www.raisecom.com

# ISCOM5508-GP (A) Configuration Guide (Rel_02)

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: 8610-58963399

Fax: 8610-58963399-8886

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 introduces supported features and related configurations of the ISCOM5508-GP, including basic configuration, GPON service configuration, multicast service configuration, MAC address configuration, VLAN configuration, Spanning Tree configuration, routing configuration, DHCP configuration, QoS configuration, system security configuration, link security configuration, and system management configuration. In addition, this document 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 ISCOM5508-GP, as well as networking with the ISCOM5508-GP.

## Versions

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

| Product name | Hardware version | Software version |
|---|---|---|
| ISCOM5508-GP | A.00 or later | V2.41 or later |

## Related manuals

The following table lists manuals and their contents related to the ISCOM5508-GP.

| Name | Description |
|---|---|
| *ISCOM5508-GP Hardware Description* | This guide mainly introduces the hardware structure and cards, including product overview, components, fiber and cables, pluggable optical module, lookup table of LEDs, lookup table of weight and power consumption. |

| Name | Description |
|---|---|
| *ISCOM5508-GP Configuration Guide* | This guide mainly introduces supported services of the ISCOM5508-GP from aspects of service introduction, default configurations, configuration methods, and configuration examples, including basic configuration, GPON service configuration, multicast service configuration, MAC address table configuration, VLAN configuration, Spanning Tree configuration, routing configuration, DHCP configuration, QoS configuration, system security configuration, link security configuration, and system management configuration. |

# Conventions

## Symbol conventions

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

| 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** | Names of files, directories, folders, and users are in **boldface**. For example, log in as user **root**. |
| *Italic* | Book titles are in *italics*. |
| `Lucida Console` | Terminal display is in `Lucida Console`. |

## 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. |
| [ 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 02 (2015-06-15)

- Added configurations on theVoIP profile and SIP dial plan profile.
- Modified known Bugs.

# Issue 01 (2013-11-29)

Initial commercial release

# Contents

# Figures

# Tables

# 1 Basic configurations

This chapter introduces basic configurations and configuration process of the ISCOM5508-GP, and provides related configuration examples, including the following sections:

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

## 1.1 CLI

### 1.1.1 Overview

Command Line Interface (CLI) is the path for communication between users and the ISCOM5508-GP. You can configure, monitor, and manage the ISCOM5508-GP by executing related commands.

You can log in to the ISCOM5508-GP through a PC that runs the terminal emulation program or the CPE device. You can enter into 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.
- Keystrokes can be used to execute commands.

- Check a historical command by checking command history. The last 5000 historical commands can be saved on the ISCOM5508-GP.
- Online help is available by inputting "?" 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 ISCOM5508-GP uses hierarchy 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, etc. 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, TFTP commands, etc.

### 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 line 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 ISCOM5508-GP. If the ISCOM5508-GP 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 **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.

## Mode list

The ISCOM5508-GP supports the following CLI modes:

| Mode | Enter method | Description |
|---|---|---|
| User EXEC | Log in to the ISCOM5508-GP, input correct username and password | `Raisecom>` |

| Mode | Enter method | Description |
|---|---|---|
| Privileged EXEC | In user EXEC mode, input the **enable** command and correct password. | `Raisecom#` |
| Global configuration | In privileged EXEC mode, input the **config** command. | `Raisecom(config)#` |
| GE interface configuration | In global configuration mode, input the **interface gigabitethernet** *slot-id/port-id* command. | `Raisecom(config-if-gigabitethernet-slot-id:port-id)#` |
| GE interface batch configuration | In global configuration mode, input the **interface range gigabitethernet** *slot-id/port-list* command. | `Raisecom(config-if-gigabitethernet-range)#` |
| 10GE interface configuration | In global configuration mode, input the **interface ten-gigabitethernet** *slot-id/port-id* command. | `Raisecom(config-if-ten-gigabitethernet-slot-id:port-id)#` |
| 10GE interface batch configuration | In global configuration mode, input the **interface ten-gigabitethernet** *slot-id/port-list* command. | `Raisecom(config-if-ten-gigabitethernet-range)#` |
| Aggregation group interface configuration | In global configuration mode, input the **interface port-channel** *group-id* command. | `Raisecom(config-port-channel-group-id)#` |
| VLAN interface configuration | In global configuration mode, input the **interface vlanif** *vlan-id* command. | `Raisecom(config-vlanif-id)#` |
| VLAN configuration | In global configuration mode, input the **vlan** *vlan-id* command. | `Raisecom(config-vlan-id)#` |
| GPON interface configuration | In global configuration mode, input 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, input the **interface range gpon-olt** *slot-id/port-list* command. | `Raisecom(config-if-gpon-olt-range)#` |
| RIP configuration | In global configuration mode, input the **router rip** command. | `Raisecom(config-rip)#` |
| KeyChain configuration | In global configuration mode, input the **key-chain** *keychainname* command. | `Raisecom(config-keychain)#` |
| MSTP region configuration | In global configuration mode, input the **spanning-tree region-configuration** command. | `Raisecom(config-region)#` |

| Mode | Enter method | Description |
|---|---|---|
| GPON ONU remote management configuration | In global configuration mode, input the **gpon-onu** *slot-id/olt-id/onu-id* command. | `Raisecom(config-gpon-onu-slot-id/olt-id:onu-id)#` |
| GPON ONU remote management batch configuration | In global configuration mode, input 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/olt-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 ONU alarm profile configuration | In global configuration mode, input the **snmp-trap-gpon-onu-profile** *profile-id* command. | `Raisecom(config-snmp-trap-gpon-onu-profile:profile-id)#` |
| GPON ONU line profile configuration | In global configuration mode, input the **gpon-onu-line-profile** *profile-id* command. | `Raisecom(config-gpon-onu-line-profile:profile-id)#` |
| GPON ONU service profile configuration | In global configuration mode, input the **gpon-onu-service-profile** *profile-id* command. | `Raisecom(config-gpon-onu-service-profile:profile-id)#` |
| L2 ACL configuration | In global configuration mode, input the **l2-access-list** *acl-id* command. | `Raisecom(config-l2-acl-acl-id)#` |
| L2 ACL sub-rule configuration | In L2 ACL configuration mode, input the **rule** *rule-id* command. | `Raisecom(config-l2-acl-acl-id-rule-rule-id)#` |
| IPv4 ACL configuration | In global configuration mode, input the **ip-access-list** *acl-id* command. | `Raisecom(config-ip-acl-acl-id)#` |
| IPv4 ACL sub-rule configuration | In IPv4 ACL configuration mode, input the **rule** *rule-id* command. | `Raisecom(config-ip-acl-acl-id-rule-rule-id)#` |
| IPv6 ACL configuration | In global configuration mode, input the **ipv6-access-list** *acl-id* command. | `Raisecom(config-ipv6-acl-acl-id)#` |
| IPv6 ACL sub-rule configuration | In IPv6 ACL configuration mode, input the **rule** *rule-id* command. | `Raisecom(config-ipv6-acl-acl-id-rule-rule-id)#` |

| Mode | Enter method | Description |
|---|---|---|
| Hybrid ACL configuration | In global configuration mode, input the **hybrid-access-list** *acl-id* command. | `Raisecom(config-hybrid-acl-acl-id)#` |
| Hybrid ACL sub-rule configuration | In Hybrid ACL configuration mode, input the **rule** *rule-id* command. | `Raisecom(config-hybrid-acl-acl-id-rule-rule-id)#` |
| User ACL configuration | In global configuration mode, input the **user-access-list** *acl-id* command. | `Raisecom(config-user-acl-acl-id)#` |
| User ACL sub-rule configuration | In User ACL configuration mode, input the **rule** *rule-id* command. | `Raisecom(config-user-acl-acl-id-rule-rule-id)#` |
| VLAN ACL configuration | In global configuration mode, input the **vlan-access-list** *acl-id* command. | `Raisecom(config-qinq-acl-rule-id)#` |

## 1.1.4 Keystrokes

The ISCOM5508-GP supports following keystrokes.

| Keystroke | Description |
|---|---|
| Up cursor key (↑) | Show previous command if there is any command input earlier; the display has no change if the current command is the earliest one in history records. |
| Down cursor key (↓) | Show next command if there is any newer command; the display has no change if the current command is the newest one in history records. |
| Left cursor key (←) | Move the cursor one character to left; the display has no change if the cursor is at the beginning of command. |
| Right cursor key (→) | Move the cursor one character to right; the display has no change if the cursor is at the end of command. |
| **Backspace** | Delete the character before the cursor; the display has no change if the cursor is at the beginning of command. |

| Keystroke | Description |
|---|---|
| **Tab** | Click **Tab** after inputting a complete keyword, cursor will automatically appear a space to the end; click **Tab** again, the system will show the follow-up inputting keywords.<br>Click **Tab** after inputting an incomplete keyword, system automatically executes partial helps:<br>System take the complete keyword to replace input if the matched keyword is the one and only, and leave one word space between the cursor and end of keyword;<br>In case of mismatch or matched keyword is not the one and only, display prefix at first, then click **Tab** to check words circularly, no space from cursor to the end of keyword, click **Space** key to input the next word;<br>If input incorrect keyword, click **Tab** will change to the next line and prompt error, the input keyword will not change. |
| **Ctrl**+**A** | Move the cursor to the head of line. |
| **Ctrl+C** | Break off some running operation, such as ping, traceroute and so on. |
| **Ctrl+D** or **Delete** | Delete the cursor location characters |
| **Ctrl+E** | Move the cursor to the end of line. |
| **Ctrl+K** | Delete all characters behind the cursor (including cursor location). |
| **Ctrl+X** | Delete all characters before the cursor (except cursor location). |
| **Ctrl+Z** | Return to privileged EXEC mode from other modes (except user EXEC mode). |
| **Space** or **Y** | When the terminal printing command line information exceeds the screen, continue to show the information in next screen. |
| **Enter** | When the terminal printing command line information exceeds the screen, continue to show the information in next 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 Keystrokes about display features

| Function key | Description |
|---|---|
| Press **Space** or **Y** | Scroll down one screen. |

| Function key | Description |
|---|---|
| Press **Enter** | Scroll down one line. |
| Press any letter key (except **Y**) | Stop displaying and executing commands. |

### Filtering display information

The ISCOM5508-GP 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 more commands starting with the **show** parameter, see related manuals.

The **show** command of the ISCOM5508-GP supports three kinds of filtering modes:

- | **begin** *string*: show all lines starting from 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 keystrokes listed in Table 1-2. If page-break is disabled, all messages are displayed when they are displayed at more than one screen.

Configure page-break for the ISCOM5508-GP as below.

