is, VLAN+CoS mapping. You can use the **no vlan-mapping cos-aware** command to disable this function.
4	`Raisecom(config-if-*-*:*)#vlan-mapping { egress | ingress } drop-unmatched`	Drop packets which mismatch VLAN mapping rules. You can use the **no vlan-mapping** { **egress** | **ingress** } **drop-unmatched** command to disable this function.

6.5.4 Configuring 1:1 VLAN mapping

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** { **ten-gigabitethernet** | **gpon-olt** } *slot-id/port-id*	Enter physical interface configuration mode.
3	Raisecom(config-if-*-*:*)#**vlan-mapping** { **ingress** | **egress** } **outer** *before-outer* **translate outer** *after-outer* **inner** { **add** *vlan-id* | **remove** | *vlan-id* | **unchange** }	Configure 1:1 VLAN mapping rules in the ingress or egress direction of the interface (translate the outer VLAN Tag only).
4	Raisecom(config-if-*-*:*)#**vlan-mapping** { **ingress** | **egress** } **outer** *before-outer* **inner** *before-inner* **translate outer** *after-outer* **inner** { *vlan-id* | **remove** }	Configure 1:1 VLAN mapping rules in the ingress or egress direction of the interface (translate both the outer VLAN Tag and inner VLAN Tag).
5	Raisecom(config-if-*-*:*)#**vlan-mapping ingress outer** *before-outer* **translate outer** *after-outer* **inner copy-from-outer**	Configure 1:1 VLAN mapping rules in the mapping mode in the ingress direction of the interface.

6.5.5 Configuring N:1 VLAN mapping

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** { **ten-gigabitethernet** | **gpon-olt** } *slot-id/port-id*	Enter physical interface configuration mode.
3	Raisecom(config-if-*-*:*)#**vlan-mapping outer** *before-outer* **aggregate outer** *after-outer* **inner** { **add** *vlan-id* | **unchange** }	Configure N:1 VLAN mapping rules based on interface (translate the outer VLAN Tag and add the inner VLAN Tag).

6.5.6 Checking configurations

No.	Command	Description
1	Raisecom#**show interface** { **gpon-olt** | **ten-gigabitethernet** } *slot-id/port-id* **vlan-mapping** { **ingress** | **egress** } **translate**	Show 1:1 VLAN mapping rules in the egress direction of the interface.
2	Raisecom#**show interface** { **gpon-olt** | **ten-gigabitethernet** } *slot-id/port-id* **vlan-mapping aggregate**	Show N:1 VLAN mapping rules in the egress direction of the interface.

6.6 Configuring VLAN partitioning

6.6.1 Preparing for configurations

Scenario

- VLAN partitioning by MAC address

After MAC-VLAN is enabled on an interface, MAC-VLAN association on the interface becomes invalid. When the interface receives packets, it matches the source MAC address of these packets with the MAC-VLAN. If the matching is successful, the interface forwards packets according to matched VLAN ID and priority. If the matching fails, the interface matches packets according to other matching rules.

- VLAN partitioning by IP subnet

If the device is enabled with IP subnet VLAN, it will match the source IP address of received packets with the ip-subnet-vlan entry after receiving packets. If the matching is successful, it forwards packets according to the matched VLAN and priority.

- VLAN partitioning by Ethernet type

Partitioning VLANs by Ethernet type associates the specified protocol type with VLANs, and determines the VLAN, to which the packets of different protocol types belong to, according to the association relation, and automatically assigns packet with the VLAN for transmission. It is used on the network which uses different transmission paths according to diferent protocol types.

Prerequisite

N/A

6.6.2 Default configurations

Default configurations of VLAN partitioning on the ISCOM6820 are as below.

Function	Default value
MAC-VLAN	Disable
VLAN partitioning based on IP subnet	Disable
VLAN partitioning based on protocol	Disable

6.6.3 Configuring VLAN based on MAC address

Configure the VLAN based on MAC address for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mac-vlan** *mac-address* [*mask*] **vlan** *vlan-id* [**priority** *value*]	Associate a MAC address with a VLAN

Step	Command	Description
3	Raisecom(config)#**mac-vlan enable**	Enable MAC-VLAN.

Caution

- If the MAC address is a multicast MAC address, all-0 or all-F address, the configuration will fail.
- If you associate a created MAC address to a VLAN but this association conflict with an existing association (for example, the MAC address is associated with different VLANs), the association will fail.

6.6.4 Configuring VLAN based on IP subnet

Configure the VLAN based on IP subnet for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip-subnet-vlan** { *ip-address/prefix-length* | *ipv6-address/prefix-length* } **vlan** *vlan-id* [**priority** *value*]	Associate a VLAN with an IP subnet.
3	Raisecom(config)#**ip-subnet-vlan enable**	Enable VLAN partitioning based on IP subnet.

Caution

- If the IP address or subnet mask is invalid, the configuration will fail.
- If you associate a created IP subnet to a VLAN but this association conflict with an existing association (for example, the IP subnet is associated with different VLANs), the association will fail.

6.6.5 Configuring VLAN based on protocol

Configure the VLAN based on protocol for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**protocol-vlan** { *ethertype* | **ipv4** | **ipv6** | **arp** | **pppoe** | **pppoedisc** } **vlan** *vlan-id* [**priority** *value*]	Configure the rule for associating the protocol VLAN with Ethernet packets.
3	Raisecom(config)#**protocol-vlan enable**	Enable VLAN partitioning based on protocol.

6.6.6 Checking configurations

No.	Command	Description
1	Raisecom#**show mac-vlan** { **all** | **vlan** *vlan-id* | *mac-address* [*mask*] }	Show configurations of MAC-VLAN.
2	Raisecom#**show ip-subnet-vlan**{ **all** | **vlan** *vlan-id* | *ip-address* | *ip-address/prefix-length* | *ipv6-address* | *ipv6-address/prefix-length* }	Show configurations of the IP subnet VLAN.
3	Raisecom#**show protocol-vlan** { *ethertype* | **ipv4** | **ipv6** | **arp** | **pppoe** | **pppoedisc** | **all** | **vlan** *vlan-id* }	Show configurations of all protocol VLANs.

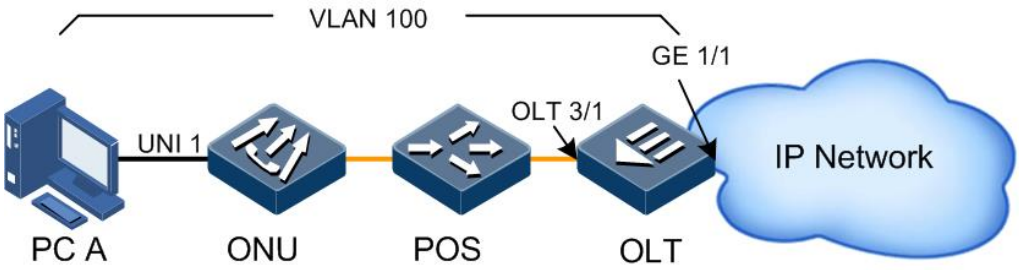
6.7 Configuration examples

6.7.1 Example for configuring VLAN

Networking requirements

As shown in Figure 6-3, the user connects the ONU through UNI 1 and the user VLAN is 100. The OLT connects the IP network through 10GE interface 10/1, and connects the ONU downstream through OLT PON interface 3/1. Under this network topology, activate the data service.

Figure 6-3 Configuring VLAN



Configuration steps

- Configure the OLT.

Step 1 Create a VLAN.

```
Raisecom#config
Raisecom(config)#create vlan 100 active
```

Step 2 Configure the uplink GE interface VLAN.

```
Raisecom(config)#interface ten-gigabitethernet 1/1
Raisecom(config-if-ten-gigabitethernet-1:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-1:1)#switchport trunk allowed vlan
100
Raisecom(config-if-ten-gigabitethernet-1:1)#exit
```

Step 3 Configure the VLAN of the PON interface.

```
Raisecom(config)#interface gpon-olt 3/1
Raisecom(config-if-gpon-olt-3:1)#switchport mode trunk
Raisecom(config-if-gpon-olt-3:1)#switchport trunk allowed vlan 100
Raisecom(config-if-gpon-olt-3:1)#end
```

Step 4 Configure ONU auto-registration.

```
Raisecom(config)#interface gpon-olt 3/1
Raisecom(config-if-gpon-olt-3:1)#authorization mode none
Raisecom(config-if-gpon-olt-3:1)#exit
```

- Configure the ONU.

Step 5 Configure the user data VLAN.

```
Raisecom(config)#gpon-onu uni thernet 3/1/1/1
Raisecom(config-gpon-onu-thernet-3/1/1:1)#vlan mode tagged
Raisecom(config-gpon-onu-thernet-3/1/1:1)#native vlan 100
Raisecom(config-gpon-onu-thernet-3/1/1:1)#end
```

Checking results

Show VLAN configurations of OLT GE interface 1/1 and PON interface respectively.

```
Raisecom#show interface ten-gigabitethernet 1/1 vlan
Port: 1/1
Administrative Mode: trunk
Operational Mode: trunk
Access Mode VLAN: 1
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
Drop Untagged: No
```

```
Raisecom#show interface gpon-olt 3/1 vlan
Port: 3/1
Administrative Mode: trunk
Operational Mode: trunk
Access Mode VLAN: 1
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
Drop Untagged: No
```

Show the registered ONU.

```
Raisecom#show interface gpon-onu creation-information
ONU ID   MAC Address    Mode   Creation Date    Device Type       State
Mng-mode
------------------------------------------------------------------------
3/1/1   000e.5e0a.7a0e  auto   2000-01-01,08:00  ISCOM5104(C)      active
oam
```

Show UNI VLAN configurations of the ONU.

```
Raisecom#show gpon-onu 3/1/1 uni ethernet 1 vlan
Port ID: 3/1/1/1
   VLAN mode        : Tagged
   Native VLAN      : 100(CoS 0)
   Trans-rule list  : n/a
   Trunk allowed VLAN: n/a
      Agg-rule list    : n/a
```

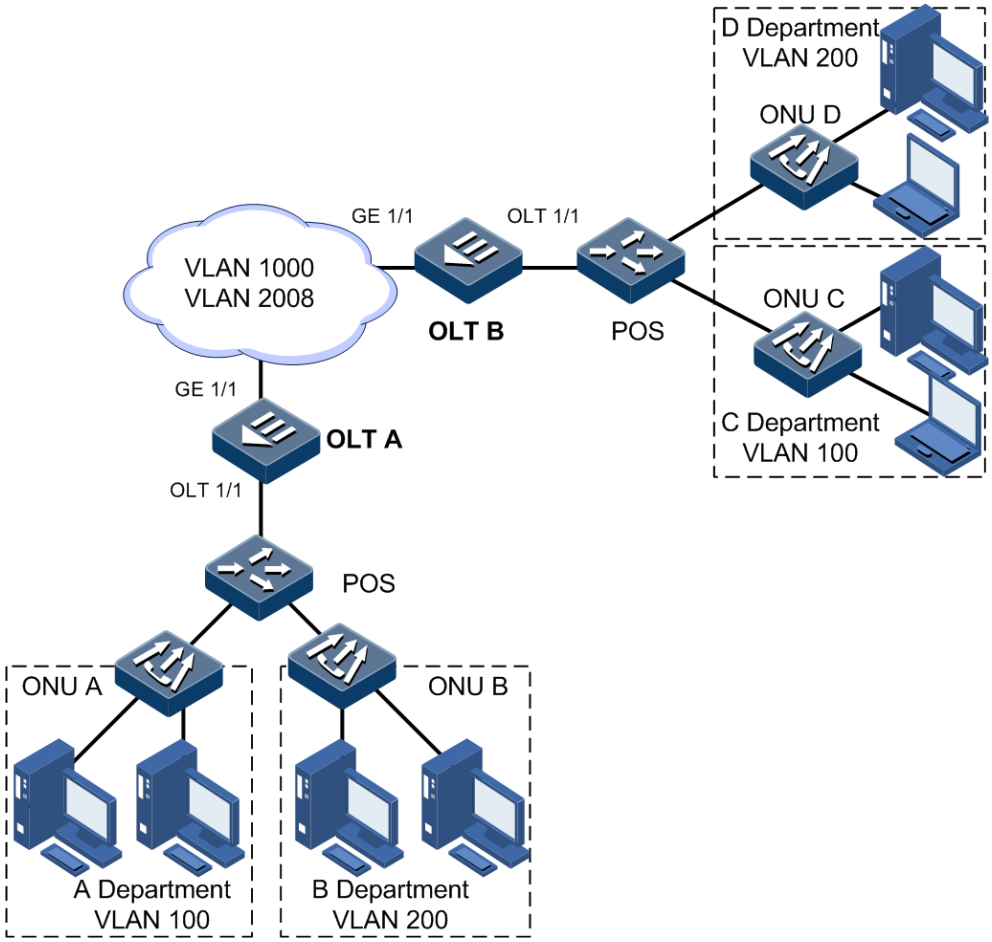
6.7.2 Example for configuring VLAN mapping

Networking requirements

As shown in Figure 6-4, OLT A connects Department A in VLAN 100 and Department B in VLAN 200 through OLT 3/1; OLT B connects Department C in VLAN 100 and Department D in VLAN 200 through OLT 3/1. In the carrier network, assign VLAN 1000 for Department A and Department C; and assign VLAN 2008 for Department B and Department D.

Configure 1:1 VLAN mapping on OLT A and OLT B to implement proper communication between the PC user or terminal user, and the server.

Figure 6-4 Configuring VLAN mapping



Configuration steps

Configurations on OLT A and OLT B are identical. Take OLT A for example.

Step 1 Create a VLAN and activate it.

```
Raisecom#config
Raisecom(config)#create vlan 100,200,1000,2008 active
```

Step 2 Configure uplink 10GE interface 1/1 to Trunk mode and allow VLAN 1000 and VLAN 2008 to pass.

```
Raisecom(config)#interface ten-gigabitethernet 1/1
Raisecom(config-if-ten-gigabitethernet-1:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-1:1)#switchport trunk allowed vlan
1000,2008 confirm
Raisecom(config-if-ten-gigabitethernet-1:1)#exit
```

Step 3 Configure the OLT interface 3/1 to Trunk mode and allow VLANs 100, 200, 1000, and 2008 to pass, and enable VLAN mapping.

```
Raisecom(config)#interface gpon-olt 3/1
Raisecom(config-if-epon-olt-3:1)#switchport mode trunk
Raisecom(config-if-gpon-olt-3:1)#switchport trunk allowed vlan
100,200,1000,2008confirm
Raisecom(config-if-gpon-olt-3:1)#vlan-mapping ingress outer 100 translate
outer 1000 inner copy-from-outer
Raisecom(config-if-gpon-olt-3:1)#vlan-mapping ingress outer 200 translate
outer 2008 inner copy-from-outer
Raisecom(config-if-gpon-olt-3:1)#switchport trunk untagged vlan 1000,2008
confirm
```

Checking results

Use the **show interface gpon-olt** *slot-id/olt-id* **vlan-mapping** { **ingress** | **egress** } **translate** command to show 1:1 VLAN mapping configurations.

```
Raisecom#show interface gpon-olt 3/1 vlan-mapping ingress translate
                     Old      Old    New   New   IVLAN
Port ID               OVID     IVID   OVID  IVID  Mapping Action
-------------------------------------------------------------------------
gpon-olt3/1            100      --     1000  --    copy-from-outer
gpon-olt3/1            200      --     2008  --    copy-from-outer
```

7 Configuring LLDP

This chapter describes LLDP and configuration procedures on the ISCOM6820, including the following sections:

- Introduction
- Configuring LLDP

7.1 Introduction

With the enlargement of network scale and increase of network devices, the network topology becomes more and more complex and network management becomes more important. A lot of network management software adopts auto-detection function to trace changes of network topology, but most of the software can only analyze the Layer 3 network and cannot ensure the interfaces to be connected to other devices.

Link Layer Discovery Protocol (LLDP) is based on IEEE 802.1ab standard. The NMS can fast grip the Layer 2 network topology and changes.

LLDP organizes the local device information in different Type Length Value (TLV) and encapsulates in Link Layer Discovery Protocol Data Unit (LLDPDU) to transmit to straight-connected neighbor. It also saves the information from neighbor as standard Management Information Base (MIB) for the NMS querying and judging link communication.

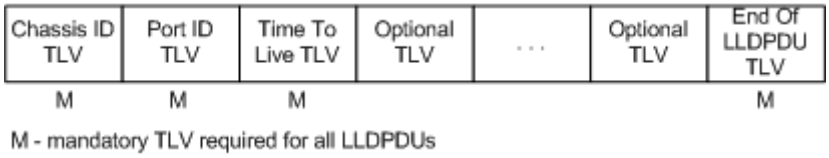
LLDP packet

The LLDP packet is used to encapsulate LLDPDU Ethernet packet in data unit and transmitted by multicast.

LLDPDU is the data unit of LLDP. The device encapsulates local information in TLV before forming LLDPDU, then several TLV fit together in one LLDPDU and encapsulated in Ethernet data for transmission.

As shown in Figure 7-1, LLDPDU is made by several TLV, including 4 mandatory TLV and several optional TLV.

Figure 7-1 Structure of a LLDPDU



As shown in Figure 7-2, each TLV denotes a piece of information at local. For example, the device ID and interface ID correspond with the Chassis ID TLV and Port ID TLV respectively, which are fixed TLVs.

Figure 7-2 Structure of a TLV packet

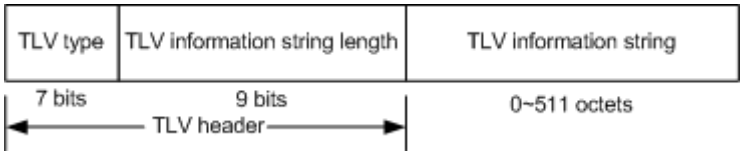


Table 7-1 lists TLV types. At present only types 0–8 are used.

Table 7-1 TLV types

TLV type	Description	Optional/Required
0	End Of LLDPDU	Required
1	Chassis ID	Required
2	Interface number	Required
3	Time To Live	Required
4	Interface description	Optional
5	System name	Optional
6	System description	Optional
7	System capabilities	Optional
8	Management address	Optional

Principles

LLDP is a point-to-point one-way issuance protocol, which notifies local device link status to the peer end by sending LLDPDU (or sending LLDPDU when link status changes) periodically from the local end to the peer end.

The procedure of packet exchange:

- When the local device transmits packet, it gets system information required by TLV, gets configurations from LLDP MIB, generates TLV, form LLDPDU, and transmits the LLDPDUs to the peer.
- The peer receives the LLDPDU and analyzes TLV information. If there is any change, the information will be updated in neighbor MIB table of LLDP and notifies the NMS.

When the device status is changed, the device sends a LLDP packet to the peer. To avoid sending LLDP packet continuously because of frequency change of device status, you can configure a delay timer for sending the LLDP packet.

The aging time of Time To Live (TTL) in local device information about the neighbor node can be adjusted by modifying the parameter values. TTL = Min { 65535, (interval for sending LLDP packets to the neighbor node × hold-multiplier) }.

7.2 Configuring LLDP

7.2.1 Preparing for configurations

Scenario

When you obtain connection information between devices through the NMS for topology discovery, the device needs to enable LLDP, notify their information to the neighbors mutually, and store neighbor information to facilitate the NMS queries.

Prerequisite

N/A

7.2.2 Enabling global LLDP

Enable global LLDP for the device as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#lldp enable`	Enable global LLDP. By default, it is disabled.
3	`Raisecom(config)#snmp trap lldp enable`	Enable LLDP Trap. By default, it is disabled.

7.2.3 Enabling interface LLDP

Enable interface LLDP for the device as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *`interface-type interface-number`*	Enter interface configuration mode.
3	`Raisecom(config-port)#lldp enable`	Enable interface LLDP. By default, it is enabled.

7.2.4 Configuring basic functions of global LLDP

Caution

When configuring the delay timer and period timer, the value of the delay timer should be smaller than or equal to a quarter of the period timer value.

Configure basic functions of global LLDP for the device as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#lldp message-transmission interval` *second*	(Optional) configure the period timer of the LLDP packet. By default, it is 30s.
3	`Raisecom(config)#lldp message-transmission delay` *second*	(Optional) configure the delay timer of the LLDP packet. By default, it is 2s.
4	`Raisecom(config)#lldp message-transmission hold-multiplier` *coefficient*	(Optional) configure the hold-multiplier of LLDP packets. By default, it is 4.
5	`Raisecom(config)#lldp restart-delay` *second*	(Optional) configure the restart timer. After global LLDP is disabled, you can re-enable global LLDP only after the delay timer expires. By default, it is 2s.

7.2.5 Configuring the LLDP trap

When the network changes, you need to enable LLDP trap to send topology update alarms to the NMS immediately.

Configure the LLDP Trap for the device as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#lldp trap-interval` *second*	(Optional) configure the interval for sending LLDP Traps. By default, it is 5s.

Note

After LLDP Trap is enabled, the device will send Traps when detecting neighbor aging, neighbor joining, and neighbor information change.

7.2.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show lldp local config**	Show local LLDP configurations.
2	Raisecom#**show** [**interface** *interface-type interface-number*] **lldp local system-data**	Show information about the LLDP local system.
3	Raisecom#**show** [**interface** *interface-type interface-number*] **lldp remote** [**detail**]	Show information about the LLDP neighbor.
4	Raisecom#**show lldp statistic** [*interface-type interface-number*]	Show statistics about LLDP packets.

7.2.7 Maintenance

Maintain the device as below.

Command	Description
Raisecom(config)# **clear** [**interface** *interface-type interface-number*] **lldp statistic**	Clear LLDP statistics on the specified interface.
Raisecom(config)# **clear** [**interface** *interface-type interface-number*] **lldp remote-table**	Clear information about LLDP neighbors on the specified interface.

8 Configuring routing

This chapter describes the routing feature and configure process of the device, and provides related configuration examples, including the following sections:

- Introduction
- Configuring ARP
- Configuring static routes
- Configuring NDP
- Configuring IPv6 basic functions
- Configuring equivalent route
- Configuration examples

8.1 Introduction

8.1.1 ARP

In the TCP/IP network, each host is assigned with a 32-bit IP address, which is called a logical address. To transmit packets through physical links, the device must learn the physical address of the destination host. It means that the device should translate the IP address into a physical address.

In the Ethernet, a physical address is a 48-bit MAC address. The Address Resolution Protocol (ARP) can establish a mapping between IP addresses and MAC addresses, which can translate IP addresses into MAC addresses.

Entries in the ARP address table are classified into the following types:

- Static ARP entry: is used to perform static binding on an IP address and a MAC address. It is used to prevent ARP dynamic learning fraud.
  - Static ARP entries should be manually added and deleted.
  - Static ARP entries are not aged.
- Dynamic ARP entry: entries that are automatically established through ARP
  - Dynamic ARP entries are automatically generated by the device.
  - Dynamic ARP entries are aged when the aging time is exceeded, on conditions that dynamic ARP entries are not used.

The device support **learn-all** ARP entry dynamic learning mode. The device learns ARP request and response packets in this mode. For example, when Device A sends the ARP request packet to Device B, it writes the mapping between its IP address and its MAC address into the ARP request packet. Device B learns this mapping to its own ARP table after receiving the ARP request packet. Therefore, no ARP request is performed when Device B sends packets to Device A later.

8.1.2 Route management

Routing is a behavior of passing a message through a network to a destination, and uses a routing table to forward it during the delivery process. Routing is required when devices between different VLANs communicate, or devices in the same VLAN wish to communicate across different networks.

Route management uniformly manages routing tables, static routes, and various dynamic routing protocols through routing device identification.

8.1.3 Static route

Routing is used to select a route and forward packets to make devices in different network segments communicate. The routing is realized through routing protocols. Routing protocols, rules to maintain the routing table between devices, are used to discover routes, generate the routing table, and instruct packet forwarding.

Devices select a route though a routing table and then instruct packet forwarding through Forwarding Information Base (FIB). Each device saves a routing table and a FIB table at least.

The routing table saves routes discovered based on various routing protocols. According to route sources, routes in the routing table are grouped as below:

- Interface route or directly-connected route: routes discovered by link-layer protocols
- Static route: routes manually configured by the administrator
- Dynamic route: routes discovered by dynamic routing protocols

Each entry in a FIB indicates the physical interface or logical interface where packets of a network segment or a host should be forwarded to the next-hop device.

Default route

The default route is a special type of route. It takes effect when no other route can be matched in the routing table. In the routing table, the default route is designated as 0.0.0.0/0. If the destination IP address of a packet mismatches with any entry in the routing table, this packet will select the default route.

If no default route is configured for a device and the destination IP address of a packet is not in the routing table, the device will discard the packet and send an Internet Control Message Protocol (ICMP) packet to the sender, which indicates that the destination address or network is unreachable.

Static route

Static route refers to a type of route that is manually configured. The static route has the following advantages:

- Do not consume network bandwidth.
- Cannot be aged.

- Can accurately control the direction of data packets.

However, the static route has some disadvantages:

- Be configured manually.
- Increase workload of the administrator.

The static route is mainly applied to small- and medium-sized network.

8.1.4 NDP

Neighbor Discovery Protocol (NDP) is a neighbor discovery mechanism used on IPv6 devices in the same link. It is used to discover neighbors, obtain MAC addresses of neighbors, and maintain neighbor information.

NDP obtains data link layer addresses of neighbor devices in the same link, namely, MAC address, through the Neighbor Solicitation (NS) message and Neighbor Advertisement (NA) message.

8.2 Configuring ARP

8.2.1 Preparing for configurations

Scenario

The mapping between IP addresses and MAC addresses is saved in the ARP address table.

In general, ARP address entries are maintained by devices dynamically. The device searches the mapping between IP addresses and MAC addresses automatically according to ARP. You need to configure the device manually only when adding static ARP address entries to prevent dynamic ARP learning spoofing.

Prerequisite

N/A

8.2.2 Default configurations

Default configurations of ARP on the ISCOM6820 are as below.

Function	Default value
Static ARP entries	N/A
Dynamic ARP learning mode	learn-all
Dynamically learning ARP by interfaces	Enable
Aging time of dynamic ARP entries	1200s

8.2.3 Configuring static ARP entries

- The IP address of a static ARP entry must be in the same IP network segment with the Layer 3 interface.
- You need to add or delete static ARP entries manually.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**arp** ip-address mac-address	Configure static ARP entries. You can use the **no arp** *ip-address* command to delete the entry.

8.2.4 Configuring proxy ARP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)**arp proxy**	Enable global ARP proxy.
3	Raisecom(config)#**interface vlanif** *vlan-id*	Enter VLAN interface configuration mode.
4	Raisecom(config-vlanif-*)**arp proxy**	Enable ARP proxy on the VLAN interface.

8.2.5 Checking configurations

No.	Command	Description
1	Raisecom#**show arp**	Show all ARP address entries.
2	Raisecom#**show arp** [*ip-address*]	Show information about proxy ARP.

8.2.6 Maintenance

No.	Command	Description
1	Raisecom(config)#**clear arp [all | static |** *ip-address* **]**	Clear ARP statistics.

8.3 Configuring static routes

8.3.1 Preparing for configurations

Scenario

Configure static routes for simple topology networks. You need to configure static routes manually to create an interconnected network.

Prerequisite

Configure the IP address of the Layer 3 interface correctly.

8.3.2 Configuring default gateway

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip route 0.0.0.0 0.0.0.0** *ip-address*	Configure the IP address of the IPv4 default gateway.

Note

On the device, if the packet to be forwarded does not have a corresponding route, you can use the **ip route** command to configure the default gateway to forward the packet to the default gateway. The IP address of the default gateway should be in the same network segment as the local IP address.

8.3.3 Configuring IPv4 static routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip route** *ip-address mask nexthopip* [**distance** *value*] [**description** *description*] [**tag** *tag-id*]	Configure the IPv4 static route. You can use the **no ip route** *ip-address mask nexthopip* command to disable this function.
3	Raisecom(config)#**ip route static distance** *value*	(Optional) configure the default IPv4 administrative distance. You can use the **no ip route static distance** command to restore default configurations.
4	Raisecom(config)#**ip routing**	(Optional) enable IP routing. You can use the **no** form of this command to disable this function.
5	Raisecom(config)#**ip route vrf** *vrf-name*	(Optional) configure the VPN routing/forwarding instance.

Step	Command	Description
6	Raisecom(config)# **interface vlanif** *** Raisecom(config-vlanif-*)#**ipv4** { **enable** | **disable** }	Enable IPv4 functions of the Layer 3 interface.

8.3.4 Configuring IPv6 static route

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip routing**	Enable routing. You can use the **no ip routing** command to disable this function.
3	Raisecom(config)#**ipv6 route** [**vrf** *vrf-name*]{ *ipv6-address/ prefi -length* | *ipv6-address* } *next-hop* [**distance** *distance*] [**description** *description*] [**tag** *tag-id*]	Configure IPv6 static routes. You can use the **no** form of this command to delete this configuration.

8.3.5 Checking configurations

No.	Command	Description
1	Raisecom#**show ip route**	Show information about the IPv4 route.
2	Raisecom#**show ip route** *ip-address* **[** *ip-mask* **] [longer-prefixes] [detail]** Raisecom#**show ip route** *start-ip-address start-ip-mask end-ip-address end-ip-mask* **[detail]**	Show information about routes of the specified IP address or an IP address range.
3	Raisecom#**show ip route all [protocol { connected | static | llinfo }] [detail]**	Show routing information about the specified routing protocol.
4	Raisecom#**show ip route summary**	Show statistics on IPv4 routes.
5	Raisecom#**show ip route vrf** *vrf-name* **summary**	Show statistics on IPv4 routing/forwarding instances.
6	Raisecom#**show ip route vrf** *vrf-name*	Show information about the VPN routing/forwarding instance.
7	Raisecom#**show ipv6 route [vrf** *vrf-name* **]**{ *ipv6-address/prefix-length* | *ipv6-address* / **all** / **static** / **summary** }	Show information about the IPv6 routing table.
8	Raisecom#**show ipv6 route vrf** *vrf-name* **summary**	Show information about the IPv6 VPN routing/forwarding instance.

8.4 Configuring NDP

8.4.1 Configuring static neighbor entries

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 neighbor** *ipv6-address mac-address*	Configure static neighbor entries. You canuse the **no ipv6 neighbor** *ipv6-address* command to delete the configuration.
3	Raisecom(config)# **interface vlanif** *** Raisecom(config-vlanif-*)#**ipv6 neighbor max-learning-num** *number*	Configure the maximum number of NDPs allowed to be learned.

8.4.2 Checking configurations

No.	Command	Description
1	Raisecom#**show ipv6 neighbors**	Show learnt IPv6 neighbors .

8.4.3 Maintenance

No.	Command	Description
1	Raisecom(config)#**clear ipv6 neighbors**	Clear all IPv6 neighbor entries.

8.5 Configuring IPv6 basic functions

8.5.1 Preparing for configurations

Scenario

With the rapid development of the network, the IPv4 protocol slowly shows weaknesses, and the IPv6 protocol has more advantages than the IPv4 protocol. For example, IPv6 has a large number of address spaces, highly flexible message formats, and efficient route forwarding efficiency. IPv6 can not only solve the problem of network address resource limitation, but also solve the problem of limitations of device access to the Internet.