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

## 1.1.6 Command history

The ISCOM5508-GP supports checking or executing some historical 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 1/1/1
   0000:00:20:41  success      raisecom         ex
   0000:00:20:09  success      raisecom         gpon-onu uni ethernet
1/1/1/1
   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 1/1/1 uni
ethernet snmp trap
   0000:00:06:08  success      raisecom         config
   0000:00:05:24  success      raisecom         gpon-onu uni ethernet
1/1/1/1
   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** 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** 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  Install a card
```

- After you enter a command, press **Space**, 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 ISCOM5508-GP prints 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. You can connect the Console interface on the ISCOM5508-GP to the RS-232 serial interface of a PC through a specified cable, and run the terminal emulation program on the PC to locally configure the ISCOM5508-GP.

**Note**

For technical specifications of the Console interface and the corresponding configuration cable, see *ISCOM5508-GP (A) Hardware Description*.

You can log in to the ISCOM5508-GP through the Console interface only under the following two conditions:

- The ISCOM5508-GP is configured for the first time.
- You cannot log in to the ISCOM5508-GP through Telnet.

If you want to access the ISCOM5508-GP 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 ISCOM5508-GP.

Figure 1-1 Accessing the ISCOM5508-GP through a PC connected with Console interface

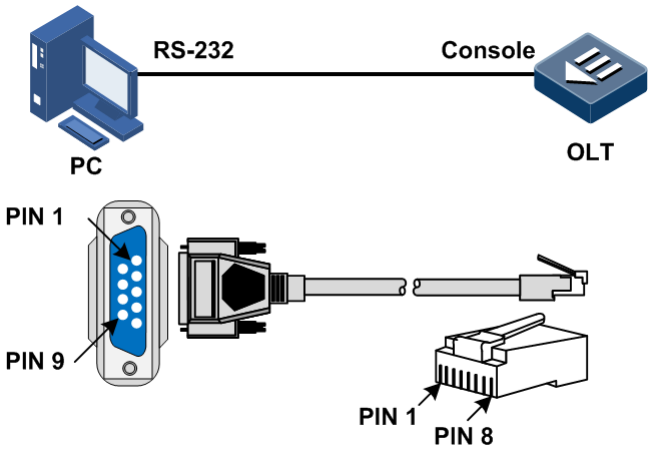
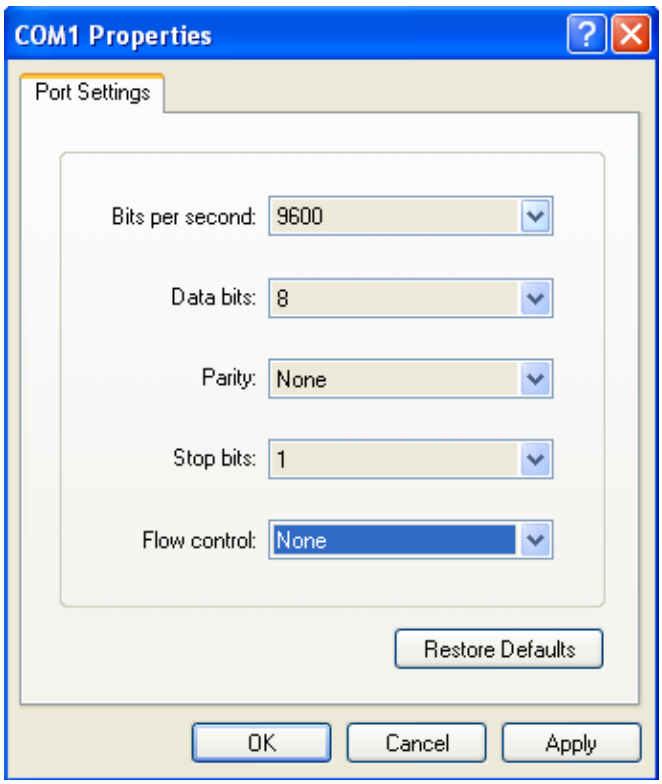



Figure 1-2 Communication parameters in Hyper Terminal



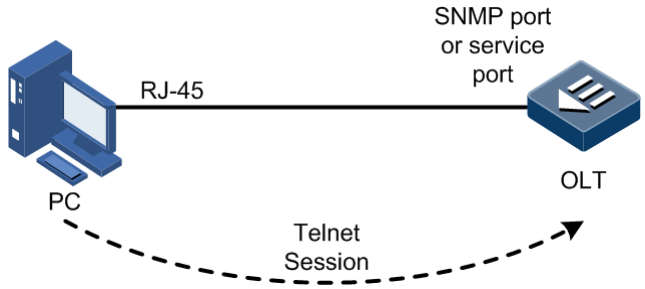

## 1.2.2 Accessing through Telnet

To use a PC to log in to the ISCOM5508-GP remotely through Telnet, log in to an ISCOM5508-GP from the PC at first, and then Telnet other ISCOM5508-GP devices on the network. Thus, you do not need to connect a PC to each ISCOM5508-GP. Moreover, you need to ensure that the ISCOM5508-GP can ping through the PC.

The ISCOM5508-GP provides the following Telnet services:

- Telnet Server: run the Telnet client program on a PC to log in to the ISCOM5508-GP, 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

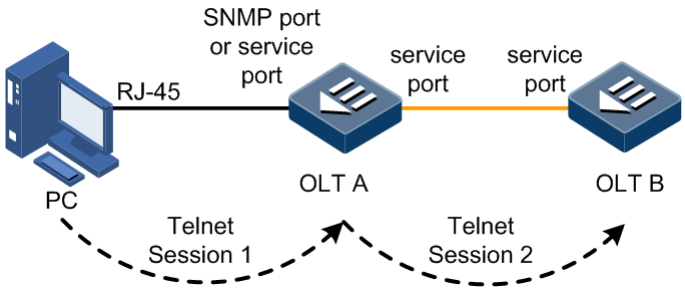



Before accessing the ISCOM5508-GP through Telnet, you need to log in to the ISCOM5508-GP through the Console interface and enable Telnet services. Configure the ISCOM5508-GP as below.

| 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-num)#ip address` *ip-address* [ *ip-mask* ] | Configure the IP address and mask and bind the IP address to the VLAN. |
| 4 | `Raisecom(config-vlanif-num)#exit` | Exit VLAN interface configuration mode. |
| 5 | `Raisecom(config)#telnet-server accept { add \| remove } interface { gigabitethernet \| ten-gigabitethernet \| gpon-olt }` *slot-id/port-id* | (Optional) add/delete the interface enabled with Telnet.<br>By default, Telnet is enabled on all interfaces. |
| 6 | `Raisecom(config)#telnet-server max-session` *number* | (Optional) configure the maximum number of Telnet sessions. |
| 7 | `Raisecom(config)#telnet-server close terminal-telnet` *session-number* | (Optional) disconnect a specified Telnet session. |

- 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 ISCOM5508-GP working as the Telnet client as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#telnet { ipv4-address \| ipv6-address [ scopeid string ] } [ 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 ISCOM5508-GP through SSHv2, you must log in to the ISCOM5508-GP through the Console interface and enable the SSHv2 service.

### Default configurations

Default configurations of the SSHv2 service on the ISCOM5508-GP 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 |

### Configuring SSHv2

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**generate ssh-key** [ *key-length* ] | Generate the local SSHv2 server key pair. The key length can be configured. |
| 3 | Raisecom(config)#**ssh2 server** | Enable the SSHv2 server.<br>You can use the **no ssh2 server** command to disable the SSHv2 server. |
| 4 | Raisecom(config)#**ssh2 server authentication** { **password** \| **rsa-key** \| **public-key** } | Configure the SSHv2 authentication mode and register the Public-Key function.<br>You can use the **no ssh2 server authentication** command to restore default configurations. |
| 5 | Raisecom(config)#**ssh2 server authentication-timeout** *timeout* | (Optional) configure the SSHv2 authentication timeout. The ISCOM5508-GP refuses to authenticate and disconnects the connection when client authentication time exceeds the upper threshold.<br>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 allowable times for SSHv2 authentication failure. The ISCOM5508-GP refuses to authenticate and disconnects the connection when client authentication failure times exceed the upper threshold. |
| 7 | Raisecom(config)#**ssh2 server port** *port-id* | Configure the SSHv2 interception interface ID.<br>You can use the **no ssh2 server port** command to restore default configurations.<br>**Note**<br>When configuring the SSHv2 interception interface ID, input parameters cannot take effect immediately without rebooting the SSHv2 service. |
| 8 | Raisecom(config)#**ssh2 server session** *session-list* { **enable** \| **disable** } | Enable/Disable a specified SSHv2 session. |

## 1.2.4 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show telnet-server** | Show interfaces supporting Telnet and the maximum number of Telnet sessions. |

| No. | Command | Description |
|---|---|---|
| 2 | Raisecom#**show ssh2 server** | Show the SSHv2 server. |
| 3 | Raisecom#**show ssh2 session** | Show SSHv2 session. |
| 4 | Raisecom#**show ssh2 public-key authentication** | Show the SSHv2 authentication key. |
| 5 | Raisecom#**show ssh2 public-key rsa** | Show the SSHv2 RSA key. |

# 1.3 Managing users

## 1.3.1 Default configurations

Default configurations of ISCOM5508-GP users are as below.

| Function | Default value |
|---|---|
| Default user | User name: raisecom<br>Password: raisecom<br>User privilege: 15 (Administrator) |
| New user privilege | 15 (Administrator) |

**Note**

We recommend modifying the default user name and password to prevent illegal visits from breaking down the ISCOM5508-GP.

## 1.3.2 Creating/Deleting users

Configure the ISCOM5508-GP 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<br>please input password:<br>please input again: | Modify the password. |
| 3 | Raisecom#**no username** *username* | Delete a specified user.<br>**Caution**<br>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 ISCOM5508-GP 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-user** \| **radius-local** \| **radius-user** \| **tacacs-user** \| **tacacs-local** \| **local-tacacs** } | (Optional) configure the authentication mode for user login. |
| 4 | Raisecom#**enable login** { **local-radius** \| **local-user** \| **radius-local** \| **radius-user** \| **tacacs-user** \| **tacacs-local** \| **local-tacacs** } | (Optional) configure the authentication mode for login in privilege EXEC mode. |

## 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, each of which 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.

User privilege refining cannot be operated on the administrator.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**command-set** *comsetname* | Create a command set can enter command set configuration mode.<br>You can use the **no command-set** *comsetname* command to delete the command set.<br>**Note**<br>When you delete a command set, the system prompts deleting successfully if the command set does not exist; the system prompts deleting unsuccessfully if the command set is in use. |
| 2 | Raisecom(command-set:*)#**command** "*comkeywords*" | You can use the keyword to add commands to the command set.<br>You can use the **no command-set** { **all** \| *comnum* } command to delete commands in the command set. |
| 3 | Raisecom(command-set:*)#**end** | Exit command set configuration mode. |
| 4 | Raisecom#**user** *username* { **allow-exeset** \| **disallow-exeset** } *comsetname* | Configure the command set privilege, that is, to allow or forbid some user to execute commands in the command set.<br>You can use the **no user** *username* { **allow-exeset** \| **disallow-exeset** } *comsetname* command to delete configurations of the command set privilege. |

**Note**

When using the **command** "*comkeywords"* command to add commands to the command set, pay attention to the following points:

- *comkeywords* refers to the keyword, which does include the parameter in the command line.
- *comkeywords* should be put between the double quotation marks ("").
- If you need to add a command only, input all keywords of the command. If you want to add commands in batch, input the shared part of the commands.

For example, when you need to add the **create vlan** *vlan-id* command to the command set, operate as below:

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

When you need to add commands containing the "vlan*"* keyword, operate as below:

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

### 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. |
| 2 | `Raisecom#show command-set` | Show information about all command sets, including the name, number of commands, and user status. |
| 3 | `Raisecom#show command-set detail [ comsetname ]` | Show details of the command set, including the name, number of commands, detailed commands, and user status. |

## 1.4 Managing cards

### 1.4.1 Default configurations

Default configurations of cards on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Created type | Slots 1–3: null<br>Slots 4–5: ISCOM5508-GP-power, which cannot be configured<br>Slot 6: ISCOM5508-GP-fan, which cannot be configured |
| Actual type | N/A |
| Serial number | N/A |
| Card status | Not-used |
| Power satus | Off |
| Fan management mode | Auto |
| Fan speed level | 40 at the maximum |

### 1.4.2 Creating cards

The ISCOM5508-GP supports defining the card status through the following two types:

- Created type: the card type specified by users using the **creat 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.

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 ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |
| 2 | `Raisecom(config)#create card slot` *slot-id* `type { gp4a \| ge4b }` | Create a card on the ISCOM5508-GP.<br>You can use the **no create card slot** *slot-id* [ **now** ] command to delete the card. |
| 3 | `Raisecom(config)#device description` *description* | (Optional) configure descriptions for the ISCOM5508-GP to identify different devices.<br>You can use the **no device description** command to delete the descriptions. |
| 4 | `Raisecom(config)#slot` *slot-id* `description` *description* | (Optional) configure descriptions for a specified slot.<br>You can use the **no slot** *slot-id* **description** command to delete the descriptions. |

## 1.4.3 Rebooting cards

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#reboot slot { slot-id \| all } [ now ]` | Reboot the card in a specified slot or all cards. |

### 1.4.4 Managing fan

The ISCOM5508-GP supports the intelligent fan. You can configure the speed of the fan manually.

Configure the ISCOM5508-GP 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.<br>You can use the **no fan speed mode** command to restore default configurations. |
| 3 | Raisecom(config)#**fan speed manual** *level* | Configure the fan speed level.<br>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.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**show card** | Show information about all cards. |
| 2 | Raisecom#**show cpu-utilization** [ **dynamic** \| **slot** *slot-id* ] | Show the CPU utilization rate of the card. |
| 3 | Raisecom#**show device** | Show information about the ISCOM5508-GP, including the type, MAC address, serial number, and slots on the main control card. |
| 4 | Raisecom#**show version slot** *slot-id* | Show version information about the card in a specified slot, including the type, hardware version, software version, bootrom version, firmware version, and CPLD version. |
| 5 | Raisecom#**show slot** *slot-id* | Show features of a specified slot, including the list of supported card types, descriptions, status, serial number, actual card type, and supposed card type.<br>If the supposed card type is not specified, the value is null. If the actual card is not inserted into the slot, the value is null. |
| 6 | Raisecom#**show fan** | Show the fan status. |

## 1.5 Managing interfaces

### 1.5.1 Default configurations

Default configurations of interfaces on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Status | Enable |
| Rate and duplex mode | Self-adaption |
| Flow control | Disable |
| Auto-MDI/MDIX | Normal |
| MTU | 1522 Bytes |
| Interval of dynamic statistics | 2s |

## 1.5.2 Enabling/Disabling interfaces

Configure the ISCOM5508-GP as below.

| 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-*-*:*)#**shutdown** | Shut down the current interface.<br>You can use the **no shutdown** command to enable the interface. |

## 1.5.3 Configuring basic properties of interfaces

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**system mtu** *size* | Configure the global MTU.<br>You can use the **no system mtu** command to restore default configurations. |
| 3 | Raisecom(config)#**interface gigabitethernet** *slot-id/port-id* | Enter GE interface configuration mode. |
| 4 | Raisecom(config-if-gigabitethernet-*:*)#**speed** { **100** \| **1000** \| **auto** } | Configure the interface rate. |
| 5 | Raisecom(config-if-gigabitethernet-*:*)#**description** *word* | Configure descriptions of the interface.<br>You can use the **no description** command to restore default configurations. |

## 1.5.4 Configuring interface statistics

Configure the ISCOM5508-GP 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.<br>You can use the **no dynamic statistics time** command to restore default configurations. |
| 3 | Raisecom(config)#**clear interface** { **gpon-olt** \| **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-id* **statistics** | Clear interface statistics saved on the ISCOM5508-GP. |

## 1.5.5 Configuring flow control on interfaces

Configure the ISCOM5508-GP as below.

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

## 1.5.6 Configuring VLAN interface

Configure the ISCOM5508-GP 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 ] [ *vlan-id* ] | (Optional) configure the IP address of the VLAN interface.<br>You can use the **no ip address** *ip-address* command to delete the IP address. |
| | Raisecom(config-vlanif-*)#**ipv6 address** *ipv6-address/prefix-length* [ **eui-64** ] [ **link-local** ] [ *vlan-id* ] | (Optional) configure the IPv6 address of the VLAN interface.<br>You can use the **no ip address** *ip-address* command to delete the IPv6 address. |

| Step | Command | Description |
|---|---|---|
| 4 | Raisecom(config-vlanif-*)#**ip vlan** *vlan-id* | Configure mapping between the interface and VLAN. You can use the **no ip vlan** command to delete the mapping. |

## 1.5.7 Configuring out-of-band network management interface

The SNMP interface is used for out-of-band network management. Before configuring out-of-band network management, you need to configure the IP address of the SNMP interface.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**management-port ip address** *ip-address* [ *mask* ] | Configure the IP address for the out-of-band management interface. |
| | Raisecom(config)#**management-port ipv6 address** *ip-address* [ **link-local** ] | Configure the IPv6 address of the out-of-band management interface. |

IP addresses of the out-of-band interface and the VLAN interface cannot be in the same network segment.

## 1.5.8 Cutting interface services

When the source interface fails, you can transfer all configurations on the specified source interface to the destination interface. When links under the source interface are switched to the destination interface, all services continue to run normally.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**running-config from interface gigabitethernet** *slot-id/port-id* **to interface gigabitethernet** *slot-id/port-id* [ **clear-source** ] | Cut the GE interface. |
| | Raisecom(config)#**running-config from interface ten-gigabitethernet** *slot-id/port-id* **to interface ten-gigabitethernet** *slot-id/port-id* [ **clear-source** ] | Cut the 10GE interface. |
| | Raisecom(config)#**running-config from interface gpon-olt** *slot-id/port-id* **to interface gpon-olt** *slot-id/port-id* [ **clear-source** ] | Cut the GPON interface. |
| | Raisecom(config)#**running-config from port-channel** *group-id* **to port-channel** *group-id* [ **clear-source** ] | Cut the LAG interface. |

**Note**

When enabling interface service cutting, pay attention to the following matters:

- Types of the source and destination interfaces should be consistent and they cannot be the same one.
- The source and destination interfaces cannot belong to any interface backup group, uplink interface protection group, or PON protection group.
- When cutting the GPON interface, there cannot be any online ONU under the destination PON interface.

### 1.5.9 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show interface** { **gpon-olt** \| **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/olt-id* | Show interface status, including enabling/disabling status, rate, duplex mode, and forwarding mode. |
| 2 | Raisecom#**show interface** { **gpon-olt** \| **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/olt-id* **description** | Show descriptions of a specified physical interface. |
| 3 | Raisecom#**show interface** { **gpon-olt** \| **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/olt-id* **statistics** | Show interface statistics. |
| 4 | Raisecom#**show interface** { **gpon-olt** \| **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/olt-id* **flowcontrol** | Show flow control information about the interface. |
| 5 | Raisecom#**show system mtu** | Show the maximum length of forwarding frame. |
| 6 | Raisecom#**show management-port** [ **ip-address** ] | Show information about the out-of-band network management interface. |
| 8 | Raisecom#**show interface vlanif** [ *vlan-id* ] [ **detail** ] | Show VLAN interface configurations. |
| 9 | Raisecom#**show interface vlanif** [ *vlan-id* ] **statistics** | Show VLAN interface statistics. |

## 1.6 Managing time

### 1.6.1 Default configurations

Default configurations of time management on the ISCOM5508-GP 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 |

| Function | Default value |
|---|---|
| Default DST | Disable |
| IP address of NTP server | 0.0.0.0 |
| IP address of NTP symmetric peer | 0.0.0.0 |
| NTP mode | Slave |
| SNTP Client | Disable |
| IP address of SNTP server | 224.0.1.1 |

## 1.6.2 Configuring time and time zone

### Configuring time

Configure the ISCOM5508-GP 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 ISCOM5508-GP as below.

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

## 1.6.3 Configuring DST

Daylight Saving Time (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 ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**clock summer-time** | Enable DST.<br>Use the **no clock summer-time** command to disable DST. |

| Step | Command | Description |
|---|---|---|
| 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 DST.<br>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 advance the clock one hour faster 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 ISCOM5508-GP can provide different applications over a unified time. Meanwhile, NTP can ensure very high accuracy, with accuracy of 10ms around.

The ISCOM5508-GP in support of NTP cannot only accept synchronization from other clock source, but also synchronize other devices as a clock source.

The ISCOM5508-GP adopts multiple NTP working modes for time synchronization:

- Server mode

In this mode, the ISCOM5508-GP 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 ISCOM5508-GP 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 ISCOM5508-GP as below.

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

**Note**

If the ISCOM5508-GP is configured as the NTP reference clock source, it cannot be configured as the NTP server 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 for the ISCOM5508-GP to synchronize its system time with the SNTP server, thus realizing time synchronization on the whole network.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**sntp-client** | Enable SNTP Client.<br>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.<br>You can use the **no sntp-client server** command to restore default configurations. |

SNTP and NTP are mutually exclusive.

### 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 ISCOM5508-GP 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 corrcupted 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 Configuring server

The ISCOM5508-GP supports upgrade and backup through the FTP/TFTP server.

Before upgrading system software through FTP/TFTP, you should build a FTP/TFTP environment. Basic requirements are as below:

- The ISCOM5508-GP is connected to the FTP/TFTP server correctly.
- Configure the FTP/TFTP server and ensure the server can be accessed.
- Configure related parameters of the FTP/TFTP server on the ISCOM5508-GP to enable it to access the FTP/TFTP server.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**ftp** *ip-address username password* | Configure the IPv4 parameters of the FTP. |
| 2 | Raisecom#**ftp** *ipv6-address* [ **scopeid** *scopeid-id* ] *username password* | Configure the IPv6 parameters of the FTP. |
| 3 | Raisecom#**tftp** *ip-address* | Configure the IPv4 parameters of the TFTP. |
| 4 | Raisecom#**tftp** *ipv6-address* [ **scopeid** *scopeid-id* ] | Configure the IPv6 parameters of the TFTP. |

## 1.7.3 Upgrading system files

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**download** { **mainrom1** \| **mainrom2** \| **system1** \| **system2** \| **cpld** \| **startup-config** } **ftp** *ip-address username password filename* **slot 1** | (Optional) upgrade the system boot file or startup file through FTP. |
| | Raisecom#**download** { **mainrom1** \| **mainrom2** \| **system1** \| **system2** \| **cpld** \| **startup-config** } **tftp** *ip-address filename* **slot 1** | (Optional) upgrade the system boot file or startup file through TFTP. |
| 2 | Raisecom#**commit** { **mainrom1** \| **mainrom2** \| **system1** \| **system2** } | Specify the version of the system software or startup software to be loaded.<br>**Note**<br>After specifying the version, you need to reboot the ISCOM5508-GP to switch to the specified version. |
| 3 | Raisecom#**write startup-config** | Save the current configurations. |
| 4 | Raisecom#**erase startup-config** | (Optional) clear the current system configuration file.<br>**Caution**<br>Clearing the system configuration file may lead to service interruption. Use this command with caution. |

## 1.7.4 Backing up system files

Configure the ISCOM5508-GP as below.

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

| Step | Command | Description |
|---|---|---|
| 2 | Raisecom#**upload history-cmd ftp** *ip-address username password filename* | (Optional) back up the historical operation file through FTP. |

## 1.7.5 Configuring auto-save

The ISCOM5508-GP supports the auto-save feature. This feature can avoid loss of system configurations due to human carelessness, such as forgetting to save the configuration.

Configure the ISCOM5508-GP as below.

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

## 1.7.6 Configuring ONU auto-upgrade

ONU auto-upgrade refers that you can configure a specified ONU to automatically download files to be upgraded from the FTP/TFTP server at a specified time and then upgrade these files in batch. This function facilitates manage and maintain ONUs connected to OLTs in batch.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**auto-upgrade** { **enable** \| **disable** } | Enable/Disable auto-upgrade. |
| 3 | Raisecom(config)#**auto-upgrade time** *start-time* | Configure the time for executing auto-upgrade. You can use the **no auto-upgrade time** command to restore the default value. |
| 4 | Raisecom(config)#**auto-upgrade add device-type** *onu-type* { **ftp** *ip-address username password filename* \| **tftp** *ip-address filename* } | Add an auto-upgrade plan (based on FTP/TFTP). |
| | Raisecom(config)#**auto-upgrade delete device-type** *onu-type* | (Optional) delete an auto-upgrade plan. |
| 5 | Raisecom(config)#**auto-upgrade device-type** { *type-name* **now** \| **all** } | Perform auto-upgrade on specified ONUs or all ONUs immediately. |

## 1.7.7 Configuring ONU performance template

The file name of the ONU performance template in the OLT system is onu-template.ini. The template contains the manageable ONU models and remote management performance differences of those ONU models.

By upgrading the ONU performance template, you can enable the OLT to manage more ONU models.

The ONU performance template is the basis for the OLT to remotely manage the ONU. We do not recommend modifying and downloading the template.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**download onu-template** { **ftp** *ip-address username password filename* \| **tftp** *ip-address filename* } | (Optional) download the ONU performance template through FTP/TFTP. |
| 2 | Raisecom#**upload onu-template** { **ftp** *ip-address username password filename* \| **tftp** *ip-address filename* } | (Optional) back up the ONU performance template through FTP/TFTP. |

## 1.7.8 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show** { **ftp** \| **tftp** } | Show FTP/TFTP default configuration parameters. |
| 2 | Raisecom#**show startup-config** | Show configurations loaded upon the startup of the device. |
| 3 | Raisecom#**show running-config** | Show running configurations of the device. |
| 4 | Raisecom#**show version** | Show versions of the system. |
| 5 | Raisecom#**show version** [ **slot** *slot-id* \| **gpon-onu** *slot-id/olt-id/onu-list* ] | Show the specified slot or ONU version. |
| 6 | Raisecom#**show auto-write** | Show configurations of auto-save. |
| 7 | Raisecom#**show auto-upgrade information** | Show configurations of auto-upgrade and operation information. |

# 1.8 Task scheduling

## 1.8.1 Introduction

When you need to use some commands periodically or at a specified time, configure task scheduling.

The ISCOM5508-GP supports realizing task scheduling by combining a schedule list to command lines. You just need to specify the start time, interval, and end time of the task in the schedule list, and then bind the schedule list to command lines to realize the periodic execution of command lines.

## 1.8.2 Default configurations

N/A

## 1.8.3 Configuring task scheduling

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**schedule-list** *number* **start** { **up-time** *days time* [ **every** *days time* [ **stop** *days time* ]] \| **date-time** *date time* [ **every** { **day** \| **week** \| *days time* } [ **stop** *date time* ] ] } | Add or modify entries in the schedule list, including the start time, interval, and end time of the task.<br>You can use the **no schedule-list** *list-no* command to delete the schedule list. |
| 3 | Raisecom(config)#*command-string* **schedule-list** *number* | Add commands to the schedule list.<br>You can use the **no schedule-list** *list-no* **command** *cmd-no* command to delete commands in the schedule list. |

## 1.8.4 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show schedule-list** | Show configurations of the schedule list. |

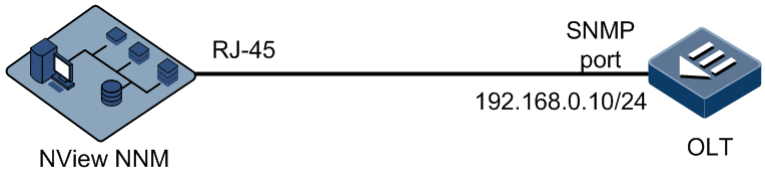
# 1.9 Configuration examples

## 1.9.1 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
VRF                            IF         Address         NetMask
-------------------------------------------------------------------------
Default-IP-Routing-Table    mottsec0    192.168.0.10   255.255.255.0
```

## 1.9.2 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 Layer 3 IP address 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 gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:1)#switchport trunk allowed vlan 2
Raisecom(config-if-gigabitethernet-1:1)#exit
```

Step 2 Configure the IP address of the Layer 3 IP interface and associate it with the VLAN ID.

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

## Checking results

Show the IP address of the Layer 3 IP interface.

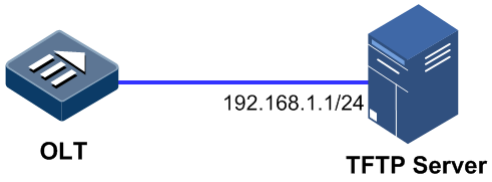
```
Raisecom#show interface vlanif
VRF                          IF                Address        NetMask
-------------------------------------------------------------------------------
Default-IP-Routing-Table  vlan2             192.168.0.1   255.255.255.0
```

# 1.9.3 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 ISCOM5508B-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 ISCOM5508B-
ROAP_2.41.1_20150611
```

Step 2 Write the configured file to the memory.

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

Step 3 Reboot the ISCOM5508-GP and it will automatically load the downloaded system startup file.

```
Raisecom#reboot
```

## Checking results

Show OLT versions.

```
Raisecom#show version
   Copyright (c) 2010-2012 Raisecom Technology Co., Ltd .
   Slot ID: 1
      Card Type        : ISCOM5508-GPSC
      Product  Version  : --
      System1  Version  : ISCOM5508B_ROAP_2.41.1_20150611
   (active)  (committed)
      System2  Version  : ISCOM5508B_ROAP_2.3.2_20130607
      Bootrom  Version  : ISCOM5508B_FLASH_BOOTROM_2.0.2_20130607
      Firmware1 Version  : --
      Firmware2 Version  : --
      CPLD     Version  : V1.0
      Mainrom1  Version  : ISCOM5508B_FLASH_BOOTROM_2.0.2_20130607
(active)  (committed)
      Mainrom2  Version  : ISCOM5508B_FLASH_BOOTROM_2.0.2_20130607
      Active   Version  : ISCOM5508B_ROAP_2.2.2_20130607
      System   Uptime   : 0 days, 9 hours, 57 minutes
```

# 1.9.4 Example for configuring ONU auo-upgrade

## Networking requirements

As shown in Figure 1-8, the ONU auto-upgrade feature can periodically upgrade the ONU remotely according to configurations. Basic requirements are as below:

- IP address of the TFTP server: 192.168.1.1/24
- ONU type: ISCOM5304
- Auto-upgrade time: 2:00 a.m.
- Auto-upgrade system file: startup_config

Figure 1-8 Configuring ONU auto-upgrade


## Configuration steps

Step 1 Configure the IP address of the TFTP server and add an auto-upgrade configuration program.

```
Raisecom#config
Raisecom(config)#auto-upgrade add device-type 5304 tftp 192.168.1.1
startup_config
```

Step 2 Configure the start time of auto-upgrade to 2:00 am.

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

Step 3 Enable auto-upgrade.

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

## Checking results

Show auto-upgrade configurations and operation information.

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

# 1.9.5 Example for refining user privileges

## Networking requirements

To refining user privileges, create a common set cmd1, which contains the level 15 command, **create vlan** *vlan-id*. Create a level 10 user, user 1; and allow the user to execute commands in cmd1.

## Configuration steps

Step 1 Create a command set cmd1 and add related commands to the command set.

```
Raisecom#command-set cmd1
Raisecom(command-set:cmd1)#command “create vlan”
Raisecom(command-set:cmd1)#exit
```

Step 2 Create user1 and specify the user privilege to 10.

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

Step 3 Configure the privilege of user1 in cmd1.

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

## Checking results

Show details of user1.

```
Raisecom#show user detail
Username: raisecom
Priority: 15
Server:  Local
Userstatus: online

Username: user1
Priority: 10
Server:  Local
Userstatus: offline
User command control config:
Type     Command set name
-----------------------------------
allow    cmd1
```

# 2 Configuring GPON services

This chapter introduces GPON services and the configuration process of the ISCOM5508-GP, and provides related configurations examples, including the following sections:

- Overview of GPON services
- Configuring registration and deregistration
- Configuring GPON interface
- Configuring key update
- Configuring alarm profile
- Configuring DBA profile
- Configuring line profile
- Configuring service profile
- Configuring rate limiting profile
- Configuring VoIP profile
- Configuring SIP dial plan profile
- Managing GPON ONU

## 2.1 Overview of GPON services

### 2.1.1 GPON system

The Gigabit Passive Optical Network (GPON) system adopts the point-to-multipoint network topology and uses fiber to achieve full access and rapid transmission of data, voice, and video services.

The classical GPON system consists of the following three parts:

- Optical Line Terminal (OLT): it is a switch/router, as well as a multi-service platform. It provides fiber interfaces for the PON. The OLT is the core component of the GPON system.
- Optical Network Unit (ONU) or Optical Network Termination (ONT): it is a user-side device in the PON system. It provides various physical interfaces and broadband services.

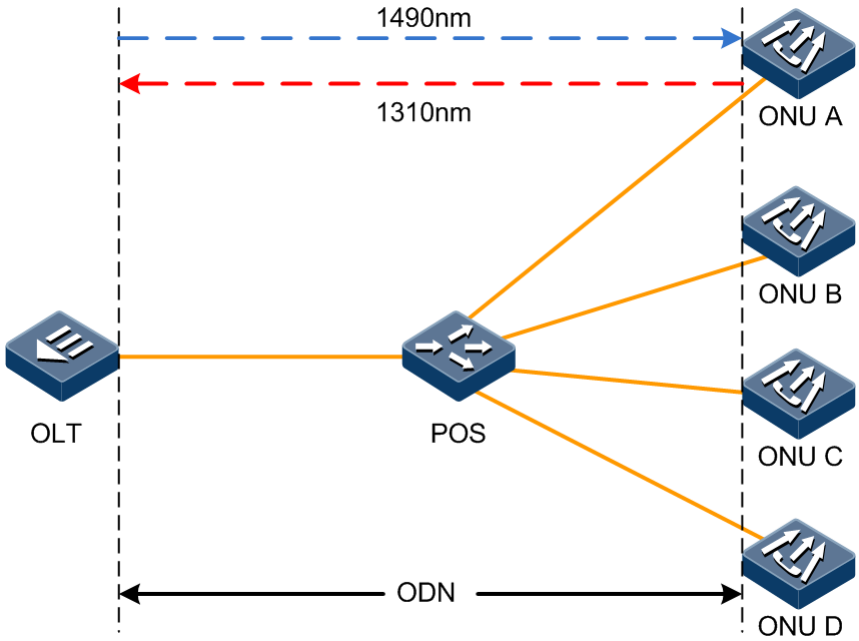
- Optical Distribution Network (ODN): it is composed of the Passive Optical Splitter (POS) and fiber. The POS is used to connect the OLT and ONU, and distribute downlink data and integrate uplink data.

The GPON complies with the ITU-T G.984.x standard, with the downlink rate to 1.2 Gbit/s or 2.4 Gbit/s and the uplink rate to 155 Mbit/s, 622 Mbit/s, 1.2 Gbit/s, or 2.4 Gbit/s.

## 2.1.2 GPON principle

Figure 2-1 shows the principle of GPON.

Figure 2-1 Principle of GPON



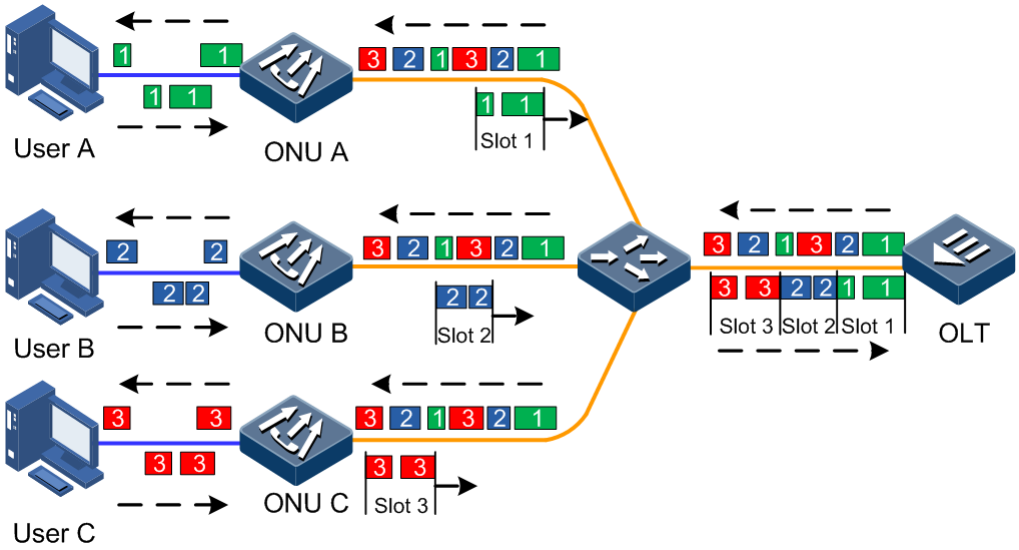

The GPON adopts the optical transmission method of single-fiber Wavelength Division Multiplexing (WDM), and complies with the wavelength distribution defined by the ITU-T G.984.2, of which the uplink wavelength is 1310 nm and the downlink wavelength is 1490 nm. Thus, it realizes single-fiber bidirectional data transmission to ONUs.

To split bidirectional signals from multiple users on the same fiber, adopt the following two multiplexing technologies:

- For downlink data traffic, adopt the broadcast technology. Each ONU receives data belonging to itself only and the transmission rate is 2.4 Gbit/s.
- For uplink data traffic, adopt the TDMA technology. Each ONU sends data in the specified timeslot and the transmission rate is 1.2 Gbit/s.

Figure 2-2 shows the principle of GPON uplink and downlink transmission.

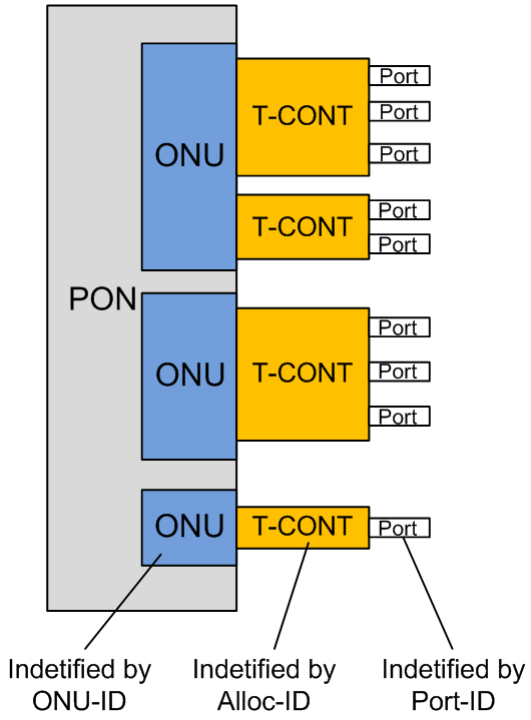
Figure 2-2 Principle of GPON uplink and downlink transmission




## 2.1.3 Basic principle

The ISCOM5508-GP works as an OLT on the GPON, and is connected downlink to ONUs. The OLT communicate with the ONU through transmitting the G-PON Encapsulation Method (GEM) frame. The GEM frame is identified by the GEM Port-ID, and is carried by T-CONT in the uplink direction, as shown in Figure 2-3.

Figure 2-3 GPON multiplexing structure (GEM)



### T-CONT

The GPON uses T-CONT to realize service aggregation. T-CONT is the most basic control unit for uplink service traffic in the GPON system. One T-CONT corresponds to one bandwidth type of service traffic. Each bandwidth type of service traffic has its own QoS features, mainly reflecting on the bandwidth assurance, such as, fixed bandwidth, assured bandwidth, assured/non-assured bandwidth, best-effort, hybrid mode (corresponding to Type 1 to Type 5 in Table 2-1).

Table 2-1 T-CONT types

| Bandwidth type | Delay-sensitive | Allocation mode | T-CONT type | | | | |
|---|---|---|---|---|---|---|---|
| | | | Type 1 | Type 2 | Type 3 | Type 4 | Type 5 |
| Fixed | Yes | Provisioned | Yes | No | No | No | Yes |
| Assured | No | Provisioned | No | Yes | Yes | No | Yes |
| Non-assured | No | Dynamic | No | No | Yes | No | Yes |
| Best-effort | Yes | Dynamic | No | No | No | No | Yes |

Each T-CONT is identified by the unique Alloc-ID, ranging from 0 to 4095. The Alloc-ID is globally allocated by the OLT, that is, each ONU under an OLT cannot use the T-CONT with the identical Alloc-ID.

### GEM port

Each T-CONT is composed of one or multiple GEM ports. Each GEM port transmits one kind of service traffic. So one T-CONT can carry one or multiple kinds of service traffic through the GEM port.

Each GEM port is identified by the unique Port-ID, ranging from 0 to 4095. The Port-ID is globally allocated by the OLT, that is, you cannot use the GEM port with identical Port-ID under the same PON interface.

The GEM port is used to identify the service virtual channel between the OLT and ONU, that is, the channel to carry services, which is similar to the VPI/VCI in the ATM virtual connection.

# 2.2 Configuring registration and deregistration

## 2.2.1 Default configurations

Default configurations of registration and deregistration on the ISCOM5508-GP are as below.

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

# 2.2.2 Configuring ONU registration

## Configuring ONU registration distance

Configure the ISCOM5508-GP 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-*:*)#**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. |
| 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 auto-registration mode. |
| 4 | Raisecom(config-if-gpon-olt-*:*)#**auto-authorization line-profile-id** *profile-id* | Configure the line profile for ONU auto-registration. |
| 5 | Raisecom(config-if-gpon-olt-*:*)#**auto-authorization service-profile-id** [ **add** \| **remove** ] *profile-id* | Configure the service profile for ONU auto-registration. |

## Creating ONU manually

Configure the ISCOM5508-GP 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-*:*)#**authorization mode** { **loid** \| **loid-checkcode** \| **sn** \| **sn-password** \| **password** } | Configure the ONU registration mode.<br>You can use the **no authorization mode** command to restore default configurations. |

| Step | Command | Description |
|---|---|---|
| 4 | Raisecom(config-if-gpon-olt-*:*)#**create gpon-onu** [ *onu-id* ] **sn** *snstring* [ **password** *password* ] { **line-profile-id** *line-profile-id* \| **line-profile-name** *line-profile-name* } { **service-profile-id** *service-profile-id* \| **service-profile-name** *service-profile-name* } | (Optional) create the ONU registered based on the SN or SN+PASSWORD, and bind the corresponding line profile and service profile.<br>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* { **line-profile-id** *line-profile-id* \| **line-profile-name** *line-profile-name* } { **service-profile-id** *service-profile-id* \| **service-profile-name** *service-profile-name* } | (Optional) create the ONU registered based on the PASSWORD, and bind the corresponding line profile and service profile.<br>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* ] { **line-profile-id** *line-profile-id* \| **line-profile-name** *line-profile-name* } { **service-profile-id** *service-profile-id* \| **service-profile-name** *service-profile-name* } | (Optional) create the ONU registered based LOID or LOID+CHECKCODE, and bind the corresponding line profile and service profile.<br>You can use the **no create gpon-onu** *onu-id* command to delete the ONU. |

## 2.2.3 Configuring ONU deregistration

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.

Configure the ISCOM5508-GP 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 remote management configuration mode. |
| 3 | Raisecom(config-if-gpon-onu-*/*:*)#**deregister** | Configure ONU deregistration. |

## 2.2.4 Activating ONU

### Activating all ONUs

Configure the ISCOM5508-GP 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. |

| Step | Command | Description |
|---|---|---|
| 3 | Raisecom(config-if-gpon-olt-*:*)#**active all-suspend-onu** | Activate all ONUs in suspended status.<br>**Note**<br>When the ONU is activated, it will restart the registration process. |

Activating single ONU

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

## 2.2.5 Clearing illegal ONU information

Configure the ISCOM5508-GP 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-*:*)#**clear illegal-onu** | Clear information about illegal ONUs. |

## 2.2.6 Checking configurations

Use the following commands to check configuration results.

| Step | 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 ONU registration information based on SN. |
| 3 | Raisecom#**show interface gpon-onu** *slot-id/olt-id/onu-id* **loid** | Show ONU registration information based on LOID. |
| 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. |

| Step | Command | Description |
|---|---|---|
| 6 | Raisecom#**show interface gpon-olt** *slot-id/olt-id* **illegal-onu** | Show information about illegal ONU registration under a GPON interface. |

# 2.3 Configuring GPON interface

## 2.3.1 Default configurations

Default configurations of GPON interface on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| FEC in downstream direction | Disable |
| GPON interface bound alarm profile | 1 |
| GEM port used by broadcast, unknown multicast, and unknown unicast packets | 4095 |
| GEM port used by multicast packets | 4094 |

## 2.3.2 Configuring GPON interface

Configure the ISCOM5508-GP 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 in downstream direction. |
| 4 | Raisecom(config-if-gpon-olt-*:*)#**multicast gemport** *port-id* | (Optional) configure the GEM port used by multicast packets.<br>You can use the **no multicast gemport** command to restore default configurations. |
| 5 | Raisecom(config-if-gpon-olt-*:*)#**reset** | (Optional) reset the GPON interface.<br>**Note**<br>When the ISCOM5508-GP fails, you can use this command to reset the interface to resume services. |

### 2.3.3 Checking configurations

Use the following commands to check configuration results.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**show interface gpon-olt** *slot-id/olt-id* **basic information** | Show GPON interface configurations. |

## 2.4 Configuring key update

### 2.4.1 Default configurations

Default configurations of key update on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Key update | Disable |
| Key update period | 10min |

### 2.4.2 Configuring key update

Configure the ISCOM5508-GP as below.

| Step | 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 key update period. |

### 2.4.3 Checking configurations

Use the following commands to check configuration results.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**show gpon-slot** *slot-id* **encryption key-update** | Show key update configurations. |

# 2.5 Configuring alarm profile

## 2.5.1 Default configurations

### Default configurations of OLT alarm profile

Default configurations of the OLT alarm profile with a default ID of 1 on the ISCOM5508-GP 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 |
| ONU laser-always-on alarm | Disable |
| ONU laser-always-on alarm threshold | 12 |

## Default configurations of ONU alarm profile

Default configurations of the ONU alarm profile with a default ID of 1 on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Alarm profile ID | 1 |
| Alarm profile name | profile-1 |
| GEM port packet loss alarm threshold | 0 |
| GEM port packet mistransmission alarm threshold | 0 |
| GEM port impaired data block alarm threshold | 0 |
| FCS error frame alarm threshold | 0 |
| Excessive collision frame alarm threshold | 0 |
| Tx delay collision alarm threshold | 0 |
| Oversized frame alarm threshold | 0 |
| Rx buffer overflow alarm threshold | 0 |
| Tx buffer overflow alarm threshold | 0 |
| Single-collision Tx frame alarm threshold | 0 |
| Multi-collision Tx frame alarm threshold | 0 |
| Synchronous queue element test error alarm threshold | 0 |
| Delay frame alarm threshold | 0 |
| Alarm threshold of Tx failure frame due to MAC sub-layer transmission error | 0 |
| Carrier sense loss error alarm threshold | 0 |
| Unaligned frame alarm threshold | 0 |
| Alarm threshold of Rx failure frame due to MAC sub-layer receiving error | 0 |
| Alarm threshold of discarded frame due to PPPoE frame filtering | 0 |
| Alarm threshold of discarded frame event due to resource shortage | 0 |
| Undersized frame alarm threshold | 0 |
| Fragment alarm threshold | 0 |
| Jabber frame alarm threshold | 0 |
| Alarm threshold of discarded frame due to timeout | 0 |
| Alarm threshold of discarded frame due to oversized MTU | 0 |

| Function | Default value |
|---|---|
| Rx error frame alarm threshold | 0 |
| FEC corrected byte alarm threshold | 0 |
| FEC corrected code word alarm threshold | 0 |
| FEC uncorrected code word alarm threshold | 0 |
| FEC duration alarm threshold | 0 |

## 2.5.2 Configuring OLT alarm profile

### Configuring OLT alarm profile

Configure the ISCOM5508-GP as below.

| 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.<br>You can use the **no snmp-trap-gpon-olt-profile** *profile-id* command to delete the profile.<br>**Note**<br>If the profile exists, enter profile configuration mode directly.<br>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-frame-loss { enable \| disable }` | (Optional) enable/disable LOF alarm on the PON interface. |
| 6 | `Raisecom(config-snmp-trap-gpon-olt-profile:*)#onu-frame-loss { enable \| disable }` | (Optional) enable/disable ONU LOF alarm. |
| 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. |

| Step | Command | Description |
|---|---|---|
| 9 | Raisecom(config-snmp-trap-gpon-olt-profile:*)#**onu-remote-defect-indication** { **enable** \| **disable** } | (Optional) enable/disable ONU remote indication alarm. |
| 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 OLT alarm profile

Configure the ISCOM5508-GP 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-*:*)#**snmp-trap-gpon-olt-profile** *profile-id* | Configure the GPON interface bound alarm profile. |

## 2.5.3 Configuring ONU alarm profile

### Configuring ONU alarm profile

Configure the ISCOM5508-GP as below.

| 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.<br>You can use the **no snmp-trap-gpon-olt-profile** *profile-id* command to delete the profile. |
| 3 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**name** *profile-name* | (Optional) configure the name of the ONU alarm profile. |
| 4 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**gemport-lost-packets threshold** *value* | (Optional) configure GEM port packet loss alarm threshold. |
| 5 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**gemport-misinserted-packets threshold** *value* | (Optional) configure GEM port packet mistransmission alarm threshold. |
| 6 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**gemport-impaired-blocks threshold** *value* | (Optional) configure GEM port impaired data block alarm threshold. |
| 7 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**ethernet-fcs-error-packets threshold** *value* | (Optional) configure FCS error frame alarm threshold. |
| 8 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**ethernet-excessive-collision-packets threshold** *value* | (Optional) configure excessive collision frame alarm threshold. |
| 9 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**ethernet-late-collision-counter threshold** *value* | (Optional) configure Tx delay collision alarm threshold. |
| 10 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**ethernet-too-long-packets threshold** *value* | (Optional) configure oversized frame alarm threshold. |

| Step | Command | Description |
|---|---|---|
| 11 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**ethernet-rx-buffer-overflow-counter threshold** *value* | (Optional) configure Rx buffer overflow alarm threshold. |
| 12 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**ethernet-tx-buffer-overflow-counter threshold** *value* | (Optional) configure Tx buffer overflow alarm threshold. |
| 13 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**ethernet-single-collision-packets threshold** *value* | (Optional) configure single-collision Tx frame alarm threshold. |
| 14 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**ethernet-multiple-collision-packets threshold** *value* | (Optional) configure multi-collision Tx frame alarm threshold. |
| 15 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**ethernet-sqe-counter threshold** *value* | (Optional) configure synchronous queue element test error alarm threshold. |
| 16 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**ethernet-deferred-transmission-packets threshold** *value* | (Optional) configure delay frame alarm threshold. |
| 17 | Raisecom(config-snmp-trap-gpon-onu-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-snmp-trap-gpon-onu-profile:*)#**ethernet-carrier-sense-error-counter threshold** *value* | (Optional) configure carrier sense loss error alarm threshold. |
| 19 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**ethernet-alignment-error-packets threshold** *value* | (Optional) configure unaligned frame alarm threshold. |
| 20 | Raisecom(config-snmp-trap-gpon-onu-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-snmp-trap-gpon-onu-profile:*)#**ethernet-pppoe-filter-packets threshold** *value* | (Optional) configure alarm threshold of discarded frame due to PPPoE frame filtering. |
| 22 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**ethernet-drop-event-counter threshold** *value* | (Optional) configure alarm threshold of discarded frame event due to resource shortage |
| 23 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**ethernet-undersize-packets threshold** *value* | (Optional) configure undersized frame alarm threshold. |
| 24 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**ethernet-fragments-packets threshold** *value* | (Optional) configure fragment alarm threshold. |
| 25 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**ethernet-jabbers-packets threshold** *value* | (Optional) configure Jabber frame alarm threshold. |
| 26 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**mac-bridge-port-delay-exceeded-discard-packets threshold** *value* | (Optional) configure alarm threshold of discarded frame due to timeout. |
| 27 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**mac-bridge-port-mtu-exceeded-discard-packets threshold** *value* | (Optional) configure Alarm threshold of discarded frame due to oversized MTU. |

| Step | Command | Description |
|---|---|---|
| 28 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**mac-bridge-port-rx-error-discard-packets threshold** *value* | (Optional) configure Rx error frame alarm threshold. |
| 29 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**fec-corrected-bytes threshold** *value* | (Optional) configure FEC corrected byte alarm threshold. |
| 30 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**fec-corrected-code-words threshold** *value* | (Optional) configure FEC corrected code word alarm threshold. |
| 31 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**fec-uncorrected-code-words threshold** *value* | (Optional) configure FEC corrected code word alarm threshold. |
| 32 | Raisecom(config-snmp-trap-gpon-onu-profile:*)#**fec-seconds threshold** *value* | (Optional) configure FEC duration alarm threshold. |

### Binding ONU alarm profile

Configure the ISCOM5508-GP as below.

| 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.<br>You can use the **no snmp-trap-gpon-onu-profile** command to cancel the binding. |

## 2.5.4 Checking configurations

Use the following commands to check configuration results.

| Step | 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. |

# 2.6 Configuring DBA profile

## 2.6.1 Default configurations

Default configurations of the DBA profile with a default ID of 1 on the ISCOM5508-GP 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 | 1000 Kbit/s |
| Maximum bandwidth | 1000000 Kbit/s |

## 2.6.2 Creating DBA profile

Configure the ISCOM5508-GP as below.

| 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.<br>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.<br>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.<br>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.<br>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.<br>You can use the **no create dba-profile** *profile-id* command to delete the profile. |

The profile in use cannot be deleted.