Prerequisite

N/A

8.5.2 Default configurations

Function	Default values
Layer 3 interface Ipv6	Disable
Stateless autoconfiguration address	Disable

8.5.3 Configuring IPv6 basic functions

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface vlanif** *vlan-id*	Enter VLAN interface configuration mode.
3	Raisecom(config-vlanif-*)#**ipv6 enable**	Enable IPv6 on the Layer 3 interface. You can use the **disable** form of this command to disable the function.
4	Raisecom(config-vlanif-*)#**ipv6 address** *ipv6-address/prefix-length* [**eui-64**]	Configure the IPv6 address of the VLAN interface.
5	Raisecom(config-vlanif-*)#**ipv6 address** *ipv6-address* **link-local**	(Optional) configure the IPv6 local link address of the VLAN interface.
6	Raisecom(config-vlanif-*)#**ipv6 address** *ipv6-address/prefix-length* **anycast**	(Optional) configure the IPv6 anycast address on the VLAN interface.
7	Raisecom(config-vlanif-*)#**ipv6 address auto**	(Optional) enable IPv6 address stateless autoconfiguration in VLAN interface mode.

8.5.4 Checking configurations

No.	Command	Description
1	Raisecom#**show interface vlanif** *vlan-id* **ipv6 detail**	Show IPv6 address configurations of the interface.

8.6 Configuring equivalent route

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip route ecmp loading-sharing mode** { **sip** | **dip** | **sxordip** }	Configure the load balancing mode of the equivalent route.

Step	Command	Description
3	Raisecom(config)#**ipv6 route ecmp loading-sharing mode { sip | dip | sxordip }**	Configure the load balancing mode of the IPv6 equivalent route.

8.6.1 Checking configurations

No.	Command	Description
1	Raisecom#**show interface vlanif** *vlan-id* **ipv6 detail**	Show IPv6 address configurations of the interface.

8.7 Configuration examples

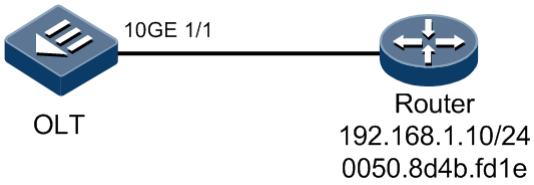
8.7.1 Example for configuring ARP

Networking requirements

As shown in Figure 8-1, the OLT device is connected to the host, and is connected to the upper-layer router through 10GE interface 10/1. The IP address of the router is 192.168.1.10/24, and the MAC address is 0050.8d4b.fd1e.

You need to configure a corresponding static ARP entry on the OLT to enhance the communication security between the OLT and router.

Figure 8-1 ARP networking



Configuration steps

Step 1 Add a static ARP entry.

```
Raisecom#config
Raisecom(config)#arp 192.168.1.10 0050.8d4b.fd1e
```

Step 2 Enable ARP proxy.

```
Raisecom#config
```

```
Raisecom(config)#interface vlanif 1
Raisecom(config-vlanif-1)#arp proxy
```

Checking results

Use the **show arp** command to show all entries in the ARP address table.

```
Raisecom#show arp
ARP aging-time: 1200 seconds(default: 1200s)
ARP mode: Learn all
ARP max neighbour num: 131072 (128 * 1024)
ARP table:
Total: 5     Static: 1     Dynamic: 4

IP Address      Mac Address     Interface                    Type
Age(s)    status
-------------------------------------------------------------------------
---------------------------
192.168.1.10     0050.8D4B.FD1E   snmp                        static   --
PERMANENT
199.0.0.61       D85D.4C74.9098   vlan4051                    dynamic
1505      REACHABLE
199.0.0.118      00E0.4C16.0F4C   vlan4051                    dynamic
1468      REACHABLE
199.0.0.158      0013.3B13.047D   vlan4051                    dynamic
1495      REACHABLE
199.0.0.215      1C1B.0D2B.CBD9   vlan4051                    dynamic
1495      REACHABLE
```

Use the **show arp proxy** command to show the status of ARP proxy.

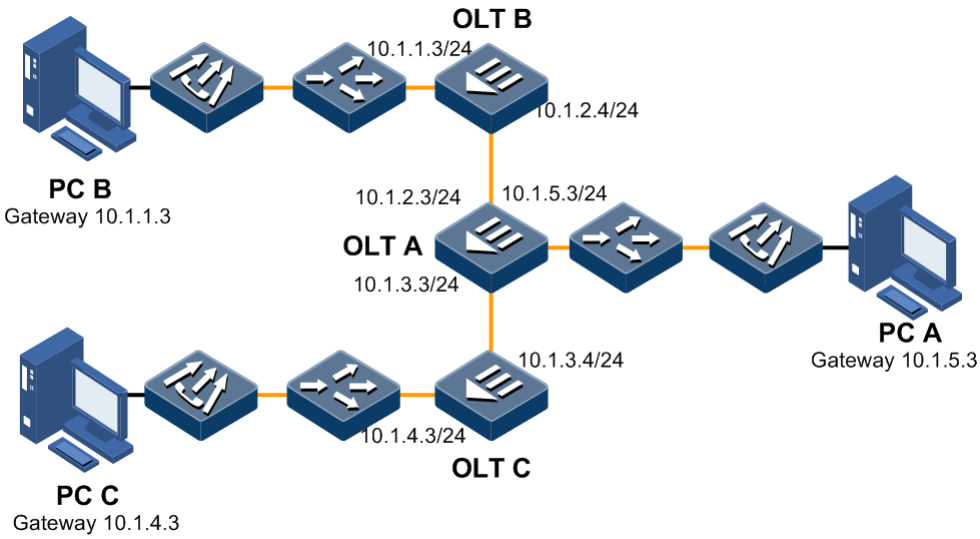
```
Raisecom#show arp proxy
Proxy ARP: Enable
------------------------
IF          Proxy ARP
------------------------
1           Enable
```

8.7.2 Example for configuring static routes

Networking requirements

Configure a static route so that any two PCs or OLTs in Figure 8-2 can ping each other. The IP addresses of the two interfaces of OLT B are 10.1.1.3/24 and 10.1.2.4/24; the IP addresses of the three interfaces of OLT A are 10.1.2.3/24, 10.1.5.3/24, and 10.1.3.3/24. The IP addresses of the two interfaces of OLT C are 10.1.3.4/24 and 10.1.4.3/24.

Figure 8-2 Configuring static routes



Configuration steps

Step 1 Configure the IP address of each device. The details are as below:

Step 2 Configure static routes on OLT A.

```
Raisecom#config
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 Configure static routes on OLT B.

```
Raisecom(config)#ip route 10.1.3.0 255.255.255.0 10.1.2.3
Raisecom(config)#ip route 10.1.4.0 255.255.255.0 10.1.2.3
Raisecom(config)#ip route 10.1.5.0 255.255.255.0 10.1.2.3
```

Step 4 Configure static routes on OLT C.

```
Raisecom(config)#ip route 10.1.1.0 255.255.255.0 10.1.3.3
Raisecom(config)#ip route 10.1.2.0 255.255.255.0 10.1.3.3
Raisecom(config)#ip route 10.1.5.0 255.255.255.0 10.1.3.3
```

Step 5 Configure the default gateway of PC A to 10.1.5.3. Detailed configurations are as below.

Configure the default gateway of PC B to 10.1.1.3. Detailed configurations are as below.

Configure the default gateway of PC C to 10.1.4.3. Detailed configurations are as below.

Checking results

You can perform the following operations on any OLT to check whether all devices can communicate with each other.

```
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
```

9 Configuring DHCP

This chapter describes the DHCP feature and configuration process of the device, and provides related configuration examples, including the following sections:

- Introduction
- Configuring DHCP Snooping
- Configuring DHCP Relay
- Configuring DHCP Option 82
- Configuration examples

9.1 Introduction

With constant expansion of network scales, it becomes more and more complicated to manage the network IP addresses, which is manifested as below:

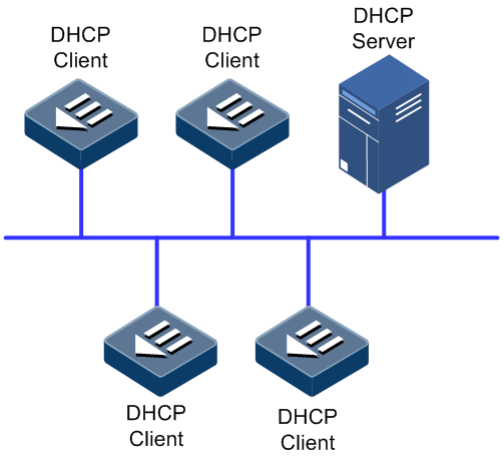
- The constant increase of computers in the network makes the workload of manually configuring and changing the IP addresses heavier.
- There are a lot of portable computers in the network, whose location changes frequently. Therefore, administrators need to change the IP addresses of them frequently.
- To improve the efficiency of managing IP addresses, it is ergent to implement centralized management on IP addresses.

To solve the above-mentioned problems, some people developed Dynamic Host Configuration Protocol (DHCP) which can automatically assign IP addresses to all clients in the network, alleviating administrators' workload and implementing centralized management on IP addresses.

DHCP works in client/server mode. The client sends IP request to the server. After receiving the request, the server provides an IP address and related configurations to the client, thus implementing automatic assignment of IP addresses.

There should be at least one DHCP server and multiple clients (including PC and portable computers) in typical DHCP applications, as shown in Figure 9-1.

Figure 9-1 Typical DHCP application



DHCP working principle

The DHCP server provides IP configurations for the DHCP client as below:

- Requesting IP address: the DHCP client broadcasts one DHCPDiscover packet to check whether a DHCP server exists in this network segment for IP address and related configurations.
- Providing IP address: after all DHCP servers in this network have received the IP request, they will broadcast back one DHCPOffer packet. The DHCPOffer packet contains the IP address and related configurations and the ID of the DHCP server.
- Selecting IP address: after receiving the DHCPOffer packet (maybe more than 1), the DHCP client will select one as its own configurations and then broadcast one DHCPRequest packet informing other DHCP servers that it has selected one server to provide configurations and requesting other servers to retake the provided configurations.
- Confirming IP address: after receiving the feedback from the DHCP client, the DHCP server will send one DHCPAck packet to the DHCP client for confirmation.

Till now, the DHCP server has provided an IP address and related configurations to the DHCP client.

DHCP lease renewal

After obtaining an IP address from the DHCP server, the DHCP client cannot use the IP address forever. The IP address has a fixed validity period which is called lease period. The lease period can be specified by the user. If the DHCP client wishes to use the obtained IP address and configurations for a long time, it must send lease renewal request to the DHCP server. The steps of lease renewal are as below:

- When the lease period arrives at 50%, the DHCP client will send DHCPRequest packet to the DHCP server for renewing the lease. If succeeded, the lease period will become an integrated period. Otherwise, the DHCP client will send renewal request again when the lease period arrives at 87.5%.
- When the lease period arrives at 87.5%, the DHCP client will send DHCPRequest packet to the DHCP server again for renewing the lease. If succeeded, the lease period will become an integrated period. Otherwise, the lease period renewal will fail and the IP address and configurations will be retaken once the lease period expires.

DHCP application scenario

Generally, the IP addresses assigned by the DHCP server can be used in the following scenarios:

- The network scale is large and the workload of manually configuring the IP address is heavy.
- The number of hosts in the network is larger than that of the available IP addresses. In this case, it is impossible to assign a fixed IP address to the each host and limits will be imposed on the number of hosts accessing the network concurrently.

Only a few hosts in the network need fixed IP addresses. Most hosts do not need fixed IP addresses.

9.1.1 DHCP packet

Figure 9-2 shows the DHCP packet structure.

Figure 9-2 DHCP packet structure

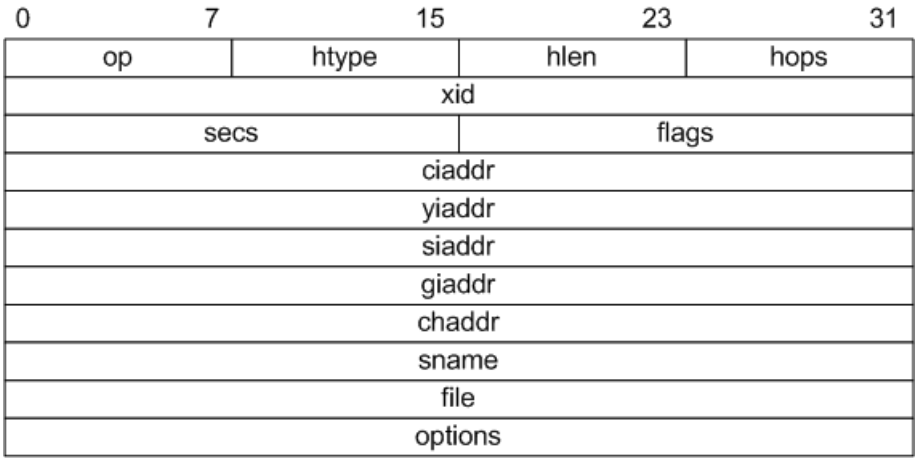


Table 9-1 lists meanings of fields in the DHCP packet.

Table 9-1 Meanings of fields in the DHCP packet

Name	Length (B)	Description
op	1	Packet type • 1: request packet • 2: response packet
htype	1	Hardware address type of a DHCP client
hlen	1	Hardware address length of a DHCP client
hops	1	Number of DHCP relays that DHCP request packet pass The value is added by 1 every time the DHCP request packet passes through a DHCP relay.
xid	4	Transaction ID, a random number chosen by the DHCP client. It is used to identify an address request process.

Name	Length (B)	Description
secs	2	Time elapsed since the DHCP client initiates a DHCP request. At present, it is not used and is set to 0.
flags	2	The left first bit is a broadcast response identifier, which is used to identify the DHCP server sends response packets in the unicast/broadcast mode • 0: unicast • 1: broadcast Other bits are reserved.
ciaddr	4	IP address of the DHCP client, which is padded when the DHCP client is being bound, updated, or rebounded. In addition, this IP address can be used to respond the ARP request.
yiaddr	4	IP address of the DHCP client allocated by the DHCP server
siaddr	4	IP address of the DHCP server
giaddr	4	IP address of the first DHCP relay where the DHCP request packet
chaddr	16	Hardware address of the DHCP client
sname	64	Name of the DHCP server
file	128	Startup configuration file name and routing information about the DHCP client specified by the DHCP server
options	Variable	Optional variable fields, including the packet type, valid lease, IP address of the Domain Name System (DNS) server, and IP address of the Windows Internet Name Server (WINS).

9.1.2 DHCP Snooping

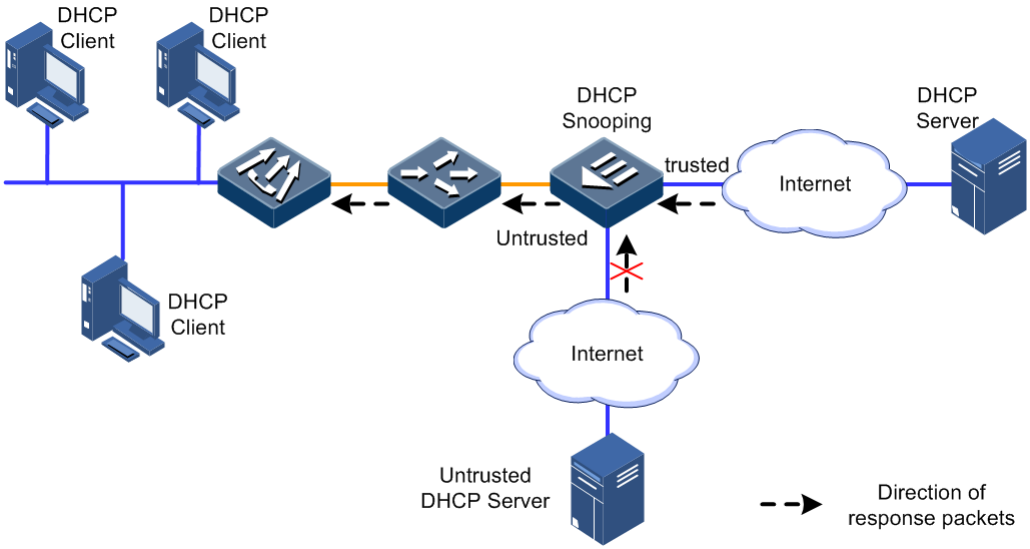
Overview of DHCP Snooping

The DHCP Snooping is a security feature of the DHCP, supporting the following functions:

- Ensure that DHCP clients obtain IP addresses from a legal DHCP server only.

When there is a private DHCP server in the network, DHCP clients may obtain incorrect IP addresses and related configurations, making network communication failed, as shown in Figure 9-3. To ensure that DHCP clients obtain IP addresses from a legal DHCP server, the DHCP Snooping mechanism allows configuring interfaces as trusted/untrusted interfaces. Trusted interfaces can forward received DHCP packets properly while untrusted interfaces will discard packets from DHCP servers.

Figure 9-3 DHCP Snooping networking



- Recoding the relationship between IP addresses and MAC addresses of DHCP clients

The DHCP Snooping records DHCP Snooping entries by listening requests and response packets received by trusted interfaces, including MAC addresses of DHCP clients, obtained IP addresses, interfaces connected to DHCP clients, and VLAN information of these interfaces. With this information, the DHCP Snooping can implement the following functions:

  - Dynamic ARP Inspection (DAI): judge whether a user, who sends the ARP packet, is legal or not based on DHCP Snooping entries. It helps prevent illegal users' ARP attack.
  - IP Source Guard: filter packets forwarded by an interface by dynamically obtaining DHCP Snooping entries. It helps prevent illegal packets from passing through the interface.

DHCP Snooping supporting Option

Option fields of a DHCP packet records the location information of DHCP clients. With these Option fields, the administrator can locate DHCP clients, and implement security and accounting control of DHCP clients.

If the device is enabled with DHCP Snooping supporting Option, it takes the following two actions when receiving a DHCP packet.

- When the device receives a DHCP request packet, it processes the packet based on whether Option fields are contained in the packet, configured processing policies, and padding modes, and then sends the processed packet to the DHCP server.
- When the device receives a DHCP response packet, if the packet contains an Option field, the device deletes this Option Field and forwards the DHCP request packet to DHCP clients. Otherwise, the device directly sends the DHCP request packet to DHCP clients.

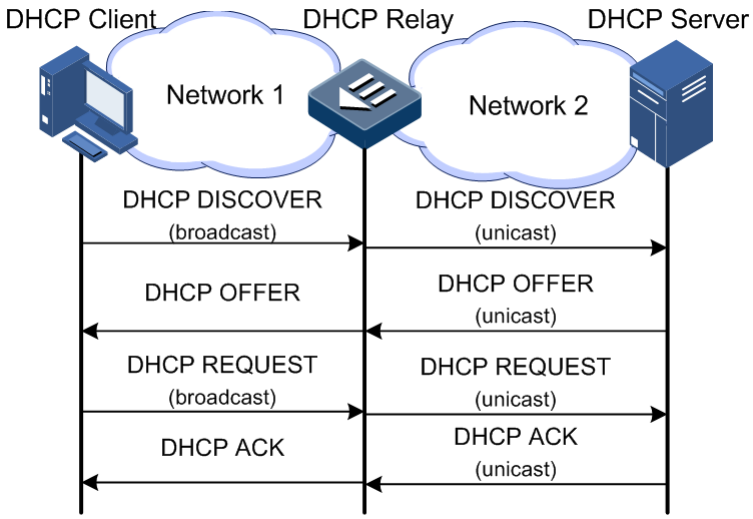
9.1.3 DHCP Relay

The initial DHCP asks DHCP clients and the DHCP server to be at the same network segment. For a network that contains multiple network segments, you must configure a DHCP server for each network segment, which consuming DHCP server resources.

The DHCP relay helps solve this problem. The DHCP relay provides relay services for DHCP clients and DHCP servers at different network segments. Therefore, DHCP clients at different network segments can share a DHCP server.

Figure 9-4 shows the working principle of DHCP Relay.

Figure 9-4 Working principle of DHCP Relay



As shown in Figure 9-4, a DHCP client sends a request packet to a DHCP server through the DHCP Relay. The DHCP Relay receives, processes, and forwards this packet to the DHCP server at a specified network segment. Based on information contained in the request packet, the DHCP server sends a packet back to the DHCP client through the DHCP Relay to finish dynamic configurations on the DHCP client.

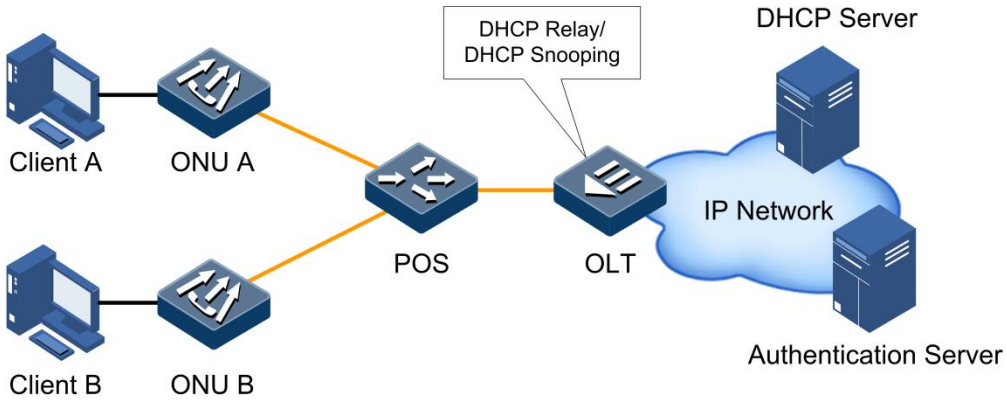
9.1.4 DHCP Option 82

RFC 3046 defines Option 82 (DHCP Relay Agent Information Option), adding some options in the DHCP request packet. These options help the DHCP server locate users more accurately and adopt various address allocation policies for users.

The DHCP Option 82 contains 2 sub-options

- Remote ID (remote ID sub-option)
- Circuit ID (circuit ID sub-option)

Figure 9-5 Working principle of DHCP Option 82



As shown in Figure 9-5, the working process of DHCP Option 82 is as below.

Step 2 Before a client is authenticated and gets a dynamic IP address, only authentication packets and DHCP packets can pass through the OLT enabled with DHCP Option 82.

Step 3 The client sends an authentication request to the authentication server through the DHCP Relay/DHCP Snooping. The authentication server can manage the authority of the user.

Step 4 After the authentication server authenticates the client's legality, it sends an authentication response packet to the client, informing the client's authority.

Step 5 Based on the authority assigned by the authentication server, the client initiates an IP address request to the DHCP server. At the same time, the client adds its authority information to the DHCP Option 82 option fields.

Step 6 The DHCP server, which supports DHCP Option 82 address allocation policy, allocates an IP address for the client based on the specified authority information carried in the DHCP Option 82 fields.

By combining the DHCP Option 82, authentication system, and the DHCP server that supports DHCP Option 82 address allocation policy together, you can use DHCP Option 82's Circuit ID and Remote ID sub-options to allocate different IP addresses to users. On one hand, this helps manage IP addresses more accurately. On the other hand, the device can perform policy routing based on the source IP address. Therefore, users with different IP addresses can have various routing rules and network access privileges.

9.2 Configuring DHCP Snooping

9.2.1 Preparing for configurations

Scenario

DHCP Snooping is a DHCP security feature, used to guarantee the DHCP client to get an IP address from the legal DHCP server and record the corresponding relationship between IP addresses and MAC addresses of the DHCP client.

The Option field of a DHCP packet records location information of the DHCP client. Administrators can locate the DHCP client through the Option field and control client security and accounting. The ISCOM6820 configured with DHCP Snooping and Option can perform related operations according to the Option field.

Prerequisite

- DHCP Snooping and DHCP Relay are mutually exclusive. So you need to disable DHCP Relay before configuring DHCP Snooping.
- DHCP Snooping on the interface can take effect only after global DHCP Snooping is enabled. So you need to enable global DHCP Snooping before configuring DHCP Snooping on the interface.

9.2.2 Default configurations

Default configurations of DHCP Snooping on the ISCOM6820 are as below.

Function	Default value
Global DHCP Snooping	Disable
DHCP Snooping trust status on interface	Untrusted
DHCP Option 82	Disable

Default configurations of DHCP Snooping on the Raisecom ONU devices are as below.

Function	Default value
Interface DHCP Snooping	Disable
Interface DHCP Snooping trusted status	Untrusted
DHCP Option 82	Disable

9.2.3 Configuring DHCP Snooping on the VLAN interface

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#vlan range` *`list`*	Enter VLAN range configuration mode.
3	`Raisecom(config-vlan-range-*:*)#{ ip | ipv6 } dhcp snooping`	Enable DHCP Snooping on the VLAN interface. You can use the **no ip dhcp snooping** command to disable this function.

9.2.4 Configuring DHCP Snooping trust on interface

Configuring DHCP Snooping trust on interface

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface { ten-gigaethernet | gpon-olt }` *`slot-id/port-id`*	Enter physical interface configuration mode.
3	`Raisecom(config-if-*-*:*)#ip dhcp snooping trust`	Enable DHCP Snooping trust on the interface.

9.2.5 (Optional) configuring DHCP Snooping supporting Option 82

Configuring OLT DHCP Snooping Option 82

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp information option**	Configure DHCP Snooping supporting Option 82. You can use the **no ip dhcp information option** command to disable this function.

9.2.6 Checking configurations

No.	Command	Description
1	Raisecom#**show ip dhcp snooping**	Show DHCP Snooping configurations.
2	Raisecom#**show ip dhcp snooping binding**	Show information about the DHCP Snooping binding table.
4	Raisecom#**show ip dhcp snooping statistics**	Show DHCP Snooping statistics.
5	Raisecom#**show vlan** *vlan-id* **ip dhcp snooping**	Show configurations of the DHCP Snooping of the VLAN.

9.2.7 Maintenance

No.	Command	Description
1	Raisecom(config)#**clear ip dhcp snooping binding**	Clear DHCP Snooping binding table.
2	Raisecom(config)#**clear ip dhcp snooping statistics**	Clear DHCP Snooping statistics.

9.3 Configuring DHCP Relay

9.3.1 Preparing for configurations

Scenario

When the DHCP client and DHCP server are in different network segments, you can use DHCP Relay to solve the problem. It can make the DHCP client and DHCP server in different network segments bear relay services, and relay DHCP protocol packets through network segments to the destination DHCP server, so that DHCP clients in different network segments can share the same DHCP server.

Prerequisite

- DHCP Snooping and DHCP Relay are mutually exclusive. So you need to disable DHCP Snooping before configuring DHCP Relay.
- DHCP Relay on the interface can take effect only after global DHCP Relay is enabled. So you need to enable global DHCP Relay before configuring DHCP Relay on the interface.

9.3.2 Default configurations

Default configurations of DHCP Relay on the ISCOM6820 are as below.

Function	Default value
Global DHCP Relay	Disable
DHCP Relay on interface	Enable
Destination IP address of interface enabled with DHCP Relay	N/A
Destination IP address of interface enabled with DHCP Relay on ONU	N/A
DHCP Relay trust status on interface	Untrusted
DHCP Option 82	Unsupported
Processing policy of request packets containing Option 82 field	Replace

9.3.3 Configuring the destination IP address of DHCP Relay of the VLAN interface

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface vlanif` *num*	Enter VLAN interface configuration mode.
3	`Raisecom(config-vlanif-*)#ip dhcp relay`	Enable DHCP Relay on the VLAN interface. You can use the **no ip dhcp relay** command to disable this function.
4	`Raisecom(config-vlanif-*)#ipv6 dhcp relay`	Enable DHCPv6 Relay on the VLAN interface.
5	`Raisecom(config-vlanif-*)#ip dhcp relay target-ip` *ip-address*	(Optional) configure the destination IP address of DHCP Relay of the VLAN interface.
6	`Raisecom(config-vlanif-*)#ipv6 dhcp relay target-ip` *ipv6-address*	(Optional) configure the destination IP address and the egress interface of the VLAN interface. The device uses the IP address and the egress interface as the IP address of the server or next relay.

- Each IP interface can be configured with up to 4 destination IP addresses.

- When the DHCP client connects the DHCP server through multiple DHCP relays, we recommend that the number of DHCP relays does not exceed 4.

9.3.4 Configuring DHCP Relay trusted interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** { **ten-gigabitethernet** | **gpon-olt** } *slot-id/port-id*	Enter interface configuration mode.
3	Raisecom(config-if-*-*:*)#**ip dhcp relay information trusted**	Configure the interface as the DHCP Relay trusted interface. You can use the **no ip dhcp relay information trusted** command to restore default configuration.

Note

Interface trust can take effect only when DHCP Relay supports DHCP Option 82.

9.3.5 Checking configurations

No.	Command	Description
1	Raisecom#**show ip dhcp relay statistics**	Show DHCP Relay statistics.

9.3.6 Maintenance

No.	Command	Description
1	Raisecom#**clear ip dhcp relay statistics**	Clear DHCP Relay statistics.

9.4 Configuring DHCP Option 82

9.4.1 Preparing for configurations

Scenario

RFC 3046 defines DHCP Option 82 and adds some option information in the DHCP request packet to make the DHCP server determine user's location more accurately, and then take different address assignment strategies to different users.

Prerequisite

Enable DHCP Snooping or DHCP Relay.

- Before configuring DHCP Option 82, you need to enable customized DHCP Option 82 firstly.
- To enable customized DHCP Option 82, see section 9.2.5 (Optional) configuring DHCP Snooping supporting Option 82.

9.4.2 Default configurations

Default configurations of DHCP Option 82 on the ISCOM6820 are as below.

Function	Default value
Global DHCP Option 82	Disable
Global DHCP Option attach-string	N/A
Global remote-id	Switch-mac
Circuit-id of interface	N/A
Processing policy of DHCP packets containing Option 82 field	Transparent

Default configurations of DHCP Option 82 on the Raisecom ONU devices are as below.

Function	Default value
Global DHCP Option 82	Disable
Global DHCP Option attach-string	Null
Global remote-id mode	onumac
Interface circuit-id	Null

9.4.3 Enabling DHCP Option 82

Enabling DHCP Option82 on OLT

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ip dhcp information option`	Enable DHCP Option 82. You can use the **no ip dhcp information option** command to disable this function.

Enabling DHCP Option82 on ONU

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu** *slot-id/olt-id/onu-id*	Enter EPON ONU management configuration mode.
3	Raisecom(config-gpon-onu-*/*:*)#**ip dhcp information option82** [**enable** | **disable**]	Enable/Disable ONU Option82.
4	Raisecom(config-gpon-onu-*/*:*)#**ip dhcp information option82 circuit-id** *circuit-id*	Configure the circuit ID of the sub-option of Option82 on the ONU UNI.

9.4.4 Configuring global DHCP Option remote ID

Configuring global DHCP Option remote ID on OLT

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp information remote-id option**	Configure the DHCPv6 packets to be added with the remote ID.
2	Raisecom(config)#**ip dhcp information option remote-id** { **switch-mac** | **client-mac** | **switch-mac-string** | **client-mac-string** | **hostname** | **string** *string* }	Configure the remote ID of Option 82.

Configuring global DHCP Option remote ID on ONU

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)# **gpon-onu** *slot-id/olt-id/onu-id*	Enter PON ONU remote management configuration mode.
3	Raisecom(config-*-onu-*/*:*)#**ip dhcp information option82 remote-id string** *string*	Configure the remote ID of the sub-option of Option 82. You can use the **no ip dhcp information option82 remote-id string** command to restore default configurations.
4	Raisecom(config-*-onu-*/*:*)#**ip dhcp information option82 remote-id mode** { **client-mac** | **client-mac-string** | **hostname** | **onu-mac** | **onu-mac-string** | **user-defined** *string* }	Configure the filling mode of Option 82 remote ID. You can use the **no ip dhcp information option82 remote-id mode** command to restore default configurations.

9.4.5 Configuring global DHCP Option interface ID

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp information interface-id option**	Configure the DHCPv6 packets to be added with the interface ID.

9.4.6 Configuring DHCP Option circuit ID on interface

Configuring DHCP Option circuit ID on OLT interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** { **ten-gigabitethernet** | **gpon-olt** } *slot-id/port-id*	Enter interface configuration mode.
3	Raisecom(config-if-*-*:*)#**ip dhcp information option circuit-id** *string*	Configure the circuit ID of Option 82 on the interface. You can use the **no ip dhcp information option82 circuit-id** command to restore default conditions.

9.4.7 Configuring processing policy of Option 82 packet

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** { **ten-gigabitethernet** | **gpon-olt** } *slot-id/port-id*	Enter physical interface configuration mode.
3	Raisecom(config-if-*-*:*)#**ip dhcp information option overwrite-policy** { **drop** | **transparent** }	Configure the processing policy to the DHCP request packet containing Option 82 on the interface. You can use the **no ip dhcp information option overwrite-policy** command to restore default configuration.
4	Raisecom(config-if-*-*:*)#**ip dhcp information option overwrite-policy circuit-id replace** { **length** *len* }	Configure the processing policy to the circuit ID of the DHCP request packet containing Option 82. You can use the **no ip dhcp information option overwrite-policy** command to restore default conditions.

9.4.8 Checking configurations

Checking OLT configurations

No.	Command	Description
1	`Raisecom#show ip dhcp information option`	Show DHCP Option configurations.

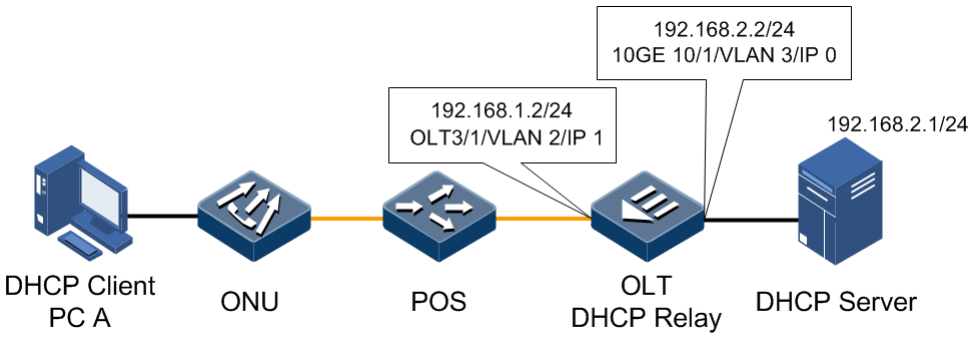
9.5 Configuration examples

9.5.1 Example for configuring DHCP Relay

Networking requirements

As shown in Figure 9-6, the OLT, which works as a DHCP Relay device, needs to ensure that the DHCP client can obtain IP addresses through network segments. In addition, the OLT supports DHCP Option 82 to manage the DHCP client.

Figure 9-6 DHCP Relay networking



Configuration steps

Step 1 Configure DHCP Relay in VLAN 1 of the Layer 3 interface.

```
Raisecom#config
Raisecom(config)#interface vlanif 1
Raisecom(config-vlanif-1)#ip dhcp relay
```

Step 2 Configure the destination IP address of IP interface 1.

```
Raisecom(config-vlanif-1)#ip dhcp relay target-ip 192.168.2.1
```

Step 3 Configure the device to support Option82.

```
Raisecom(config)#ip dhcp information option
```

Step 4 Configure 10GE interface 1/1 as the DHCP Relay trusted interface.

```
Raisecom(config)#interface ten-gigabitethernet 1/1
Raisecom(config-if-ten-gigabitethernet-1:1)#ip dhcp relay information
trusted
```

Checking results

Use the **show interface vlanif ip dhcp relay** command to show DHCP Relay configurations.

```
Raisecom#show interface vlanif 1 ip dhcp relay
-----------------------------------------------
1           Enabled       192.168.2.1
```

10 Configuring QoS

This chapter describes the QoS feature and configuration process of the ISCOM6820, and provides related configuration examples, including the following sections:

- Introduction
- Configuring traffic classification
- Configuring traffic monitoring
- Configuring traffic shaping
- Configuring congestion avoidance
- Configuring congestion management
- Configuring traffic policy
- Configuration examples

10.1 Introduction

Generally, Internet (IPv4), which bases on the store-and-forward mechanism, only provides "best-effort" service for users. When the network is overloaded or congested, this service mechanism cannot ensure that packets be transmitted timely and completely.

With the ever-growing of network application, users bring different service quality requirements on network application. Then network should distribute and schedule resources for different network applications according to users' demands.

Quality of Service (QoS) can ensure real-time and integrated service when the network is overloaded or congested and guarantee that the whole network runs efficiently.

10.1.1 Priority trust

Priority trust refers to that a packet adopts its own priority as the classification standard to perform follow-up QoS management on the packet. In general, the bigger the value is, the higher the priority is.

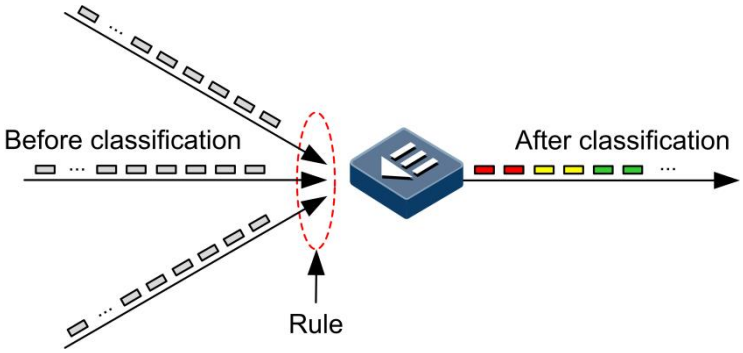
The ISCOM6820 supports port-based priority trust. The priorities are divided into priority based on Differentiated Services Code Point (DSCP) of IPv4 packets, priority based on Class of Service (CoS) of VLAN packets, and priority based on Traffic Class (TC) of IPv6 packets.

10.1.2 Traffic classification

Traffic classification is a process that recognizes specified packets according to some certain rules. Packets matching different rules will be implemented with different QoS policies. Traffic classification is the prerequisite and basis for providing services differently.

The ISCOM6820 supports traffic classification based on Type of Service (ToS) priority and DSCP priority of IPv4 packets, TC of IPv6 packets, Access Control List (ACL) rules, and VLAN IDs. Figure 10-1 shows the traffic classification process.

Figure 10-1 Traffic classification process



ToS priority and DSCP priority

Figure 10-2 shows the IP packet header structure. An 8-bit ToS field is contained in this packet. The RFC1349 defines the first 3 bits of the ToS field representing the ToS priority, ranging from 0 to 7. In the RFC2474, the ToS field is re-defined. The first 6 bits (0–5 bits) represent the priority of IP packets, which is called DSCP priority, ranging from 0 to 63, where the last 2 bits (6 and 7 bits) are reserved bits. Figure 10-3 shows structures of ToS and DSCP priority packets.

Figure 10-2 IP packet header structure

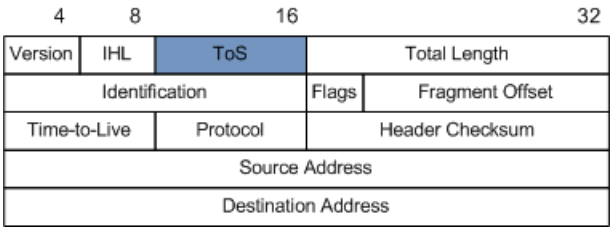
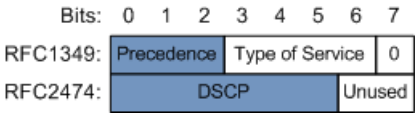


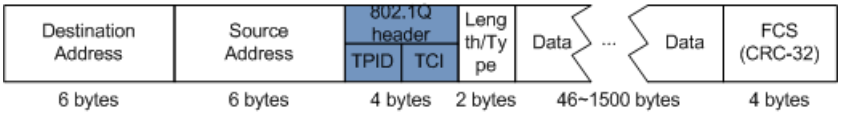
Figure 10-3 Structures of ToS priority and DSCP priority packets



CoS priority

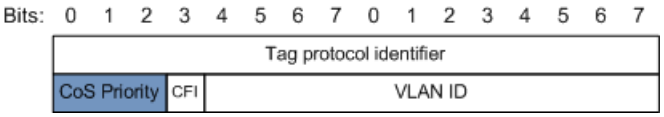
IEEE802.1Q-based VLAN packets are a modification of Ethernet packets. A 4-bit 802.1Q header is added between the source MAC address and protocol type, as shown in Figure 10-4. The 802.1Q header consists of a 2-bit Tag Protocol Identifier (TPID, valuing 0x8100) filed and a 2-bit Tag Control Information (TCI) field.

Figure 10-4 VLAN packet structure



The first 3 bits of TCI field represent the CoS priority, which ranges from 0 to 7, as shown in Figure 10-5. The bigger the number is, the higher the CoS priority is. CoS priority is used for ensuring service quality in Layer 2 network.

Figure 10-5 CoS priority packet structure



FL priority and TC priority

The IPv6 protocol supports FL priority-based and TC priority-based data traffic classification.

An IPv6 data packet contains a 40-byte basic header and an extension header with a fixed length. The TC field and FL field in the basic header of an IPv6 packet are related to QoS.

- TC field: an 8-bit field, like ToS of the TPv4 packet header, is used to identify service types of packets.
- FL field: a 20-bit field, used to identify packets from of same service flow. In addition, it can be used to re-classify packets of the same flow. Together with source and destination addresses, FL is uniquely identifying a service flow. All packets from the same service flow share the same FL. Therefore, the system can adopt identical processing modes on these packets.

10.1.3 Traffic policy

After performing traffic classification on packets, you need to perform different operations on packets in different categories. A traffic policy is a QoS policy in which traffic classification is bound to traffic behaviors.

Rate limiting based on traffic policy

Rate limiting refers to limiting network traffics. Rate limiting is used to control the rate of traffic in the network and drop the traffic that exceeds the rate. Therefore, you can control the traffic rate within a reasonable range. In addition, network resources and Carrier's benefits are protected.

Redirection

Redirection refers to that a packet is not forwarded according to the mapping between the original destination address and the interface. Instead, the packet is redirected to a specified interface for forwarding, realizing policy routing.

Remarking

Re-marking refers to reconfiguring some priority fields of the packet, so that devices can re-classify packets based on their own standards. In addition, downstream nodes can provide differentiated QoS services depending on remarking information.

10.1.4 Priority mapping

Priority mapping refers to sending packets to different queues with different local priorities according to configured mapping between external priority and local priority. Therefore, packets in different queues can be scheduled on the egress interface.

Note

The local priority refers to an internal priority that is assigned to the packet. It is related to the queue number on the egress interface. The bigger the value is, the more quickly the packet is processed.

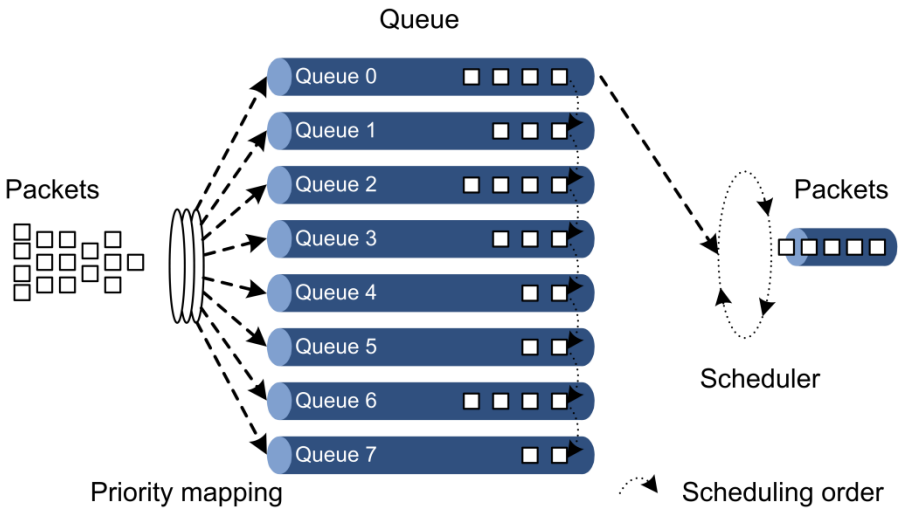
10.1.5 Congestion management

You need to perform the queue scheduling when delay-sensitive services need better QoS services than non-delay sensitive services and when the network is congested once in a while.

Queue scheduling adopts different scheduling algorithms to send packets in a queue. Scheduling algorithms supported by the ISCOM6820 include Strict Priority (SP), Weight Round Robin (WRR), Deficit Round Robin (DRR), and SP+WRR. All scheduling algorithms are designed for addressing specified traffic problems. And they have different effects on bandwidth distribution, delay, and jitter.

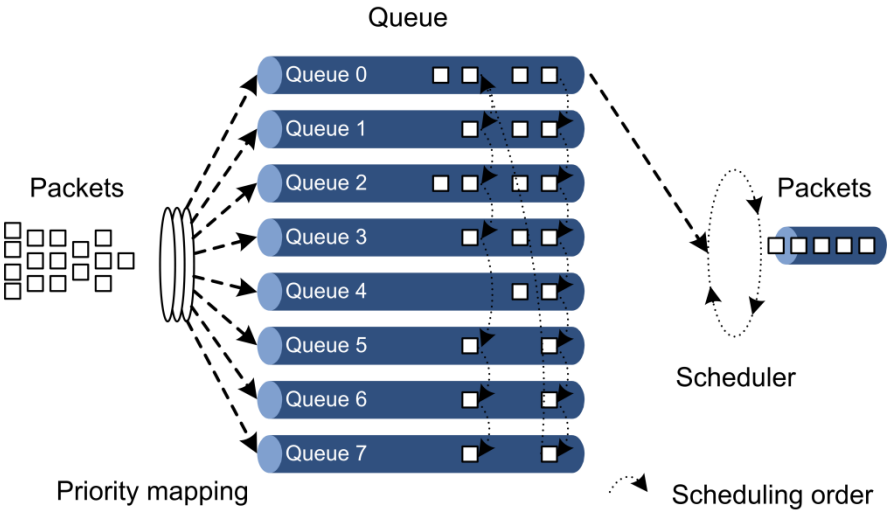
- SP: the device strictly schedules packets in a descending order of priority. Packets with lower priority cannot be scheduled until packets with higher priority are scheduled, as shown in Figure 10-6.

Figure 10-6 SP scheduling



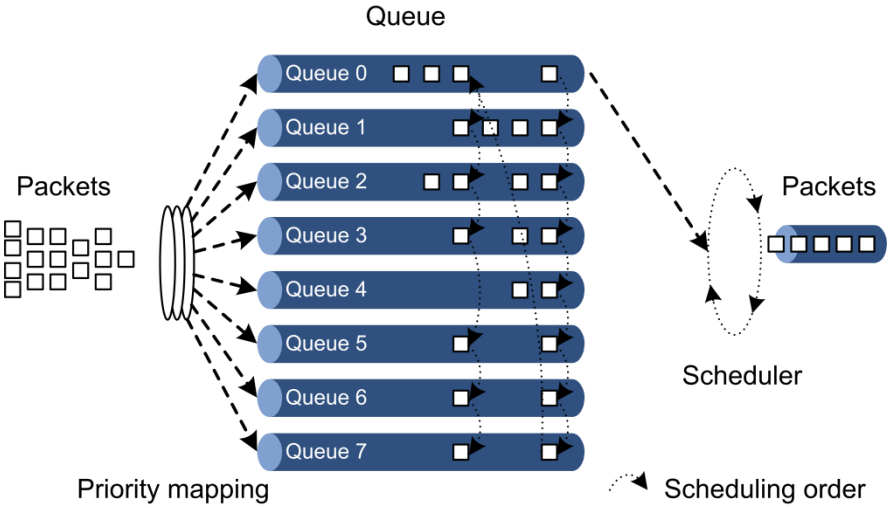
- WRR: on the basis of scheduling packets in a polling manner according to the priority, the device schedules packets according to the weight of the queue, as shown in Figure 10-7.

Figure 10-7 WRR scheduling



- DRR: on the basis of scheduling packets in a polling manner according to the priority, the device schedules packets according to the weight of the queue. In addition, during the scheduling, if one queue has redundant bandwidth, the device will temporarily assign this bandwidth to another queue. During next scheduling, the assigned schedule will return equal bandwidth to the original queue, as shown in Figure 10-8.

Figure 10-8 DRR scheduling



- SP+WRR: a scheduling mode combining the SP scheduling and the WRR scheduling together. In this mode, queues on a port are divided into 2 groups. You can specify the some queues to perform SP scheduling and others to perform WRR scheduling.

10.2 Configuring traffic classification

10.2.1 Preparing for configurations

Scenario

Traffic classification refers to identifying certain packets according to specified rules and performing different QoS policies on packets matched with different rules. Traffic classification is the premise and basis for differentiated services.

Traffic classification refers to indexing the mapping table according to the priority (such as DSCP priority) of the packet and mapping the packet priority to the local priority for traffic monitoring, congestion avoidance, and congestion management. Traffic classification is mainly used in the core nodes on the network and trusts priority information carried by the packet.

Prerequisite

N/A

10.2.2 Default configurations

Priority trust

Default configurations of priority trust are as below.

Function	Default value
Priority trust type on OLT	CoS
Default priority of OLT interface	0

Priority mapping

Mapping among the CoS priority, local priority, and queue on the ISCOM6820 is as below.

CoS priority	0	1	2	3	4	5	6	7
Local priority	0	1	2	3	4	5	6	7
Queue	0	1	2	3	4	5	6	7

Mapping among the DSCP priority, local priority, and queue on the ISCOM6820 is as below.

DSCP priority	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
Local priority	0	1	2	3	4	5	6	7
Queue	0	1	2	3	4	5	6	7

10.2.3 Configuring priority trust

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface { gpon-olt | gigabitethernet | ten-gigabitethernet } slot-id/port-id`	Enter physical interface configuration mode.
3	`Raisecom(config-if-*-*:*)#mls qos trust dscp`	Configure the protocol type trusted by the OLT interface.
4	`Raisecom(config-if-*-*:*)#mls qos priority value`	Configure the default priority of the interface. You can use the **no mls qos priority** command to restore default configuration. **Note** For packets without the 802.1p field, use the default priority.

10.2.4 Configuring priority mapping

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#mls qos mapping localpriority local-priority to queue queue-id`	Configure the mapping between the internal priority and queue.

10.2.5 Configuring the mapping from the DSCP priority to local priority

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#mls qos mapping dscp-to-local-priority profile-id`	Create a profile of the mapping from the DSCP priority to local priority and color, and enter dscp-to-pri configuration mode.

Step	Command	Description
3	Raisecom(dscp-to-pri)#**dscp** *dscp-value* **to local-priority** *localpri-value* [**color** { **green** | **red** | **yellow** }]	Configure the mapping from the DSCP priority to local priority and color.
4	Raisecom(dscp-to-pri)#**exit** Raisecom(config)#**interface gigaethernet** *unit-id/slot-id/port-id*	Exit dscp-to-pri configuration mode. Enter interface configuration mode.
5	Raisecom(config-gigaethernet*/*/*)#**mls qos mapping dscp** *dscp-value* **to localpriority** *local-priority*	Apply the profile of the mapping from the DSCP priority to local priority and color to the interface.

10.2.6 Configuring the mapping from the CoS priority to local priority

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos mapping cos-to-local-priority** *profile-id*	Create a profile of the mapping from the CoS priority to local priority and color, and enter cos-to-pri configuration mode.
3	Raisecom(cos-to-pri)#**cos** *cos-value* **to local-priority** *localpri-value* [**color** { **green** | **red** | **yellow** }]	Configure the mapping from the CoS priority to local priority and color.
4	Raisecom(cos-to-pri)#**exit** Raisecom(config)#**interface gigaethernet** *unit-id/slot-id/port-id*	Exit cos-to-pri configuration mode. Enter interface configuration mode.
5	Raisecom(config-gigaethernet*/*/*)# **mls qos mapping dscp** *dscp-value* **to localpriority** *local-priority*	Apply the profile of the mapping from the CoS priority to local priority and color to the interface.

10.2.7 Configuring CoS priority remarking

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#**mls qos mapping cos-remark** *profile-id*	Create a CoS priority remarking profile, and enter cos-remark configuration mode.
3	Raisecom(cos-remark)#**exit** Raisecom(config)#**interface gigaethernet** *unit-id/slot-id/port-id*	Exit cos-remark configuration mode. Enter interface configuration mode.
4	Raisecom(config-gigaethernet*/*/*)#**mls qos cos-remark** *profile-id*	Apply the CoS remarking profile to the interface.

10.2.8 Checking configurations

No.	Command	Description
1	Raisecom#**show mls qos mapping localpriority**	Show information about the mapping from the CoS priority to local priority and queue.
2	Raisecom#**show mls qos mapping dscp-to-local-priority** [**default** | *profile-id*]	Show information about the mapping from the DSCP priority to local priority and color.
3	Raisecom#**show mls qos mapping cos-remark** [**default** | *profile-id*]	Show information about the CoS priority remarking profile.
4	Raisecom#**show mls qos mapping cos-to-local-priority** [**default** | *profile-id*]	Show information about the mapping from the CoS priority to local priority and color.

10.3 Configuring traffic monitoring

10.3.1 Preparing for configurations

Scenario

Traffic monitoring is mainly used on the ingress interface of traffic, aiming to limit the input traffic.

To control the traffic, a mechanism is needed to measure the traffic of the device. The token bucket is the most widely used for measuring traffic at present.

The token bucket is a container to store tokens with a preset capacity. Tokens are arranged to the token bucket at a configured rate. When the bucket is full, excessive tokens will overflow. The token bucket is divided into single-token bucket and dual-token bucket by the quantity of the bucket. For the dual-token bucket, it is divided into single-rate and dual-rate by the input rate.

Prerequisite

N/A

10.3.2 Default configurations

N/A

10.3.3 Configuring rate limiting

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)#**mls qos** { **aggregate-policer** | **single-policer** } *policer-id* **cir** *cir* **cbs** *cbs* [**red** { **drop** | **recolor** { **red** | **green** } | **set-cos** *value* | **set-dscp** *value* }] [**green** { **drop** | **recolor** { **red** | **green** } | **set-cos** *value* | **set-dscp** *value* }]	Create rate limiting rules and specify the action taken when the rate exceeds the threshold (single-token bucket monitoring).
3	Raisecom(config)#**mls qos** { **aggregate-policer** | **single-policer** } *policer-id* **cir** *cir* **cbs** *cbs* [**pir** *pir*] **pbs** *pbs* [**red** { **drop** | **recolor** { **red** | **green** | **yellow** } | **set-cos** *value* | **set-dscp** *value* }] [**green** { **drop** | **recolor** { **red** | **green** | **yellow** } | **set-cos** *value* | **set-dscp** *value* }] [**yellow** { **drop** | **recolor** { **red** | **green** | **yellow** } | **set-cos** *value* | **set-dscp** *value* }] [**color-aware**]	Create rate limiting rules and specify the action taken when the rate exceeds the threshold (dual-token bucket monitoring).

Note

- When you configure the PIR parameter, the rate limiter works in dual-token bucket mode. Otherwise, it works in single-token bucket mode.
- Rate limiting in the ingress direction is not supported.

10.3.4 Checking configurations

No.	Command	Description
1	Raisecom#**show mls qos policer** [*policer-id*]	Show configurations of the rate limiter.

10.4 Configuring traffic shaping

10.4.1 Preparing for configurations

Scenario

Traffic shaping aims to eliminate the burst traffic and smooth output traffic. Traffic shaping is usually used on the egress interface.

Similar to traffic monitoring, traffic shaping also adopts the token bucket to measure traffic while it will not drop packets. It either sends the packet or does not send the packet. Whether a packet is dropped or not depends on the drop policy for congestion avoidance when the packet is scheduled to a queue.

Prerequisite

N/A

10.4.2 Default configurations

Queue	CIR (kbit/s)	CBS (kbit/s)	Gts-buffer (Byte)
0	0	0	1000
1	0	0	1000
2	0	0	1000
3	0	0	1000
4	0	0	1000
5	0	0	1000
6	0	0	1000
7	0	0	1000

10.4.3 Configuring traffic shaping

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** { **gigabitethernet** | **ten-gigabitethernet** | **gpon-olt** } *slot-id/port-id*	Enter physical interface configuration mode.
3	Raisecom(config-if-*-*:*)#**mls qos shaping** [**queue** *queue-id*] **cir** *cir* **cbs** *cbs* [**gts-buffer** *size*]	Configure traffic shaping.

10.4.4 Checking configurations

No.	Command	Description
1	Raisecom#**show interface** { **gigabitethernet** | **ten-gigabitethernet** | **epon-olt** | **ten-giga-epon-olt** | **gpon-olt** } *slot-id/port-id* **mls qos queue shaping**	Show configurations of traffic shaping.

10.5 Configuring congestion avoidance

10.5.1 Preparing for configurations

Scenario

Queue scheduling can only ease network congestion to some degree. When the congestion is continuous, the queue buffer will be used up and packet loss cannot be avoided. The simplest and most intuitive policy is tail drop.

However, if a number of TCP packets are dropped, this will cause TCP timeout, thus initiating the TCP slow start and congestion avoidance mechanism. Then, the Tx end of TCP decreases the Tx frequency of packets. When packets of multiple TCP connections are dropped, multiple TCP connections may enter slow start and congestion avoidance mode at the same time, which is called TCP global synchronization. In this case, multiple TCP connections decrease the Tx frequency of packets, thus lowering the bandwidth utilization rate of links.

To avoid TCP global synchronization and increase bandwidth utilization rate, Weighted Random Early Detection (WRED) drop policy is adopted.

Prerequisite

N/A

10.5.2 Default configurations

N/A

10.5.3 Configuring WRED scheduling

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** { **gigabitethernet** | **ten-gigabitethernet** | **gpon-olt** } *slot-id/port-id*	Enter physical interface configuration mode.
3	Raisecom(config-if-*-*:*)#**mls qos wred** [**queue** *queue-id*] [**red** | **green** | **yellow**] **low-limit** *value* **high-limit** *value* **drop-probability** *value*	Configure WRED scheduling parameters.

10.5.4 Checking configurations

No.	Command	Description
1	Raisecom#**show interface** { **gigabitethernet** | **ten-gigabitethernet** | **gpon-olt** } *slot-id/port-id* **mls qos queue wred**	Show WRED configurations.

10.6 Configuring congestion management

10.6.1 Preparing for configurations

Scenario

Congestion management refers to allocating and controlling bandwidth when the network is congested. Congestion management adopts the queue technology to cache packets according to traffic classification, and then send packets to corresponding queues according to queue scheduling algorithms, thus providing differentiated services when the network is congested.

Prerequisite

N/A

10.6.2 Default configurations

Scheduling mode

Default configurations of the queue scheduling mode are as below.

Function	Default value
OLT queue scheduling mode	SP

Queue weight

Default weights of WDRR and WRR queues on the ISCOM6820 are as below.

Queue	0	1	2	3	4	5	6	7
WDRR weight	1	1	1	1	1	1	1	1
WRR weight	1	1	1	1	1	1	1	1

10.6.3 Configuring SP scheduling

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** { **gpon-olt** | **gigabitethernet** | **ten-gigabitethernet** } *slot-id/port-id*	Enter physical interface configuration mode.
3	Raisecom(config-if-*-*:*)#**mls qos queue scheduler sp**	Configure the queue scheduling mode to SP.

10.6.4 Configuring WRR scheduling

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** { **gpon-olt** | **gigabitethernet** | **ten-gigabitethernet** } *slot-id/port-id*	Enter physical interface configuration mode.
3	Raisecom(config-if-*-*:*)#**mls qos queue scheduler wrr**	Configure the queue scheduling mode to WRR. You can use the **no mls qos queue scheduler** command to restore default configuration.

Step	Command	Description
4	Raisecom(config-if-*-*:*)**mls qos queue** {**wrr | wdrr**} { *weigh1 weight2 weight3…weight8* }	Configure the weight of each queue in WRR scheduling mode.

10.6.5 Checking configurations

No.	Command	Description
1	Raisecom#**show interface** { **gigabitethernet** | **ten-gigabitethernet** | **gpon-olt** } *slot-id/port-id* **mls qos**	Show QoS configurations on the interface, including the interface trust mode, default CoS value, and queue scheduling mode.
2	Raisecom#**show interface** { **gigabitethernet** | **ten-gigabitethernet** | **gpon-olt** } *slot-id/port-id* **mls qos queue**	Show configurations of queue weights on interfaces.
3	Raisecom#**show interface** { **gigabitethernet** | **ten-gigabitethernet** | **gpon-olt** } *slot-id/port-id* **mls qos queue wred**	Show configurations of WRED queues.

10.7 Configuring traffic policy

10.7.1 Preparing for configurations

Scenario

After traffic classification, you need to perform different operations on packets of different types.

Prerequisite

N/A

10.7.2 Default configurations

N/A

10.7.3 Configuring OLT traffic policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#{ **ip-access-list** *list-number* | **ipv6-access-list** *list-number* | **l2-access-list** *list-number* | **hybrid-access-list** *list-number* | **user-access-list** *list-number* }	Create an ACL and enter ACL configuration mode.

Step	Command	Description
3	Raisecom(config-*-acl-*)#**rule** *rule-id*	Create an ACL sub-rule and enter ACL sub-rule configuration mode.
4	Raisecom(config-*-acl-*-rule-*)#**set** { **ip dscp** *value* | **ip precedence** *value* | **cos** *cos* | **vlan** *vlan-id* }	Mark the data traffic.
5	Raisecom(config-*-acl-*-rule-*)#**redirect-to** { **gigaethernet** *unit-id/slot-id/port-id* | **ten-gigabitethernet** *slot-id/port-id*	Configure the data traffic to be redirected to other interfaces.
6	Raisecom(config-*-acl-*-rule-*)# **mirror-to** { **gigaethernet** *unit-id/slot-id/port-id* | **ten-gigabitethernet** *slot-id/port-id*	Configure the data traffic to be mirrored to other interfaces.
7	Raisecom(config-*-acl-*-rule-*)# **policer** *policer-name*	Quote a traffic policing template in the traffic policy.

10.8 Configuration examples

10.8.1 Example for configuring queue scheduling

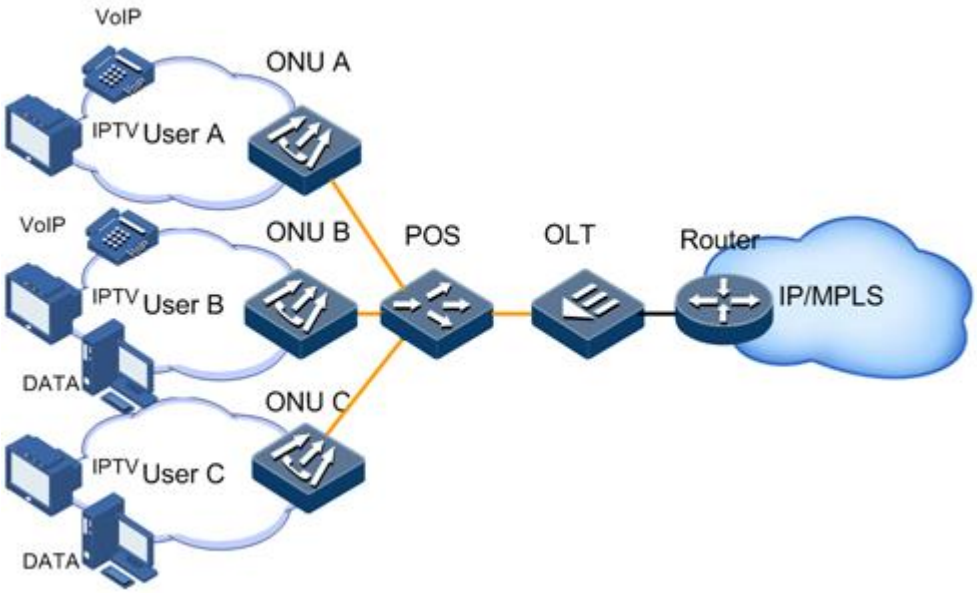
Networking requirements

As shown in Figure 10-9, User A provides voice and video services; User B provides voice, video, and data services; and User C provides video and data services.

CoS priority of voice services is 5; CoS priority of video services is 4; and CoS priority of data services is 2. Local priority of the above services is 6, 5, and 2 respectively.

- For voice services, perform SP scheduling to make the traffic transmitted preferentially.
- For video services, perform WRR scheduling and the weight is 15.
- For data services, perform WRR scheduling and the weight is 10. In addition, configure the drop threshold to 15 to avoid network congestion caused by too heavy burst traffic.

Figure 10-9 Configuring queue scheduling



Configuration steps

Step 1 Configure interface priority trust.