## 2.6.3 Modifying DBA profile

Configure the ISCOM5508-GP as below.

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

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

## 2.6.4 Checking configurations

Use the following commands to check configuration results.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**show dba-profile** { **all** \| *profile-list* } | Show DBA profile configurations. |

# 2.7 Configuring line profile

## 2.7.1 Default configurations

N/A

## 2.7.2 Configuring line profile

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**gpon-onu-line-profile** *profile-id* | Create the line profile and enter line profile configuration mode.<br>You can use the **no gpon-onu-line-profile** *profile-id* command to delete the profile.<br>**Note**<br>If the profile exists, enter profile configuration mode directly.<br>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 name of the line profile. |
| 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 the GEM port and configure its binding relationship with T-CONT.<br>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 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* \| **ethernet** *port-id* **vlan** *vlan-id* [ **priority** *pri* ] \| **ethernet** *port-id* **priority** *pri* } | (Optional) configure mapping between the GEM port and ONU-side services.<br>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* **encryption** { **enable** \| **disable** } | (Optional) enable/disable GEM port encryption. |

| Step | Command | Description |
|---|---|---|
| 10 | Raisecom(config-gpon-onu-line-profile:*)#**gem** *gem-index* { **upstream** \| **downstream** } **policing-profile** *profile-id* | (Optional) bind the GEM port with the rate limiting profile to limit the rate of GEM port.<br>You can use the **no gem** *gem-index* { **upstream** \| **downstream** } **policing-profile** command to cancel the binding.<br>**Note**<br>For uplink rate limiting, support the maximum bandwidth and maximum burst size.<br>For downlink rate limiting, support the assured bandwidth and assured burst size, as well as maximum bandwidth and maximum burst size. |
| 11 | Raisecom(config-gpon-onu-line-profile:*)#**gem** *gem-index* **mac-address-learning limit** *count* | (Optional) configure MAC address learning limit on the GEM port.<br>You can use the **no gem** *gem-index* **mac-address-learning limit** command to restore default configurations. |
| 12 | Raisecom(config-gpon-onu-line-profile:*)#**create tcont** *tcont-id* **dba-profile** *profile-id* | (Optional) create the T-CONT and configure its binding relationship with the DBA profile.<br>You can use the **no create tcont** *tcont-id* command to delete the configuration. |
| 13 | Raisecom(config-gpon-onu-line-profile:*)#**tcont** *tcont-id* **dba-profile** *profile-id* | (Optional) configure the DBA profile bound to TCONT. |
| 14 | Raisecom(config-gpon-onu-line-profile:*)#**commit** | Commit the profile configurations to enable the profile.<br>**Caution**<br>In ONU line profile configuration mode, all modification to parameters takes effect only after you execute the **commit** command. |

## 2.7.3 Binding line profile

Configure the ISCOM5508-GP 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 remote management configuration mode. |
| 3 | Raisecom(config-if-gpon-onu-*/*:*)#**line-profile-id** *profile-id* | (Optional) change the line profile configured on the ONU through modifying the line profile ID. |
| | Raisecom(config-if-gpon-onu-*/*:*)#**line-profile-name** *profile-name* | (Optional) change the line profile configured on the ONU through modifying the line profile name. |

Note

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

### 2.7.4 Checking configurations

Use the following commands to check configuration results.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**show gpon-onu-line-profile** { **all** \| *profile-list* } | Show line profile configurations. |

## 2.8 Configuring service profile

### 2.8.1 Default configurations

N/A

### 2.8.2 Configuring service profile

#### Configuring global parameters

| 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.<br>You can use the **no gpon-onu-service-profile** *profile-id* command to delete the profile.<br>Note<br>● If the profile exists, enter profile configuration mode directly.<br>● If the profile does not exist, you need to create the profile first, and then enter profile 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:*)#**mac-address-table learning** { **enable** \| **disable** } | (Optional) enable/disable ONU dynamic MAC address learning. |

| Step | Command | Description |
|---|---|---|
| 5 | Raisecom(config-gpon-onu-service-profile:*)#**mac-address-table learning aging-time** *time* | (Optional) configure the aging time of ONU dynamic MAC addresses.<br>You can use the **no mac-address-table aging-time** command to restore default configurations. |
| 6 | Raisecom(config-gpon-onu-service-profile:*)#**mac-address-table dlf discard** { **enable** \| **disable** } | (Optional) enable/disable ONU DLF packet discard. |
| 7 | Raisecom(config-gpon-onu-service-profile:*)#**multicast mode** { **snooping** \| **ctrl-multicast** \| **transparent** } | (Optional) configure the ONU multicast mode.<br>You can use the **no multicast mode** command to restore default configurations. |
| 8 | Raisecom(config-gpon-onu-service-profile:*)#**multicast vlan** { **strip** \| **translation** \| **transparent** } | (Optional) configure the ONU processing policy on the downstream multicast VLAN.<br>You can use the **no multicast vlan** command to restore default configurations. |
| 9 | Raisecom(config-gpon-onu-service-profile:*)#**multicast vlan translation** *vlan-id* | (Optional) configure the destination VLAN ID for the ONU translating the downstream multicast VLAN. |
| 10 | Raisecom(config-gpon-onu-service-profile:*)#**igmp-forward** { **translation** *vlan-id* [ *priority* ] \| **transparent** \| **tag** *vlan-id* [ *priority* ] } | (Optional) configure the ONU processing policy on the upstream multicast VLAN. |
| 11 | Raisecom(config-gpon-onu-service-profile:*)#**igmp-version** { **v2** \| **v3** } | (Optional) configure the ONU IGMP version. |
| 12 | Raisecom(config-gpon-onu-service-profile:*)#**immediate-leave** { **enable** \| **disable** } | (Optional) configure ONU immediate-leave. |
| 13 | Raisecom(config-gpon-onu-service-profile:*)#**commit** | Commit the profile configurations to enable the profile.<br>**Caution**<br>In ONU service profile configuration mode, all modification to parameters takes effect only after you execute the **commit** command. |

## Configuring interface parameters

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

| Step | Command | Description |
|---|---|---|
| 2 | Raisecom(config)#**gpon-onu-service-profile** *profile-id* | Create a service profile and enter service profile configuration mode.<br>You can use the **no gpon-onu-service-profile** *profile-id* command to delete the profile.<br>**Note**<br>● If the profile exists, enter profile configuration mode directly.<br>● If the profile does not exist, you need to create the profile first, and then enter profile configuration mode. |
| 3 | 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, |
| 4 | Raisecom(config-gpon-onu-service-profile:*)#**switchport isolation** { **enable** \| **disable** } | (Optional) enable/disable ONU UNI interface isolation. |
| 5 | 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.<br>You can use the **no uni ethernet** *uni-id* **vlan mode** command to restore default configurations. |
| 6 | 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.<br>You can use the **no uni ethernet** *uni-id* **native vlan** command to restore default configurations. |
| 7 | Raisecom(config-gpon-onu-service-profile:*)#**uni ethernet** *uni-id* **vlan translation-rule** *rule-id* | (Optional) configure the VLAN translation rule of the ONU UNI.<br>You can use the **no uni ethernet** *uni-id* **vlan translation-rule** command to restore default configurations. |
| 8 | 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.<br>You can use the **no uni ethernet** *uni-id* **vlan aggregation-rule** command to restore default configurations. |
| 9 | Raisecom(config-gpon-onu-service-profile:*)#**uni ethernet** *uni-id* **vlan trunk allowed** *vlan-list* | (Optional) configure the allowed VLAN list on the ONU UNI in Trunk mode.<br>You can use the **no uni ethernet** *uni-id* **vlan trunk allowed** command to restore default configurations. |

| Step | Command | Description |
|---|---|---|
| 10 | Raisecom(config-gpon-onu-service-profile:*)#**uni ethernet** *uni-id* **mac-address-table threshold** { *value* \| **unlimited** } | (Optional) configure the MAC address threshold on the ONU UNI.<br>You can use the **no uni ethernet** *uni-id* **mac-address-table threshold** command to restore default configurations. |
| 11 | Raisecom(config-gpon-onu-service-profile:*)#**uni ethernet** *uni-id* **max-frame-size** *size* | (Optional) configure the maximum frame size on the ONU UNI.<br>You can use the **no uni ethernet** *uni-id* **max-frame-size** command to restore default configurations. |
| 12 | Raisecom(config-gpon-onu-service-profile:*)#**uni ethernet** *uni-id* { **ingress** \| **egress** } **policing-profile** *profile-id* | (Optional) bind the ONU UNI with the rate limiting profile.<br>You can use the **no uni ethernet** *uni-id* { **ingress** \| **egress** } **policing-profile** to delete the binding. |
| 13 | Raisecom(config-gpon-onu-service-profile:*)#**commit** | Commit the profile configurations to enable the profile.<br>**Caution**<br>In ONU service profile configuration mode, all modification to parameters takes effect only after you execute the **commit** command. |

## 2.8.3 Binding service profile

Configure the ISCOM5508-GP 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 remote management configuration mode. |
| 3 | Raisecom(config-if-gpon-onu-*/*:*)#**service-profile-id** *profile-id* | (Optional) change the service profile configured on the ONU through modifying the service profile ID. |
| | Raisecom(config-if-gpon-onu-*/*:*)#**service-profile-name** *profile-name* | (Optional) change the service profile configured on the ONU through modifying the service profile name. |

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

### 2.8.4 Checking configurations

Use the following commands to check configuration results.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**show gpon-onu-service-profile** { **all** \| *profile-list* } | Show service profile configurations. |

## 2.9 Configuring rate limiting profile

### 2.9.1 Default configurations

N/A

### 2.9.2 Configuring rate limiting profile

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**create policing-profile** *profile-id* **name** *profile-name* | Create the rate limiting profile.<br>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 limiting profile. |
| 4 | Raisecom(config)#**policing-profile** *profile-id* **cir** *cir* **pir** *pir* **cbs** *cbs* **pbs** *pbs* | Configure parameters of the rate limiting profile. |

### 2.9.3 Binding rate limiting profile

Configure the ISCOM5508-GP as below.

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

| Step | Command | Description |
|---|---|---|
| 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 the ONU UNI with the rate limiting profile.<br>You can use the **no policing-profile** { **ingress** \| **egress** } command to delete the binding. |

### 2.9.4 Checking configurations

Use the following commands to check configuration results.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**show policing-profile** { **all** \| *profile-list* } | Show rate limiting profile configurations. |

## 2.10 Configuring VoIP profile

### 2.10.1 Default configurations

N/A

### 2.10.2 Configuring VoIP profile

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**create access-code-profile** *profile-id* **name** *profile-name* | Create a VoIP profile. |
| 3 | Raisecom(config)#**access-code-profile** *profile-id* **attend-call-transfer** *string* | (Optional) configure the call transfer access code. |
| 4 | Raisecom(config)#**access-code-profile** *profile-id* **call-hold** *string* | (Optional) configure the call hold access code. |
| 5 | Raisecom(config)#**access-code-profile** *profile-id* **call-park** *string* | (Optional) configure the call park access code. |
| 6 | Raisecom(config)#**access-code-profile** *profile-id* **cid-activate** *string* | (Optional) configure the CID activation access code. |
| 7 | Raisecom(config)#**access-code-profile** *profile-id* **cid-deactivate** *string* | (Optional) configure the CID deactivation access code. |
| 8 | Raisecom(config)#**access-code-profile** *profile-id* **unattended-blind-call-transfer** *string* | (Optional) configure the unattended blind call transfer access code. |

### 2.10.3 Binding VoIP profile

| 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-*/*:*)#**access-code-profile** *profile-id* | Bind the ONU VoIP profile to the ONU POTS interface. |

### 2.10.4 Checking configurations

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show access-code-profile** { **all** \| *profile-list* } | Show VoIP profile configurations. |

## 2.11 Configuring SIP dial plan profile

### 2.11.1 Default configurations

N/A

### 2.11.2 Configuring SIP dial plan profile

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**create sip-dialplan** *profile-id* **name** *profile-name* | Create a SIP dial plan profile.<br>You can use the **no create sip-dialplan** *profile-id* command to delete the file. |
| 3 | Raisecom(config)#**name** *name* | (Optional) configure the name of the SIP dial plan profile. |
| 4 | Raisecom(config)# **sip-dialplan** *profile-id* **critical-dial-timeout** *value* | (Optional) configure the critical dial timeout. |
| 5 | Raisecom(config)# **sip-dialplan** *profile-id* **digit-map** *string* | (Optional) configure the digit-map string. |
| 6 | Raisecom(config)# **sip-dialplan** *profile-id* { **h248** \| **ncs-format** \| **not-defined** \| **vendor-specific** } | (Optional) configure the dial plan format. |
| 7 | Raisecom(config)# **sip-dialplan** *profile-id* **partial-dial-timeou***t value* | (Optional) configure the partial dial timeout. |

### 2.11.3 Binding SIP dial plan profile

| 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-*/*:*)#**sip-dialplan** *profile-id* | Bind the ONU SIP dial plan profile to the ONU POTS interface. |

### 2.11.4 Checking configurations

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show sip-dialplan** { **all** \| *profile-list* } | Show SIP dial plan profile configurations. |

## 2.12 Managing GPON ONU

### 2.12.1 Basic configurations

Configure the ISCOM5508-GP as below.

| 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) reboot the ONU.<br>**Note**<br>The system supports using the **reboot gpon-onu** [ **all** \| *slot-id/olt-id/onu-id* ] [ **now** ] command to reboot the ONU in privileged EXEC mode. |

Configure the ISCOM5508-GP as below.

| 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 remote management configuration mode. |
| 3 | Raisecom(config-if-gpon-onu-*/*:*)#**state** { **active** \| **suspend** } | Activate or suspend the ONU. |

## 2.12.2 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 management configuration mode. |
| 3 | Raisecom(config-gpon-onu-*/*:*)#**reboot** [ **now** ] | (Optional) reboot the ONU. |
| 4 | Raisecom(config-gpon-onu-*/*:*)#**mng-ip** { **dhcp** \| **static** } | (Optional) configure the ONU management IP configuration mode. |
| 5 | Raisecom(config-gpon-onu-*/*:*)#**mng-ip static address** *ip-address* [ **mask** *ip-mask* ] **default-gw** *ip-address* [ **primary-dns** *ip-address* ] [ **secondary-dns** *ip-address* ] **vlan** *vlan-id* [ **priority** *value* ] | (Optional) configure the management IP address of the ONU.<br>You can use the command to delete the management IP address. |
| 6 | Raisecom(config-gpon-onu-*/*:*)#**mng-ip vlan** *vlan-id* [ **priority** *id* ] | (Optional) configure the Layer 3 interface IP address of the ONU VLAN. |
| 7 | Raisecom(config-gpon-onu-*/*:*)#**h248 primary-mgc** *ip-address* [**secondary-mgc** *ip-address* ]{ **format** { **binary** \| **text-long** \| **text-short** } **tid-base** *string* **msg-id** *message* | (Optional) configure the ONU H.248 primary and secondary MGC information. |
| 8 | Raisecom(config-gpon-onu-*/*:*)#**onu-rx-power high-threshold** *value* **low-threshold** *value* | (Optional) configure the ONU Rx optical power alarm threshold. |
| 9 | Raisecom(config-gpon-onu-*/*:*)#**onu-tx-power high-threshold** *value* **low-threshold** *value* | (Optional) configure the ONU Tx optical power alarm threshold. |

Configure the following items on devices which need to be configured with ONU management parameters.

| 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 management configuration mode. |

| Step | Command | Description |
|---|---|---|
| 3 | Raisecom(config-if-gpon-onu-*/*:*)#**rebind sn** *sn* | (Optional) configure the ONU SN-based registration keyword. |
| 4 | Raisecom(config-if-gpon-onu-*/*:*)#**password** *password* | (Optional) configure the ONU Password-based registration keyword. |
| 5 | Raisecom(config-if-gpon-onu-*/*:*)#**loid checkcode** *checkcode* | (Optional) configure the ONU LOID-based registration keyword. |
| 6 | Raisecom(config-if-gpon-onu-*/*:*)#**mng-mode** { **omic** \| **snmp** } | (Optional) configure the ONU management mode. |

## 2.12.3 Configuring UNI

Configure the ISCOM5508-GP 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 GPON ONU UNI configuration mode. |
| 3 | Raisecom(config-if-gpon-onu-ethernet-*/*/*:*)#**shutdown** | (Optional) shut down the interface. |
| 4 | Raisecom(config-if-gpon-onu-ethernet-*/*/*:*)#**native vlan** *vlan-id* | (Optional) configure interface Native VLAN. |
| 5 | Raisecom(config-if-gpon-onu-ethernet-*/*/*:*)#**speed auto**<br>Raisecom(config-if-gpon-onu-ethernet-*/*/*:*)#**speed** { **10** \| **100** \| **1000** } **duplex** { **half** \| **full** } | (Optional) configure the rate and duplex mode of the interface. |
| 6 | Raisecom(config-if-gpon-onu-ethernet-*/*/*:*)#**loopback** { **enable** \| **disable** } | (Optional) enable/disable loopback detection on the interface. |
| 7 | Raisecom(config-if-gpon-onu-ethernet-*/*/*:*)#**flowcontrol** { **enable** \| **disable** } | (Optional) enable/disable flow control on the interface. |
| 8 | Raisecom(config-if-gpon-onu-ethernet-*/*/*:*)#**alarm-control** { **enable interval** *time* \| **disable** } | (Optional) enable/disable alarm inhibition on the interface. |
| 9 | Raisecom(config-if-gpon-onu-ethernet-*/*/*:*)#**pppoe-filter** { **enable** \| **disable** } | (Optional) enable/disable PPPoE packet filtering on the interface.<br>**Note**<br>When this function is enabled, the interface allows the PPPoE packet to pass. |
| 10 | Raisecom(config-if-gpon-onu-ethernet-*/*/*:*)#**poe pse** { **enable** \| **disable** } | (Optional) enable/disable interface PoE. |

# 2.12.4 Configuring RSTP

## Configuring global RSTP

Configure the ISCOM5508-GP as below.

| 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-*/*:*)#**spanning-tree** { **enable** \| **disable** } | Enable/Disable RSTP. |
| 4 | Raisecom(config-gpon-onu-*/*:*)#**spanning-tree priority** *value* | (Optional) configure ONU global priority. |
| 5 | Raisecom(config-gpon-onu-*/*:*)#**spanning-tree max-age** *time* | (Optional) configure the maximum lifetime of RSTP. |
| 6 | Raisecom(config-gpon-onu-*/*:*)#**spanning-tree hello-time** *time* | (Optional) configure the interval to send Hello packets. |
| 7 | Raisecom(config-gpon-onu-*/*:*)#**spanning-tree forward-delay** *time* | (Optional) configure the Forward Delay. |

## Configuring interface RSTP

Configure the ISCOM5508-GP 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 GPON ONU UNI configuration mode. |
| 3 | Raisecom(config-if-gpon-onu-ethernet-*/*/*:*)#**spanning-tree priority** *value* | (Optional) configure the UNI priority. |
| 4 | Raisecom(config-if-gpon-onu-ethernet-*/*/*:*)#**spanning-tree path-cost** *value* | (Optional) configure UNI path cost. |
| 5 | Raisecom(config-if-gpon-onu-ethernet-*/*/*:*)#**spanning-tree topology-change** { **enable** \| **disable** } | (Optional) enable/disable detection upon topology change. |

# 2.12.5 Configuring VoIP

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

| Step | Command | Description |
|---|---|---|
| 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-*/*:*)#**shutdown** | (Optional) shut down the POTS interface. |
| 4 | Raisecom(config-gpon-onu-*/*:*)#**codec-selection** { **cn** \| **div4-11025** \| **div4-16000** \| **div4-22050** \| **div4-8000** \| **g722** \| **g723** \| **g728** \| **g729** \| **gsm** \| **l16-2channels** \| **l16-channel** \| **lpc** \| **mpa** \| **pcma** \| **pcmu** \| **qcelp** } | (Optional) configure the coder/decoder. |
| 5 | Raisecom(config-gpon-onu-*/*:*)#**echo cancellation** { **enable** \| **disable** } | (Optional) configure echo cancellation. |
| 6 | Raisecom(config-gpon-onu-*/*:*)#**fax mode** { **t30** \| **t38** } | (Optional) configure the fax mode. |
| 7 | Raisecom(config-gpon-onu-*/*:*)#**hook-flash-time min** value **max** value | (Optional) configure the hook flash time. |
| 8 | Raisecom(config-gpon-onu-*/*:*)#**local-port** { **mix** *port-id* \| **max** *port-id* } | (Optional) configure the local interface. |
| 9 | Raisecom(config-gpon-onu-*/*:*)#**oob-dtmf** { **enable** \| **disable** } | (Optional) configure the out-of-band DTMF. |
| 10 | Raisecom(config-gpon-onu-*/*:*)#**packet-period** *value* | (Optional) configure the packet period. |
| 11 | Raisecom(config-gpon-onu-*/*:*)#**silence-suppression** { **enable** \| **disable** } | (Optional) configure the silence suppression. |
| 12 | Raisecom(config-gpon-onu-*/*:*)#**sip-agent sip-proxy** *name* **outbound** *name* **sip-registrar** *name* **primary-dns** *ip-address* **secondary-dns** *ip-address* | (Optional) configure the SIP Proxy. |
| 13 | Raisecom(config-gpon-onu-*/*:*)#**sip-agent reg-exp-time** *value* | (Optional) configure the SIP session registration expiration time. |
| 14 | Raisecom(config-gpon-onu-*/*:*)#**sip-agent url-format** { **sip** \| **tel** } | (Optional) configure the URL format. |
| 15 | Raisecom(config-gpon-onu-*/*:*)#**sip-user aor** *user-aor* **username** *name* **password** *password* | (Optional) configure the SIP user registration address. |
| 16 | Raisecom(config-gpon-onu-*/*:*)#**sip-user display-name** *name* | (Optional) configure the name of the SIP calling party. |
| 17 | Raisecom(config-gpon-onu-*/*:*)#**sip-user roh-time** *value* | (Optional) configure the off-hook time. |

## 2.12.6 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **information** | Show ONU basic information. |
| 2 | Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **detail-information** | Show ONU detailed information. |

| No. | Command | Description |
|---|---|---|
| 3 | Raisecom#**show version gpon-onu** *slot-id/olt-id/onu-id* | Show ONU version information. |
| 4 | Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **capability** | Show ONU capability information. |
| 5 | Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **fec** | Show ONU FEC configurations. |
| 6 | Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **mac-address-table l2-address** { **all** \| **dynamic** \| **static** } | Show the ONU MAC address table. |
| 7 | Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **mng-ip** | Show ONU management IP address configurations. |
| 8 | Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **onu-power-threshold** | Show the ONU power threshold. |
| 9 | Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **transceiver** | Show the ONU optical module information. |
| 10 | Raisecom#**show onu-remote vlan translation-rule-gpon** | Show created VLAN translation configurations on the ONU. |
| 11 | Raisecom#**show onu-remote vlan aggregation-rule-gpon** | Show created VLAN aggregation configurations on the ONU. |

## Showing ONU interface configurations

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **uni ethernet** [ *uni-id* ] **information** | Show ONU UNI configurations. |
| 2 | Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **uni ethernet** [ *uni-id* ] { **statistics** \| **statistics-15min** } | Show ONU UNI statistics. |
| 3 | Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **uni ethernet** [ *uni-id* ] **vlan** | Show ONU UNI VLAN configurations. |
| 4 | Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **mac-address-table l2-address uni ethernet** *port-id* | Show ONU UNI MAC address table. |
| 5 | Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **gemindex** [ *gem-index* ] **statistics-15min** | Show ONU GEM Port statistics. |
| 6 | Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **uni pots** [ *uni-id* ] **information** | Show ONU POTS interface configurations. |
| 7 | Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **uni pots** [ *uni-id* ] **line-status** | Show ONU POTS interface line status. |
| 8 | Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **uni pots** [ *uni-id* ] **media** | Show ONU POTS interface VoIP service configurations. |
| 9 | Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **uni pots** [ *uni-id* ] **sip-agent** | Show ONU POTS interface SIP Proxy configurations. |

| No. | Command | Description |
|---|---|---|
| 10 | Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **uni pots** [ *uni-id* ] **sip-user** | Show ONU POTS interface SIP user information. |
| 11 | Raisecom#**show gpon-onu** *slot-id/olt-id/onu-id* **uni pots** [ *uni-id* ] statistics rtp | Show ONU POTS interface Rx and Tx packet statistics. |

# 3 Configuring multicast services

This chapter introduces multicast services of the ISCOM5508-GP and configuration process, including the following sections:

- Overview of multicast services
- Configuring static multicast
- Configuring IGMP Snooping
- Configuring IGMP Proxy
- Configuring MVR
- Configuring dynamic controllable multicast
- Configuring MLD Snooping
- Configuring MLD Proxy
- Configuring multicast VLAN
- Maintenance

## 3.1 Overview of multicast services

### 3.1.1 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.

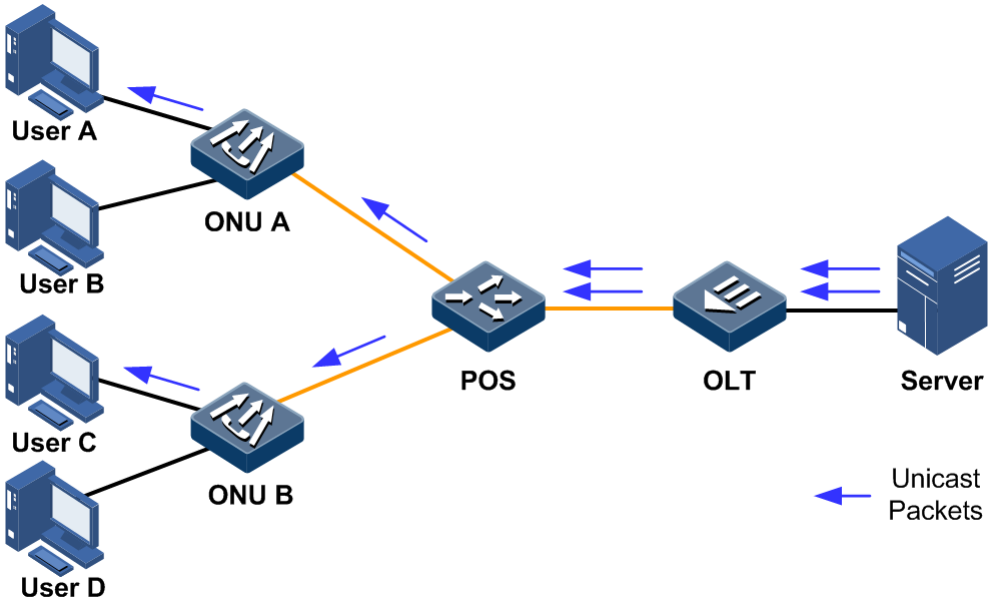
#### Comparisons among unicast, broadcast, and multicast

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 3-1, assume that User A and User C need a certain packet. 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.

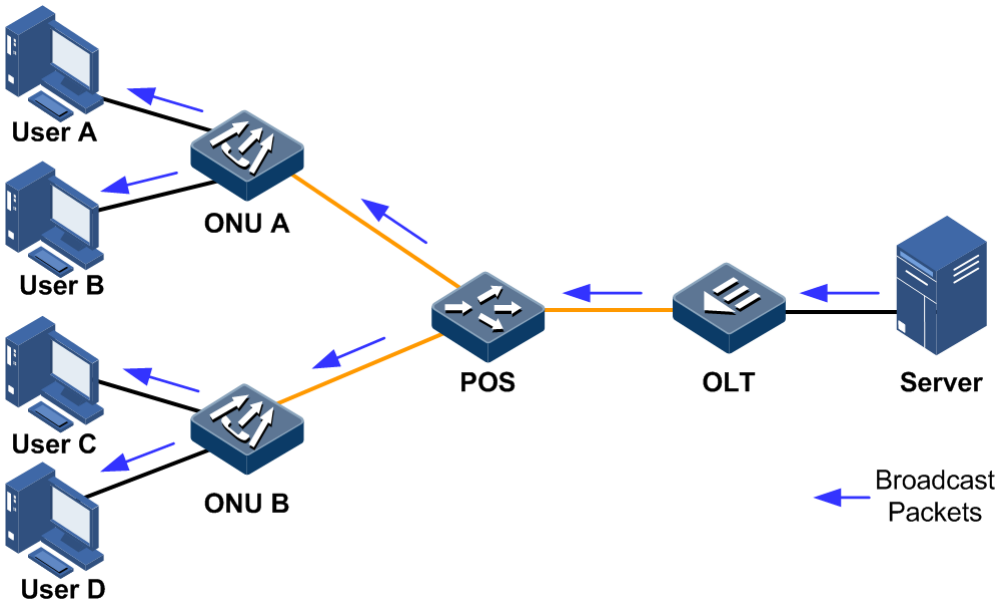
Figure 3-1 Unicast transmission mode




- 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 3-2, assume that User A and User C need a certain packet. In the broadcast transmission mode, the Server floods this packet through a router and all users (including User B) will also receive this packet. The security and non-gratuitousness of the packet cannot be ensured. In addition, network resources cannot be well utilized when few users need this packet.

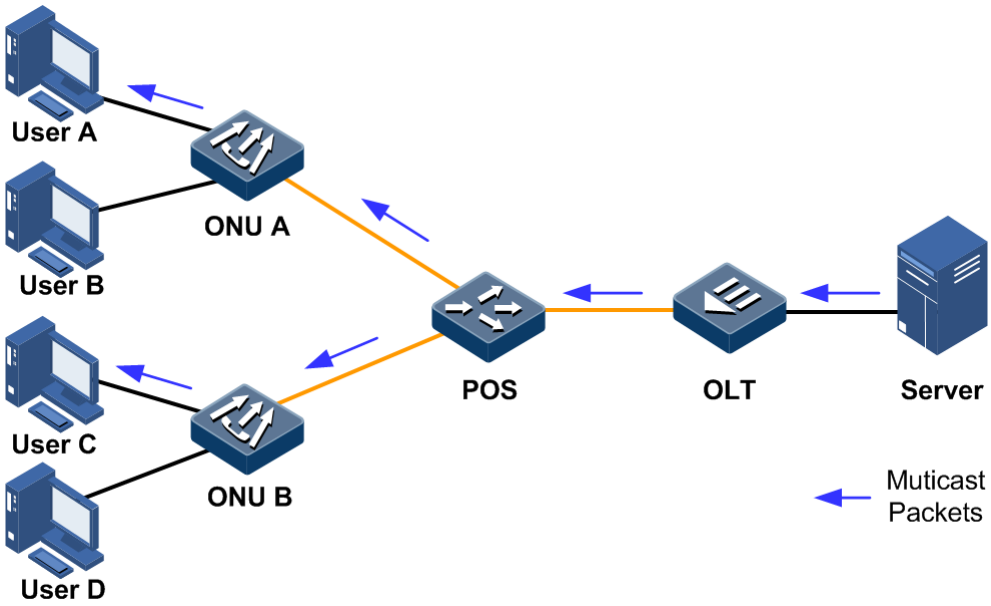
Figure 3-2 Broadcast transmission mode




- 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 3-3, 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 ISCOM5508-GP 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 3-3 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 ISCOM5508-GP 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, realize multicast routing, and to conduct forwarding multicast packets.
- Router interface: an interface on the ISCOM5508-GP, 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 ISCOM5508-GP. 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.

IPv6 multicast addresses are preceded with FF. The first 8 bits are set to 1. If the third hexadecimal number is set to 0, it indicates the IPv6 multicast address is a commonly-used multicast address. If it is set to 1, it indicates the IPv6 multicast address is a temporary multicast address. The fourth hexadecimal number indicates the multicast range. The remaining hexadecimal numbers indicate specific multicast groups.

- 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 3-4 shows the mapping relationship between an IPv4 multicast address and a multicast MAC address.

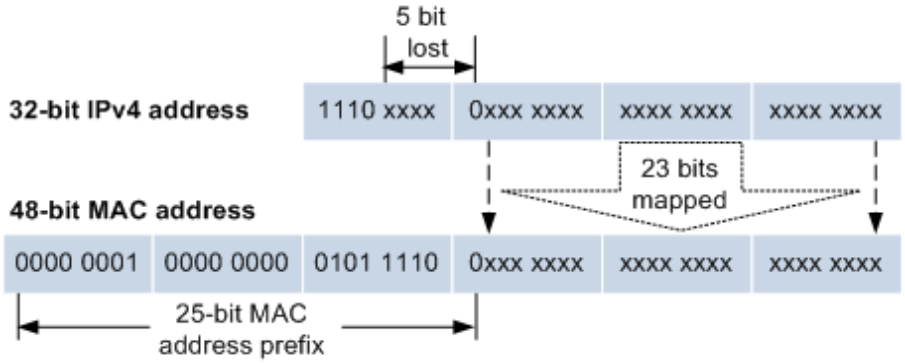



Figure 3-4 Mapping relationship between an IPv4 multicast address and a multicast MAC address

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 ISCOM5508-GP will receive other multicast data. These redundant multicast data will be filtered on the upper layer of the ISCOM5508-GP.

IPv6 multicast MAC addresses are preceded with 0x3333. The last 32 bits is related to the last 32 bits of an IPv6 multicast address. Finally, a 48-bit multicast MAC address is formed. For example, the IPv6 multicast address FF1E::F30E:101 is related to the multicast MAC address 33-33-F3-0E-01-01.

## 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 realize multicast services, you need to deploy various multicast protocols at different nodes of the network. These multicast protocols cooperate with each other to realize 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 3-5 shows operating positions of the IGMP and Layer 2 multicast protocols.

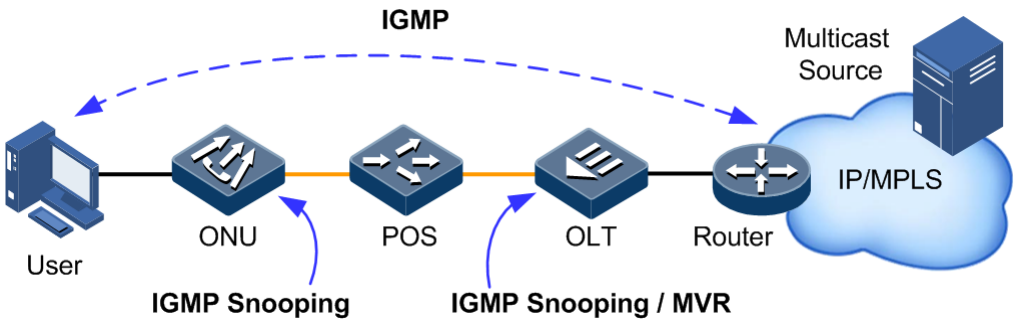


Figure 3-5 Operating positions of the IGMP and Layer 2 multicast protocols

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.

## 3.1.2 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 ISCOM5508-GP listens to an IGMP Report packet sent to a multicast group by a host, the ISCOM5508-GP will add the interface, which is connected to the host, to the forwarding table of the multicast group. Similarly, when the ISCOM5508-GP 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 ISCOM5508-GP will delete the interface from the multicast group.

IGMP Snooping forwards multicast data through Layer 2 multicast forwarding table. When the ISCOM5508-GP 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 either dynamically learn or manually configure the Layer 2 multicast forwarding table.

## 3.1.3 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.

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 ISCOM5508-GP 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 ISCOM5508-GP 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 ISCOM5508-GP 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.

## 3.1.4 MVR

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

By configuring multicast VLANs, MVR adds member ports of different Customer VLAN (CVLAN) of the ISCOM5508-GP 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.

### 3.1.5 Dynamic controllable multicast

In the Gigabit Passive Optical Network (GPON), dynamic controllable multicasts forward multicast services in a form of SCB+IGMP. The ISCOM5508-GP 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.

## 3.2 Configuring static multicast

### 3.2.1 Preparing for configurations

#### Scenario

The ISCOM5508-GP supports 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

## 3.2.2 Default configurations

N/A

## 3.2.3 Configuring static multicast

The ISCOM5508-GP adds the member interface to the multicast routing table by identifying the IGMP packet sent by the host automatically. You can manually configure the ISCOM5508-GP to add member interfaces for a specified multicast routing table.

Configure the ISCOM5508-GP as below.

| 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* \| **gigabitethernet***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** { **gpon-olt** *slot-id/olt-id* \| **gigabitethernet** *slot-id/olt-id* \| **ten-gigabitethernet** *slot-id/olt-id* \|**port-channel** *group-id*} | (Optional) add/remove an entry to/from a static multicast MAC address table. |

## 3.2.4 Configuring unknown multicat filter

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**mac-address-table unknown-multicast filter vlanlist** *vlan-list* | (Optional) configure the VLAN list for unknown multicast filter. |

## 3.2.5 Checking configurations

Use the following commands to check configuration results.

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

# 3.3 Configuring IGMP Snooping

## 3.3.1 Preparing for configurations

### Scenario

If multiple ONU users need to receive data from the multicast source, you can enable IGMP Snooping on the ISCOM5508-GP or ONU, and create and maintain the multicast forwarding table 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 ISCOM5508-GP to achieve multicast information distribution based on PON interface.
- Create a multicast forwarding table recording the corresponding relationship between the multicast packet and UNI interface on the ONU to achieve multicast information distribution based on UNI interface.

### Prerequisite

Create and configure the related VLAN.

## 3.3.2 Default configurations

Default configurations of IGMP Snooping on the ISCOM5508-GP 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 |
| Immediate-leave | Disable |
| Static multicast routing table | N/A |

## 3.3.3 Configuring IGMP Snooping

Configure the ISCOM5508-GP as below.

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

**Note**

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.

## 3.3.4 Configuring aging time of multicast routing entries

In IGMP Snooping, when the ISCOM5508-GP does not receive the IGMP packet about Layer 2 multicast routing in a period of time, maybe the relevant host or router has left 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.

Configure the ISCOM5508-GP as below.

| 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.<br>You can use the **no igmp snooping timeout** command to restore default configurations. |

## 3.3.5 Configuring immediate-leave

When the user host sends the IGMP leave packet, the ISCOM5508-GP does not delete multicast route immediately, 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.

Configure the ISCOM5508-GP as below.

| 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* \| **ten-gigabitethernet** *slot-id/olt-id* \| **port-channel** *group-id*} | Enter physical interface configuration mode. |
| 3 | Raisecom(config-if-*-*:*)#**igmp snooping immediate-leave multicast-vlan***vlan-list* | Configure immediate-leave.<br>You can use the **no igmp snooping immediate-leave multicast-vlan***vlan-list* command to disable this function. |

### 3.3.6 Checking configurations

Use the following commands to check configuration results.

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

## 3.4 Configuring IGMP Proxy

### 3.4.1 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 configuration and management of the multicast router to client subnet 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.

### 3.4.2 Default configurations

Default configurations of IGMP Proxy on the ISCOM5508-GP 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 |

| Function | Default value |
|---|---|
| IGMP Proxy robustness coefficient | 2 |

## 3.4.3 Configuring IGMP Proxy

**Note**

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.

Configure the ISCOM5508-GP as below.

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

# 3.5 Configuring MVR

## 3.5.1 Preparing for configurations

### Scenario

When multiple user hosts need to receive data from the multicast source, and when different user hosts, host and multicast router belong to different VLANs, you can configure MVR on the multicast router and the IISCOM5508-GP 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.

## 3.5.2 Default configurations

Default configurations of MVR on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Global MVR | Disable |

## 3.5.3 Configuring basic MVR

Configure the ISCOM5508-GP as below.

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

## 3.5.4 Checking configurations

Use the following commands to check configuration results.

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

# 3.6 Configuring dynamic controllable multicast

## 3.6.1 Preparing for configurations

### Scenario

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

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

### Prerequisite

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

## 3.6.2 Default configurations

Default configurations of dynamic controllable multicast on the ISCOM5508-GP 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 |

## 3.6.3 Configuring global function

Configure the ISCOM5508-GP as below.

| 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.<br>You can use the **no multicast-ctrl max-non-igmp-report-duration** command to restore default configurations. |

## 3.6.4 Configuring user management

Configure the ISCOM5508-GP as below.

| 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* | Specify the channel package for the specified user. |

## 3.6.5 Configuring channel management

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**multicast-ctrl channel id** *id* **name** *channel-name* **group-ip** *ip-address* | Create a multicast channel.<br>You can use the **no multicast-ctrl channel name** command to delete the configuration. |
| 3 | Raisecom(config)#**multicast-ctrl channel** *channelname* **cdr** | (Optional) enable CDR on the channel.<br>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.<br>You can use the **no multicast-ctrl package** *packagename* command to delete the configuration. |
| 5 | Raisecom(config)#**multicast-ctrl package** *packagename* **channel** *channelname* { **deny** \| **permit** \| **preview** } [ **peview-profile** *profile* ] | Add channels to the package.<br>You can use the **no multicast-ctrl package** *packagename* **channel** *channelname* command to restore default configurations. |

## 3.6.6 Configuring preview rules

Configure the ISCOM5508-GP as below.

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

## 3.6.7 Configuring CDR

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**multicast-ctrl cdr** | Enable CDR management.<br>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.<br>You can use the **no multicast-ctrl cdr max-records** command to restore default configurations. |
| 4 | Raisecom(config)#**multicast-ctrl cdr report** | Configure reporting CDR manually. |
| 5 | Raisecom(config)#**multicast-ctrl cdr report-interval** *report-interval* | Configure the interval for reporting CDR manually.<br>You can use the **no multicast-ctrl cdr report-interval** command to restore default configurations. |
| 6 | Raisecom(config)#**multicast-ctrl cdr report-threshold** *value* | Configure the threshold for reporting CDR manually.<br>You can use the **no multicast-ctrl cdr report-threshold** command to restore default configurations. |
| 7 | Raisecom(config)#**multicast-ctrl cdr aware-time** *value* | Configure the CDR aware time. |

## 3.6.8 Checking configurations

Use the following commands to check configuration results.

| 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 for users. |
| 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. |

| No. | Command | Description |
|---|---|---|
| 10 | Raisecom#**show multicast-ctrl preview-profile** [ *profile* ] | Show preview profile configurations. |

# 3.7 Configuring MLD Snooping

## 3.7.1 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 realize the multicast function in an IPv6 network, you need to configure the MLD multicast function.