```
Raisecom#config
Raisecom(config)#interface gpon-olt 1/1
Raisecom(config-if-1:1)#no mls qos trust dscp
```

Step 2 Configure mapping between the CoS priority and local priority.

```
Raisecom(config-if-1:1)#exit
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 scheduling.

```
Raisecom(config)#interface gpon-olt 1/1
Raisecom(config-if-gpon-olt-1:1)#mls qos queue scheduler wrr
Raisecom(config-if-gpon-olt-1:1)#mls qos queue wrr 1 1 10 1 1 15 0 0
```

Checking results

Use the **show mls qos mapping** command to show mapping configurations for specified priorities.

```
Raisecom#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
```

11 Configuring system security

This chapter describes the system security feature and configuration process of the ISCOM6820, and provides related configuration examples, including the following sections:

- Introduction
- Configuring ACL
- Configuring TACACS+
- Configuring RADIUS
- Configuring storm control
- Configuring interface isolation
- Configuring attack prevention
- Configuring anti-DoS attacks
- Configuring URPF
- Configuration examples

11.1 Introduction

11.1.1 ACL

Access Control List (ACL) is a set of ordered rules, which can control the device to receive or discard some data packets, thus preventing illegal packets from impacting network performance.

ACL is composed of **permit** | **deny** sentences. The rules are described by the source/destination MAC address, source/destination IP address, and interface ID of data packets. The device judges whether to receive or discard packets according to these rules.

11.1.2 TACACS+

Terminal Access Controller Access Control System (TACACS+) is a network access authentication protocol similar to RADIUS. Compared with RADIUS, TACACS+ has the following features:

- Use the TCP port, providing higher transmission reliability. RADIUS uses a UDP port.

- Encapsulate the whole standard TACACS+ packet except for the TACACS+ header. Compared with RADIUS which encapsulates the user password only, TACACS+ provides higher security.
- Separate TACACS+ authentication from TACACS+ authorization and TACACS+ accounting, providing a more flexible deployment mode.

Therefore, compared with RADIUS, TACACS+ is more secure and reliable. However, as an open protocol, RADIUS is more widely used.

11.1.3 Attack prevention

Single-packet attack

The single packet attack is also known as malformed packet attack. The attacker sends flawed IP packets to the target system, such as fragment overlapping packets and TCP flag bit illegal packets, causing the target system to make errors and to crash in processing such IP packets, causing losses to the target system, or causing attacks by sending a large number of useless packets that occupy network bandwidth. Table 11-1 lists types of malformed packets that can be prevented by the device.

Table 11-1 Types of malformed packets that can be prevented by the device

Type of malformed packets	Description
Land-Base	The attacker sends a large number of TCP SYN packets with both the source IP address and destination IP address as the target host, causing the target host to run out of semi-connection resources and to malfunction.
Large ICMP	After some hosts or devices receive oversized packets, the memory is incorrectly allocated and the protocol stack crashes. The attacker crashes the target host by sending large ICMP packets, thus achieving the attack goal.
Smurf	The attackers sends ICMP response requests to the target network, setting the destination address of the request packet to the broadcast address of the target network. In this way, all hosts on the network will respond to this ICMP response request, causing network congestion and achieving the attack goal of the Denial of Service (DoS) of the target network host.

URPF

The main function of Unicast Reverse Path Forwarding (URPF) is to prevent network attacks based on source address spoofing, such as DoS attacks and Distributed Denial of Service (DDoS) attacks based on source address spoofing.

The source address spoofing attacks generates a series of packets with forged source addresses. For applications that use the IP address for authentication, this attack method can result in unauthorized users gaining access to the system as someone else, or even with administrator privileges. Even if the response packet cannot reach the attacker, it will still cause damage to the attacked object.

URPF can verify the source address of packets and filter them based on their legality to prevent source address spoofing attacks.

11.1.4 Storm control

In most scenarios of the Layer 2 network, unicast traffic is much heavier than broadcast traffic. If the rate for broadcast traffic is not limited, much bandwidth will be occupied when a broadcast storm is generated. Therefore, network performance is reduced and forwarding of normal unicast packets is seriously affected. Moreover, communication between devices may be interrupted.

Configuring storm control on Layer 2 devices can prevent broadcast storm when broadcast packets increase sharply on the network. Therefore, it ensures that unicast packets can be properly forwarded.

11.1.5 Interface isolation

Interface isolation adopts the isolation group method to implement data isolation among multiple interfaces on the device, thus enhancing network access security.

The ISCOM6820 devices support the following three types of port isolation:

- OLT physical port isolation: include isolation between different ports on the same interface card and isolation between different ports on different interface cards.
- Port isolation in an OLT VLAN: one VLAN can have multiple isolation groups. The ports in the isolation group cannot communicate with each other. The ports between different isolation groups can communicate with each other. A port that is not added to an isolation group in a VLAN can communicate with any port in the VLAN.
- ONU UNI isolation

11.2 Configuring ACL

11.2.1 Preparing for configurations

Scenario

ACL can help the network device recognize and filter specified data packets. Only after the device recognizes the specified packets, it can permit/deny the access of packets according to the configured policy.

ACL can be divided into the following types.

- IP ACL: classification rules are formulated according to the source or destination address, TCP or UDP port ID, and other data packet attributes carried by the IP header.
- Layer 2 ACL: classification rules are formulated according to the source MAC address, the destination MAC address, Layer 2 protocol type, and other Layer 2 information carried by the Layer 2 frame header.
- Hybrid ACL: classification rules are formulated according to the IP header and Layer 2 frame header. This type of ACL mixes characteristics of IP ACL and Layer 2 ACL.

The ACL application mode can be divided into the following three types according to actual scenarios:

- Based on the whole device
- Based on uplink and downlink of the interface
- Based on traffic from the ingress interface to egress interface

Prerequisite

N/A

11.2.2 Default configurations

N/A

11.2.3 Configuring IP ACL

Configuring IPv4 ACL

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip-access-list** *list-number*	Create an IPv4 ACL and enter IPv4 ACL configuration mode. You can use the **no ip-access-list** { **all** | l*ist-numbe*r } command to delete the ACL.
3	Raisecom(config-ip-acl-*)#**description** *desc-string*	(Optional) configure descriptions of the IPv4 ACL.
4	Raisecom(config-ip-acl-*)#**rule** *rule-number*	Configure the ID of IPv4 ACL sub-rules and enter sub-rule configuration mode.
5	Raisecom(config-ip-acl-*-rule-*)#**access-type** { **permit** | **deny** }	Configure the access type of the IPv4 ACL sub-rule.
6	Raisecom(config-ip-acl-*-rule-*)#**match ip destination-address** *ip-address* [*mask*]	Configure the destination IP address of the IPv4 ACL sub-rule.
7	Raisecom(config-ip-acl-*-rule-*)#**match ip source-address** *ip-address* [*mask*]	Configure the source IP address of the IPv4 ACL sub-rule.
8	Raisecom(config-ip-acl-*-rule-*)#**match ip precedence** { *pri* | **routine** | **priority** | **immediate** | **flash** | **flash-override** | **critical** | **internet** | **network** }	Configure matching the IPv4 ACL sub-rule with the source IP precedence.
9	Raisecom(config-ip-acl-*-rule-*)#**match ip tos** { *service-value* | **normal** | **min-monetary-cost** | **min-delay** | **max-reliability** | **max-throughput** }	Configure matching the IPv4 ACL sub-rule with the IP ToS.
10	Raisecom(config-ip-*-rule-*)#**match ip dscp** { *diff-service-code* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41** | **af42** | **af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **ef** | **default** }	Configure matching the IPv4 ACL sub-rule with IP DSCP.

Step	Command	Description
11	Raisecom(config-ip-acl-*-rule-*)#**match ip** { **fragments** | **no-fragments** }	Configure matching the IPv4 ACL sub-rule with the fragmented or non-fragmented packet.
12	Raisecom(config-ip-*-rule-*)#**match ip protocol** { *protocol-num* | **ahp** | **esp** | **gre** | **icmp** | **igmp** | **igrp** |**ipinip** | **ospf** | **pcp** | **pim** | **tcp** | **udp** }	Configure matching the IPv4 ACL sub-rule with the IP upper protocol type.
13	Raisecom(config-ip-*-rule-*)#**match ip tcp** { **destination-port** | **source-port** } { *port-num* | **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** }	Configure matching the IPv4 ACL sub-rule with the destination/source interface ID of the TCP packet. The packet type refers to the classical interface ID.
14	Raisecom(config-ip-*-rule-*)#**match ip tcp** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }	Configure matching the IPv4 ACL sub-rule with the TCP packet flag.
15	Raisecom(config-ip-*-rule-*)#**match ip udp** { **destination-port** | **source-port** } { *port-num* | **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** }	Configure matching the IPv4 ACL sub-rule with the destination/source interface ID of the UDP packet.

Configuring IPv6 ACL

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6-access-list** *list-number*	Create an IPv6 ACL and enter IPv6 ACL configuration mode.
3	Raisecom(config-ipv6-acl-*)#**description** *text*	(Optional) configure descriptions of the IPv6 ACL.
4	Raisecom(config-ipv6-acl-*)#**rule** *rule-number*	Configure the number of the IPv6 ACL sub-rule and enter sub-rule configuration mode.
5	Raisecom(config-ipv6-acl-*-rule-*)#**access-type** { **permit** | **deny** }	Configure the access type of the IPv6 ACL sub-rule.
6	Raisecom(config-ipv6-acl-*-rule-*)#**match ip destination-address** *ipv6-address/prefix-length*	Configure the destination IP address of the IPv6 ACL sub-rule.
7	Raisecom(config-ipv6-acl-*-rule-*)#**match ip source-address** *ipv6-*	Configure the source IP address of the IPv6 ACL

Step	Command	Description
	address/prefix-length	sub-rule.
8	Raisecom(config-ipv6-acl-*-rule-*)#**match ip traffic-class** *user-level*	Configure the IPv6 ACL sub-rule matching with the user level of the IPv6 packet.
9	Raisecom(config-ipv6-acl-*-rule-*)#**match ip protocol** *ipv6-protocol-id*	Configure the IPv6 ACL sub-rule matching with IP upper protocol type.
10	Raisecom(config-ipv6-acl-*-rule-*)#**match ip tcp** { **destination-port** | **source-port** } { *port-num* | **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** }	Configure matching the IPv6 ACL sub-rule with the destination/source interface ID of the TCP packet.
11	Raisecom(config-ipv6-acl-*-rule-*)#**match ip tcp** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }	Configure matching the IPv6 ACL sub-rule with the TCP packet flag.
12	Raisecom(config-ipv6-acl-*-rule-*)#**match ip flow-label** *lable-valu*	Configure matching the IPv6 ACL sub-rule with the flow label of the IPv6 packet.
13	Raisecom(config-ipv6-acl-*-rule-*)#**match ip udp** { **destination-port** | **source-port** } { *port-num* | **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** }	Configure matching the IPv6 ACL sub-rule with the destination/source interface ID of the UDP packet.

11.2.4 Configuring Layer 2 ACL

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**l2-access-list** *list-number*	Create a Layer 2 ACL and enter Layer 2 ACL configuration mode. You can use the **no l2-access-list** *acl-numb*er command to delete the ACL.
3	Raisecom(config-l2-acl-*)#**description**	(Optional) configure descriptions of the Layer 2 ACL.
4	Raisecom(config-l2-acl-*)#**rule** *rule-number* **example:** Raisecom(config-l2-acl-1)#rule 2	Configure the number of the Layer 2 ACL sub-rule.
5	Raisecom(config-l2-acl-*-rule-*)#**access-type** { **permit** | **deny** }	Configure the access type of the Layer 2 ACL sub-rule.

Step	Command	Description
6	Raisecom(config-l2-acl-*-rule-*)#**match mac destination** *mac* [*mac-mask*]	Configure the destination MAC address of the Layer 2 ACL sub-rule.
7	Raisecom(config-l2-acl-*-rule-*)#**match mac source** *mac* [*mac-mask*]	Configure the source MAC address of the Layer 2 ACL sub-rule.
8	Raisecom(config-l2-acl-*-rule-*)#**match svlan** *svlan-id*	Configure matching the Layer 2 ACL sub-rule with the source SVLAN ID.
9	Raisecom(config-l2-acl-*-rule-*)#**match svlan-cos** *svlan-cos*	Configure matching the Layer 2 ACL sub-rule with the SVLAN CoS.
10	Raisecom(config-l2-acl-*-rule-*)#**match cvlan** *cvlan-id*	Configure matching the Layer 2 ACL sub-rule with the source CVLAN ID.
11	Raisecom(config-l2-acl-*-rule-*)#**match cvlan-cos** *cvlan-cos*	Configure matching the Layer 2 ACL sub-rule with the CVLAN CoS.
12	Raisecom(config-l2-acl-*-rule-*)#**match ethertype** *frame-type frame-type mask*	Configure matching the Layer 2 ACL sub-rule with the frame type in the Layer 2 frame head.
13	Raisecom(config-l2-acl-*-rule-*)#**match ethertype** { **arp** | **eapol** | **flowcontrol** |**ip** | **loopback** | **mpls** | **mpls-mcast** | **pppoe** | **pppoedisc** | **x25** | **x75** }	Configure matching the Layer 2 ACL sub-rule with the protocol type in the Layer 2 frame head.

11.2.5 Configuring hybrid ACL

Configuring IPv4 hybrid ACL

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**hybrid-access-list** *list-number*	Create a hybrid ACL and enter hybrid ACL configuration mode. You can use the **no hybrid-access-list** { **all** | l*ist-numb*er } command to delete the ACL.
3	Raisecom(config-hybrid-acl-*)#**description**	(Optional) configure the description of hybrid ACL.
4	Raisecom(config-hybrid-acl-*)#**rule** *rule-number* **example:** Raisecom(config-l2-acl-1)#rule 2	Configure the ID of the hybrid ACL sub-rule.
5	Raisecom(config-hybrid-acl-*-rule-*)#**access-type** { **permit** | **deny** }	Configure the access type of the hybrid ACL sub-rule.
6	Raisecom(config-hybrid-acl-*-rule-*)#**match mac destination** *mac* [*mac-mask*]	Configure the destination MAC address of the hybrid ACL sub-rule.

7	Raisecom(config-hybrid-acl-*-rule-*)#**match mac source** *mac* [*mac-mask*]	Configure the source MAC address of the hybrid ACL sub-rule.
8	Raisecom(config-hybrid-acl-*-rule-*)#**match svlan** *svlan-id*	Configure matching the hybrid ACL sub-rule with the source SVLAN ID.
9	Raisecom(config-hybrid-acl-*-rule-*)#**match svlan-cos** *svlan-cos*	Configure matching the hybrid ACL sub-rule with the SVLAN CoS.
10	Raisecom(config-hybrid-acl-*-rule-*)#**match cvlan** *cvlan-id*	Configure matching the hybrid ACL sub-rule with the source CVLAN ID.
11	Raisecom(config-hybrid-acl-*-rule-*)#**match cvlan-cos** *cvlan-cos*	Configure matching the hybrid ACL sub-rule with the CVLAN CoS.
12	Raisecom(config-hybrid-acl-*-rule-*)#**match ethertype** *ethertype frame-type frame-type-mask*	Configure matching the hybrid ACL sub-rule with the frame type in the hybrid frame head.
13	Raisecom(config-hybrid-acl-*-rule-*)#**match ethertype** { **arp** | **eapol** | **flowcontrol** |**ip** | **loopback** | **mpls** | **mpls-mcast** | **pppoe** | **pppoedisc** | **x25** | **x75** }	Configure matching the hybrid ACL sub-rule with the protocol type in the hybrid frame head.
14	Raisecom(config-hybrid-acl-*-rule-*)#**match ip destination-address** *ip-address* [*mask*]	Configure the destination IP address of the hybrid ACL sub-rule.
15	Raisecom(config-hybrid-acl-*-rule-*)#**match ip source-address** *ip-address* [*mask*]	Configure the source IP address of the hybrid ACL sub-rule.
16	Raisecom(config-hybrid-acl-*-rule-*)#**match ip precedence** { *pri* | **routine** | **priority** | **immediate** | **flash** | **flash-override** | **critical** | **internet** | **network** }	Configure matching the hybrid ACL sub-rule with the source IP precedence.
17	Raisecom(config-hybrid-acl-*-rule-*)#**match ip tos** { *service-type* | **normal** | **min-monetary-cost** | **min-delay** | **max-reliability** | **max-throughput** }	Configure matching the hybrid ACL sub-rule with the IP ToS.
18	Raisecom(config-hybrid-acl-*-rule-*)#**match ip dscp** { *diff-service-code* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41**| **af42** |**af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7** | **ef** | **default** }	Configure hybrid ACL subrule to match IP DSCP.
19	Raisecom(config-hybrid-acl-*-rule-*)#**match ip** { **fragments** | **no-fragments** }	Configure matching the hybrid ACL sub-rule with the fragmented or non-fragmented packet.
20	Raisecom(config-hybrid-acl-*-rule-*)#**match ip protocol** { *protocol-num* | **ahp** | **esp** | **gre** | **icmp** | **igmp** | **igrp** |**ipinip** | **ospf** | **pcp** | **pim** | **tcp** | **udp** }	Configure matching the hybrid ACL sub-rule with the IP upper protocol type.

21	Raisecom(config-hybrid-acl-*-rule-*)#**match ip tcp** { **destination-port** | **source-port** } { *port-num* | **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** }	Configure matching the hybrid ACL sub-rule with the destination/source interface ID of the TCP packet.
22	Raisecom(config-hybrid-acl-*-rule-*)#**match ip tcp** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }	Configure matching the hybrid ACL sub-rule with the TCP packet flag.
23	Raisecom(config-hybrid-acl-*-rule-*)#**match ip udp** { **destination-port** | **source-port** } { *port-num* | **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** }	Configure the hybrid ACL subrule to match the destination/source interface ID of the UDP packet.

Configuring IPv6 hybrid ACL

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6-hybrid-access-list** *list-number*	Create an IPv6 hybrid ACL and enter hybrid ACL configuration mode.
3	Raisecom(config-ipv6-hybrid-acl-*)#**description** *text*	(Optional) configure the description of IPv6 hybrid ACL.
4	Raisecom(config-ipv6-hybrid-acl-*)#**rule** *rule-number*	Configure the ID of the IPv6 hybrid ACL sub-rule and enter sub-rule configuration mode.
5	Raisecom(config-ipv6-hybrid-acl-*-rule-*)#**access-type** { **permit** | **deny** }	Configure the access type of the IPv6 hybrid ACL sub-rule.
6	Raisecom(config-ipv6-hybrid-acl-*-rule-*)#**match mac destination** *mac* [*mac-mask*]	Configure the destination MAC address of the IPv6 hybrid ACL sub-rule.
7	Raisecom(config-ipv6-hybrid-acl-*-rule-*)#**match mac source** *mac* [*mac-mask*]	Configure the source MAC address of the IPv6 hybrid ACL sub-rule.
8	Raisecom(config-ipv6-hybrid-acl-*-rule-*)#**match svlan** *svlan-id*	Match the IPv6 hybrid ACL sub-rule with the source SVLAN ID.
9	Raisecom(config-ipv6-hybrid-acl-*-rule-*)#**match svlan-cos** *svlan-cos*	Match the IPv6 hybrid ACL sub-rule with the source SVLAN CoS.
10	Raisecom(config-ipv6-hybrid-acl-*-rule-*)#**match cvlan** *cvlan-id*	Configure matching the IPv6 hybrid ACL sub-rule with the source CVLAN ID.

Step	Command	Description
11	Raisecom(config-ipv6-hybrid-acl-*-rule-*)#**match cvlan-cos** *cvlan-cos*	Configure matching the IPv6 hybrid ACL sub-rule with the CVLAN CoS.
12	Raisecom(config-ipv6-hybrid-acl-*-rule-*)#**match ethertype** *frame-type frame-type-mask*	Configure matching the IPv6 hybrid ACL sub-rule with the frame type in the L2 frame head.
13	Raisecom(config-ipv6-hybrid-acl-*-rule-*)#**match ethertype** { **arp** | **eapol** | **flowcontrol** |**ip** | **ipv6** | **loopback** | **mpls** | **mpls-mcast** | **pppoe** | **pppoedisc** | **x25** | **x75** }	Configure matching the IPv6 hybrid ACL sub-rule with the protocol type in the L2 frame head.
14	Raisecom(config-ipv6-hybrid-acl-*-rule-*)#**match ip destination-address** *ip-address* [*mask*]	Configure the destination IP address of the IPv6 hybrid ACL sub-rule.
15	Raisecom(config-ipv6-hybrid-acl-*-rule-*)#**match ip source-address** *ip-address* [*mask*]	Configure the source IP address of the IPv6 hybrid ACL sub-rule.
16	Raisecom(config-ipv6-hybrid-acl-*-rule-*)#**match ip traffic-class** *user-level*	Configure matching the IPv6 hybrid ACL sub-rule with the user level in the IPv6 packet.
17	Raisecom(config-ipv6-hybrid-acl-*-rule-*)#**match ip protocol** *protocol-id*	Configure matching the IPv6 hybrid ACL sub-rule with the IP upper protocol type.
18	Raisecom(config-ipv6-hybrid-acl-*-rule-*)#**match ip tcp** { **destination-port** | **source-port** } { *port-num* | **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** }	Configure matching IPv6 hybrid ACL subrule with the source/destination interface ID of the TCP packet. The packet type represents the classic interface ID.
19	Raisecom(config-ipv6-hybrid-acl-*-rule-*)#**match ip udp** { **destination-port** | **source-port** } { *port-num* | **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** }	Configure matching the IPv6 hybrid ACL subrule with the destination/source interface ID of the UDP packet.

11.2.6 Configuring user ACL

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)#**user-access-list profile field** *field-id* **layer** { **l2** | **l3** | **l4** } **offset** *offset-value*	Configure customized ACL match objects.
3	Raisecom(config)#**user-access-list** *acl-number*	Create a customized ACL and enter user ACL configuration mode.
4	Raisecom(config-user-acl-*)#**description** *text*	(Optional) configure descriptions of the user ACL. You can use the **no description** command to delete the description.
5	Raisecom(config-user-acl-*)#**rule** *rule-number*	Configure the number of the user ACL sub-rule and enter sub-rule configuration mode.
6	Raisecom(config-user-acl-*-rule-*)#**access-type** { **permit** | **deny** }	Configure the access type of the user ACL sub-rule.
7	Raisecom(config-user-acl-*-rule-*)#**match field** *field-id content* [*mask*]	Configure the content of the ACL match field.
8	Raisecom(config-user-acl-*-rule-*)#**match tag-type** { **double-tag** | **s-tagged** | **untagged** }	Configure matching the user ACL with packets of different Tag types.

11.2.7 Applying ACL to device

Note

The ACL can be valid on the device only when an ACL is added to the filter. Multiple ACL matching rules can be added to the filter to form multiple filtering rules. When a filter is configured, the order in which ACL matching rules are added determines the priority of these rules. The earlier the rule is added, the higher the priority is. If there are conflicts in the matching calculation, the rule with the highest priority should prevail. When configuring commands, be careful when arranging the priorities of those rules in order to properly filter the packets.

Applying ACL based on uplink and downlink of interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**filter** { **l2-access-list** | **ip-access-list** | **hybrid-access-list** } *acl-num* **egress interface** {**gpon-olt** | **ten-gigabitethernet** } *slot-id/port-list* [**statistics**]	Configure the downlink to the interface for applying the ACL filtering rule. If the **statistics** parameter is configured, statistics will be gathered according to filtering rules.
3	Raisecom(config)#**filter** { **l2-access-list** | **ip-access-list** | **hybrid-access-list** } *acl-num* **ingress interface** {**gpon-olt** *slot-id/port-list* | **ten-gigabitethernet** *slot-id/port-list* | **port-channel** *group-id* } [**statistics**]	Configure the uplink to the interface for applying the ACL filtering rule. If the **statistics** parameter is configured, statistics will be gathered according to filtering rules.

Applying ACL based on traffic from ingress interface to egress interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**filter** { **l2-access-list** | **ip-access-list** | **hybrid-access-list** } *acl-num* **from interface** { **gpon-olt** | **ten-gigabitethernet** } *slot-id/port-list* **to interface** { **epon-olt** | **gpon-olt** | **ten-gigabitethernet** } *slot-id/port-list* [**statistics**]	Configure ACL filtering rules based on traffic from the ingress interface to egress interface. If the **statistics** parameter is configured, statistics will be gathered according to filtering rules. **Note** When you use this command, the ingress and egress interfaces should be on the same card.

11.2.8 Checking configurations

Checking OLT configurations

No.	Command	Description
1	Raisecom#**show ip-access-list** [*list-number*]	Show IPv4 ACL configurations.
2	Raisecom#**show ipv6-access-list** [*list-number*]	Show IPv6 ACL configurations.
3	Raisecom#**show l2-access-list** [*list-number*]	Show Layer 2 ACL configurations.
4	Raisecom#**show hybrid-access-list** [*list-number*]	Show hybrid ACL configurations.
5	Raisecom#show ipv6-hybrid-access-list [*list-number*]	Show IPv6 hybrid ACL configurations.
6	Raisecom#**show user-access-list** [*list-number*]	Show user ACL configurations.
7	Raisecom#**show user-access-list profile**	Show the customized ACL match field.
8	Raisecom#**show interface vlanif ip-access-list**	Show ACL configurations of the VLAN interface.
9	Raisecom#**show filter** [filter-*number*] **statistics**	Show filter statistics.
10	Raisecom#**show epon-onu** *slot-id/olt-id/onu-id* **uni ethernet** *uni-id* **filter**	Show filters already configured on the ONU interface.

11.2.9 Maintenance

No.	Command	Description
1	Raisecom(config)#**clear filter** [*filter-number*] **statistics**	Clear ACL filter statistics.

11.3 Configuring TACACS+

11.3.1 Preparing for configurations

Scenario

You can deploy the TACACS+ server on the network to perform authentication and accounting to control users from accessing the device and network. TACACS+ is safer and more reliable than RADIUS. The device can be used as an agent of the TACACS+ server, which authorizes users to access according to feedback from the TACACS+ server.

Prerequisite

N/A

11.3.2 Default configurations

By default, the ISCOM6820 are not configured with TACACS+ authentication server address and shared key. Both the user login mode and the enable login mode are local-user.

Function	Default value
IP address of TACACS+ authentication server	0.0.0.0
Shared key	N/A
User login mode	local-user
Enable login mode	local-user

11.3.3 Configuring TACACS+

Step	Command	Description
1	Raisecom#**tacacs-server** [**backup**] { *ip-address* / *ipv6-address* }	Specify the IPv4 address of the TACACS+ authentication server. You can use the **backup** parameter to specify the backup TACACS+ authentication server.
2	Raisecom#**tacacs-server key** *string*	Configure the shared key of TACACS+ authentication.
3	Raisecom#**user login**{ **local-tacacs** | **local-user** | **tacacs-local** | **tacacs-user** }	Configure login authentication of users through TACACS+.
4	Raisecom#**enable login** { **local-tacacs** | **local-user** | **tacacs-local** | **tacacs-user** }	Configure the authentication mode for users to enter privileged EXEC mode to TACACS+.

11.3.4 Configuring TACACS+ accounting

Step	Command	Description
1	Raisecom#**aaa accounting login** { **enable** | **disable** }	Enable AAA accounting.
2	Raisecom#**aaa accounting fail** { **online** | **offline** }	Configure the processing policy upon accounting failure.
3	Raisecom#**aaa accounting update** *period*	Configure the period for sends accounting update packets. If it is configured to 0, no accounting update packets will be sent.
4	Raisecom#**tacacs** [**backup**] **accounting-server** { *ip-address* | *ipv6-address* }	Configure the IP address of the TACACS+ accounting server.

11.3.5 Checking configurations

No.	Command	Description
1	Raisecom#**show tacacs-server**	Show configurations of the TACACS+ server.

11.3.6 Maintenance

No.	Command	Description
1	Raisecom#**clear tacacs statistics**	Clear TACACS+ statistics.

11.4 Configuring RADIUS

11.4.1 Preparing for configurations

Scenario

You can deploy the RADIUS server on the network to perform authentication and accounting to control users from accessing the device and network. The device can be used as an agent of the RADIUS server, which authorizes users to access according to feedback from the RADIUS server.

Prerequisite

N/A

11.4.2 Default configurations

Default configurations of RADIUS on the ISCOM5508 are as below.

Function	Default value
RADIUS accounting	Disable
IP address and UDP port number of RADIUS authentication server	• IP address: 0.0.0.0 • UDP port number: 1812
IP address and UDP port number of RADIUS accounting server	• IP address: 0.0.0.0 • UDP port number: 1813
Shared key used to communicate with the RADIUS accounting server	N/A
Processing policy upon accounting failure	online
Time for sending accounting update packets	0

11.4.3 Configuring RADIUS authentication

Step	Command	Description
1	Raisecom#**radius** [**backup**] *ip-address* [**auth-port** *port-id*]	Specify the IPv4 address and interface ID of the RADIUS authentication server. You can use the **backup** parameter to specify the backup RADIUS authentication server.
	Raisecom#**radius** [**backup**] *ipv6-address* [**scopeid** *string*] [**auth-port** *port-id*]	Specify the IPv6 address and interface ID of the RADIUS authentication server. You can use the **backup** parameter to specify the backup RADIUS authentication server.
2	Raisecom#**radius-key** *word*	Configure the shared key of RADIUS authentication.
3	Raisecom#**user login** { **radius-user** | **radius-local** } **server-no-response**	Configure the user login mode to RADIUS authentication.

11.4.4 Configuring RADIUS accounting

Step	Command	Description
1	Raisecom#**aaa accounting login enable**	Enable AAA accounting. You can use the **aaa accounting login disable** command to disable this function.
2	Raisecom#**radius** [**backup**] **accounting-server** *ip-address* [**acct-port** *port-id*]	Specify the IPv4 address and UDP port number of the RADIUS accounting server. You can use the **backup** parameter to specify the backup RADIUS accounting server.