### Prerequisite

N/A

## 3.7.2 Default configurations

Default configurations of MLD on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Global MLD multicast | Disable |
| Aging time of MLD Snooping | 300s |

## 3.7.3 Configuring MLD Snooping

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**mld** | Enable MLD Snooping.<br>You can use the **no mld** command to disable this function. |
| 3 | Raisecom(config)#**mld snooping timeout** { *period* \| **infinite** } | (Optional) configure the aging time of MLD Snooping.<br>You can use the **no mld snooping timeout** command to restore default configurations. |

### 3.7.4 Checking configurations

Use the following commands to check configuration results.

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

## 3.8 Configuring MLD Proxy

### 3.8.1 Preparing for configurations

#### Scenario

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

#### Prerequisite

N/A

### 3.8.2 Default configurations

Default configurations of MLD on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Global MLD multicast | Disable |
| MLD multicast IP address | Local link address, that is, 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 |

| Function | Default value |
|---|---|
| MLD Proxy version | v2 |

## 3.8.3 Configuring MLD Proxy

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |
| 2 | `Raisecom(config)#mld` | Enable MLD Proxy.<br>You can use the **no mld** command to disable this function. |
| 3 | `Raisecom(config)#mld proxy source-ip` *ip-address* | Configure the MLD Proxy multicast IP address.<br>You can use the **no mld proxysource-ip** command to delete the configuration. |
| 4 | `Raisecom(config)#mld proxy query-interval` *seconds* | (Optional) configure the MLD Proxy query interval.<br>You can use the **no mld proxy query-interval** command to restore default configurations. |
| 5 | `Raisecom(config)#mld proxy query-max-response` *seconds* | (Optional) configure the maximum response time of MLD Proxy query.<br>You can use the **no mld proxy query-max-response** command to restore default configurations. |
| 6 | `Raisecom(config)#mld proxy last-query-interval` *seconds* | (Optional) configure the query interval of MLD Proxy last member.<br>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.<br>You can use the **no mld proxy last-query-count** command to restore default configurations. |
| 8 | `Raisecom(config)#mld proxy source-ip` *ip-address* | (Optional) configure the source IP address of the query packet sent by the MLD Proxy querier.<br>You can use the **no mld proxy source-ip** command to restore default configurations. |
| 9 | `Raisecom(config)#mld proxy robustness` *robustness* | (Optional) configure the robustness coefficient of MLD Proxy.<br>You can use the **no mld proxy robustness** command to restore default configurations. |

## 3.8.4 Checking configurations

Use the following commands to check configuration results.

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

# 3.9 Configuring multicast VLAN

## 3.9.1 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

## 3.9.2 Default configurations

Default configurations of multicast VLAN on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Multicast VLAN | N/A |
| 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 |

## 3.9.3 Configuring multicast VLAN

Configure the ISCOM5508-GP as below.

| 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.<br>You can use the **no multicast-vlan** *vlan-id* **group** { *group-address* [ *count* ] \| **any** } command to restore default configurations. |
| 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* \| **gigabitethernet** *slot-id/olt-id* \| **ten-gigabitethernet** *slot-id/olt-id* \| **port-channel** *group-id* } | Enter physical interface configuration mode. |
| 9 | Raisecom(config-if-*-*:*)#**multicast-vlan** *vlan-id* **router** | Configure an interface as the multicast VLAN router interface.<br>**Note**<br>Before you use this command to configure the interface role for the multicast VLAN, the system supports dynamically learning the interface role. |
| 10 | Raisecom(config-if-*-*:*)#**multicast-vlan** *vlan-id* **member** | Configure an interface as the multicast VLAN member interface.<br>**Note**<br>Before you use this command to configure the interface role for the multicast VLAN, the system supports dynamically learning the interface role. |

## 3.9.4 Checking configurations

Use the following commands to check configuration results.

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

# 3.10 Maintenance

Maintain the ISCOM5508-GP as below.

| Command | Description |
|---|---|
| Raisecom(config)#**clear igmp statistics** | Clear IGMP packet statistics. |
| Raisecom(config)#**clear interface** { **gpon-olt** *slot-id/olt-id* \| **gigabitethernet** *slot-id/olt-id* \| **ten-gigabitethernet** *slot-id/olt-id* \| **port-channel** *group-id* } **igmp statistics** | Clear IGMP packet statistics on a specified interface. |
| Raisecom(config)#**clear mld statistics** | Clear MLD packet statistics. |
| Raisecom(config)#**clear interface** { **gpon-olt** *slot-id/olt-id* \| **gigabitethernet** *slot-id/olt-id* \| **ten-gigabitethernet** *slot-id/olt-id* \| **port-channel** *group-id* } **mld statistics** | Clear MLD packet statistics on a specified interface. |
| Raisecom(config)#**multicast-ctrl cdr clear** | Clear CDR information. |

# 4 Configuring MAC address

This chapter introduces basic principles and configuration process of the MAC address table for the ISCOM5508-GP, including the following sections:

- Overview of MAC address table
- Configuring dynamic MAC address
- Configuring static MAC address
- Maintenance and search
- Configuration examples

## 4.1 Overview of MAC address table

The ISCOM5508-GP 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 ISCOM5508-GP 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

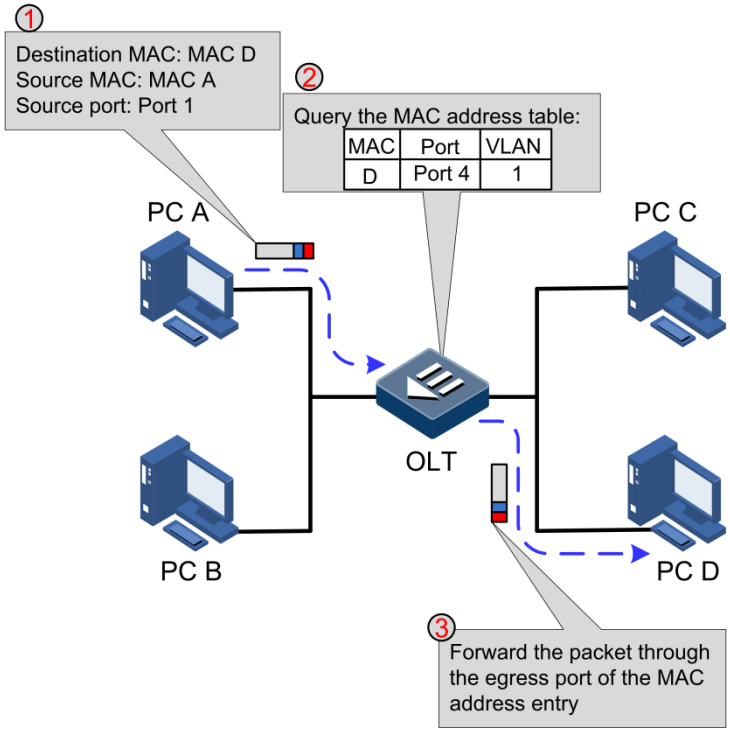
The MAC address table on the ISCOM5508-GP consists of two kinds of address entries:

- 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 ISCOM5508-GP adopts following modes:

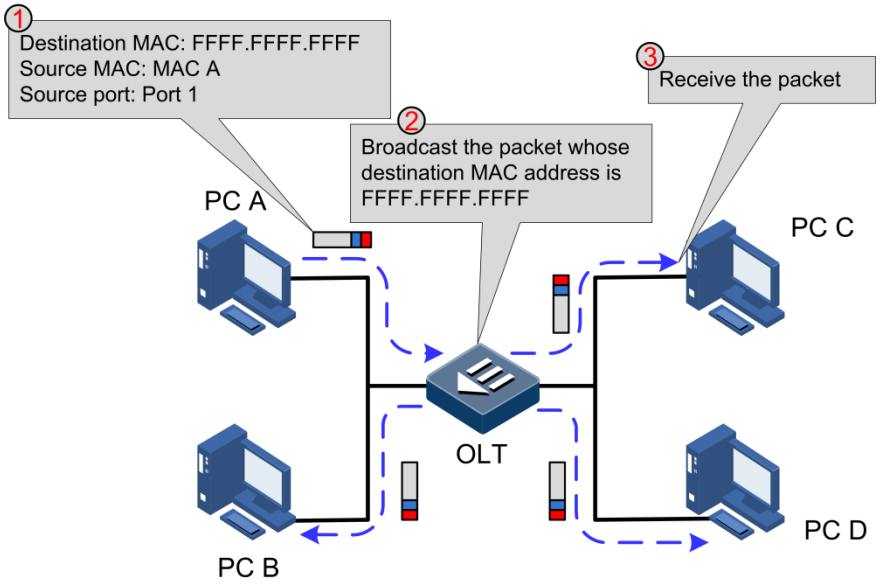
- Unicast: when a MAC address entry, which is related to the destination MAC address of a packet, is listed in the MAC address table, the ISCOM5508-GP will directly forward the packet through the egress interface. Otherwise, the ISCOM5508-GP will broadcast the packet, as shown in Figure 4-1.

Figure 4-1 Unicast forwarding mode of MAC address




- Multicast: when r the ISCOM5508-GP 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 ISCOM5508-GP will forward the packet through the egress interface. Otherwise, the ISCOM5508-GP will broadcast this packet.
- Broadcast: when the ISCOM5508-GP receives an all-F packet, or when the ISCOM5508-GP 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 4-2.

Figure 4-2 Broadcast forwarding mode of MAC address




# 4.2 Configuring dynamic MAC address

## 4.2.1 Preparing for configurations

### Scenario

Dynamic MAC address entries can be added through the MAC address learning mechanism. You can limit the number of MAC address 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 ISCOM5508-GP is rebooted.

### Prerequisite

N/A

## 4.2.2 Default configurations

Default configurations of dynamic MAC address entries on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| MAC address learning | Enable |
| Aging time of MAC address | 300s |
| MAC address limit | Unlimited |
| MAC address table move | Enable |

## 4.2.3 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 realize Layer 2 forwarding.

Configure the ISCOM5508-GP as below.

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

## 4.2.4 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.

Configure the ISCOM5508-GP as below.

| 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 address entries.<br>You can use the **no mac-address-table aging-time** command to restore default configurations.<br>**Note**<br>The value 0 refers that the MAC address is not aged. |

## 4.2.5 Configuring MAC address limit

To avoid explosive increase of the MAC address table, you need to configure the MAC address limit, thus preventing lowering performance of the device due to a too large MAC address table.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |

| Step | Command | Description |
|---|---|---|
| 2 | Raisecom(config)#**interface** { **gpon-olt** \| **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/olt-id* | Enter physical interface configuration mode. |
| 3 | Raisecom(config-if-*-*-*:*)#**mac-address-table threshold** *threshold* | Configure the threshold of MAC addresses allowed to be learnt by the interface.<br>You can use the **no mac-address-table threshold** command to restore default configurations. |

## 4.2.6 Configuring MAC address table move

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

## 4.2.7 Checking configurations

Use the following commands to check configuration results.

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

# 4.3 Configuring static MAC address

## 4.3.1 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

## 4.3.2 Default configurations

N/A

## 4.3.3 Configuring static unicast MAC address

Static MAC address can be set for fixed servers, special persons (manager, financial staff, etc.) 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.

Configure the ISCOM5508-GP as below.

| 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-olt** *slot-id/port-id* \| **gigabitethernet** *slot-id/port-id* \| **ten-gigabitethernet** *slot-id/port-id* \| **port-channel** *group-id* } | Configure static unicast MAC address entries.<br>You can use the **no mac-address-table static unicast** *mac-address* **vlan** *vlan-id* command to delete the configuration. |

## 4.3.4 Configuring static multicast MAC address

Configure the ISCOM5508-GP as below.

| 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** { **gpon-olt** *slot-id/port-id* \| **gigabitethernet** *slot-id/port-id* \| **ten-gigabitethernet** *slot-id/port-id* \| **port-channel** *group-id* } | Configure static multicast MAC address entries.<br>You can use the **no mac-address-table static multicast** *mac-address* **vlan** *vlan-id* **port-list** *port-list* command to delete the configuration. |

### 4.3.5 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show mac-address-table static unicast** [ **vlan** *vlan-id* \| **interface** { **gpon-olt** *slot-id/port-id* \| **gigabitethernet** *slot-id/port-id* \| **ten-gigabitethernet** *slot-id/port-id* \| **port-channel** *group-id* } ] | Show static unicast MAC addresses. |
| 2 | Raisecom#**show mac-address-table statistics unicast** [ **vlan** *vlan-id* \| **interface** { **gpon-olt** *slot-id/port-id* \| **gigabitethernet** *slot-id/port-id* \| **ten-gigabitethernet** *slot-id/port-id* \| **port-channel** *group-id* } ] | Show static unicast MAC address statistics. |
| 3 | Raisecom#**show mac-address-table multicast** [ **statistics** ] | Show static multicast MAC addresses. |

### 4.3.6 Checking configurations

Use the following commands to check configuration results.

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

## 4.4 Maintenance and search

### 4.4.1 Preparing for configurations

#### Scenario

The ISCOM5508-GP 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.

Use the **search** command, you can search for the content of the MAC address entry and related information.

#### Prerequisite

N/A

## 4.4.2 Default configurations

N/A

## 4.4.3 Clearing MAC address

Configure the ISCOM5508-GP as below.

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

## 4.4.4 Searching MAC address

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**search mac-address** *mac-address* | Search for information about a specified MAC address. |

## 4.4.5 Tracing MAC address

Configure the ISCOM5508-GP as below.

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

## 4.4.6 Checking configurations

Use the following commands to check configuration results.

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

| No. | Command | Description |
|---|---|---|
| 4 | Raisecom#**show mac-address-table static unicast** [ **vlan** *vlan-id* \| **interface** { **gpon-olt** *slot-id/port-id* \| **gigabitethernet** *slot-id/port-id* \| **ten-gigabitethernet** *slot-id/port-id* \| **port-channel** *group-id* } ] | Show information about the static unicast MAC address entry. |
| 5 | Raisecom#**show mac-address-table statistics unicast** [ **vlan** *vlan-id* / **interface** { **gpon-olt** *slot-id/port-id* \| **gigabitethernet** *slot-id/port-id* \| **ten-gigabitethernet** *slot-id/port-id* \| **port-channel** *group-id* } ] | Show static unicast MAC address statistics. |

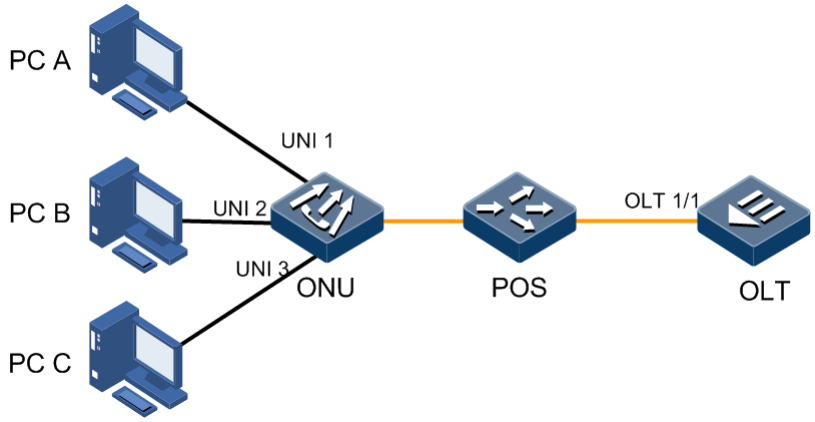
# 4.5 Configuration examples

## 4.5.1 Example for configuring dynamic MAC address

### Networking requirements

As shown in Figure 4-3, the ONU is connected uplink to multiple hosts. To avoid explosive increase of the MAC address table on the ONU, you need to enable MAC address learning on PON interface 1/1 and set the aging time of the dynamic MAC address table on the OLT to 500s.

Figure 4-3 Configuring dynamic MAC address




### Configuration steps

Step 1 Enable MAC address learning on the PON interface OLT 1/1.

```
Raisecom#config
Raisecom(config)#interface gpon-olt 1/1
Raisecom(config-if-gpon-olt-1:1)#mac-address-table learning
Raisecom(config-if-gpon-olt-1:1)#exit
```

Step 2 Configure the aging time of dynamic MAC addresses on the OLT.

```
Raisecom(config)#mac-address-table aging-time 500
Raisecom(config)#end
```

### Checking results

Show the MAC address learning status and aging time.

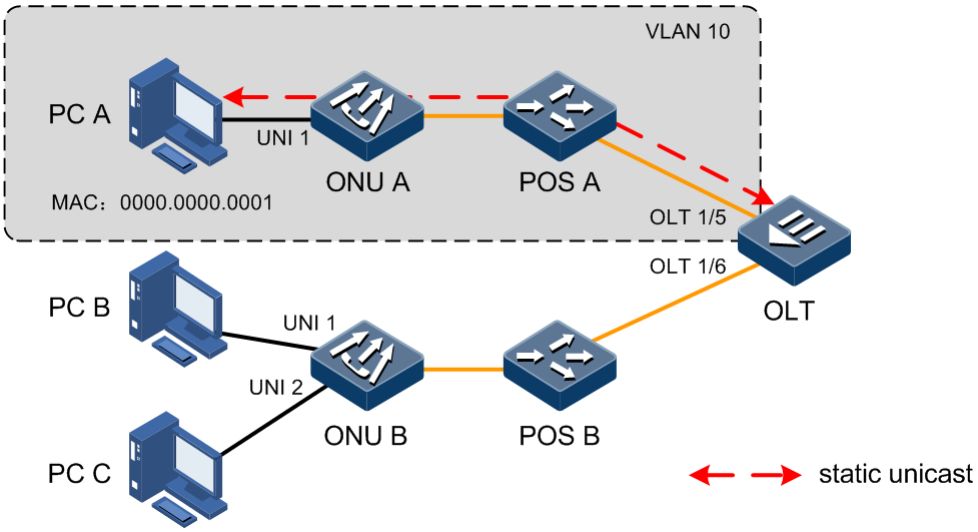
```
Raisecom#show interface gpon-olt 1/1 mac-address-table
Port ID  MAC-learning  MAC-threshold
-----------------------------------
gpon-olt1/1     Enable       0

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

## 4.5.2 Example for configuring static MAC address

### Networking requirements

As shown in Figure 4-4, the position of PC A is fixed and important. Configure a static unicast MAC address for PC A on the OLT. The MAC address of PC A is 0000.0000.0001. PC A belongs to VLAN 10.

Figure 4-4 Configuring static MAC address




### Configuration steps

Step 1 Create a VLAN and configure the interface mode on the OLT.

```
Raisecom#config
Raisecom(config)#create vlan 10 active
Raisecom(config)#interface gpon-olt 1/1
Raisecom(config-if-gpon-olt-1:1)#switchport mode trunk
Raisecom(config-if-gpon-olt-1:1)#switchport trunk allowed vlan 10
Raisecom(config-if-gpon-olt-1:1)#exit
```

Step 2 Configure the static unicast MAC address on the OLT.

```
Raisecom(config)#mac-address-table static unicast 0000.0000.0001 vlan 10
interface gpon-olt 1/1
```

## Checking results

Show information about the MAC address under a VLAN on the OLT.