Step	Command	Description
	Raisecom#**radius** [**backup**] **accounting-server** *ipv6-address* [**scopeid** *string*] [**acct-port** *port-id*]	Specify the IPv6 address and UDP port number of the RADIUS accounting server. You can use the **backup** parameter to specify the backup RADIUS accounting server.
3	Raisecom#**radius accounting-server key** *string*	Configure the shared key used to communicate with the RADIUS accounting server. The shared key should be consistent with that configured on the RADIUS accounting server; otherwise, accounting fails.
4	Raisecom#**aaa accounting login** { **enable** | **disable** }	Enable RADIUS accounting.
5	Raisecom#**aaa accounting fail** { **online** | **offline** }	Configure the processing policy upon accounting failure.
6	Raisecom#**aaa accounting update** *period*	Configure the period for sending accounting update packets. If it is configured to 0, no accounting update packets will be sent.

11.4.5 Checking configurations

No.	Command	Description
1	Raisecom#**show radius-server**	Show RADIUS server configurations.
2	Raisecom#**show aaa accounting**	Show RADIUS accounting server running conditions.

11.5 Configuring storm control

11.5.1 Preparing for configurations

Scenario

Configuring storm control on Layer 2 devices can prevent broadcast storm occurring when broadcast packets increase sharply on the network. Therefore, it makes sure that unicast packets can be properly forwarded.

The following forms of traffic may cause broadcast traffic, so you need to limit the bandwidth for them on Layer 2 devices.

- DLF traffic: the unicast traffic whose destination MAC address is not in the MAC address table, which is broadcasted by Layer 2 devices.
- Unknown multicast traffic: the multicast traffic whose destination MAC address is not in the MAC address table, which is broadcasted by Layer 2 devices.

- Broadcast traffic: the traffic whose destination MAC address is a broadcast MAC address, which is broadcasted by Layer 2 devices.

Prerequisite

Connect the interface, configure its physical parameters, and make it Up at the physical layer.

11.5.2 Default configurations

Default configurations of storm control on the ISCOM6820 are as below.

Function	Default value
Broadcast storm control	Enable
Multicast group storm control	Disable
DLF storm control	Disable
Rate threshold	• 1024 kbit/s for the 1000 Mbit/s interface • 4096 kbit/s for the 10 Gbit/s interface
Burst length	• 512 Kbytes for the 1000 Mbit/s interface • 2048 Kbytes for the 10 Gbit/s interface

Default configurations of storm control on Raisecom ONU devices are as below.

Function	Default value
Storm control over broadcast packets	Enable
Storm control over multicast packets	Enable
DLF storm control	Disable
Rate threshold	1000 kbit/s
Burst length threshold	4B
Packet rate threshold	1000pps

11.5.3 Configuring storm control

Configuring storm control on OLT

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface { ten-gigabitethernet | gpon-olt } slot-id/port-id`	Enter interface configuration mode.
3	`Raisecom(config-if-*-*:*)#storm-control { all | broadcast | dlf | multicast }`	Enable storm control over all traffic, broadcast traffic, multicast traffic, or DLF traffic.

Step	Command	Description
4	Raisecom(config-if-*-*:*)#**storm-control mode** { **bps** | **pps** }	Confiugre the storm control mode.
5	Raisecom(config-if-*-*:*)#**storm-control** { **broadcast** | **dlf** | **multicast** } { **bps** *rate burst* | **pps** *rate* }	Configure the storm control rate of broadcast traffic, multicast traffic, or DLF traffic.

Checking configurations

No.	Command	Description
1	Raisecom#**show interface** { **gpon-olt** | **ten-gigabitethernet** } *slot-id/port-id* **storm-control**	Show configurations of OLT storm control.

11.6 Configuring interface isolation

11.6.1 Preparing for configurations

Scenario

Interface isolation, a Layer 2 isolation mode, implements data isolation among multiple interfaces on the device by adopting isolation groups. You can isolate different physical interfaces and interfaces in the same VLAN by creating isolation groups to enhance safety of network access.

Prerequisite

N/A

11.6.2 Default configurations

Default configurations of interface isolation on the ISCOM6820 are as below.

Function	Default value
OLT Layer 2 isolation	Enable. In other words, ONUs under the same OLT PON interface are isolated from each other and cannot access each other at Layer 2.
ONU Layer 2 isolation	Enable. In other words, UNIs on the same ONU are isolated from each other.

11.6.3 Configuring OLT interface isolation

Configuring physical interface isolation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** {**gpon-olt** *slot-id/port-id* | **ten-gigabitethernet** *slot-id/port-id* | **port-channel** *group-id* }	Enter physical interface configuration mode.
3	Raisecom(config-if-*-*:*)#**isolate-group** *group-id*	Create the isolation group for physical interfaces. If a specified isolation group exists, add interfaces to the group. You can use the **no isolate-group** { *group-id* | **default** } command to delete the isolation group or interfaces from the specified isolation group.

Configuring VLAN interface isolation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** { **gpon-olt** | **ten-gigabitethernet** } *slot-id/olt-id*	Enter physical interface configuration mode.
3	Raisecom(config-if-*-*:*)#**vlan** *vlan-id* **isolate-group** *group-id* [**confirm**]	Create an isolation group in the VLAN. If a specified isolation group exists, add interfaces to the group. You can use the **no vlan** *vlan-id* **isolate-group** *group-id* command to delete the isolation group or interfaces from the specified isolation group.

11.6.4 Configuring ONU interface isolation

Configuring ONU UNI isolation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu uni ethernet** *slot-id/olt-id/onu-id/uni-id*	Enter ONU UNI configuration mode.
3	Raisecom(config-gpon-onu-ethernet-*/*:*)# **isolate-group default**	Create an isolation group of the PON interface.

11.6.5 Checking configurations

No.	Command	Description
1	Raisecom#**show isolate-group** [*group-id*]	Show configurations of physical interface isolation.
2	Raisecom#**show vlan-isolate-group vlan** *vlan-id* [*group-id*]	Show configurations of the VLAN isolation group.

11.7 Configuring attack prevention

11.7.1 Preparing for configurations

Scenario

To avoid packet attacks, you can configure attack prevention to filter extra packets.

Prerequisite

N/A

11.7.2 Default configurations

Function	Default value
Land packet attack prevention	Disable
Smurf packet attack prevention	Disable
Oversized ICMP frame attack prevention	Disable
Framelength of the unltralong ICMP frame attack prevention	512 Bytes
URPF packet attack prevention	Disable

11.7.3 Configuring packet attack prevention

No.	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**attack-defense land**	(Optional) prevent LAND attacks.
3	Raisecom(config)#**attack-defense large-icmp** [**size** *size*]	(Optional) prevent oversized ICMP packet attacks.
4	Raisecom(config)#**attack-defense smurf**	(Optional) prevent SMURF attacks.
5	Raisecom(config)#**attack-defense urpf**	(Optional) prevent URPF attacks.

11.7.4 Checking configurations

No.	Command	Description
1	Raisecom#**show attack-defense**	Show configurations of attack prevention.

11.8 Configuring anti-DoS attacks

11.8.1 Preparing for configurations

Scenario

To prevent DoS attack packets, you can configure this command to filter different protocols.

Prerequisite

N/A

11.8.2 Default configurations

N/A

11.8.3 Configuring anti-DoS attacks

No.	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**anti-dos** { **ack** | **arp** | **dhcp** | **dns** | **icmp** | **igmp** | **syn** | **udp** }	Configure the type of anti-DoS attack protocol.
3	Raisecom(config)#**anti-dos aging-time** *time*	Configure the aging time of anti-DoS attack.
4	Raisecom(config)#**anti-dos rate-limit** *rate*	Limit the rate of DoS attack packets.

11.8.4 Checking configurations

No.	Command	Description
1	Raisecom#**show anti-dos black-list**	Show configurations of anti-DoS attacks.

11.8.5 Maintenance

No.	Command	Description
1	aisecom(config)#**clear filter** *filter-number* [**rule** *rule-list*] **statistics** Raisecom(config)#**clear filter** *filter-list* **statistics**	Clear ACL filter statistics.
2	Raisecom(config)#**clear tacacs statistics**	Clear TACACS+ statistical data.

11.9 Configuring URPF

11.9.1 Preparing for configurations

Scenario

To prevent source address spoofing attacks, you can enable URPF. After it is enabled, it checks the validity of the source address. If the check passes, the device will search for the entry for the destination IP address, and the process for forwarding the packet will start; otherwise, the packet will be discarded.

Prerequisite

N/A

11.9.2 Configuring URPF

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface vlanif** *vlan-id*	Enter VLAN interface configuration mode.
3	Raisecom(config-vlanif-*)#**ip urpf** { **loose** | **strict** } [**allow-default-route**]	Configure the URPF mode.
4	Raisecom(config-vlanif-*)#**ipv6 urpf** { **loose** | **strict** } [**allow-default-route**]	Configure the IPv6 URPF mode.

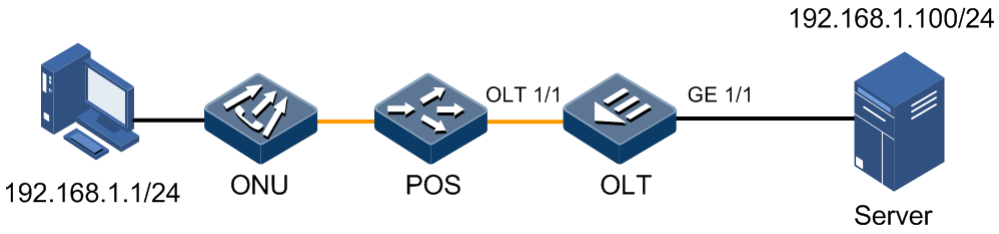
11.10 Configuration examples

11.10.1 Example for configuring ACL

Networking requirements

As shown in Figure 11-1, to control users' access to the server, you can configure ACL forbidding 192.168.1.1 to access the server 192.168.1.100.

Figure 11-1 ACL networking



Configuration steps

Step 1 Configure IP ACL.

```
Raisecom#config
Raisecom(config)#ip-access-list 1001
Raisecom(config-ip-acl-1001)#rule 1
Raisecom(config-ip-acl-1001-rule-1)#access-type deny
Raisecom(config-ip-acl-1001-rule-1)#match ip destination-address
192.168.1.100 255.255.255.0
Raisecom(config-ip-acl-1001-rule-1)#match ip source-address 192.168.1.1
255.255.255.0
Raisecom(config-ip-acl-1001-rule-1)#exit
Raisecom(config-ip-acl-1001)#rule 2
Raisecom(config-ip-acl-1001-rule-2)#access-type permit
Raisecom(config-ip-acl-1001-rule-2)#match ip destination-address 0.0.0.0
255.255.255.255
Raisecom(config-ip-acl-1001-rule-2)#match ip source-address 0.0.0.0
255.255.255.255
```

Step 2 Apply ACL on the interface OLT 1/1.

```
Raisecom(config)#filter ip-access-list 1001 ingress interface gpon-olt
3/1
```

Checking results

Use the **show ip-access-list** to show IP ACL configurations.

```
Raisecom#show ip-access-list 1001
 description ACL-1001
 rule 1
  match ip source-address 255.255.255.0 255.255.255.0
    match ip destination-address 255.255.255.0 255.255.255.0
  access-type deny

 rule 2
  match ip source-address 255.255.255.255
```

```
  match ip destination-address 255.255.255.255
access-type permit
```

Use the **show filter** command to show filter configurations.

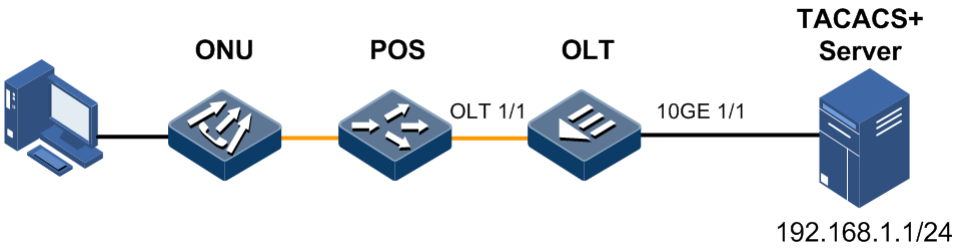
```
Raisecom#show filter
Filter ID : 1001
ACL ID    : 1
Hardware   : Yes
Egress Port  : epon-olt 3/1
Ingress Port : epon-olt 3/1
Statistics  : Disable
```

11.10.2 Example for configuring TACACS+

Networking requirements

As shown in Figure 13-3, to control user access to the device, you need to deploy the TACACS+ authentication feature on the OLT to authenticate users logging in to the OLT.

Figure 11-2 TACACS+ application networking



Configuration steps

Step 1 Configure TACACS+ authentication for login users.

```
Raisecom#tacacs-server 192.168.1.1
Raisecom#tacacs-server key raisecom
Raisecom#user login tacacs-user
```

Checking results

Use the **show tacacs-server** command to check whether TACACS+ configurations are correct.

```
Raisecom#show tacacs-server
Server Address:        192.168.1.1
Backup server Address:     0.0.0.0
```

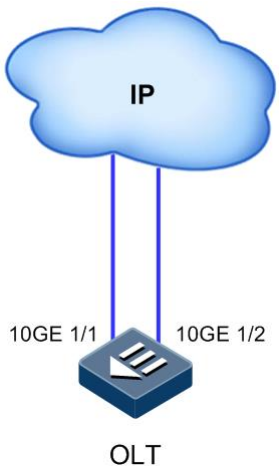
```
Sever Shared Key:        raisecom
Total Packet Sent:       0
Total Packet Recv:       0
Num of Error Packets:      0
Accounting server Address:   0.0.0.0
Backup Accounting server Address: 0.0.0.0
```

11.10.3 Example for configuring strom control

Networking requirements

As shown in Figure 11-3, to limit effects on the OLT by broadcast storm, you need to deploy storm control on the OLT to limit broadcast and unknown unicast packets. The threshold is 2000 kbit/s and the burst size value is 1024 Kbytes.

Figure 11-3 Storm control networking



Configuration steps

Configure storm control on the OLT.

```
Raisecom#config
Raisecom(config)#interface ten-gigabitethernet 1/1
Raisecom(config-if-ten-gigabitethernet-1:1)#storm-control broadcast bps
2000 1024
Raisecom(config-if-ten-gigabitethernet-1:1)#storm-control dlf bps 2000
1024
Raisecom(config-if-ten-gigabitethernet-1:1)#exit
Raisecom(config)#interface ten-gigabitethernet 1/2
Raisecom(config-if-ten-gigabitethernet-1:2)#storm-control broadcast bps
2000 1024
Raisecom(config-if-ten-gigabitethernet-1:2)#storm-control dlf bps 2000
1024
```

Checking results

Use the **show interface storm-control** to show storm control configurations.

```
Raisecom#show interface ten-gigabitethernet 1/1 storm-control
Port: ten-gigabitethernet1/1
Pkt Type      Admin        Threshold       Burst
---------------------------------------------------------------
Broadcast     enable       2000(2046)KB/s   1024KB
Multicast     disable      4096(4224)KB/s   2048KB
DLF_Unicast   disable      2000(2046)KB/s   1024KB
```

12 Configuring link security

This chapter describes the link security feature and configuration process of the ISCOM6820, and provides related configuration examples, including the following sections:

- Introduction
- Configuring xGPON interface protection (TypeB)
- Configuring link aggregation
- Configuring loop detection
- Configuring interface backup
- Configuring HA hot backup
- Configuration examples

12.1 Introduction

12.1.1 GPON interface link protection

The ISCOM6820 supports Type B PON interface protection and cross-OLT PON interface dual-homed Type B protection. The main protection forms are as below:

- OLT backbone fiber protection (Type B): redundancy of the backbone fiber and OLT PON interface.
- Cross-OLT PON interface dual-homed Type B protection: it is an extension of standard Type B protection. It provides redundancy of the backbone fiber, OLT, PON interface, and uplink interface.

OLT backbone fiber protection (Type B)

OLT backbone fiber protection (Type B) refers to the redundancy protection of the backbone fiber and OLT PON interface. The two PON interfaces on the OLT use independent PON MAC chips and optical modules for protection.

Type B protection is applicable to the protection of PON interfaces on the same OLT. The requirements are as below:

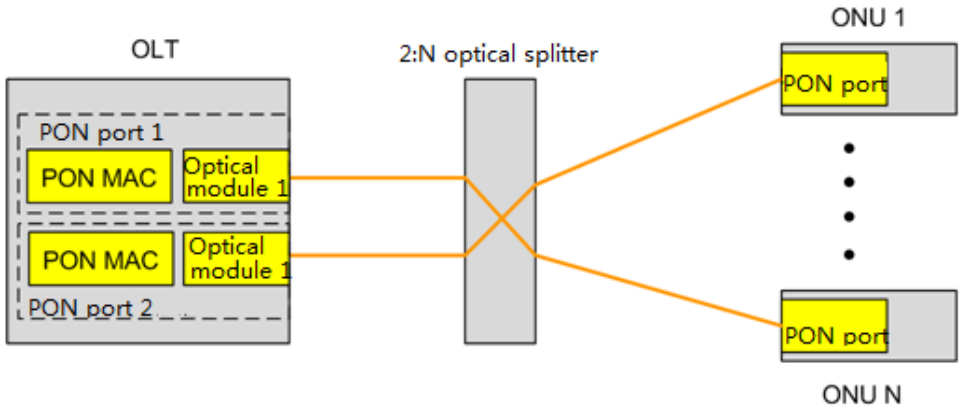
- OLT: the standby OLT PON interface is in cold backup status. The OLT detects the link status and the PON interface status, and the switching is implemented by the OLT. The OLT should ensure that the service information of the primary PON interface can be

backed up to the backup PON interface synchronously, so that the backup PON interface can maintain the ONU service attributes unchanged during the protection process.

- Optical splitter: use a 2:N optical splitter.
- ONU: no special requirements.

Figure 12-1 shows the principle of OLT backbone fiber protection (Type B).

Figure 12-1 Principle of OLT backbone fiber protection (Type B)



Cross-OLT PON interface dual-homed protection (Type B)

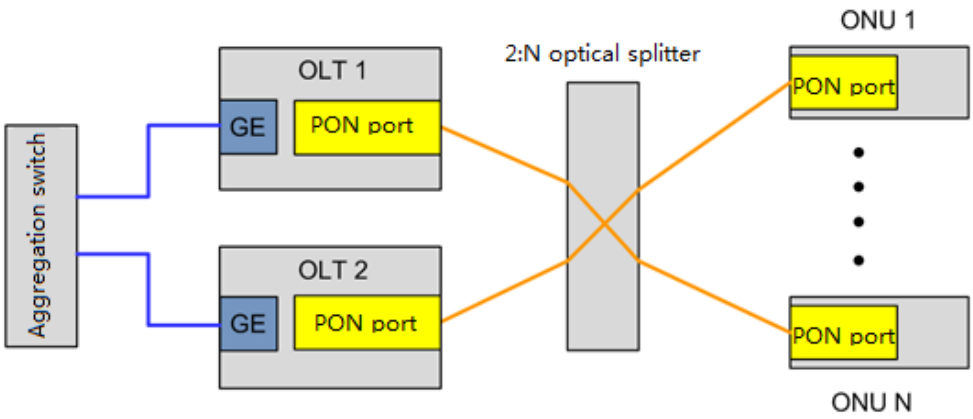
Cross-OLT PON interface dual-homed protection (Type B) is an extension of the standard Type B protection, providing redundancy protection for the backbone fiber, OLT, PON interface, and uplink interface.

Cross-OLT PON interface dual-homed protection (Type B) is applicable to protection between PON interfaces on different OLTs. The requirements are as below:

- OLT: the standby OLT optical module is in cold backup status. The OLT will detect the link status and PON interface status and implement switching.
- Optical splitter: use a 2:N optical splitter.
- ONU: no special requirements.

Figure 12-2 shows principle of cross-OLT PON interface dual-homed protection (Type B).

Figure 12-2 Principle of cross-OLT PON interface dual-homed protection (Type B)



12.1.2 Link aggregation

With link aggregation, multiple physical Ethernet interfaces are combined to form a logical Link Aggregation Group (LAG). Multiple physical links in one LAG are taken as a logical link. Link aggregation helps share loads among members in a LAG. Link aggregation can not only implement load balancing among member interfaces but also improve link reliability and bandwidth.

Manual link aggregation refers to a process that multiple physical interfaces are aggregated to a logical interface. Links under a logical interface share loads. In this mode, the status of link aggregation interfaces is not easy to be observed.

12.1.3 Loop detection

Loop detection can address the influence on network caused by a loop, providing the self-detection, fault-tolerance, and robustness.

The device processes loops as below:

Step 1 Each interface on the device periodically (configurable, being 4s by default) sends the Loopback-detection packet.

Step 2 The device checks the source MAC address of the loop detection packet. If the source MAC address is the MAC address of the device, this indicates that a loop occurs on some interface on the device.

- If the sending interface ID of the packet is the same as the receiving interface ID, shut down the interface.
- If the sending interface ID of the packet is different from the receiving interface ID, shut down the interface with the greater ID, and keep the interface with the smaller ID as available.

12.1.4 Interface backup

Interface backup is another solution for STP. You can manually configure interface backup when STP is disabled to achieve basic link redundancy.

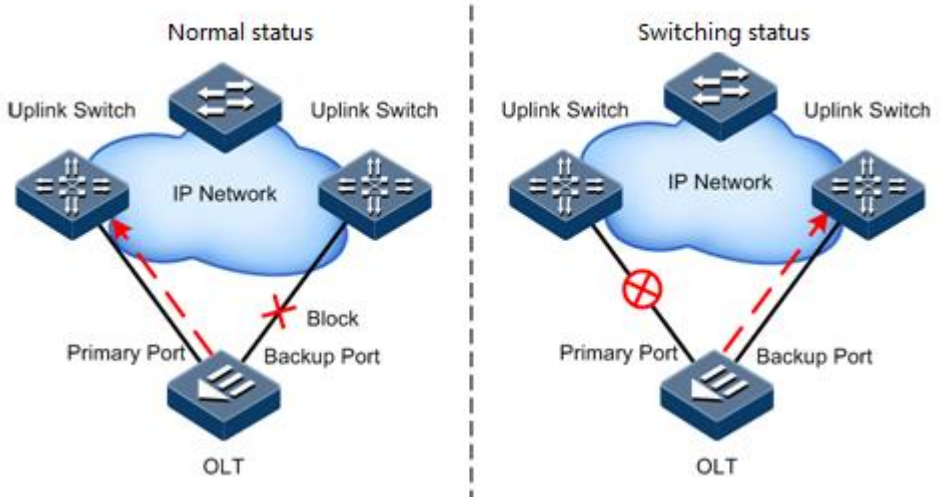
Interface-based interface backup

Interface backup relies on an interface backup group. An interface backup group consists of a pair of interfaces, including a primary interface and a backup interface. Its function is realized as below:

- When the device is in the normal forwarding state, all services will be forwarded from the primary interface.
- When the link of the primary interface fails, the device automatically switches services to the backup interface for forwarding.

Figure 12-3 shows the principle of interface backup.

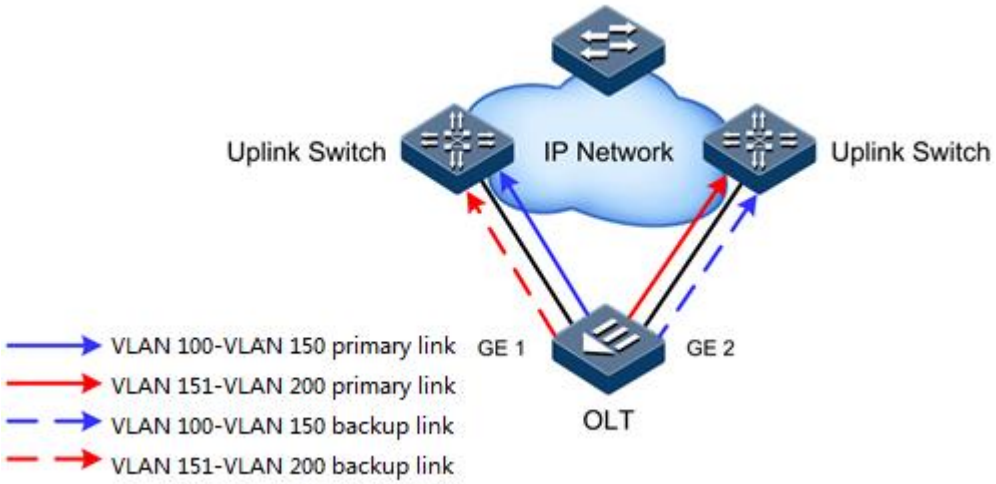
Figure 12-3 Principle of interface backup



VLAN-based interface backup

Interface backup can be applied to a VLAN, and two interfaces can simultaneously forward services in different VLANs. As shown in Figure 12-4, VLAN-based interface backup is implemented by creating a VLAN and adding interfaces to the VLAN.

Figure 12-4 VLAN-based interface backup



In different VLANs, the forwarding status of interfaces is as below:

Under normal circumstances, configure the OLT to VLAN 100–VLAN 150. GE1 is the primary interface and GE2 is the backup interface. In VLAN 151–VLAN 200, GE2 is the primary interface and GE1 is the backup interface. Then GE1 forwards traffic in VLANs 1–150, and GE2 forwards traffic in VLANs 150–200.

- When a link fault occurs on GE 1, GE 2 is responsible for forwarding traffic to VLANs 100–200.
- After GE 1 is restored to normal state for a period of time (recovery delay), GE 1 forwards traffic in VLANs 100–150, and GE 2 forwards traffic in VLANs 151–200.

With this approach, VLAN-based interface can be used for load balancing. At the same time, this application does not depend on the configuration of the uplink device, which is convenient for the user to operate.

12.2 Configuring xGPON interface protection (TypeB)

12.2.1 Preparing for configurations

Scenario

OLT GPON Type B interface protection is applicable to the following scenarios:

- Protection between PON interfaces on the same PON card of the OLT
- Protection. Between PON interfaces on different PON cards of the OLT

Prerequisite

When configuring Type B protection, ensure that:

- There is no online ONU on the primary PON link.
- There is no created ONU on the backup link.

Type B protection can be configured and shown with its parameters on the primary link only, instead of the backup link.

12.2.2 Default configurations

N/A

12.2.3 Configuring OLT GPON interface protection (Type B)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**protect-group-gpon** *id* **primary** *slot-id/olt-id* [**on-peer** *ip-address*] **secondary** *slot-id/olt-id* [**on-peer** *ip-address*] **type backbone** [**peer-description** *description*]	Configure the OLT GPON interface protection group. You can use the **no protect-group-gpon** *id* command to delete the protection group.
3	Raisecom(config)#**protect-group-gpon** *id* **enable**	Enable the GPON protection group. You can use the **disable** form of this command to disable this function.
4	Raisecom(config)#**protect-group-gpon** *id* **auto-recover-time** *time*	(Optional) configure the interval for the GPON interface protection group to switch services to the primary link. You can use the **no protect-group-gpon** *id* **auto-recover-time** command to restore to the default condition.
5	Raisecom(config)#**protect-group-gpon** *id* **forced-switch**	(Optional) forcibly switch the working link of the GPON protection group.
6	Raisecom(config)#**protect-group-gpon** *id* **lock** { **primary** | **secondary** }	(Optional) lock the working link of the GPON protection group. You can use the **no protect-group-gpon** *id* **lock** command to restore to the default condition.
7	Raisecom(config)#**protect-group-gpon** *id* **pending-switch-time** *time*	(Optional) configure the interval for the GPON protection group to switch in the pending status. You can use the **no protect-group-gpon** *id* **pending-switch-time** command to restore to delete the configuration.

12.2.4 Checking configurations

Step	Command	Description
1	Raisecom#**show protect-group-gpon** [*id*]	Show configurations of the GPON protection group.

12.3 Configuring link aggregation

Scenario

When you need to provide higher bandwidth and more reliable services for a link between two devices, you can configure link aggregation.

With link aggregation, multiple physical Ethernet interfaces are added to a LAG and are aggregated to a logical link. Link aggregation helps sharing uplink and downlink traffic among members in the LAG. Therefore, it helps get higher bandwidth and helps members in one LAG back up data for each other, thus improving the reliability of the connection.

Prerequisite

Configure physical parameters of the interface and make it Up at the physical layer.

12.3.2 Default configurations

Default configurations of link aggregation on the ISCOM6820 are as below.

Function	Default value
LAG	N/A
Load balancing mode	sxordmac
LACP system priority	32768

12.3.3 Configuring manual link aggregation

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface port-channel` *group-id*	Create a Link Aggregation Group (LAG), and enter aggreagation group configuration mode.
3	`Raisecom(config-port-channel-*)#port-channel mode manual`	Configure manual link aggregation.
4	`Raisecom(config-port-channel-*)#port-channel loading-sharing mode { dip | sip | dmac | smac | sxordip | sxordmac }`	Configure the load balancing mode of the LAG.
5	`Raisecom(config-port-channel-*)#interface ten-gigabitethernet` *slot-id/port-list*	Add interfaces to the LAG in batch. You can use the **no interface ten-gigabitethernet** *slot-id/port-list* command to delete the interface from the LAG.
	`Raisecom(config-port-channel-*)#exit` `Raisecom(config)#interface ten-gigabitethernet` *slot-id/port-id* `Raisecom(config-if-ten-gigabitethernet-*:*)#port-channel` *group-id*	Add an interface to the LAG. You can use the **no port-channel** *group-id* command to delete the interface from the LAG.

In the same LAG, member interfaces that share loads must be identically configured to avoid improper forwarding of packets. These configurations include STP, QoS, QinQ, VLAN, interface properties, and MAC address learning.

- STP: the STP status of the interface, link attributes of the link (point to point or not point to point), interface path cost, STP priority, rate limit on sending packets, loop protection status, root guard status, and edge interface or not.
- QoS: traffic policing, traffic shaping, rate limiting, SP queue, WRR queue scheduling, WFQ queue, interface priority, and interface trust mode.
- QinQ: QinQ enabling/disabling status on the interface, added outer VLAN tag, and policies for adding outer VLAN Tags for different inner VLAN IDs.
- VLAN: the allowed VLAN, default VLAN ID, link type (Trunk, Hybrid or Access) of the interface, subnet VLAN configurations, protocol VLAN configurations, and whether VLAN packets carrying Tag.
- Interface properties: whether added to the isolation group or not, interface rate, duplex mode, and link Up/Down status.
- MAC address learning: whether enabled with the MAC address learning, whether configured with the MAC address limit on the interface, and whether continuing the forwarding mechanism when the MAC address table is full.

12.3.4 Checking configurations

Step	Command	Description
1	Raisecom#**show interface port-channel** [*group-id*]	Enter global configuration mode.

12.3.5 Configuring static LACP link aggregation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**lacp system-priority** *system-priority*	(Optional) configure the LACP system priority. You can use the **no lacp system-priority** command to restore default configuration. **Note** The higher priority end is the active end. LACP chooses active and backup interfaces according to the active end configurations. The smaller the number is, the higher the priority is. By default, the LACP system priority is 32768.The device with a smaller MAC address will be chosen as the active end if the LACP system priority is identical.
3	Raisecom(config)#**interface port-channel** *port-channel-number*	Enter LAG configuration mode.
4	Raisecom(config-port-channel-*)#**port-channel mode lacp-static**	Configure the static LACP LAG.

Step	Command	Description
5	Raisecom(config-port-channel-*)#**port-channel loading-sharing mode { dip | sip | dmac | smac | sxordip | sxordmac }**	Configure the load balancing mode of the LAG.
6	Raisecom(config-port-channel-*)#**interface ten-gigabitethernet** *slot-id/port-list*	Add interfaces to the LAG in batch. You can use the **no ten-interface gigabitethernet** *slot-id/port-list* command to delete the interface from the LAG.
	Raisecom(config-port-channel-*)#**exit** Raisecom(config)#**interface ten-gigabitethernet** *slot-id/port-list* Raisecom(config-if-ten-gigabitethernet-*-*:*)#**port-channel** *group-id*	Add an interface to the LAG. You can use the **no port-channel** *group-id* command to delete the interface from the LAG.

12.3.6 Checking configurations

Step	Command	Description
1	Raisecom#**show interface port-channel** [*group-id*]	Show configurations of the link aggregation group.
2	Raisecom#**show lacp system**	Show system LACP configurations.
3	Raisecom#**show lacp neighbor**	Show information about neighbor LACP, including tags, interface priority, device ID, Age, operation key, interface ID, and interface state machine.
4	Raisecom#**show lacp internal**	Show configurations of local LACP interface.
5	Raisecom#**show lacp statistics**	Show interface LACP statistics, including the total number of received/sent LACP packets, Marker packets, and Marker Response packets, and the number of error packets.

12.3.7 Configuring dynamic LACP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** { **gigabitethernet** | **ten-gigabitethernet** } *slot-id/port-id*	Enter physical interface configuration mode.
3	Raisecom(config-if-*-*:*)#**lacp dynamic**	Enable dynamic LACP on the physical interface.

Step	Command	Description
4	Raisecom(config-if-*-*:*)#**lacp timeout** { **fast** | **slow** }	Configure the LACP timeout mode on the interface.
5	Raisecom(config-if-*-*:*)#**lacp mode** { **active** | **passive** }	Configure the LACP mode on the interface.
6	Raisecom(config-if-*-*:*)#**lacp port-priority value**	Configure the LACP priority on the interface.

12.3.8 Checking configurations

No.	Command	Description
1	Raisecom#**show interface port-channel** [*group-id*]	Show configurations of the link aggregation group.
2	Raisecom#**show lacp system**	Show system LACP configurations.
3	Raisecom#**show lacp neighbor**	Show information about neighbor LACP, including tags, interface priority, device ID, Age, operation key, interface ID, and interface state machine.
4	Raisecom#**show lacp internal**	Show configurations of local LACP interface.
5	Raisecom#**show lacp statistics**	Show interface LACP statistics, including the total number of received/sent LACP packets, Marker packets, and Marker Response packets, and the number of error packets.

12.4 Configuring loop detection

12.4.1 Preparing for configurations

Scenario

On the network, hosts or Layer 2 devices connected downstream to all access devices may form loops. Enabling loop detection on the downlink interface of the access device can avoid network congestion formed by unlimited data traffic caused by loops on the downlink interface. Once a loop is detected, Trap will be reported or the interface will be blocked.

Prerequisite

Configure physical parameters of the interface and make the interface Up at the physical layer.

12.4.2 Default configurations

Default configurations of the OLT

Default configurations of loop detection on the ISCOM6820 are as below.

Function	Default value
Global loop detection status	Disable
Interface loop detection status	Disable
Loop detection VLAN	VLAN 1
MAC address of loop detection packets	FFFF.FFFF.FFFF
Loop detection period	4s
Loop detection recovery time	300s
Action upon receiving link detection packets on the current bridge	Discarding (send Trap and block the interface)
Action upon receiving link detection packets on other bridges	Trap-only (send Trap only without blocking the interface)

Default configurations of the ONU

Default configurations of loop detection on the ONU are as below.

Function	Default value
Interface loop detection status	Enable
Loop detection period	4s
Loop detection VLAN	N/A
Shutdown time of loop interface	infinite

12.4.3 Configuring loop detection on OLT

Note

- Loop detection and STP are exclusive, so they cannot be concurrently configured at a time.
- Loop detection cannot be enabled on both ends of the directly-connected devices simultaneously; otherwise, interfaces at both ends will be blocked.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)#**loopback-detection**	Enable global loop detection. You can use the **no loopback-detection** command to disable this function.
3	Raisecom(config)#**loopback-detection destination-address** *mac-address*	(Optional) configure the destination MAC address of the loop detection packet. You can use the **no loopback-detection destination-address** command to restore default configuration.
4	Raisecom(config)#**loopback-detection down-time** { *second* | **infinite** }	(Optional) configure the shutdown time of the loopback interface. You can use the **no loopback-detection down-time** command to restore default configuration.
5	Raisecom(config)#**loopback-detection hello-time** *second*	(Optional) configure the loop detection period. You can use the **no loopback-detection hello-time** command to restore default configuration.
6	Raisecom(config)#**loopback-detection vlan** *vlan-id*	(Optional) configure the loop detection VLAN. You can use the **no loopback-detection vlan** command to restore default configuration.
7	Raisecom(config)#**interface ten-gigabitethernet** *slot-id/port-id*	Enter physical interface configuration mode.
8	Raisecom(config-if-ten-gigabitethernet-*-*:*)#**loopback-detection**	Enable loop detection on the interface. You can use the **no loopback-detection** command to disable this function.
9	Raisecom(config-if-ten-gigabitethernet-*-*:*)#**loopback-detection** { **exloop** | **loop** } { **discarding** | **trap-only** }	Configure the action of the interface upon receiving loop detection packet.
10	Raisecom(config-if-ten-gigabitethernet-*-*:*)#**no loopback-detection discarding**	(Optional) enable the blocked interface manually.

Note

When you need to perform loop detection on the ONU under the OLT, adopt the following methods:

- Enable loop detection on the OLT PON interface when detecting the links among ONUs under different PON interfaces.
- Enable loop detection on the ONU when detecting the links among ONUs under the same PON interface.

12.4.4 Checking configurations

Checking configurations on OLT

No.	Command	Description
1	Raisecom#**show** [**interface ten-gigabitethernet** *slot-id/port-id*] **loopback-detection** [**statistics**]	Show configurations and statistics of loop detection.

12.5 Configuring interface backup

12.5.1 Preparing for configurations

Scenario

Interface backup is an alternative solution of STP. You can manually configure interface backup to implement basic link redundancy when STP is disabled.

Prerequisite

Interface backup has same functions as STP, so they cannot be concurrently configured. Before configuring interface backup, disable STP.

12.5.2 Default configurations

Default configurations of interface backup on the ISCOM6820 are as below.

Function	Default value
Interface backup group	Null
Interface recovery time	15s
Interface recovery mode	Port-up (interface connection mode)

12.5.3 Creating interface backup group

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface ten-gigabitethernet** *slot-id/port-id*	Enter 10GE interface configuration mode.
3	Raisecom(config-if-ten-gigabitethernet-1:1)#**port-backup group** *group-id* { **primary-port** | **backup-port** } Raisecom(config-if-ten-gigabitethernet-1:1)#**exit**	Configure the primary interface and backup interface of the interface protection group.

Step	Command	Description
4	Raisecom(config)#**port-backup group** *group-id* **vlanlist** *vlan-list*	(Optional) configure the VLAN list of the interface backup group. You can use the **no** form of this command to restore default configurations.
5	Raisecom(config)#**port-backup group** *group-id* **restore-delay** *time*	Configure the interface recovery delay. You can use the **no** form of this command to restore default configurations.
6	Raisecom(config)#**port-backup group** *group-id* **restore-mode** { **enable** | **disable** }	(Optional) enable interface recovery on the interface backup group.

12.5.4 (Optional) configuring force switch on interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config-port)#**port-backup group** *group-id* **force-switch**	Configure force switch on the interface.

12.5.5 Checking configurations

No.	Command	Description
1	Raisecom#**show switchport backup [** *group-list* **]**	Show configurations of interface backup.

12.6 Configuring HA hot backup

12.6.1 Introduction

High Availability (HA) includes hot backup, batch backup, and realtime backup, used to implement high reliability of the system. Devices that support HA hot backup require two cards, one as the master card working in the Master mode and the other as the backup card working in the Slave mode. Whenever the main card fails, the backup card will become active and take over the work to ensure the normal operation of the system.

12.6.2 Preparing for configurations

Scenario

Switching between the main card and backup card can implement system HA.

Prerequisite

N/A

12.6.3 Configuring HA switching

Step	Command	Description
1	Raisecom#**ha force-switch**	Configure forcible switch of the main card to the backup card.

12.6.4 Checking configurations

No.	Command	Description
1	Raisecom#**show ha**	Show configurations of HA switching.
2	Raisecom#**show ha register-module**	Show HA-supportive modules and statistics.

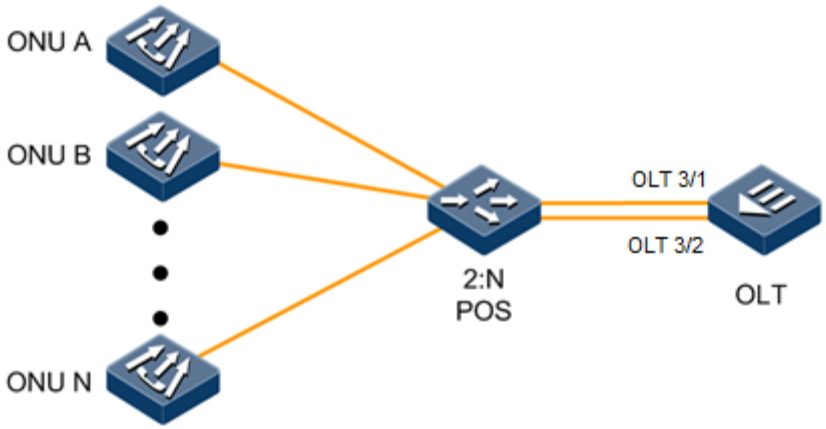
12.7 Configuration examples

12.7.1 Example for configuring GPON OLT backbone fiber protection (TypeB)

Networking requirements

As shown in Figure 12-5, to improve the reliability of the link between the OLT and the ONU, you need to configure OLT backbone fiber protection (Type B) on the OLT. Add OLT 3/1 and OLT 3/2 to the protection group, where OLT 3/1 is the primary link and OLT 3/2 is the backup link.

Figure 12-5 OLT backbone fiber protection (Type B)



Configuration steps

Step 1 Create a management VLAN, and ONU service VLAN.

```
Raisecom#config
Raisecom(config)#create vlan 20,100 active
```

Step 2 Configure the uplink interface.

```
Raisecom(config)#interface ten-gigabitethernet 1/1

Raisecom(config-if-ten-gigabitethernet-1:1)#switchport mode trunk
Raisecom(config-if-ten-gigabitethernet-1:1)#switchport trunk allowed vlan
20,100 confirm
Raisecom(config-if-ten-gigabitethernet-1:1)#quit
```

Step 3 Configure the in-band management interface.

```
Raisecom(config)#interface vlanif  20
Raisecom(config-vlanif-20)#ip address 199.0.0.22 255.255.255.0
Raisecom(config-vlanif-20)#quit
Raisecom(config)#ip route 0.0.0.0 0.0.0.0 199.0.0.1
```

Step 4 Configure the PON interface.

- Configure DBA.

```
Raisecom(config)#create dba-profile 2 name Full_Best_effort type4 max
1228800
```

- Configure the line profile.

```
Raisecom(config)#gpon-onu-line-profile 5
Raisecom(config-gpon-onu-line-profile:5)#name profile-5
Raisecom(config-gpon-onu-line-profile:5)#create tcont 1 dba-profile 2
Raisecom(config-gpon-onu-line-profile:5)#create gem 1 tcont 1
Raisecom(config-gpon-onu-line-profile:5)#gem 1 mapping 1 vlan 100
Raisecom(config-gpon-onu-line-profile:5)#quit
```

- Configure the service profile.

```
Raisecom(config)#gpon-onu-service-profile 1004
Raisecom(config-gpon-onu-service-profile:1004)#un ethernet 1-4 vlan mode
tagged
Raisecom(config-gpon-onu-service-profile:1004)#un ethernet 1-4 native
vlan 100
Raisecom(config-gpon-onu-service-profile:1004)#quit
```

- Create an ONU.

```
Raisecom(config)#interface gpon-olt 3/1
Raisecom(config-if-gpon-olt-3:1)create gpon-onu 2 sn RCMG18B0A1F1 line-
profile-id 5 service-profile-id 1004
Raisecom(config-if-gpon-olt-3:1)switchport mode trunk
Raisecom(config-if-gpon-olt-3:1)#switchport trunk allowed vlan 100
confirm
Raisecom(config-if-gpon-olt-3:1)#mac-address-table station move
Raisecom(config-if-gpon-olt-3:1)#exit
Raisecom(config)#interface gpon-olt 3/2
Raisecom(config-if-gpon-olt-3:2)#mac-address-table station move
```

Step 5 Configure inter-card PON protection.

```
Raisecom(config)#
protect-group-gpon 2 primary 3/1 secondary 3/2 type backbone
```

Step 6 Configure inter-card PON protection.

```
Raisecom(config)# protect-group-gpon 3 primary 3/3 secondary 4/3 type
backbone
```

Step 7 Configure inter-OLT PON protection.

- Configure the primary OLT.

```
Raisecom(config)#protect-group-gpon 1 primary 3/1 secondary 3/2 on-peer
199.0.0.21 type backbone peer-description hello
```

- Configure the backup OLT.

```
Raisecom(config)#protect-group-gpon 1 primary 3/1 on-peer 199.0.0.22
secondary 3/2 type backbone peer-description test
```

Checking results

Use the **show protect-group-gpon** command to check the configurations and running status of the protection group on the OLT.

On the primary OLT:

```
Raisecom(config)#show protect-group-gpon
   Group ID: 1
      Group type             : Trans-olt backbone pon protection
      Primary line           : 3/1(local)
      Primary line state      : Normal
      Secondary line         : 3/2(on-peer:199.0.0.21)
      Secondary line state    : Normal
      Group admin status      : Enabled
      Group lock status       : Unlocked
      Group working status    : Normal
      Auto-recovery time      : non-revertive
      Pend Switch time        : 30 sec
      Successful switching count: 0
      Last switching result    : Destination Port Offline
      Last switching time      : 2020-03-31,09:52:33
      Peer device description  : hello
      Handshaking status      : Normal
```

On the backup OLT:

```
Raisecom(config)#show protect-group-gpon
   Group ID: 1
      Group type             : Trans-olt backbone pon protection
```

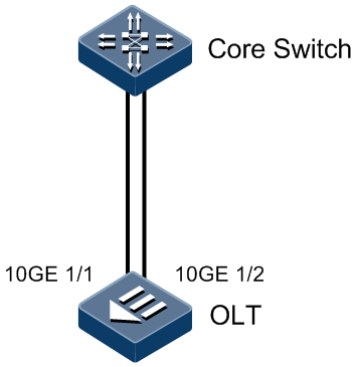
```
    Primary line           : 3/1(on-peer:199.0.0.22)
    Primary line state      : Normal
    Secondary line          : 3/2(local)
    Secondary line state     : Normal
    Group admin status      : Enabled
    Group lock status       : Unlocked
    Group working status     : Normal
    Auto-recovery time      : non-revertive
    Pend Switch time        : 30 sec
    Successful switching count: 0
    Last switching result    : Destination Port Offline
    Last switching time      : 2020-03-31,10:02:47
    Peer device description   : test
Handshaking status      : Normal
```

12.7.2 Example for configuring manual link aggregation

Networking requirements

As shown in Figure 12-6, to improve link reliability between the OLT and uplink aggregation switch, you can configure manual link aggregation on the OLT. Add 10GE 19/1 and 10GE 19/2 to the LAG to form a single logical interface. The LAG performs load balancing according to the source MAC address.

Figure 12-6 Manual link aggregation networking



Configuration steps

Step 1 Create a manual LAG and the group ID is 1.

```
Raisecom#config
Raisecom(config)#interface port-channel 1
Raisecom(config-port-channel-1)#port-channel mode manual
```

Step 2 Configure the load sharing mode for link aggregation.

```
Raisecom(config-port-channel-1)#port-channel loading-sharing mode smac
Raisecom(config-port-channel-1)#exit
```

Step 3 Add interfaces to the LAG.

```
Raisecom(config)#interface ten-gigabitethernet 1/1
Raisecom(config-if-ten-gigabitethernet-1:1)#port-channel 1
Raisecom(config-if-ten-gigabitethernet-1:1)#exit
Raisecom(config)#interface ten-gigabitethernet 1/2
Raisecom(config-if-ten-gigabitethernet-1:2)#port-channel 1
Raisecom(config-if-ten-gigabitethernet-1:2)#exit
```

Checking results

Use the **show interface port-channel** command to show global configurations of manual link aggregation.

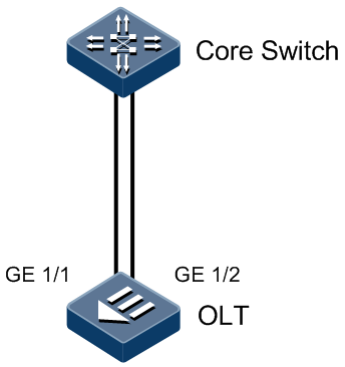
```
Raisecom#show interface port-channel 1
Port-channel ID : 1
  Mode      : Manual
  Load-sharing Mode : smac
  Member ports   : ten-gigabitethernet 1/1,2
  Efficient ports  :
```

12.7.3 Example for configuring static LACP link aggregation

Networking requirements

As shown in Figure 12-7, to improve link reliability between the OLT and uplink aggregation switch, you can configure static LACP link aggregation on the OLT. Add 10GE 19/1 and 10GE 19/2 to the LAG. 10GE 19/1 works as the primary link, and 10GE 19/2 works as the backup link.

Figure 12-7 Static LACP link aggregation networking



Configuration steps

Step 1 Create a static LACP LAG.

```
Raisecom#config
Raisecom(config)#interface port-channel 1
Raisecom(config-port-channel-1)#port-channel mode lacp-static
Raisecom(config-port-channel-1)#exit
```

Step 2 Add interfaces to the LAG.

```
Raisecom(config)#interface ten-gigabitethernet 1/1
Raisecom(config-if-ten-gigabitethernet-1:1)#port-channel 1
Raisecom(config-if-ten-gigabitethernet-1:1)#exit
Raisecom(config)#interface ten-gigabitethernet 1/2
Raisecom(config-if-ten-gigabitethernet-1:2)#port-channel 1
Raisecom(config-if-ten-gigabitethernet-1:2)#exit
```

Step 3 Configure the priority of 10GE interface 1/1 to make the 10GE 1/1 as the primary link and 10GE 1/2 as the backup link.

```
Raisecom(config)#interface ten-gigabitethernet 1/1
Raisecom(config-if-ten-gigaethgigabitethernet-1:1)#lacp port-priority
10000
Raisecom(config-if-ten-gigaethgigabitethernet-1:1)#exit
```

Checking results

Use the **show port-channel** command on the OLT to show static LACP link aggregation global configurations.

```
Raisecom#show interface port-channel
Port-channel ID : 1
  Mode      : LACP-static
  Load-sharing Mode : smac
  Member ports  : gigabitethernet 1/1,2
  Efficient ports  :
```

Use the **show lacp internal** command on the OLT to show configurations of the peer system, such as LACP interface status, flag, interface priority, management key, operation key, and status of interface state machine.

```
Raisecom#show lacp internal
Flags:
```

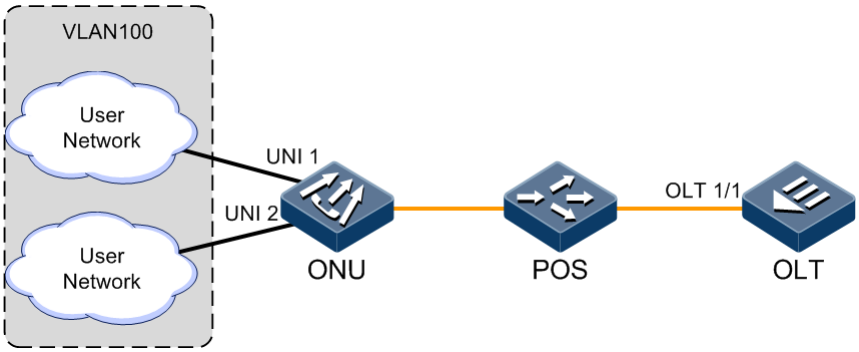
```
   S - Device is requesting Slow LACPDUs
   F - Device is requesting Fast LACPDUs
   A - Device is in Active mode
   P - Device is in Passive mode

Port  State  Flags Port-Pri  Admin-key Oper-key Port-State
--------------------------------------------------------------------
1/1  down   FA  10000   0x1    0x1    0x4d
1/2  down   FA  32768   0x1    0x1    0x4d
```

12.7.4 Example for configuring loop detection

Networking requirements

As shown in Figure 12-8, OLT 3/1 is connected to the ONU through a POS. The ONU connects the user network through UNI1 and UNI 2. You can enable loop detection on the ONU remotely on the OLT to detect loops in user VLAN 100.

Figure 12-8 Loop detection networking



Configuration steps

Step 1 Configure the VLAN which needs to be enabled with loop detection.

```
Raisecom#config
Raisecom(config)#gpon-onu 3/1/1
Raisecom(config-gpon-onu-3/1:1)#loopback-detection vlan 100
Raisecom(config-gpon-onu-3/1:1)#exit
```

Step 2 Configure the UNI which needs to be enabled with loop detection.

```
Raisecom(config)#gpon-onu uni ethernet 3/1/1/1
Raisecom(config-gpon-onu-ethernet-3/1/1:1)#loopback-detection enable
Raisecom(config-gpon-onu-ethernet-3/1/1:1)#exit
Raisecom(config)#gpon-onu uni ethernet 3/1/1/2
Raisecom(config-gpon-onu-ethernet-3/1/1:2)#loopback-detection enable
```

Checking results

Use the **show gpon-onu** *slot-id/olt-id/onu-id* **loopback-detection** command to show loop detection configurations.

```
Raisecom#show gpon-onu 3/1/1 loopback-detection
ONU ID: 3/1/1
   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
```

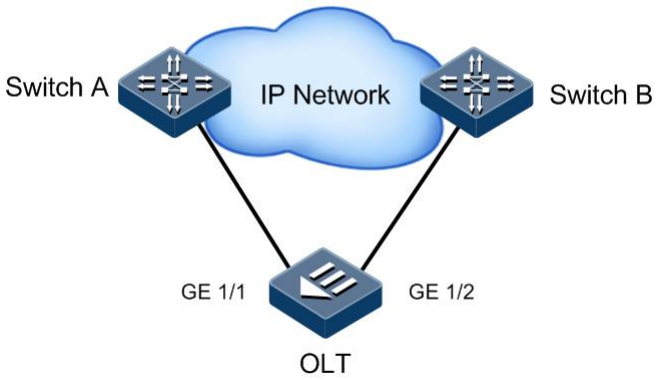
12.7.5 Example for configuring interface backup

Networking requirements

As shown in Figure 12-9, to ensure the link security of the uplink interface on the OLT, configure interface backup on it to realize link protection and load balancing. The requirements are as below:

- Create interface protection group 1, including GE interfaces 1/1 and 1/2. GE interface 1/1 is the primary interface of VLANs 100–150, and GE interface 1/2 is the backup interface of VLANs 100–150.
- Create interface protection group 2, including GE interfaces 1/1 and 1/2. GE interface 1/2 is the primary interface of VLANs 151–200, and 10GE interface 1/1 is the backup interface of VLANs 151–200.

Figure 12-9 Interface backup networking



Configuration steps

Step 1 Create interface backup groups, and configure the primary and backup interfaces.

```
Raisecom#config
Raisecom(config)#create port-backup group 1
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#port-backup group 1 primary-port
Raisecom(config-if-gigabitethernet-1:1)#exit
Raisecom(config)interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#port-backup group 1 backup-port
Raisecom(config-if-gigabitethernet-1:2)#exit
Raisecom(config)#create port-backup group 2
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#port-backup group 2 backup-port
Raisecom(config-if-gigabitethernet-1:1)#exit
Raisecom(config)interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#port-backup group 2 primary-port
Raisecom(config-if-gigabitethernet-1:2)#exit
```

Step 2 Configure the VLAN list of the interface backup group.

```
Raisecom(config)#port-backup group 1 vlanlist 100-150
Raisecom(config)#port-backup group 2 vlanlist 151-200
```

Step 3 Enable the interface backup group.

```
Raisecom(config)#port-backup group 1 enable
Raisecom(config)#port-backup group 2 enable
```

Checking results

Use the **show interface backup** command to show interface backup configurations.

```
Raisecom#show port-backup group

Portbackup Group      :1 (Enable)
Vlan List            :100-150
Primary Port         :gigabitethernet1/1
Backup Port          :gigabitethernet1/2
Primary Port STG State  :forwarding
Backup Port STG State   :discarding
Primary Port Link State :up
Backup Port Link State  :down
Switch Count         :0
Restore Mode         :Enable
Restore Delay(s)      :15

Portbackup Group      :2 (Disable)
Vlan List            :151-200
Primary Port         :gigabitethernet1/1
```

```
Backup Port           :gigabitethernet1/2
Primary Port STG State  :forwarding
Backup Port STG State   :discarding
Primary Port Link State :up
Backup Port Link State  :down
Switch Count          :0
Restore Mode          :Enable
Restore
```

13 Configuring system management

This chapter describes the basic principle and configuration process of the system management and maintenance feature of the ISCOM6820, and provides related configuration examples, including the following sections:

- Introduction
- Configuring SNMP
- Configuring optical module DDM
- Configuring PPPoE Agent
- Configuring system log
- Configuring port mirroring
- Configuring link detection
- Configuring system monitoring
- Configuring KeepAlive
- Configuring alarm and event management
- Configuring Illegal ONU alarms
- Configuring mOLT remote management
- Configuration examples

13.1 Introduction

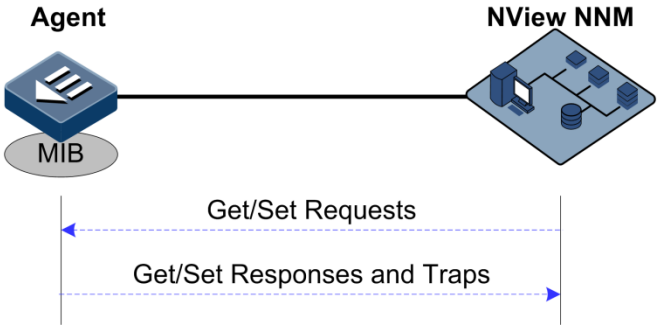
13.1.1 SNMP

Simple Network Management Protocol (SNMP) is designed by the Internet Engineering Task Force (IETF) to solve problems in managing network devices connected to the Internet. Through SNMP, a network management system can manage all network devices that support SNMP, including monitoring network status, modifying configurations of a network device, and receiving network alarms. SNMP is the most widely used network management protocol in TCP/IP networks.

Working mechanism

SNMP is divided into two parts: Agent and NMS. The Agent and NMS communicate by SNMP packets sent through UDP. The working mechanism of SNMP is shown in Figure 13-1.

Figure 13-1 Working mechanism of SNMP



Raisecom Nview NNM system can provide friendly Human Machine Interface (HMI) to facilitate network management. The below functions can be implemented through it:

- Send request packets to the managed device.
- Receive reply packets and Trap packets from the managed device, and show results.

Agent is a program stayed in the managed device, realizing the below functions:

- Receive/Reply request packets from Nview NNM system.
- Read/Write packets and generate response packets according to the packet types, and then return the results to Nview NNM system.
- Define triggering conditions according to protocol module. Enter/Exit system or restart device when conditions are satisfied. The response module sends Trap packets to Nview NNM system through agent to report current status of the device.

Note

Agent can be configured with several versions. Agent use different versions to communicate with different Nview NNM systems. However, SNMP version of the Nview NNM system must be consistent with the one on Agent when they are communicating. Otherwise, they cannot communicate properly.

Protocol versions

At present, SNMP has three versions: v1, v2c, and v3, described as below.

- SNMPv1 uses community name authentication mechanism. The community name, a string defined by an agent, acts like a password. The network management system can visit the agent only by specifying its community name correctly. If the community name carried in a SNMP message is not accepted by the device, the message will be dropped.
- Compatible with SNMPv1, SNMPv2c also uses community name authentication mechanism. SNMPv2c supports more operation types, data types, and error codes, and thus better identifying errors.
- SNMPv3 uses User-based Security Model (USM) authentication mechanism. You can configure whether USM authentication is enabled and whether encryption is enabled to provide higher security. USM authentication mechanism allows authenticated senders

and prevents unauthenticated senders. Encryption is to encrypt messages transmitted between the network management system and agents, thus preventing interception.

MIB

Management Information Base (MIB) is the collection of all objects managed by NMS. It defines attributes for the managed objects:

- Name
- Access authority
- Data type

The device-related statistic contents can be reached by accessing data items. Each proxy has its own MIB. MIB can be taken as an interface between NMS and Agent, through which NMS can read/write every managed object in Agent to manage and monitor the device.

MIB stores information in a tree structure. Its root is on the top without a name. Nodes of the tree are the managed objects, which take a unique path starting from root (OID) for identification. SNMP packets can access network devices by checking the nodes in MIB tree directory.

13.1.2 Optical module DDM

Small Form-factor Pluggables (SFP) is an optical module in optical module transceivers. The SFP Digital Diagnostic Monitoring (DDM) provides a method for monitoring performance. By analyzing monitored data provided by the SFP module, the administrator can predict the lifetime of the SFP module, isolate system faults, and verify the compatibility of the SFP module.

The SFP module provides 5 performance parameters:

- Temperature of the transceiver
- Internal Power Feeding Voltage (PFV)
- Tx bias current
- Tx optical power
- Rx optical power

13.1.3 System log

The system log refers to that the device records the system information and debugging information in a log and sends the log to the specified destination. When the device fails to work, you can check and locate the fault easily.

The system information and debugging output will be sent to the system log to be processed. According to the configuration, the system will send the log to various destinations. The destinations that receive the system log are divided into:

- Console: send the log message to the local console through Console interface.
- Host: send the log message to the host.
- Monitor: send the log message to the monitor, such as Telnet terminal.
- Buffer: send the log message to the buffer of the device.
- File: send the log message to a file.

The system log is usually in the following format:

```
timestamp module-level- Message content
```

The following is an example of system log:

```
FEB-22-2013 14:27:33 CONFIG-7-CONFIG:USER "raisecom" Run "logging on"
FEB-22-2013 06:46:20 CONFIG-6-LINK_D:port 2 Link Down
FEB-22-2013 06:45:56 CONFIG-6-LINK_U:port 2 Link UP
```

The format of system log output to the host is as below:

```
timestamp module-level- Message content
```

The following figure is an example of system log sent to the host.

```
07-01-201311:31:28Local0.Debug20.0.0.6JAN 01 10:22:15 ISCOM6820: CONFIG-
7-CONFIG:USER " raisecom " Run " logging on "
07-01-200811:27:41Local0.Debug20.0.0.6JAN 01 10:18:30 ISCOM6820: CONFIG-
7-CONFIG:USER " raisecom " Run " ip address 20.0.0.6 255.0.0.0 1 "
```

The system log is divided into eight levels by severity, as listed in Table 13-1.