```
Raisecom#show mac-address-table l2-address vlan 10
Mac Address       Port              Vlan   Flags
-------------------------------------------------
0000.0000.0001    gpon-olt1/1        10    Static
```

# 5 Configuring VLAN

This chapter introduces the VLAN features and configuration process of the ISCOM5508-GP, and provides related configuration examples, including the following sections:

- Overview of VLAN
- Configuring VLAN
- Configuring QinQ
- Configuring VLAN ACL
- Configuring VLAN translation
- Configuration examples

## 5.1 Overview of VLAN

### 5.1.1 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 sub-net 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 be collapsed. 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.

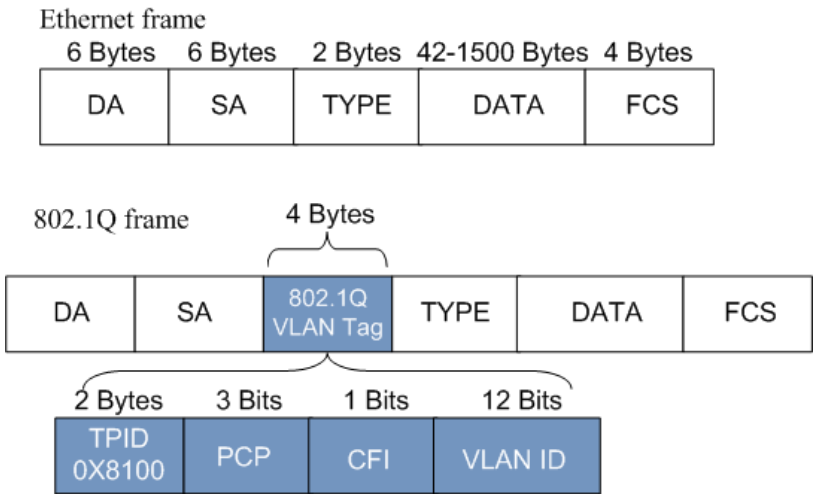
When a frame is sent to the ingress interface of a device, the device will query the VLAN where the ingress interface is and then query the MAC address table to which the VLAN is related. If the destination MAC address of the frame is listed in the MAC address table, the frame will be forwarded. Otherwise, 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 5-1 shows structures of Ethernet frame and 802.1Q frame.

Figure 5-1 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 ISCOM5508-GP sends packets with higher priorities first.

## VLAN modes of OLT interface

The interface on the ISCOM5508-GP supports two modes: Access mode and Trunk mode.

Table 5-1 lists compassion of VLAN modes and packet processing modes.

Table 5-1 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.<br>• 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. |
| 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.<br>• 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.<br>• 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 5-2 lists how ONU interfaces to process Ethernet frames in VLAN Transparent mode.

Table 5-2 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 5-3 lists how ONU interfaces to process Ethernet frames in VLAN Tagged mode.

Table 5-3 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). |
| Downlink | With VLAN Tag | Forward Ethernet packets to related UNI interfaces 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 5-4 lists how ONU interfaces to process Ethernet frames in VLAN Translation mode.

Table 5-4 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.<br>If VIDs of the original Tags are native VIDs, forward Ethernet packets after removing their Tags. |
| | Without VLAN Tag | Discard Ethernet packets. |

Table 5-5 lists how ONU interfaces to process Ethernet frames in VLAN Trunk mode.

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

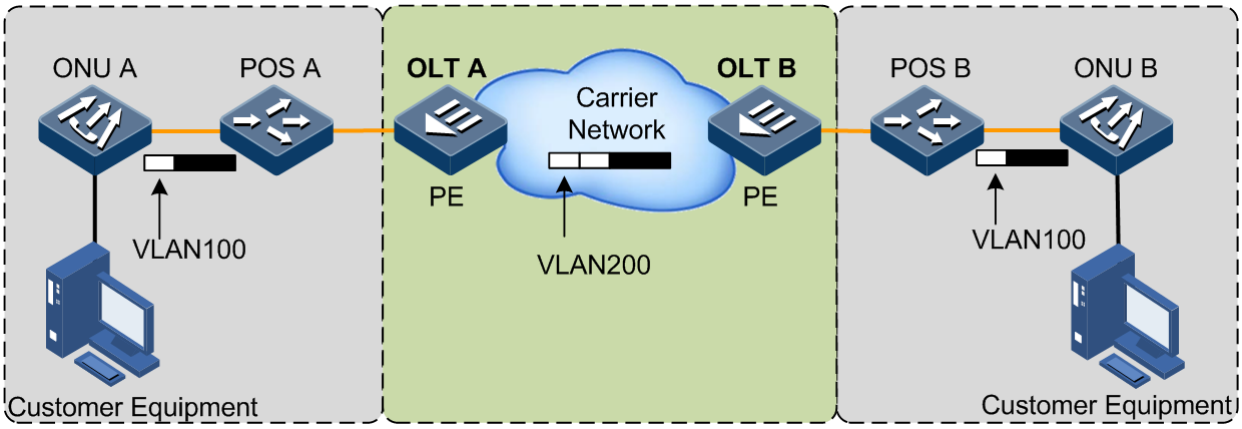
| Direction | With/without Tag | Processing mode |
|---|---|---|
| Uplink | With VLAN Tag | If VLANs carried by Ethernet packets are in allowed VLAN list of the interface, forward these Ethernet packets. Otherwise, discard these Ethernet packets. |
| | Without VLAN Tag | Forward Ethernet packets by adding 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.<br>If VLAN IDs carried by Ethernet packets are native VLANs, forward these Ethernet packets. |
| | Without VLAN Tag | Discard Ethernet packets. |

## 5.1.2 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 5-2 Basic QinQ networking




As shown in Figure 5-2, 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.

### 5.1.3 VLAN translation

VLAN translation is mainly used to replace the private VLAN Tags of Ethernet packets with Carrier's VLAN Tags, making packets 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 translation, 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 translation rules. If success, the private VLAN Tags are replaced according to configured VLAN translation rules. VLAN translation provides the following modes:

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

## 5.2 Configuring VLAN

### 5.2.1 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. The VLANs logically divide the hosts connected to the device. 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 same department has different locations, but hosts in the same department 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 cannot communicate. If hosts in different VLANs need to communicate, use the Layer 3 device such as a router.

### Prerequisite

N/A

## 5.2.2 Default configurations

Default configurations of VLAN on the ISCOM5508-GP 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<br>Downlink: Access |
| New priority used by the interface to add VLAN Tag to data | Uplink: 0<br>Downlink: 0 |
| Enable/Disable the interface to use a new priority when adding VLAN Tag to data | Uplink: disable<br>Downlink: disable |
| VLAN ID used by the interface to add VLAN Tag to data | Uplink: 1<br>Downlink: 1 |

## 5.2.3 Creating VLAN

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |
| 2 | `Raisecom(config)#create vlan` *vlan-id* { **active** \| **suspend** } | Create a VLAN.<br>You can use the **no vlan** { **all** \| *vlan-id* } command to delete the VLAN. |
| 3 | `Raisecom(config)#vlan` *vlan-id* | Enter VLAN configuration mode.<br>**Note**<br>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.<br>You can use the **no name** command to restore default configurations. |
| 5 | `Raisecom(config-vlan)#state` { **active** \| **suspend** } | (Optional) activate or suspend the VLAN. |

- 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 delete/add interfaces and set VLAN name, etc. The configurations will be saved by the system. Once the VLAN is activated, the configurations will take effect in the system.

## 5.2.4 Configuring interfaces in Access mode

Configure the ISCOM5508-GP as below.

| 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-*-*:*)#**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.<br>You can use the **no switchport access vlan** command to restore default configurations. |
| 5 | Raisecom(config-if-*-*:*)#**vlan drop-untagged** | (Optional) configure the interface to discard the untagged packet.<br>You can use the **no vlan drop-untagged** command to restore default configurations. |

- 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.

## 5.2.5 Configuring interfaces in Trunk mode

Configure the ISCOM5508-GP as below.

| 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-*-*:*)#**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.<br>You can use the **no switchport trunk native vlan** command to restore default configurations. |
| 5 | Raisecom(config-if-*-*:*)#**switchport trunk allowed vlan** { **all** \| [ **add** \| **remove** ] *vlan-list* } [ **confirm** ] | Configure the VLAN allowed to pass by the Trunk interface.<br>You can use the **no switchport trunk allowed vlan** command to restore default configurations.<br>**Note**<br>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 untagged VLAN on the Trunk egress interface.<br>You can use the **no switchport trunk untagged vlan** command to restore default configurations. |
| 7 | Raisecom(config-if-*-*:*)#**vlan drop-untagged** | (Optional) configure the interface to discard the untagged packet.<br>You can use the **no vlan drop-untagged** command to restore default configurations. |

**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.

## 5.2.6 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show vlan** [ *vlan-list* \| **static** \| **dynamic** ] | Show VLAN configurations. |

| No. | Command | Description |
|---|---|---|
| 2 | Raisecom#**show vlan** [ *vlan-list* ] **member-port** | Show information about the VLAN member interface and untagged interface. |

# 5.3 Configuring QinQ

## 5.3.1 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 take transparent transmission without conflicting with the VLAN ID in the Internet Service Provider (ISP)'s network.

### Prerequisite

N/A

## 5.3.2 Default configurations

Default configurations of QinQ on the ISCOM5508-GP are as below.

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

## 5.3.3 Configuring basic QinQ

Configure the ISCOM5508-GP as below.

| 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-*-*:*)#**vlan dot1q-tunnel** | Enable basic QinQ on the interface.<br>You can use the **no vlan dot1q-tunnel** to disable this function. |
| 4 | Raisecom(config-if-*-*:*)#**vlan tpid** *tpid* | Configure the TPID of the outer VLAN.<br>You can use the **no vlan tpid** command to restore default configurations. |

Note

- After QinQ is enabled, the interface processes the received Tagged packets as Untagged packets, that is, add outer VLAN Tags on original packets.
- After QinQ is enabled, configurations for the outer VLAN are the same with those for the general VLAN.

### 5.3.4 Checking configurations

Use the following commands to check configuration results.

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

## 5.4 Configuring VLAN ACL

### 5.4.1 Preparing for configurations

#### Scenario

Through the VLAN ACL technology, you can configure the matching rules to flexibly match the source MAC address, SVLAN, CVLAN, CoS, and Ethernet type for Layer 2 packets, and the source IPv4 address, destination IPv4 address, and IP type for Layer 3 packets. Moreover, you can take different operations on packets based on the match, such as adding outer VLAN and modifying inner VLAN.

#### Prerequisite

N/A

### 5.4.2 Default configurations

N/A

### 5.4.3 Creating ACL

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**vlan-access-list** *list-number* | Create a VLAN ACL and enter VLAN ACL configuration mode.<br>You can use the **no vlan-access-list** *acl-numb*er command to delete the ACL. |

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

## 5.4.4 Configuring matching contents

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom(config-qinq-acl-*-rule-*)#**match mac source** *mac-address* [ *mask* ] | (Optional) match the source MAC address. |
| 2 | Raisecom(config-qinq-acl-*-rule-*)#**match** { **svlan** *vlan-id* \| **svlan-cos** *cos* } | (Optional) match the SVLAN ID and CoS value. |
| 3 | Raisecom(config-qinq-acl-*-rule-*)#**match** { **cvlan** *vlan-id* \| **cvlan-cos** *cos* } | (Optional) match the CVLAN ID and CoS value. |
| 4 | Raisecom(config-qinq-acl-*-rule-*)#**match ethertype** { *frame-type frame-type-mask* \| **arp** \| **eapol** \| **flowcontrol** \| **ip** \| **ipv6** \| **loopback** \| **mpls** \| **mpls-mcast** \| **pppoe** \| **pppoedisc** \| **x25** \| **x75** } | (Optional) match the protocol type of the Layer 2 frame head. |
| 5 | Raisecom(config-qinq-acl-*-rule-*)#**match ip** { **destination-address** \| **source-address** } *ip-address* [ *mask* ] | (Optional) match the source and destination IP address. |
| 6 | Raisecom(config-qinq-acl-*-rule-*)#**match ip protocol** { *protocol-num* \| **ahp** \| **esp** \| **gre** \| **icmp** \| **igmp** \| **igrp** \|**ipinip** \| **ospf** \| **pcp** \| **pim** \| **tcp** \| **udp** } | (Optional) match the IP upper protocol type. |
| 7 | Raisecom(config-qinq-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/source interface ID of the TCP packet.<br>You can use the **no match ip tcp** { **destination-port** \| **source-port** } command to delete the configuration. |

| Step | Command | Description |
|---|---|---|
| 8 | Raisecom(config-qinq-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/source interface ID of the UDP packet.<br>You can use the **no match ip udp** { **destination-port** \| **source-port** } command to delete the configuration. |

## 5.4.5 Configuring matching actions

Configure the ISCOM5508-GP as below.

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

## 5.4.6 Applying ACL

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom(config)#**interface** { **gigabitethernet** \| **ten-gigabitethernet** \| **gpon-olt** } *slot-id/port-id* | Enter physical interface configuration mode. |

| Step | Command | Description |
|---|---|---|
| 2 | Raisecom(config-if-*-*:*)#**vlan-access-list** *list-num* | Apply the VLAN ACL to an interface.<br>You can use the **no vlan-access-list** *list-num* command to delete the VLAN ACL.<br>**Note**<br>Applying the VLAN ACL on an interface refers to processing packets on the ingress interface only without affecting packets on the egress interface. |

### 5.4.7 Checking configurations

Use the following commands to check configuration results.

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

## 5.5 Configuring VLAN translation

### 5.5.1 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.

### 5.5.2 Default configurations

Default configurations of VLAN translation on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| VLAN translation | Enable |

## 5.5.3 Configuring VLAN translation

Configure the ISCOM5508-GP as below.

| 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-*-*:*)#**vlan-mapping cos-aware** | Configure CoS-aware VLAN translation, that is, VLAN+CoS translation.<br>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 unmatched with VLAN translation rules.<br>You can use the **no vlan-mapping** { **egress** \| **ingress** } **drop-unmatched** command to disable this function. |

## 5.5.4 Configuring VLAN translation

Configure the ISCOM5508-GP as below.

| 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-*-*:*)#**vlan-mapping**{ **ingress** \| **egress** } **outer** *before-outer* **translate outer** *after-outer* **inner** { **add** *vlan-id* \| **remove** \| *vlan-id* \| **unchange** } | Configure VLAN translation rules based on the ingress/egress interface (only the outer VLAN Tag is translated). |
| 4 | Raisecom(config-if-*-*:*)#**vlan-mapping**{ **ingress** \| **egress** } **outer** *before-outer* **inner** *before-inner* **translate outer** *after-oute* **inner** { *vlan-id* \| **remove** } | Configure VLAN translation rules based on the ingress/egress interface (both the outer and inner VLAN Tags are translated). |

## 5.5.5 Configuring VLAN aggregation

Configure the ISCOM5508-GP as below.

| 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-*-*:*)#**vlan-mapping outer** *before-vlan* **aggregate outer** *after-vlan* **inner** { **add** *vlan-id* \| **unchange** } | Configure N:1 VLAN aggregation rules based on interface (the outer VLAN Tag is translated and the inner VLAN Tag is added). |
| | Raisecom(config-if-*-*:*)#**vlan-mapping outer** *before-outer* **inner** *before-innerlist* **aggregate outer** *after-outer* **inner** { *vlan-id* \| **remove** } | Configure N:1 VLAN aggregation rules based on interface (both the outer and inner VLAN Tags are translated). |

## 5.5.6 Configuring translation rules based on VLAN+CoS

Configure the ISCOM5508-GP as below.

| 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-*-*:*)#**vlan-mapping ingress cos-aware outer** *before-outer before-cos* **translate outer** *after-outer* **inner** { *vlan-id* \| **add** *vlan-id* \| **remove** \| **unchange** } | Configure VLAN translation rules based on VLAN+CoS and the ingress interface.<br>You can use the **no vlan-mapping** { **ingress** \| **egress** } **cos-aware outer** *before-outer before-cos* **translate** command to cancel this application. |

## 5.5.7 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show interface** { **gpon-olt** \| **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-id* **vlan-mapping** { **ingress** \| **egress** } **translate** | Show 1:1 VLAN translation rules on the egress interface. |
| 2 | Raisecom#**show interface** { **gpon-olt** \| **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-id* **vlan-mapping aggregate** | Show N:1 VLAN translation rules based on interface. |
| 3 | Raisecom#**show interface** { **gpon-olt** \| **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-id* **vlan-mapping cos-aware aggregate** | Show translation rules based on VLAN+CoS on the interface. |

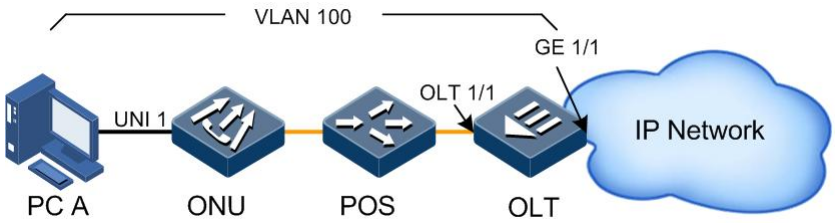
# 5.6 Configuration examples

## 5.6.1 Example for configuring VLAN

### Networking requirements

As shown in Figure 5-3, the user connects the ONU through the interface UNI 1, and the user VLAN is 100. The OLT connects the IP network through the interface GE 1/1, and connects the ONU through the PON interface OLT 1/1. Under this network topology structure, open the data service.

Figure 5-3 Configuring VLAN




### Configuration steps

Step 1 Create a VLAN.

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

Step 2 Configure the uplink GE interface VLAN.

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

Step 3 Configure the PON interface VLAN.

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

Step 4 Configure ONU auto-registration.

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

## Checking results

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

```
Raisecom#show interface 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 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
```

Show the registered ONU.

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

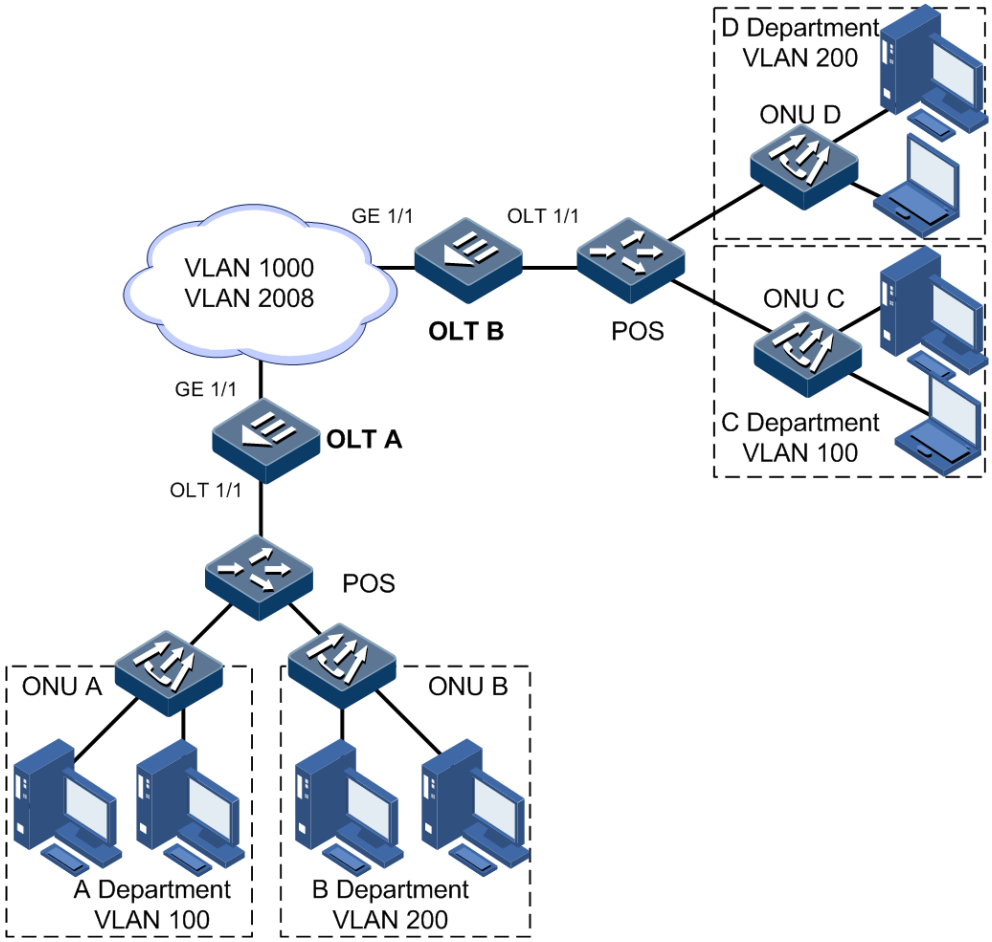
# 5.6.2 Example for configuring VLAN translation

## Networking requirements

As shown in Figure 5-4, OLT A connects Department A in VLAN 100 and Department B in VLAN 200 through the interface OLT 1/1; OLT B connects Department C in VLAN 100 and Department D in VLAN 200 through the interface OLT 1/1. In the carrier network, assign VLAN 1000 for Department A and Department C; and assign VLAN 2008 for Department B and Department D.

Configure VLAN translation on OLT A and OLT B to realize proper communication between the PC user or terminal user, and the server.

Figure 5-4 Configuring VLAN translation




## 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 the uplink interface GE 1/1 to Trunk mode and allow VLAN 1000 and VLAN 2008 to pass.

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

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

```
Raisecom(config)#interface gpon-olt 1/1
Raisecom(config-if-gpon-olt-1:1)#switchport mode trunk
Raisecom(config-if-gpon-olt-1:1)#switchport trunk allowed vlan 100,200
confirm
Raisecom(config-if-*-*:*)#vlan-mapping ingress outer 1000 inner 100 outer
translate 1000 inner unchanged
Raisecom(config-if-*-*:*)#vlan-mapping egress outer 1000 inner 100 outer
translate 1000 inner unchanged
Raisecom(config-if-*-*:*)#vlan-mapping ingress outer 2008 inner 200 outer
translate 2008 inner unchanged
Raisecom(config-if-*-*:*)#vlan-mapping egress outer 2008 inner 200 outer
translate 2008 inner unchanged
```

## Checking results

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