Table 13-1 Log levels

Severity	Level	Description
Emergencies	0	The system cannot be used.
Alerts	1	Immediate processing is required.
Critical	2	Serious status
Errors	3	Errored status
Warnings	4	Warning status
Notifications	5	Normal but important status
Informational	6	Informational event
Debugging	7	Debugging information

Note

The severity of output information can be configured manually. When you send information according to the configured severity, you can just send the information whose severity is less than or equal to that of the configured information. For

example, when the information is configured with level 3 (or the severity is errors), the information whose level ranges from 0 to 3, that is, the severity ranging from emergencies to errors, can be sent.

Classification of alarms

There are 3 kinds of alarms according to properties of an alarm:

- Fault alarm: alarms generated because of hardware failure or anomaly of important functions, such as interface Down alarm
- Recovery alarm: alarms generated when device failure or abnormal function returns to normal, such as interface Up alarm;
- Event alarm: prompted alarms or alarms that are generated because the fault alarm and recovery alarm cannot be related, such as alarms generated because of failing to Ping.

Alarms are divided into 5 types according to functions:

- Communication alarm: alarms related to the processing of information transmission, including alarms generated because of communication failure between Network Elements (NEs), NEs and NMS, or NMS and NMS
- Service quality alarm: alarms caused by service quality degradation, including congestion, performance decline, high resource utilization rate, and the bandwidth reducing
- Processing error alarm: alarms caused by software or processing errors, including software errors, memory overflow, version mismatching, and abnormal program aborts
- Environmental alarm: alarms caused by equipment location-related problems, including the temperature, humidity, ventilation. and other abnormal working conditions
- Device alarm: alarms caused by failure of physical resources, including the power supply, fan, processor, clock, input/output interface, and other hardware.

Alarm output

There are 3 alarm output modes:

- Alarm buffer: alarms are recorded in tabular form, including the current alarm table and history alarm table.
  - Current alarm table: records alarms which are not cleared, acknowledged or restored.
  - History alarm table: consists of acknowledged and restored alarms, recording the cleared, auto-restored, or manually acknowledged alarms.
- Log: alarms are generated to system log when recorded in the alarm buffer, and stored in the alarm log buffer.
- Trap: alarms sent to the Nview NNM system when the Nview NNM system is configured

Alarms will be broadcasted according to various terminals configured on the ISCOM6820, including CLI terminal and Nview NNM system.

Log output of alarms starts with the symbol "#", and the output format is:

```
#Index TimeStamp HostName ModuleName/Severity/name:Arise From Description
```

Table 13-2 lists alarm fields.

Table 13-2 Alarm fields

Field	Description
Index	Alarm index
TimeStamp	Time when an alarm is generated
ModuleName	Name of a module that generates an alarm
Severity	Alarm level
Name	Alarm name
Arise From Description	Descriptions about an alarm

Alarm levels

The alarm level is used to identify the severity degree of an alarm. The level is defined in Table 13-3.

Table 13-3 Alarm levels

Level	Description	Syslog
Critical (3)	This alarm has affected system services and requires immediate troubleshooting. Restore the device or source immediately if they are completely unavailable, even it is not during working time.	1 (Alert)
Major (4)	This alarm has affected the service quality and requires immediate troubleshooting. Restore the device or source service quality if they decline; or take measures immediately during working hours to restore all performances.	2 (Critical)
Minor (5)	This alarm has not influenced the existing service yet, which needs further observation and take measures at appropriate time so as to avoid more serious fault.	3 (Error)
Warning (6)	This alarm will not affect the current service, but maybe the potential error will affect the service, so it can be considered as needing to take measures.	4 (Warning)
Indeterminate (2)	Uncertain alarm level, usually the event alarm.	5 (Notice)
Cleared (1)	This alarm shows to clear one or more reported alarms.	5 (Notice)

13.1.4 PPPoE Agent

PPPoE Agent is used to process the Point to Point Protocol Over Ethernet (PPPoE) authentication packets, that is, to add more information about access devices to the PPPoE packet, so that the server can obtain sufficient information to identify users. PPPoE Agent can effectively prevent account sharing or account theft in the PPPoE authentication process, ensuring network security.

You can select the PPPoE dial-up mode to connect to the network. You can use this account to access the network through different interfaces of the device as long as you are successfully authenticated by the same authentication server. However, it is difficult for the server to distinguish the user based only on the authentication information including the username and password. After PPPoE agent is added, the authentication packet will carry information such as the device interface in addition to the user name and password. If the information such as the interface ID recognized by the authentication server is inconsistent with the configuration, the authentication fails. This prevents unauthorized users from stealing the accounts of other legitimate users.

The PPPoE protocol adopts the client/server mode, and the OLT acts as a relay agent. The user connects to the network through PPPoE authentication. If the server needs to locate the user, more user information is needed in the authentication packet.

Users need to go through two phases to access the network through PPPoE. The first phase is the discovery phase, namely, the authentication phase. The second phase is the session phase. PPPoE+ processes the packets in the discovery phase.

- The client accesses the network through PPPoE and then sends a broadcast PPPE Active Discovery Initiation (PADI) packet, which is used to find the authentication server.
- The authentication server that receives the PADI packet sends a unicast PPPoE Active Discovery Offer (PADO) packet to respond.
- If there are multiple authentication servers that send PADO packets, the client selects one of them and sends a unicast PADR (PPPoE Active Discovery Request) packet to request authentication.
- After receiving the PADR packet, if considering that the user is legitimate, the authentication server sends a unicast PPPoE Active Discovery Session-Confirmation (PADS) packet to respond to the PADR packet. At this point, the discovery phase is complete.
- The main function of the PPPoE Agent is to add user identification information to PADI and PADR packets. The server can determine whether the identifier information matches the user account and decide whether to allocate resources.

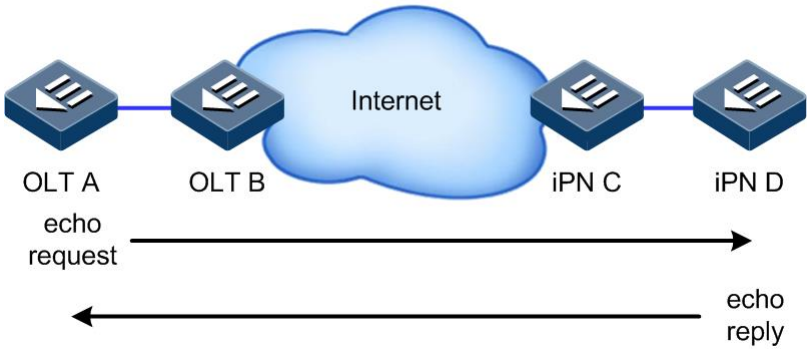
13.1.5 Ping

Ping derives from the sonar location operation, which is used to detect whether the network is normally connected.

Ping is achieved with ICMP echo packets. If an Echo Reply packet is sent back to the source address during a valid period after the Echo Request packet is sent to the destination address, it indicates that the route between source and destination address is reachable. If no Echo Reply packet is received during a valid period and timeout information is displayed on the sender, it indicates that the route between source and destination addresses is unreachable.

Figure 13-2 shows the working principle of Ping

Figure 13-2 Working principle of Ping



13.1.6 KeepAlive

The KeepAlive message is an active mechanism running in link layer protocols, such as High Level Data Link Control (HDLC). Generally, the device will send a KeepAlive message every few seconds to confirm whether the other party is online, implementing a neighbor detection mechanism.

A Trap is an unsolicited message sent by a device to the NMS, used to report some urgent and important events.

The device actively sends KeepAlive Trap messages containing OLT basic information (including the device name, device OID, MAC address, and IP address). The NMS synchronizes device information based on the IP address, thus discovering network elements in a short period, and improving the efficiency of network management, and reducing the workload of network management personnel.

13.1.7 Traceroute

Just as Ping, Traceroute is a commonly-used maintenance method in network management. Traceroute is often used to test the network nodes of packets from sender to destination, detect whether the network connection is reachable, and analyze network fault.

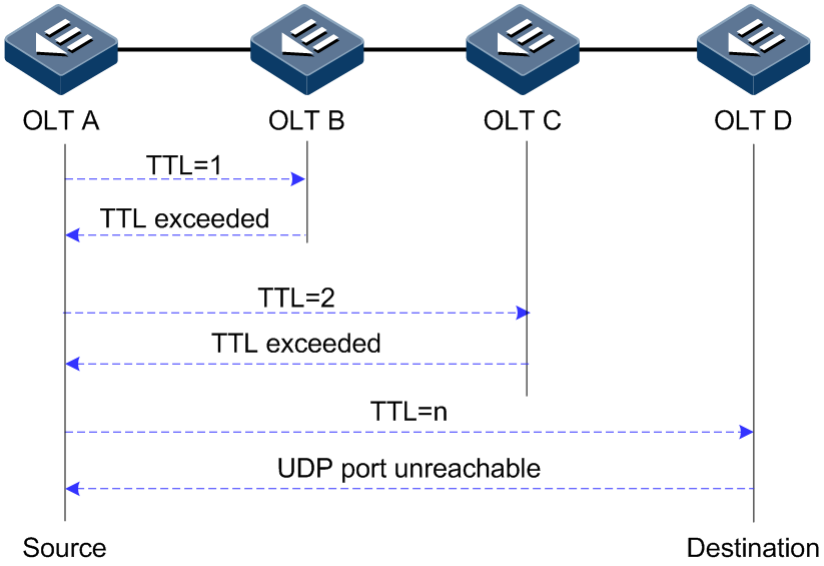
The following shows how Traceroute works:

- First, send a TTL=1 sniffer packet (where the UDP port ID of the packet is unavailable to any application programs in destination side).
- TTL deducts 1 when reaching the first hop. Because the TTL value is 0, in the first hop the device returns an ICMP timeout packet, indicating that this packet cannot be sent.
- The sending host adds 1 to TTL and resends this packet.
- Because the TTL value is reduced to 0 in the second hop, the device will return an ICMP timeout packet, indicating that this packet cannot be sent.

The above steps continue until the packet reaches the destination host which will not return ICMP timeout packets. Because the port ID of the destination host is not used, the destination host will send a port unreachable packet and finish the test. Thus, the sending host can record the source address of each ICMP TTL timeout packet and analyze the path to the destination according to the response packet.

Figure 13-3 shows the working principle of Traceroute.

Figure 13-3 Working principle of Traceroute



13.1.8 Alarm and event management

Alarm and event management refers to recording, configuring, and checking alarms and events. Through alarm and event management, you can maintain the device to ensure that it can work properly and efficiently.

Note

The difference between alarms and events is: alarms have two statuses, one is generation status and the other is elimination status; however, events only have the generation status.

Alarm and event management mainly include the following operations:

- Alarm delay: to prevent frequent occurrence of alarm report and alarm recovery report, you need to enable alarm delay. After alarm delay is enabled, alarms generated in the system are reported to the NMS after a delay rather than immediately. If the alarm recovers in the delay, it will not be reported to the NMS. The alarm is recorded in the history alarm table instead of the current alarm table. In the history alarm table, the alarm is identified as the alarm failing to be reported to the NMS due to alarm delay by the flag bit.
- Alarm filtering: you can perform alarm filtering on a specified alarm source or alarm ID. Alarms in filtering status are recorded in the current alarm table instead of being reported to the NMS. In the current alarm table, the alarm is identified as the alarm failing to be reported to the NMS due to alarm filtering by the flag bit. Alarm filtering will not stop until you disable it manually.
- Alarm masking: it is divided into general alarm masking and timed alarm masking.
  - General alarm masking: you perform general alarm masking on a specified alarm source or alarm ID, that is, NALM. The alarm in NALM status is not recorded in the current/history alarm table, and is not reported to the NMS. Alarm masking will not stop until you disable it manually.
  - Timed alarm masking: you perform timed alarm masking on a specified alarm source or alarm ID, that is, NALM-TI. The alarm in NALM-T1 status is not recorded in the

current/history alarm table, and is not reported to the NMS. Timed alarm masking will be disabled in a specified interval and it supports periodical alarm masking.

- Event masking: you perform event masking on a specified event source or event ID. The event in masking status is neither reported to the NMS nor recorded in the history event table. Event masking will not stop until you disable it manually.

13.2 Configuring SNMP

13.2.1 Default configurations

Default configurations of SNMP on the ISCOM6820 are as below.

Function	Default value			
SNMP view	By default, system, internet, and iso			
SNMP community	By default, public and private			
	Index	CommunityName	ViewName	Permission
	1	public	internet	ro
	2	private	internet	rw
SNMP access group	By default, initialnone and initial			
SNMP user	By default, none, md5nopriv, and shanopriv			
Mapping between SNMP user and access group	Index	UserName	SecModel	GroupName
	0	none	usm	initialnone
	1	md5nopriv	usm	initial
	2	shanopriv	usm	initial
Identification and contact of administrators	support@Raisecom.com			
Device location	world china raisecom			
Trap status	enable			
IP address of SNMP target host	N/A			
Interval to send KeepAlive Trap from the device to the SNMP NMS	300s			

13.2.2 Configuring basic functions of SNMPv1/v2c

To protect itself and prevent its MIB from unauthorized access, the SNMP Agent proposes the concept of community. The management station in the same community must use the community name in all Agent operations; otherwise, the request will not be accepted.

The community name refers to using different SNMP strings to identify different SNMP groups. Different communities 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 querying the device information.

SNMPv1/v2c uses the community name authentication scheme. SNMP packets which are inconsistent with the community name will be discarded.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server view** *view-name oid-tree* [**mask**] { **included** | **excluded** }	(Optional) create the SNMP view and configure the MIB variable range.
3	Raisecom(config)#**snmp-server community** *com-name* [**view** *view-name*] { **ro** | **rw** }	Create the community name and configure the corresponding view and access privilege.

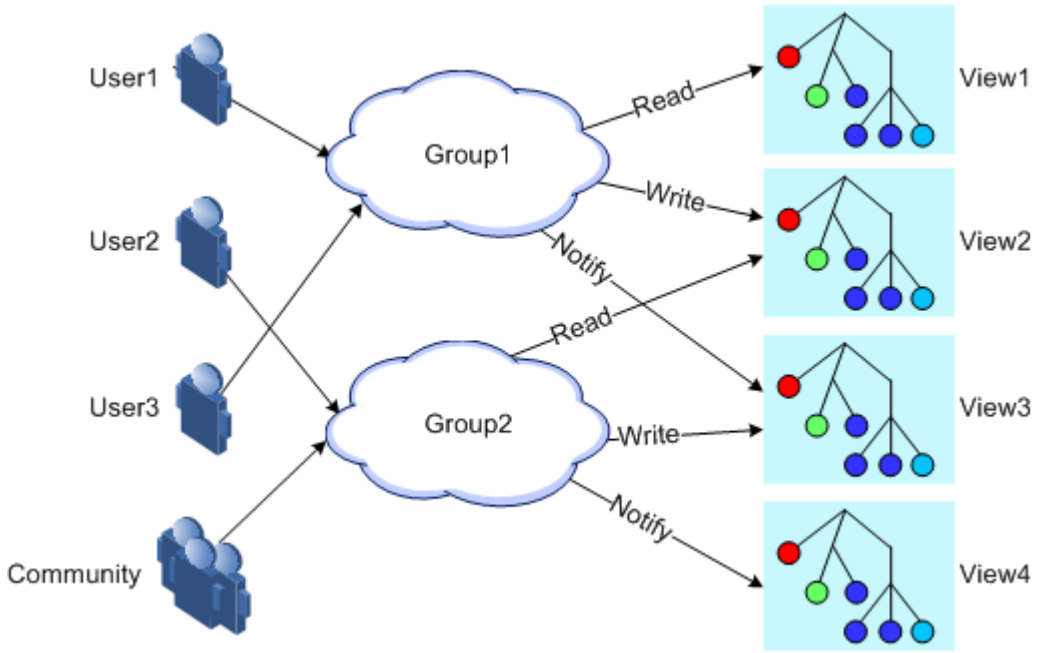
13.2.3 Configuring basic functions of SNMPv3

SNMPv3 adopts the USM user authentication mechanism. The 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 announcement views; users in the access group have access permission in this view. User access group sending the Get and Set request must have permission corresponding to the request; otherwise the request will not be accepted.

As shown in Figure 13-4, the network management station uses SNMPv3 to access the ISCOM6820 and the configuration is as below:

- Configure the user.
- Check which access group the user belongs to.
- Configure the view permission of the access group.
- Create a view.

Figure 13-4 Authentication mechanism of SNMPV3



Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server view** *view-name oid-tree* [**mask**] { **included** | **excluded** }	Create the SNMP view and configure the MIB variable range.
3	Raisecom(config)#**snmp-server user** *username* [**remote** *engineid*] **authentication** { **md5** | **sha** } *authpassword*	Create the user and configure the authentication mode.
4	Raisecom(config)#**snmp-server user** *username* [**remote** *engineid*] **authkey** { **md5** | **sha** } *authkey*	Create the user and configure information about the authentication key.
5	Raisecom(config)#**snmp-server user** *username* [**remote** *engineid*]	Create the user and configure the remote SNMP engine ID.
6	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 the SNMPv3 access group.
7	Raisecom(config)#**snmp-server group** *group-name* **user** *username* { **v1sm** | **v2csm** | **usm** }	Configure mapping between the user and access group.

13.2.4 Configuring other information about SNMP

Configure other information of SNMP, including:

- Identification and contact of administrators

- Physical location of the ISCOM6820

SNMPv1, v2c, and v3 are in support of the above configurations.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#snmp-server contact` *contact*	(Optional) configure identification and contact of administrators. **Note** For example, use the E-mail as the identification and contact of administrators.
3	`Raisecom(config)#snmp-server location` *location*	(Optional) specify the physical location of the device.

13.2.5 Configuring Trap

Note

Except for the destination host configuration, Trap configurations of SNMPv1, v2c, and v3 are identical.

Trap refers the unrequested information sent by the device to the NMS, which is used to report some critical events.

To configure the Trap feature, you need to complete the following tasks:

- Configure basic functions of SNMP. If using SNMPv1 and v2c, configure the community name; if using SNMPv3, configure the user name and SNMP view.
- Configure the routing protocol, and ensure that the route between the device and NMS is reachable.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#snmp-server host` *ip-address* `version { 1 | 2c } name [ udpport` *port-id* `]`	(Optional) configure the IPv4 Trap/Notification target host based on SNMPv1/v2.
3	`Raisecom(config)#snmp-server host` *ip-address* `version 3 { noauthnopriv | authnopriv } name [ udpport` *value* `]`	(Optional) configure the IPv4 Trap/Notification target host based on SNMPv3.
4	`Raisecom(config)#snmp-server enable traps`	Enable the OLT to send Trap. You can use the **no snmp-server enable traps** command to disable this function.
5	`Raisecom(config)#snmp-server keepalive-trap { enable | disable | pause }`	Enable/Disable/Pause the OLT to send KeepAlive Trap.
6	`Raisecom(config)#snmp-server keepalive-trap interval` *period*	Configure the interval to send KeepAlive Trap from the device to the SNMP NMS.

13.2.6 Checking configurations

No.	Command	Description
1	Raisecom#**show snmp access**	Show privilege information about all access groups.
2	Raisecom#**show snmp community**	Show configurations of the SNMP community.
3	Raisecom#**show snmp config**	Show SNMP basic configurations.
4	Raisecom#**show snmp group**	Show mapping between the SNMP user and access group.
5	Raisecom#**show snmp host**	Show information about the SNMP target host.
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.
9	Raisecom#**show keepalive**	Show configurations and statistics of KeepAlive.

13.3 Configuring optical module DDM

13.3.1 Default configurations

Default configurations of optical module DDM on the ISCOM6820 are as below.

Function	Default value
Global optical module DDM	Enable (read-only)
Global optical module DDM interface Trap	Enable (read-only)
Optical module DDM on the interface	Disable
Optical module DDM interface Trap	Disable

13.3.2 Configuring optical module DDM

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** { **gpon-olt** | **ten-gigabitethernet** } *slot-id/port-id*	Enter physical interface configuration mode.
3	Raisecom(config-if-*-*:*)#**transceiver ddm** { **enable** | **disable** }	Enable/Disable optical module DDM.
4	Raisecom(config-if-*-*:*)#**snmp trap transceiver** { **enable** | **disable** }	(Optional) enable/disable optical module DDM interface Trap.

13.3.3 Checking configurations

No.	Command	Description
1	Raisecom#**show transceiver**	Show the global and interface status of the OLT optical module measurement and diagnosis.
2	Raisecom#**show interface gpon-olt** *slot-id/olt-id* **transceiver rx-onu-power** [**violation**]	Show information about the uplink average optical power of the ONU received by the optical module under the OLT PON interface.
3	Raisecom#**show interface** { **gpon-olt** | **ten-gigabitethernet** } *slot-id/port-id* **ddm** [**detail**]	Show the current performance, alarm status, and alarm threshold of the OLT optical module.
4	Raisecom#**show interface** { **gpon-olt** | **ten-gigabitethernet** } *slot-id/port-id* **ddm history** [**15m** | **24h**]	Show history performance parameters of the OLT optical module.
5	Raisecom#**show interface** {**gpon-olt** | **ten-gigabitethernet** } *slot-id/port-id* **ddm information**	Show the status of the OLT optical module.
6	Raisecom#**show interface** { **gpon-olt** | **ten-gigabitethernet** } *slot-id/port-id* **ddm threshold-violation**	Show the time from the last violation of the OLT optical module to the present and corresponding violation value.
7	Raisecom#**show gpon-onu** *slot-id/olt-id/onu-list* **transceiver**	Show information about th eGPON ONU optical module.

13.4 Configuring PPPoE Agent

13.4.1 Default configurations

Default configurations of PPPoE Agent are as below.

Function	Default values
Global PPPoE Agent	Disable
Interface PPPoE Agent interface	Disable
Trusted interface	N/A
Packet processing policy	transparent
Overwriting start position	0
Overwriting length	24

Default configurations of Raisecom ONUs are as below.

Function	Default values
PPPoE Agent	Disable
PPPoE Agent customization	Disable
Attach-string field of the Circuit ID of PPPoE Agent	N/A
Padding mode of the Remote ID of PPPoE Agent	Onumac-binary
User-defined value of the Remote ID of PPPoE Agent	N/A

13.4.2 Configuring PPPoE Agent

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** { **ten-gigabitethernet** | **gpon-olt** } *slot-id/port-id*	Enter physical interface configuration mode.
3	Raisecom(config-if-*-*/*:*)#**pppoeagent trust**	(Optional) configure the interface as a PPPoE Agent trusted interface. You can use the **no pppoeagent trust** command to restore default configurations. **Note** When a device receives a PPPoE packet (such as PADI packet), it only forwards the packet to the trusted interface. Therefore, you should configure the port connected to the legal PPPoE server as a trusted interface.
4	Raisecom(config-if-*-*/*:*)#**pppoeagent circuit-id** *circuit-id*	(Optional) configure the Circuit ID of the interface. You can use the **no pppoeagent circuit-id** command to restore default configurations.
5	Raisecom(config-if-*-*/*:*)#**pppoeagent overwrite-policy** { **transparent** |**drop** | **replace** }	(Optional) configure the processing policy of PPPoE Agent packets.
6	raisecom(config-if-*-*/*:*)#**pppoeagent overwrite-policy replace offset** *value* **length** *value*	(Optional) configure the partially overwriting policy of PPPoE Agent packets.

13.4.3 Enabling PPPoE Agent

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**pppoeagent** { **enable** | **disable** }	Enable/Disable global PPPoE Agent.

Step	Command	Description
3	Raisecom(config)#**interface** { **ten-gigabitethernet** | **gpon-olt** } *slot-id/port-id*	Enter interface configuration mode.
4	Raisecom(config-if-*-*/*:*)#**pppoeagent** { **enable** | **disable** }	Enable/Disable PPPoE Agent on the interface.

13.4.4 Configuring PPPoE Agent (GPON ONU)

PPPoE Agent mainly processes a specific tag in the PPPoE message, which contains two fields: Circuit ID and Remote ID. Among them:

- The Circuit ID is padded with the VLAN ID, interface ID, and host name of the interface that receives the client request message.
- The Remote ID is padded with the MAC address of the client or the MAC address of the ONU.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu** *slot-id/olt-id/onu-id*	Enter GPON ONU remote management configuration mode.
3	Raisecom(config-gpon-onu-*/*:*)#**pppoe-agent** { **enable** | **disable** }	Enable/Disable PPPoE Agent.
4	Raisecom(config-gpon-onu-*/*:*)#**pppoe-agent circuit-id string** *string*	Configure the customized value of the Circuit ID of PPPoE Agent. You can use the **no pppoe-agent circuit-id string** command to restore to the default condition..
5	Raisecom(config-gpon-onu-*/*:*)#**pppoe-agent circuit-id mode** { **onu-eth-id** | **onu-mac** | **client-mac** | **user-define** }	Configure the padding mode of the Circuit ID of PPPoE Agent. You can use the **no pppoe-agent circuit-id mode** command to restore to the default condition..
6	Raisecom(config-gpon-onu-*/*:*)#**pppoe-agent remote-id string** *string*	Configure the user-defined value of the Remote ID of PPPoE Agent. You can use the **no pppoe-agent circuit-id string** command to restore to the default condition..
7	Raisecom(config-gpon-onu-*/*:*)#**pppoe-agent remote-id mode** { **onu-eth-id** | **onu-mac** | **client-mac** | **user-define** }	Configure the padding mode of the Remote ID of PPPoE Agent. You can use the **no pppoe-agent remote-id mode** command to restore to the default condition..

13.4.5 Checking configurations

Step	Command	Description
1	Raisecom#**show pppoeagent**	Show configurations of PPPoE Agent.
2	Raisecom#**show interface** [**gpon-olt** | **ten-gigabitethernet** } *slot-id/port-id*] **pppoeagent**	Show configurations of PPPoE Agent on the device.

After the ONU is configured, check it as below.

Step	Command	Description
1	Raisecom#**show gpon-onu***slot-id/olt-id/onu-list* **pppoe-agent**	Show configurations of ONU PPPoE.

13.4.6 Maintenance

No.	Command	Description
1	Raisecom(config)#**clear interface** { **gpon-olt** | **ten-gigabitethernet** } *slot-id/port-id* **pppoeagent statistic**	Clear statistics on PPPoE packets on the interface.

13.5 Configuring system log

13.5.1 Default configurations

Default configurations of system log on the ISCOM6820 are as below.

Function	Default value
System log	Enable
Output system log to the console	Enable (output level: notifications)
Log host	N/A
Output system log to the monitor	N/A
Log rate configurations	0, no limit
Timestamp configurations of system log	Absolute time

13.5.2 Configuring basic information about system log

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**logging on**	Enable system log. You can use the **no logging on** command to disable this function.
3	Raisecom(config)#**logging time-stamp** { **relative-start** | **none** }	Configure the type of timestamp.
4	Raisecom(config)#**logging rate** *rate*	Configure the Tx rate of system log.

13.5.3 Configuring output direction of system log

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**logging history**	(Optional) record system log in the buffer.
	Raisecom(config)#**logging console severity** { *severity-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** }	(Optional) output system log to the Console interface and configure parameter information.
	Raisecom(config)#**logging host** *host-id* **ip address** { *ipv4-addres / ipv6-address* } **facility** { **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** } **severity** [*log-level* | **alerts** | **critical** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**]	(Optional) output system log to the log host.
	Raisecom(config)#**logging file severity** [*log-level* | **alerts** | **critical** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**]	(Optional) output system log to a file.
	Raisecom(config)#**logging monitor severity** { *severity-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** }	(Optional) output system log to the monitor terminal and configure the alarm level.
3	Raisecom(config)#**logging command-host** { **ip address** *ip-address* | **ipv6 address** *ipv6-address* }	(Optional) configure the CLI operation log host.

13.5.4 Checking configurations

No.	Command	Description
1	Raisecom#**show logging**	Show system log configurations.
2	Raisecom#**show logging host**	Show information about the system log host.

No.	Command	Description
3	Raisecom#**show logging history**	Show information about system log buffer.
4	Raisecom#**show logging statistics**	Show statistics of system log.
5	Raisecom#**show logging file**	Show information about the system log file.
6	Raisecom#**show logging command-host**	Show information about the operation log host.

13.5.5 Maintenance

No.	Command	Description
1	Raisecom(config)#**clear logging history**	Clear history logs.
2	Raisecom(config)#**clear logging file**	Clear log files.
3	Raisecom(config)#**clear logging statistics**	Clear log statistics.

13.6 Configuring port mirroring

13.6.1 Default configurations

N/A

13.6.2 Configuring port mirroring on OLT

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mirror** { **enable** | **disable** }	Enable/Disable global port mirroring.
3	Raisecom(config)#**interface** { **ten-gigabitethernet** | **gpon-olt** } *solt-id/port-id*	Enter physical interface configuration mode.
4	Raisecom(config-if-*-*/*)#**mirror monitor-port** *uni-id*	(Optional) configure the monitor port. You can use the **no mirror monitor-port** command to delete the monitor port. **Note** The EPON interface can be configured as the source port only instead of the monitor port. The Ethernet interface can be configured as the monitor port or mirroring source port.

Step	Command	Description
5	Raisecom(config-if-*-*/*)#**mirror source-port** { **both** | **egress** | **ingress** }	(Optional) configure the mirroring source port. You can use **no mirror source-port** command to restore to the default condition..

13.6.3 Checking configurations

No.	Command	Description
1	Raisecom#**show mirror**	Show configurations of port mirroring on the OLT.

13.7 Configuring link detection

13.7.1 Ping

Step	Command	Description
1	Raisecom#**ping** *ip-address* [**count** *num*] [**size** *size*][**waittime** *timout*] [**source** *ip-address*]	Test whether the IPv4 remote host is reachable.
2	Raisecom#**ping6** *ipv6-address* [**count** *num*] [**size** *size*] [**waittime** *period*]	Test whether the IPv6 remote host is reachable.

Note

You cannot execute other operations on the device in the process of Ping. You can execute other operations after pressing **Ctrl**+**C** to interrupt Ping or the Ping process finishes.

13.7.2 Traceroute

Configure the IP address and default gateway for the device before using the Traceroute function.

Step	Command	Description
1	Raisecom#**traceroute** *ip-address* [**firstttl** *fitst-ttl*] [**maxttl** *max-ttl*] [**port** *port-number*] [**waittime** *period*] [**count** *count*] [**size** *size*]	Test the IPv4 network connectivity by using the **traceroute** command and show the packet-traversed network nodes.

13.8 Configuring system monitoring

13.8.1 Default configurations

Default configurations of system monitoring on the ISCOM6820 are as below.

Function	Default value
Temperature monitoring	Enable
Power monitoring	Enable
Fan monitoring	Enable

13.8.2 Configuring temperature monitoring

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**shelf temperature-threshold** *threshold-value*	Configure the temperature alarm threshold. When the temperature of the device exceeds the threshold, an alarm will be reported.
3	Raisecom(config)#**temperature high-alarm threshold** *threshold* [**slot** *slot-id*]	Configure the temperature alarm threshold of the device card.

13.8.3 Configuring fan monitoring

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**fan speed mode** { **auto** | **manual** }	Configure the fan controlling mode.
3	Raisecom(config)#**fan speed manual** *grade*	(Optional) configure the fan speed gear.

Note

Before manually configure the fan speed gear, configure the fan controlling mode to manual.

13.8.4 Configuring CPU monitoring

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.

Step	Command	Description
2	Raisecom(config)#**cpu threshold-trap** [**slot** *slot-list*]	Enable/Disable CPU utilization rate threshold Trap. Slot1 and Slot 2 do not support configuring system monitoring alarm parameters.
3	Raisecom(config)#**cpu rising-threshold** *threshold*	Configure the CPU alarm rising threshold.
4	Raisecom(config)#**cpu falling-threshold** *threshold*	Configure CPU alarm falling threshold.
5	Raisecom(config)#**cpu threshold-interval** *threshold*	Configure the monitoring period of CPU utilization rate.

13.8.5 Configuring memory monitoring

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**memory avail-trap** [**slot** *slot-list*]	Configure the status of idle memory utilization rate Trap.
3	Raisecom(config)#**memory avail-threshold** *threshold* [**slot** *slot-list*]	Configure the threshold of memory monitoring alarm.

13.8.6 Checking configurations

No.	Command	Description
1	Raisecom#**show fan**	Show the fan status and configurations.
2	Raisecom#**show power**	Show power card information, including the power card type, related threshold configurations, input and output voltage, related alarm status, and power card version.
3	Raisecom#**show device**	Show information about the device, including the temperature, temperature alarm threshold, power, and fan.
4	Raisecom#**show device location**	Show information about the geographical location of the device.
5	Raisecom#**show card-power** [**slot** *slot-id*]	Check the voltage information about cards in all slots (excluding voltage cards and fan slots), including voltage status and voltage. The information about the idle slot is not shown.
6	Raisecom#**show card-temperature** [**slot** *slot-id*]	Show temperature information about cards in all slots, including the current termpature, temperature alarm threshold, temperature management status, and temperature management enabling status.

No.	Command	Description
7	Raisecom#**show card-temperature management information**	Show the CPU dynamic utilization rate of the card in the specified slot.
8	Raisecom#**show cpu-utilization** [**slot** *slot-list*]	Check the memory usage of the system.
9	Raisecom#**show memory**	Check the memory usage of the card in the specified slot. This command is only available for rack-mount devices.

13.9 Configuring KeepAlive

13.9.1 Default configurations

Function	Default value
KeepAlive Trap status	Disable
KeepAlive Trap period	300s

13.9.2 Configuring KeepAlive

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server keepalive-trap** { **enable** | **disable** | **pause** }	Configure KeepAlive Trap sending.
3	Raisecom(config)#**snmp-server keepalive-trap interval** *period*	Configure the period for sending KeepAlive Traps.

Note

To prevent multiple devices from sending KeepAlive Trap with the same period in the same time point, which may overburden the NMS, configure the actual period to a random value of sending period + 5s.

13.9.3 Checking configurations

No.	Command	Description
1	Raisecom#**show keepalive**	Show KeepAlive configurations.

13.10 Configuring alarm and event management

13.10.1 Default configurations

Default configurations of alarm and event management on the ISCOM6820 are as below.

Function	Default value
Alarm Trap	Enable
Event Trap	Enable
Alarm delay	Disable
Alarm delay interval	10s
Timed alarm masking interval	3600s

13.10.2 Configuring alarm management

The alarm management feature on the ISCOM6820 includes alarm reporting, alarm masking, and alarm delay.

Configuring alarm reporting

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**alarm traps**	Enable/Disable alarm reporting.
3	Raisecom(config)#**alarm active-table delete** *listname sn*	(Optional) delete alarms in the current alarm table according to the serial number. The deleted alarms are recorded in the historical alarm table.
4	Raisecom(config)#**trap illegal-onu interval** *time* **slot** { **all** | *slot-list* }	(Optional) configure the interval for reporting the illegal ONU alarms. You can use the **no trap illegal-onu interval slot { all |** *slot-list* **}** command to restore to the default condition..
5	Raisecom(config)#**trap illegal-onu limit** *numbers* [*times*]	(Optional) configure the number of illegal ONU alarms allowed to be reported and the silence interval for reporting alarms again. You can use the **no trap illegal-onu limit** command to restore to the default condition..

Configuring alarm masking

Alarm masking supports masking alarms based on the alarm source or alarm ID. If an alarm is in masking status, the system will not monitor the alarm.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**alarm inhibit dev** [**alarm-id** *alarm-id*]	Configure alarm masking on the alarm source of the whole device. If you do not configure the **alarm-id** *alarm-id* parameter, it is believed that the alarm ID is not specified and all alarms generated on the whole device are masked.
	Raisecom(config)#**alarm inhibit** [**range**] **slot** *slot-list* [**alarm-id** *alarm-id*]	Configure alarm masking on the alarm source of the OLT slots. If you do not configure the **alarm-id** *alarm-id* parameter, it is believed that the alarm ID is not specified and all alarms generated in the OLT slots are masked.
	Raisecom(config)#**alarm inhibit** [**range**] **interface** { **ten-gigabitethernet** | **gpon-olt** } *slot-id/port-id* [**alarm-id** *alarm-id*]	Configure alarm masking on the alarm source of the OLT interfaces. If you do not configure the **alarm-id** *alarm-id* parameter, it is believed that the alarm ID is not specified and all alarms generated on the OLT interfaces are masked.
	Raisecom(config)#**alarm inhibit** [**range**] **interface** { **epon-onu** | **gpon-onu** }*slot-id/olt-id/onu-id* [**alarm-id** *alarm-id*]	Configure alarm masking on the alarm source of the ONU. If you do not configure the **alarm-id** *alarm-id* parameter, it is believed that the alarm ID is not specified and all alarms with the source of ONU ID are masked.
	Raisecom(config)#**alarm inhibit interface gpon-onu** *slot-id/olt-id/onu-id* [**range**] **uni** *uni-id* [**alarm-id** *alarm-id*]	Configure alarm masking with ONU UNI as the alarm source. If you do not configure the **alarm-id** *alarm-id* parameter, it is believed that the alarm ID is not specified and all alarms with the source of ONU UNI ID are masked.
3	Raisecom(config)#**alarm inhibit** { **dev** | **slot** | **port** | **onu** | **uni** } **alarm-id** *alarm-id*	Configure alarm masking based on alarm ID.
4	Raisecom(config)#**alarm inhibit time dev** [**alarm-id** *alarm-id*] [**interval** *interval*] [**start** *start-time* **every** *time* **stop** *end-time*]	Configure timed alarm masking on the alarm source of the whole device. If you do not configure the **alarm-id** *alarm-id* parameter, it is believed that the alarm ID is not specified and all alarms generated on the whole device are masked.

Step	Command	Description
	Raisecom(config)#**alarm inhibit time** [**range**] **slot** *slot-list* [**alarm-id** *alarm-id*] [**interval** *interval*] [**start** *start-time* **every** *time* **stop** *end-time*]	Configure timed alarm masking on the alarm source of the OLT slots. If you do not configure the **alarm-id** *alarm-id* parameter, it is believed that the alarm ID is not specified and all alarms generated in the OLT slots are masked.
	Raisecom(config)#**alarm inhibit time** [**range**] **interface** { **ten-gigabitethernet** | **gpon-olt** } *slot-id/port-id* [**alarm-id** *alarm-id*] [**interval** *interval*] [**start** *start-time* **every** *time* **stop** *end-time*]	Configure timed alarm masking on the alarm source of the OLT interfaces. If you do not configure the **alarm-id** *alarm-id* parameter, it is believed that the alarm ID is not specified and all alarms generated on the OLT interfaces are masked.
	Raisecom(config)#**alarm inhibit time** [**range**] **interface** { **epon-onu** | **gpon-onu** } *slot-id/olt-id/onu-id* [**alarm-id** *alarm-id*] [**interval** *interval*] [**start** *start-time* **every** *time* **stop** *end-time*]	Configure timing alarm masking with the alarm source being the ONU. If the **alarm-id** *alarm-id* parameter is not configured, it indicates that there is no limit on the alarm ID and all alarms with the ONU ID as the source will be masked.
	Raisecom(config)#**alarm inhibit time interface** { **gpon-onu** }*slot-id/olt-id/onu-id* [**range**] **uni** *uni-id* [**alarm-id** *alarm-id*] [**interval** *interval*] [**start** *start-time* **every** *time* **stop** *end-time*]	Configure timed alarm masking with the alarm source of ONU UNI. If the **alarm-id** *alarm-id* is not configured, the alarm ID is not restricted. As long as the source is the ONU UNI ID, all alarms are masked.
5	Raisecom(config)#**alarm inhibit time** { **dev** | **slot** | **port** | **onu** | **uni** } **alarm-id** *alarm-id* [**interval** *interval*] [**start** *start-time* **every** *time* **stop** *end-time*]	Configure timed alarm masking based on alarm ID.
6	Raisecom(config)#**alarm inhibit interval** *time*	(Optional) configure the interval of timed alarm masking.

Configuring alarm filtering

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**alarm filter dev** [**alarm-id** *alarm-id*]	Configure alarm filtering on the alarm source of the whole device. If you do not configure the **alarm-id** *alarm-id* parameter, it is believed that the alarm ID is not specified and all alarms generated on the whole device are filtered.
3	Raisecom(config)#**alarm filter** [**range**] **slot** *slot-list* [**alarm-id** *alarm-id*]	Configure alarm filtering on the alarm source of the OLT slots. If you do not configure the **alarm-id** *alarm-id* parameter, it is believed that the alarm ID is not specified and all alarms generated in the OLT slots are filtered.

Step	Command	Description
4	Raisecom(config)#**alarm filter** [**range**] **interface** { **ten-gigabitethernet** | **gpon-olt** } *slot-id/port-id* [**alarm-id** *alarm-id*]	Configure alarm filtering on the alarm source of the OLT interfaces. If you do not configure the **alarm-id** *alarm-id* parameter, it is believed that the alarm ID is not specified and all alarms generated on the OLT interfaces are filtered.
5	Raisecom(config)#**alarm filter** [**range**] **interface** { **gpon-onu** *slot-id/olt-id/onu-id* [**alarm-id** *alarm-id*]	Configure alarm filtering with the alarm source being the ONU. If the **alarm-id** *alarm-id* parameter is not configured, it indicates that there is no limit on the alarm ID and all alarms with the ONU ID as the source will be masked.
6	Raisecom(config)#**alarm filter interface gpon-onu** *slot-id/olt-id/onu-id* [**range**] **uni** *uni-id* [**alarm-id** *alarm-id*]	Configure alarm filtering with the alarm source of ONU UNI. If the **alarm-id** *alarm-id* parameter is not configured, it indicates that there is no limit on the alarm ID and all alarms with the ONU ID as the source will be masked.
7	Raisecom(config)#**alarm filter** { **dev** | **slot** | **port** | **onu** | **uni** } **alarm-id** *alarm-id*	Configure alarm filtering based on the alarm ID.

13.10.3 Configuring event management

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**event traps enable**	Enable event Traps.
3	Raisecom(config)#**event inhibit dev** [**event-id** *event-id*]	Configure event masking on the event source of the whole device. If you do not configure the **event-id** *event-id* parameter, it is believed that the event ID is not specified and all events generated on the whole device are masked.
4	Raisecom(config)#**event inhibit** [**range**] **slot** *slot-list* [**event-id** *event-id*]	Configure event masking on the event source of the OLT slots. If you do not configure the **event-id** *event-id* parameter, it is believed that the event ID is not specified and all events generated in the OLT slots will be masked.
5	Raisecom(config)#**event inhibit** [**range**] **interface** { **ten-gigabitethernet** | **epon-olt** | **gpon-olt** } *slot-id/port-id* [**event-id** *event-id*]	Configure event masking on the event source of the OLT interfaces. If you do not configure the **event-id** *event-id* parameter, it is believed that the event ID is not specified and all events generated on the OLT interfaces are masked.
6	Raisecom(config)#**event inhibit** { **dev** | **slot** | **port** | **onu** | **uni** } **event-id** *event-id*	Configure event masking based on event ID.

13.10.4 Checking configurations

No.	Command	Description
1	Raisecom#**show alarm inhibit**	Show alarm masking configurations.
2	Raisecom#**show alarm filter**	Show alarm filtering configurations.
3	Raisecom#**show alarm active-table slot** *slot-id* [**detail**]	Show the alarm table in the current slot according to the alarm source, alarm type, or alarm generation time.
4	Raisecom#**show alarm alarm-id** *alarm-id*	Show alarm details.
5	Raisecom#**show event inhibit**	Show event masking configurations.
6	Raisecom#**show event history-table** [**slot** *slot-id* | **onu** *slot-id/olt-id/onu-id* | **port** *solt-id/port-id* | **dev** | **event-id** *event-id* | **start_time** *start-time* **end_time** *end-time*] [**detail**]	Show history event table, which can be checked based on event source, event type, and event generation time.
7	Raisecom#**show event event-id** *event-id*	Show details of the alarm event.
8	Raisecom#**show trap illegal-onu limit**	Show the number of illegal ONU alarms allowed to be reported and the silence interval for reporting alarms again.
9	Raisecom#**show trap illegal-onu interval slot { all |** *slot-list* **}**	Show the interval for reporting illegal ONU alarms.
10	Raisecom#**show cpu-utilization alarm** [**slot** *slot-id*]	Show the CPU alarm threshold.

13.11 Configuring Illegal ONU alarms

13.11.1 Default configurations

Function	Default value
Illegal ONU alarm allows the configuration of the number of entries to be reported and the recovery time when the alarm is received again after silence.	Illegal ONU alarms allow no limit on the number of entries that can be reported. By default, it will not be recovered when only the number of entries is configured but the recovery time is not configured.
Interval for reporting illegal ONU alarms	60s

13.11.2 Configuring illegal ONU alarm reporting

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**trap illegal-onu limit** *numbers* [*times*]	(Optional) configure the number of allowed entries for illegal ONU alarms and the recovery time when the alarm is received again after silence. You can use the **no trap illegal-onu limit** command to restore to the default condition. **Note** The first parameter is the number of traps for illegal ONU alarms that are allowed to be reported. When this value is exceeded, the alarm is silent and no more alarm will be reported. When the ONU is powered off and restarted, if the interval for receiving the alarm again exceeds the configured recovery time, it will directly report the alarm. At this time, you need to limit the interval again, otherwise it will continue to remain silent.
3	Raisecom(config)#**trap illegal-onu interval** *time* **slot** { **all** | *slot-list* }	(Optional) configure the interval for reporting illegal ONU alarms. You can use the **no trap illegal-onu interval slot { all** | *slot-list* **}** command to restore to the default condition.

13.11.3 Checking configurations

Step	Command	Description
1	Raisecom#**show trap illegal-onu limit**	Show the number of allowed illegal alarm reports and the recovery time.
2	Raisecom#**show trap illegal-onu interval slot** { **all** | *slot-list* }	Show the reporting interval of illegal ONU alarm reporting.

13.12 Configuring mOLT remote management

13.12.1 Configuring the mOLT device

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gpon-onu** *slot-id/olt-id/onu-id*	Enter GPON ONU remote management configuration mode.
3	Raisecom(config-gpon-onu-*/*:*)#**molt-device** *device-id* **lan** *lan-id vlan-id* [*priority*]	Configure the LAN of the mOLT device.

Step	Command	Description
4	Raisecom(config-gpon-onu-*/*:*)#**no molt-device** *device-id*	Delete registration information on the mOLT device.
5	Raisecom(config-gpon-onu-*/*:*)#**no molt-device** *device-id* **lan** *lan-id*	Delete LAN information on the specified LAN interface on the mOLT device.

13.12.2 Configuring the mOLT management profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**create molt-mng-profile** *profile-id*	Create an mOLT management profile.
3	Raisecom(config)#**molt-mng-profile** *profile-id* **name** *profile-name*	Configure the name of the mOLT management profile.
4	Raisecom(config)#**molt-mng-profile** *profile-id* **master-lan** *lan-num-master* Raisecom(config)#**molt-mng-profile** *profile-id* **slave-device** *num-slave* Raisecom(config)#**molt-mng-profile** *profile-id* **slave-lan** *lan-num-slave* Raisecom(config)#**molt-mng-profile** *profile-id* **pre-alloc-vlan-start** *vlan-id-start* Raisecom(config)#**molt-mng-profile** *profile-id* **pre-alloc-vlan-num** *vlan-num*	Configure parameters of the mOLT management profile.
5	Raisecom(config)#**gpon-onu-service-profile** *profile-id*	Enter GPON ONU service profile configuration mode.
6	Raisecom(config-gpon-onu-service-profile:profile-id)#**molt-mng-profile** *profile-id* Raisecom(config-gpon-onu-service-profile:profile-id)#**molt-mng-profile name** *profile-name*	Bind the mOLT management profile with the GPON ONU service profile.

13.12.3 Checking configurations

No.	Command	Description
1	Raisecom#**show molt-mng-profile** { **all** | *profile-list* }	Show configurations of the mOLT management profile.
2	Raisecom#**config**	Enter global configuration mode.
3	Raisecom(config)#**gpon-onu** *slot-id/olt-id/onu-id*	Enter GPON ONU remote management configuration profile.

No.	Command	Description
4	`Raisecom(config-gpon-onu-*/*:*)#show gpon-onu [ slot-id/olt-id/onu-list ] molt-device [ device-list ] information`	Show configurations of the mOLT device.
5	`Raisecom(config-gpon-onu-*/*:*)#show gpon-onu [ slot-id/olt-id/onu-list ] molt-device [ device-list ] lan [ lan-list ] information`	Show configurations of the LAN interface on the mOLT device.

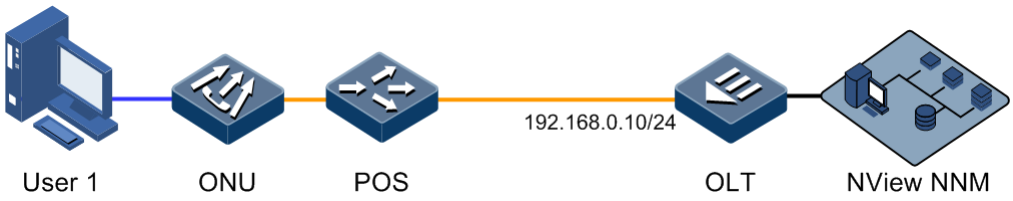
13.13 Configuration examples

13.13.1 Example for configuring SNMP

Networking requirements

As shown in Figure 13-5, the IP address of the OLT is 192.168.0.10. User 1 adopts the md5 authentication algorithm (the authentication password is raisecom) to access mib2 view with all MIB variables under 1.3.6.1.2.1. Create the access group of the guestgroup with the security mode of USM, the security level as authentication without encryption, and the readable view name is mib2. Complete mapping from User 1 with the security level of USM to the guestgroup, and show the results.

Figure 13-5 SNMPv3 networking



Configuration steps

Step 1 Configure the IP address.

```
Raisecom(config)#interface vlanif 2
Raisecom(config-vlanif-2)#ip address 192.168.0.10 10
Raisecom(config-vlanif-2)#exit
```

Step 2 Configure the 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 the SNMP user.

```
Raisecom(config)#snmp-server user guestuser1 authentication md5 raisecom
```

Step 4 Configure the SNMP access group.

```
Raisecom(config)#snmp-server access guestgroup read mib2 usm authnopriv
```

Step 5 Configure users belonging to a specified access group.

```
Raisecom(config)#snmp-server group guestgroup user user1 usm
```

Checking results

Show names and attributes of all access groups.

```
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 mapping between all access groups and their names.

```
Raisecom#show snmp group
Index  UserName      SecModel    GroupName
------------------------------------------------------------
 0   none        usm      initialnone
 1   user1       usm      guestgroup
 2   md5nopriv     usm      initial
 3   shanopriv     usm      initial
```

13.13.2 Example for outputting system log to host

Networking requirements

As shown in Figure 13-6, to output log information to the log host for the convenience of users to check it at any time, configure the system log function.

Figure 13-6 Outputting system log to host

Configuration steps

Step 1 Configure the IP address of the OLT.

```
Raisecom#config
Raisecom(config)#interface vlanif 2
Raisecom(config-vlanif-2)#ip address 192.168.0.6 255.255.255.0 1
Raisecom(config-vlanif-2)#exit
```

Step 2 Configure outputting system log to the log host.

```
Raisecom(config)#logging on
Raisecom(config)#logging time-stamp relative-start
Raisecom(config)#logging rate 10
Raisecom(config)#logging host 1 ip address 192.168.0.168 facility local0
severity warnings
```

Checking results

Use the **show logging** command to show system log configurations.

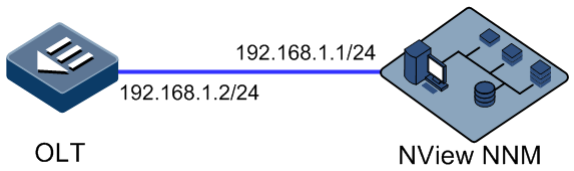
```
Raisecom#show logging
Syslog logging   : Enable
Rate-limited    : 10 messages per second
Logging time-stamp : Relative time-stamp
Console logging  : Enable
Conslole severity : Notifications
Monitor logging  : Disable
Monitor severity  : Informational
History logging  : Enable
History severity  : Debugging
File logging    : Disable
File severity   : Informational
File logging      : Disable
File severity     : Warnings
```

13.13.3 Example for configuring KeepAlive Trap

Networking requirements

The IP address of the OLT is 192.168.1.2, the target host address of the SNMP v2c Trap is 192.168.1.1, the read and write community name is public, and the SNMP version is v2c. Configure the interval for the OLT to send KeepAlive Trap to the SNMP network management station to 120s, and enable KeepAlive Trap.

Figure 13-7 KeepAlive networking



Configuration steps

Step 1 Configure the management IP address of the OLT.

```
Raisecom(config)#interface vlanif 2
Raisecom(config-vlanif-2)#ip address 192.168.1.2 255.255.255.0 1
Raisecom(config-vlanif-2)#exit
```

Step 2 Configure the Trap destination host IP address of SNMP.

```
Raisecom(config)#snmp-server host 192.168.1.1 version 2c pulic
```

Step 3 Configure KeepAlive Trap.

```
Raisecom(config)#snmp-server keepalive-trap enable
Raisecom(config)#snmp-server keepalive-trap interval 120
```

Checking results

Use the **show keepalive** command to check KeepAlive basic configurations.

```
Raisecom#show keepalive
Keepalive Admin State:Enable
Keepalive trap interval:120s
Keepalive trap count:1
```

14 Appendix

This chapter includes the following sections:

- Terms
- Acronyms and abbreviations

14.1 Terms

A

Alarm	Alarm refers to a human-observable indication that draws attention to a failure (detected fault) usually giving an indication of the severity of the fault. It is reported when a fault is detected by a device or by the NMS during the process of polling devices. Each alarm corresponds to a recovery alarm. After a recovery alarm is received, the status of the corresponding alarm changes to cleared.
Alarm Filtering	The RCView system does not receive alarms that do not comply with filtering rules from a device.
Alarm masking	The device does not record alarms complying with the masking rules nor report the alarms to the NMS.
Alarm inhibition	The device only records and reports root alarms except correlative alarms when alarm inhibition is enabled.

C

Current alarm	The current alarm is defined according to the operation status of the alarm. All uncleared or unfiltered alarms are called as current alarms.

D

Device Scan	The device scans network devices in the IP address range, and adds them automatically to the NMS.

Dynamic ARP Inspection (DAI)	A security feature that can be used to verify the ARP data packets in the network. With DAI, the administrator can intercept, record, and discard ARP packets with invalid MAC address/IP address to prevent common ARP attacks.
Dynamic Bandwidth Allocation (DBA)	A mechanism to dynamically allocate uplink bandwidth in the interval of μs or ms. It can increase the uplink bandwidth utilization rate of the PON interface in the EPON and GPON system.
Dynamic Host Configuration Protocol (DHCP)	A technology used for assigning IP address dynamically. It can automatically assign IP addresses for all clients in the network to reduce workload of the administrator. In addition, it can implement centralized management of IP addresses.

F

Forward Error Correction (FEC)	It is a method to increase the transmission distance by adding an Error Correcting Code (ECC). It supports longer transmission distance and larger splitting ratio.

I

Internet Assigned Numbers Authority (IANA)	The organization operated under the IAB. IANA delegates authority for IP address-space allocation and domain-name assignment to the NIC and other organizations. IANA also maintains a database of assigned protocol identifiers used in the TCP/IP suite, including autonomous system numbers.
In-band Network Management	The NMS exchanges information with a device through service networks.

L

Link Aggregation	With link aggregation, multiple physical Ethernet interfaces are combined to form a logical aggregation group. Multiple physical links in one aggregation group are taken as a logical link. Link aggregation helps share traffic among member interfaces in an aggregation group. In addition to effectively improving the reliability on links between devices, link aggregation can help gain greater bandwidth without upgrading hardware.

N

Network Element (NE)	A network device to be managed by the NMS as a network element

Network Management System	Computer programs that manage network devices
NMS Monitor	It refers to auxiliary programs of the NMS, which can manage various service programs and monitor the operation status of the system.
Network Time Protocol (NTP)	A time synchronization protocol defined by RFC1305. It is used to synchronize time between distributed time server and clients. NTP is used to perform clock synchronization on all devices that have clocks in the network. Therefore, the devices can provide different applications based on a unified time. In addition, NTP can ensure a very high accuracy with an error of 10ms or so.

O

Open Shortest Path First (OSPF)	An internal gateway dynamic routing protocol, which is used to decide the route in an Autonomous System (AS)
Optical Distribution Network (ODN)	It refers to the optical transmission channel between the OLT and ONU.
Out-of-band network management	The mode in which the NMS and device communicate network management information through another network independent of the service network

Q

QinQ	802.1Q in 802.1Q (QinQ), also called Stacked VLAN or Double VLAN, is extended from 802.1Q and defined by IEEE 802.1ad recommendation. This VLAN feature allows the equipment to add a VLAN tag to a tagged packet. The implementation of QinQ is to add a public VLAN tag to a packet with a private VLAN tag, making the packet encapsulated with two layers of VLAN tags. The packet is forwarded over the ISP's backbone network based on the public VLAN tag and the private VLAN tag is transmitted as the data part of the packet. In this way, the QinQ feature enables the transmission of the private VLANs to the peer end transparently. There are two QinQ types: basic QinQ and selective QinQ.
Quality of Service (QoS)	A network security mechanism, used to solve problems of network delay and congestion. When the network is overloaded or congested, QoS can ensure that packets of important services are not delayed or discarded and the network runs high efficiently. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio.

R

Resource	It refers to the managed objects in the NMS, including the device, chassis, card, and interface.

S

Symbol	A schematic topology node, which helps clearly show the network structure while cannot be managed
Simple Network Management Protocol (SNMP)	A network management protocol defined by Internet Engineering Task Force (IETF) used to manage devices in the Internet. SNMP can make the network management system to remotely manage all network devices that support SNMP, including monitoring network status, modifying network device configurations, and receiving network event alarms. At present, SNMP is the most widely-used network management protocol in the TCP/IP network.
Spanning Tree Protocol (STP)	STP can be used to eliminate network loops and back up link data. It blocks loops in logic to prevent broadcast storms. When the unblocked link fails, the blocked link is re-activated to act as the backup link.
SyncE	A technology that adopts Ethernet link code stream to recover clocks, and provides high-precision frequency synchronization for the Ethernet similar to SDH clock synchronization. Different from the traditional network which just synchronizes data packets on the receiving node, the internal clock synchronization mechanism of the SyncE is real-time.
Syslog	Device log complying with the format of the Syslog defined by RFC3164

T

Topology	Topology includes routes and devices, describing the interconnection relationship among network nodes. It also refers to the network structure in general sense, namely, the physical layout of connected devices.
Trap	It refers to a way of sending alarms to the NMS. Alarms are reported to the system through SNMP packets.
Time Division Multiplexing (TDM)	TDM is a method of transmitting multiple independent signals (digitalized data, voice, or video signals) over a common signal path by means of synchronized switches at each end of the transmission line so that each signal appears on the line only a fraction of time in an alternating pattern.

Time Division Multiple Access (TDMA)	TDMA is a channel access method for shared medium networks. It allows several users to share the same frequency channel by dividing the signal into different timeslots. The users transmit in rapid succession, one after the other, each using its own timeslot. This allows multiple base stations to share the same transmission medium while using only a part of its channel capacity. On the condition of fixed time and synchronization, the base station can receive signals of each mobile terminal from each timeslot without interference. Meantime, signals sent by the base station to the mobile terminals are transmitted through the specified timeslots in sequence. As long as each mobile terminal receives signals from the specified timeslot, corresponding signals will be identified from the multiplexed signals and received in sequence.
U	
User	A user using the NMS client, with available NMS features determined by a set of management domains of users and user groups, and operation rights
User group	A user group can provide the same management domain and operation right for group members.
V	
Virtual Local Area Network (VLAN)	VLAN is a protocol proposed to solve broadcast and security issues for Ethernet. It divides devices in a LAN into different segments logically rather than physically, thus implementing multiple virtual work groups which are based on Layer 2 isolation and do not affect each other.

14.2 Acronyms and abbreviations

A	
ACL	Access Control List
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
B	
BPDU	Bridge Protocol Data Unit
C	
CATV	Community Antenna Television
CDR	Calling Detail Records

CFI	Canonical Format Indicator
CIR	Committed Information Rate
CoS	Class of Service
CPU	Central Processing Unit
CWDM	Coarse Wavelength Division Multiplexing

D

DAI	Dynamic ARP Inspection
DBA	Dynamic Bandwidth Allocation
DHCP	Dynamic Host Configuration Protocol
DoS	Deny of Service
DSCP	Differentiated Services Code Point

E

EoC	Ethernet over Coaxial

F

FEC	Forward Error Correction
FIB	Forwarding Information Base
FIR	Fixed Information Rate
FTP	File Transfer Protocol
FTTB	Fiber to the Building
FTTH	Fiber to the Home

G

GE	Gigabit Ethernet
GPON	Gigabit-Capable PON

H

HDLC	High-Level Data Link Control

I

IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol

IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP Snooping	Internet Group Management Protocol Snooping
IGMP	Internet Group Management Protocol
IP	Internet Protocol
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector

L

LACP	Link Aggregation Control Protocol
LLID	Logical Link Identifier

M

MAC	Medium Access Control
MIB	Management Information Base
MPCP	Multi-Point Control Protocol
MTU	Maximum Transferred Unit
MVR	Multicast VLAN Registration

N

NAT	Network Address Translation
NNM	Network Node Management
NTP	Network Time Protocol

O

OAM	Operation Administration and Management
ODN	Optical Distribution Network
OID	Object Identifier
OLT	Optical Line Terminal
ONU	Optical Network Unit
OSI	Open System Interconnect

P

PC	Personal Computer
PE	Provider Edge

PIR	Peak Information Rate
PoE	Power Over Ethernet
PPPoE	Point-to-Point Protocol over Ethernet

Q

QoS	Quality of Service

R

RADIUS	Remote Authentication Dial In User Service
RF	Radio Frequency

S

SFP	Small Form-factor Pluggables
SIP	Session Initiation Protocol)
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
TCP	Transmission Control Protocol
TDM	Time Division Multiplex
TDMA	Time Division Multiple Address
TFTP	Trivial File Transfer Protocol
ToS	Type of Service
TPID	Tag Protocol Identifier

U

UDP	User Datagram Protocol

V

VID	VLAN Identifiter

VLAN	Virtual Local Area Network

W

WRR	Weight Round Robin

瑞斯康达科技发展股份有限公司
RAISECOM TECHNOLOGY CO.,LTD.

Address: Raisecom Building, No. 11, East Area, No. 10 Block, East Xibeiwang Road, Haidian District, Beijing, P.R.China Postal code: 100094 Tel: +86-10-82883305
Fax: 8610-82883056 http://www.raisecom.com Email: export@raisecom.com