```
Raisecom#show interface gpon-olt 1/1 vlan-mapping egress
                        Old          New          IVLAN
Port ID               OVID  IVID   OVID  IVID  Mapping Action
-----------------------------------------------------------------
gpon-olt1/1           1000   100    1000   100    unchanged
Raisecom#show interface gpon-olt 1/1 vlan-mapping ingress
                        Old          New          IVLAN
Port ID               OVID  IVID   OVID  IVID  Mapping Action
-----------------------------------------------------------------
gpon-olt1/1           1000   100    1000 100     add
```

# 6 Configuring spanning tree

This chapter introduces the spanning tree feature and configuration process of the ISCOM5508-GP, and provides related configuration examples, including the following sections:

- Overview of spanning tree
- Configuring STP
- Configuring MSTP
- Configuration examples

## 6.1 Overview of spanning tree

### 6.1.1 STP

When you establish a network, you often need to create a redundant topology at a specified location to provide link backup and improve reliability. In addition, loops are generated in a network due to redundant links.

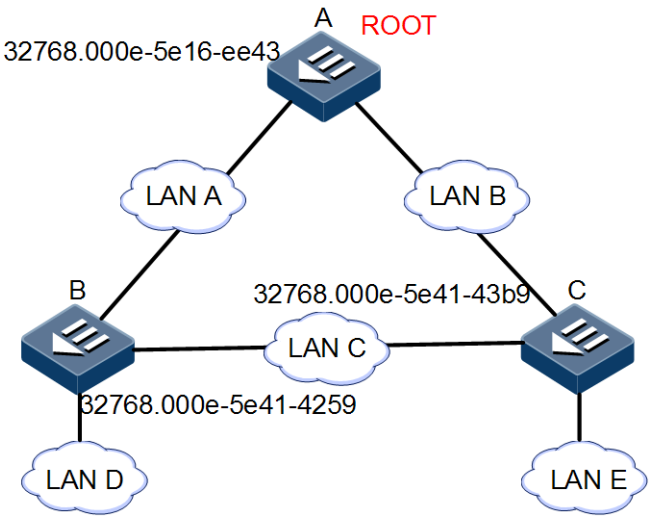
After a loop topology is generated between two devices, when these 2 devices send broadcast packets, these broadcast packets will be transmitted in the loop topology, resulting in a broadcast storm. The broadcast storm can reduce network performance, even worse, making the whole network collapsed.

Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology and data link backup. Devices, where STP runs, learn related parameters about each other by exchanging Bridge Protocol Data Units (BPDUs) and logically block loops with specified STP algorithm to prevent broadcast storm. When an unblocked link fails, the previously-blocked link is re-activated to act as a backup link.

The working process of STP is divided into the following steps:

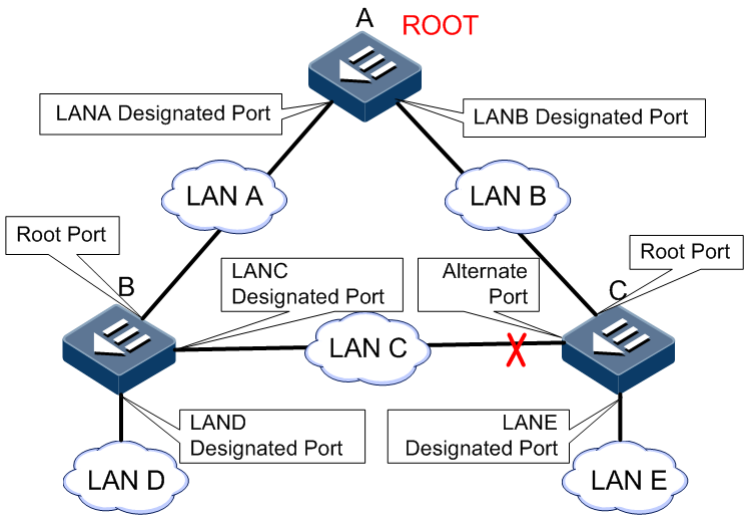
- Select a root bridge. The device selects a root bridge based on bridge IDs. The root bridge is the bridge with the smallest bridge ID. The bridge ID contains both bridge priority and the MAC address. By default, the bridge priority is set to 32768. The administrator can modify the bridge priority. To select a root bridge, the priority is compared first. The bridge with the smaller priority is the root bridge. If two bridges have equal priority, then the MAC addresses are compared. The bridge with the smaller MAC address is the root bridge. As shown in Figure 6-1, by comparing bridge IDs (bridge priority + MAC address) of all devices, Device A is selected as a root bridge.

Figure 6-1 STP (selecting a root bridge)




- Select a root port. STP selects a root port on each non-root bridge. The root port can send and receive data flow. STP selects the port with the smallest cost (a least-cost path) as the root port. When path costs of multiple ports are identical, STP selects the port with smaller bridge ID as the root port. If bridges IDs are identical, STP selects the port with smaller port identifier as the root port. As described above, the uplink ports of Device B and Device C in Figure 6-2 shows root ports.
- Select a designated port. STP selects a designated port at each network segment. Ports on the root bridge are designated ports. STP selects a designated port based on the following items in order: path cost, bridge ID, and port identifier. STP selects the port with the smallest cost (a least-cost path) as the designated port. When path costs are identical, STP selects a designated port based on bridge IDs and then based on port identifier. As shown in Figure 6-2, the port at the right side of Device B is selected as a designated port.
- Block an alternate port. Alternate ports are ports that are not the root port or designated ports. Alternated ports are in blocked status and cannot forward data. As shown in Figure 6-2, the port at the left side of Device C is selected as an alternate port, which will be blocked.

Figure 6-2 STP (confirming ports)



## 6.1.2 RSTP

Rapid Spanning Tree Protocol (RSTP) can be seen as an evolution of the 8STP. RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this. RSTP was designed to be backwards-compatible with standard STP.

## 6.1.3 MSTP

With quick development and wide application of VLAN technology, defects of the STP/RSTP are exposed gradually. STP/RSTP regards the whole network as a single spanning tree, leading to following problems:

- Some blocked links do not carry any traffic, consuming bandwidth.
- After a link is blocked, packets of some VLANs may not be forwarded.

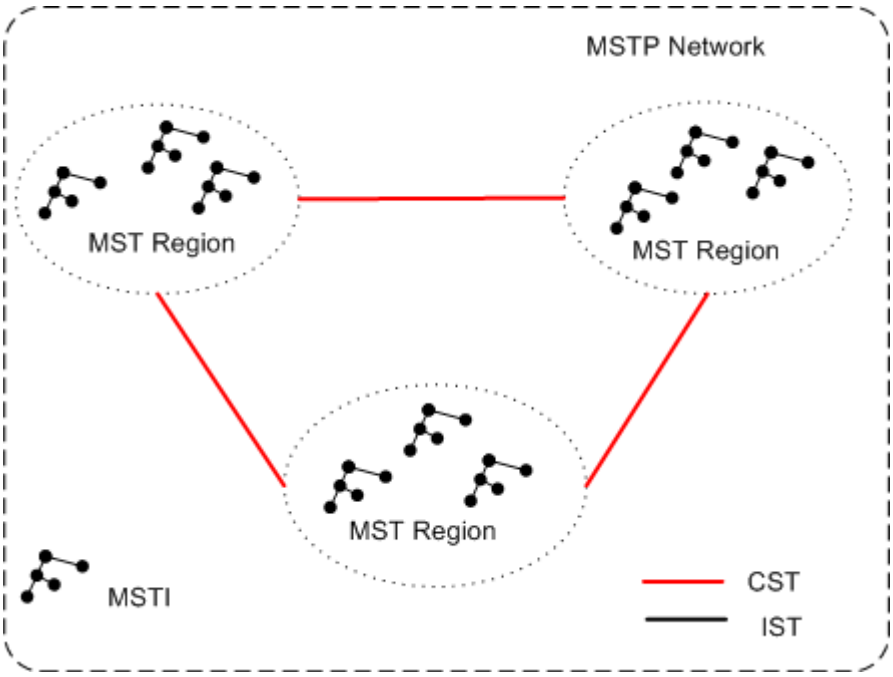
To solve the above problems, IEEE defines the 802.1s Multiple Spanning Tree Protocol (MSTP). The MSTP provides significantly faster spanning tree convergence. In addition, the MSTP ensures traffic in different VLANs being forwarded along their own paths. It provides good load-sharing mechanism.

The MSTP partitions a switching network into multiple regions, which are called MST regions. Each MST region can have multiple spanning trees, which are independent. Each spanning tree is called a Multiple Spanning Tree Instance (MSTI). MST regions are interconnected through a single spanning tree. This single spanning tree is called a Common Spanning Tree (CST). CST is used to ensure a loop-free and connected network.

You can map different VLANs to different MSTIs as required. The MSTP relates VLANs to MSTIs through the VLAN translation table (the relationship table of VLANs and MSTIs).

In each MST region, there is an MSTI whose ID is set to 0. This MSTI and CST make up of a Common Internal Spanning Tree (CIST). The CIST makes MST regions, bridges and network segments in these MST regions a fully-connected and loop-free tree. Figure 6-3 shows the relationship among MST regions, MSTIs, and CSTs.

Figure 6-3 MSTP

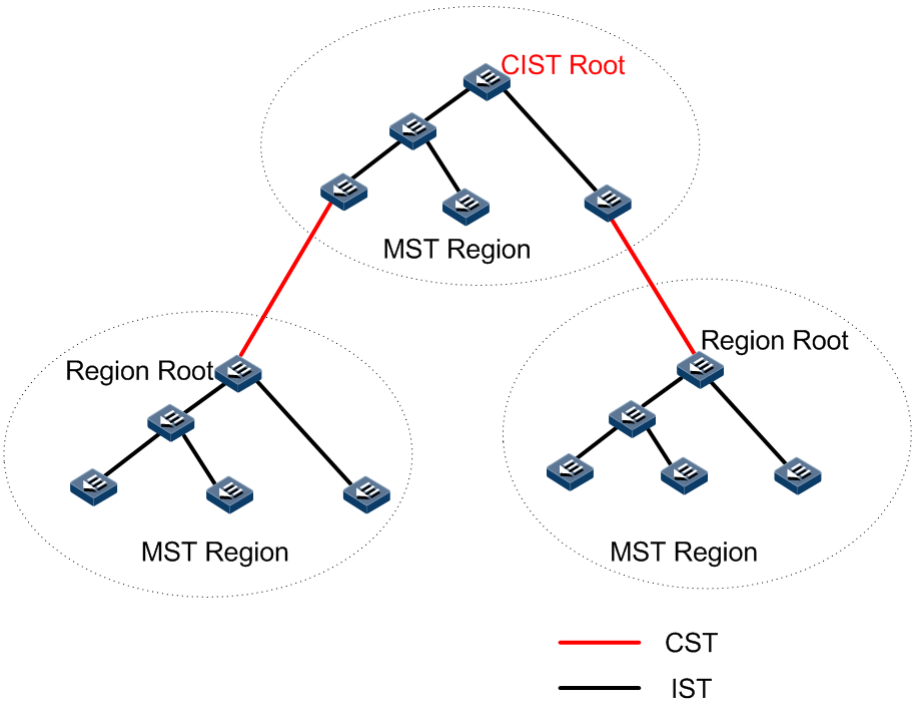



## Related concepts of MSTP

The MSTP introduces multiple new concepts and names. Figure 6-4 shows locations of related names.

- CST: a spanning tree used to connect all MST regions in a network
- IST: a spanning tree in a MST region. IST is a special MSTI. In general, it is MSTI0.
- CIST: a single spanning tree that is generated through STP/RSTP. It is used to connect all devices in a switching network. ISTs in all MST regions and CST compose a complete single spanning tree.
- Single Spanning Tree (SST): when only one device is in a MST region, this device is a SST. When you take a MST region as a device, the MSTP network is a SST.
- MST region: a MST region is composed by multiple devices in a LAN and network segments among these devices. In a LAN, there can be multiple MST regions. These MST regions are directly/indirectly connected in physical. You cam partition multiple devices into a MST region through MSTP configuration commands.
- VLAN translation table: the MSTP connects VLANs and MSTIs by configuring a VLAN translation table (the relationship table of VLANs and MSTIs).
- MSTI: a spanning tree is a MST region. MSTIs are independent. A MSTI can relate to one or more VLANs. However, a VLAN is related to a MSTI only.
- Region root: consists of an IST region root and a MSTI region root. IST region root refers to the device with smallest path cost to the root device in ISTs. MSTI region roots refer to roots of all MSTIs.
- Master bridge: a device that is most closed to the root bridge in a MST region. If the root device is in the MST region, the root device is the master bridge of the MST region.

Figure 6-4 Basic concepts of MSTP




## Port roles of MSTP

Ports of a device where MSTP is enabled work as one of the following roles:

- Root port: on a non-root device, the port with the smallest path cost to the root device is a root port of the device. The root port is used to forward data to the root device.
- Designated port: for a non-root device, the designated port is a port (except for the root port) that has the least-cost to the root bridge. All ports on the root bridge are designated ports.
- Edge port: if a designated port is located at the edge of a region and is not connected to any device, this port is called an edge port. In general, the edge port is directly connected to user devices.
- Alternate port: in terms of sending BPDUs, the Alternate port is a port that is blocked because of learning BPDUs sent by other devices. In terms of forwarding traffic, the Alternate port provides a backup path between a designated device and a root device. The Alternative port is backup port of the root port. If the root port is blocked, the Alternative port will become a new root port.
- Backup port: a loop is generated when two ports of a device is connected. The device will block one port. The backup port is the one that is blocked. In terms of sending BPDUs, the Backup port is a port that is blocked because of learning BPDUs sent by itself. In terms of forwarding traffic, as a backup of the designated port, the Backup port provides a backup path between a root device and a leaf node.
- Master port: a port that is on the shortest path of all paths connecting the MST region and the root device. It is a port that is used to connect a MST region and the root device.
- Region edge port: a port that locates at the edge of a MST region and that is used to connect other MST regions. Or it is a port that is used to connect related regions where STP/RSTP runs.

When you perform MSTP computation, roles of region edge ports on MSTI and CIST should be consistent. If the region edge port on the CIST is a master port (the port used to connect the region to the root device), it acts as a master port on all MSTIs in the region.

**Note**

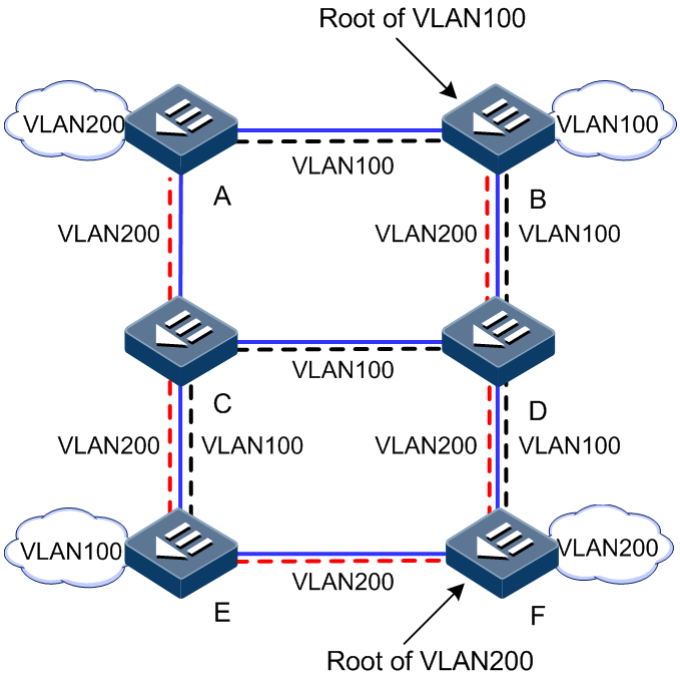
Each VLAN is related to one MSTI only. It means data of the same VLAN can be transmitted in a MSTI only. However, one MSTI can be related to multiple VLANs.

After applying MSTP to a network as shown in Figure 6-5, 2 spanning trees are generated after computation:

- MSTI 1 takes Device B as the root device, forwarding packets with VLAN 100.
- MSTI 2 takes Device F as the root device, forwarding packets with VLAN 200.

Therefore, devices in a VLAN can communicate with each other. In addition, packets of different VLANs are forwarded along different paths. It helps realize load-sharing.

Figure 6-5 MSTIs in a MST region




# 6.2 Configuring STP

## 6.2.1 Preparing for configurations

### Scenario

In a large-scale LAN, multiple devices are cascaded together to meet the need to access each other. You can enable STP on these devices to avoid loops due to device cascade, MAC address learning faults, and broadcast storm caused by quick copy and transmission of data

frames. Through the STP calculation, you can block some interface in a loop to ensure that there is only one path from data flow to destination host.

### Prerequisite

Configure physical parameters of the interface and make the interface Up at the physical layer.

## 6.2.2 Default configurations

Default configurations of STP on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Global STP | Disable |
| Port STP | Enable |
| System STP priority | 32768 |
| Port STP priority | 128 |
| Port path cost | 0 |

## 6.2.3 Enabling STP

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |
| 2 | `Raisecom(config)#spanning-tree mode stp` | Configure the spanning tree mode to STP. |
| 3 | `Raisecom(config)#spanning-tree` | Enable global STP.<br>You can use the **no spanning-tree** command to disable this function. |
| 4 | `Raisecom(config)#interface { gigabitethernet \| ten-gigabitethernet } slot-id/port-id` | Enter physical interface configuration mode. |
| 5 | `Raisecom(config-if-*-*:*)#spanning-tree` | (Optional) enable port STP. |

## 6.2.4 Configuring STP parameters

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |

| Step | Command | Description |
|---|---|---|
| 2 | Raisecom(config)#**spanning-tree** [ **instance** *instance-id* ] **priority** *priority* | (Optional) configure system priority.<br>You can use the **no spanning-tree** [ **instance** *instance-id* ] **priority** command to restore default configurations. |
| 3 | Raisecom(config)#**spanning-tree** [ **instance** *instance-id* ] **root** { **primary** \| **secondary** } | (Optional) configure the device as the root device or backup root device.<br>You can use the **no panning-tree** [ **instance** *instance-id* ] **root** command to restore default configurations. |
| 4 | Raisecom(config)#**interface** { **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-id* | Enter physical interface configuration mode. |
| 5 | Raisecom(config-if-*-*:*)#**spanning-tree** [ **instance** *instance-id* ] **priority** *priority-value* | (Optional) configure the port priority.<br>You can use the **no spanning-tree** [ **instance** *instance-id* ] **priority** command to restore default configurations. |
| 6 | Raisecom(config-if-*-*:*)#**spanning-tree** [ **instance** *instance-id* ] **inter-path-cost** *cost-value* | (Optional) configure the internal port path cost.<br>You can use the **no spanning-tree** [ **instance** *instance-id* ] **inter-path-cost** command to restore default configurations. |
| 7 | Raisecom(config-if-*-*:*)#**spanning-tree extern-path-cost** *cost-value* | (Optional) configure the external port path cost.<br>You can use the **no spanning-tree extern-path-cost** command to restore default configurations. |

### 6.2.5 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show spanning-tree** [ **instance** *instance-id* ] [ **detail** ] | Show STP basic configurations. |

## 6.3 Configuring MSTP

### 6.3.1 Preparing for configurations

#### Scenario

In a large-scale LAN or community aggregation network, aggregation devices make up a ring for link backup, which avoids loopback and realize service load sharing at the same time. The MSTP can select different and unique forwarding path for each VLAN or a group of VLANs.

### Prerequisite

Configure physical parameters of the interface and make the interface Up at the physical layer.

## 6.3.2 Default configurations

Default configurations of MSTP on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Global MSTP | Disable |
| Port MSTP | Enable |
| Maximum number of hops in MST domain | 20 |
| System priority | 32768 |
| Port priority | 128 |
| Port path cost | 0 |
| Maximum number of packets sent within in a Hello time | 3 |
| Max-Age timer | 20s |
| Hello-Time timer | 2s |
| Forward-Delay timer | 15s |
| Revision level of MST domain | 0 |

## 6.3.3 Enabling MSTP

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**spanning-tree mode mstp** | Configure the spanning tree mode to MSTP. |
| 3 | Raisecom(config)#**spanning-tree** | Enable global MSTP. |
| 4 | Raisecom(config)#**interface** { **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-id* | Enter physical interface configuration mode. |
| 5 | Raisecom(config-if-*-*:*)#**spanning-tree** | (Optional) enable port MSTP. |

## 6.3.4 Configuring MST domain and maximum number of hops

You can configure domain information for the device when it is running in MSTP mode. The MST domain depends on the domain name, VLAN mapping table, and MSTP revision level. You can configure current device to a specific MST domain through following configurations.

The maximum number of hops confines the scale of the MST domain. Starting from the root bridge in the domain, the BPDU reduces 1 hop once it is forwarded through a device; the BPDU will be discarded when the number of hop is 0. In this case, the device out of the maximum number of hops cannot take part in spanning tree calculation, thus defining the scale of the MST domain.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |
| 2 | `Raisecom(config)#spanning-tree max-hops` *hops-value* | (Optional) configure the maximum number of hops of the MST domain.<br>You can use the **no spanning-tree max-hops** command to restore default configurations. |
| 3 | `Raisecom(config)#spanning-tree region-configuration` | Enter MST domain configuration mode. |
| 4 | `Raisecom(config-region)#name` *name* | (Optional) configure the MST domain name.<br>You can use the **no name** command to restore default configurations. |
| 5 | `Raisecom(config-region)#revision-level` *level-value* | (Optional) configure the revision level of the MST domain.<br>You can use the **no revision-level** command to restore default configurations. |
| 6 | `Raisecom(config-region)#instance` *instance-id* `vlan` *vlan-list* | (Optional) configure mapping between the MST domain VLAN and the instance.<br>You can use the **no instance** *instance-id* [ **vlan** *vlan-list* ] command to restore default configurations. |

**Note**

Only when the device is the domain root, the configured maximum number of hops is that of the MST domain; configurations on non-domain root bridges do not take effect.

## 6.3.5 Configuring root bridge and backup root bridge

Two modes for MSTP root bridge selection: one is to configure the system priority and confirm the STP root bridge or backup root bridge through STP calculation; the other is to assign the root bridge or backup root bridge directly by commands.

When the root bridge fails or is powered off, the backup root bridge can replace the root bridge for related instances. In this case, if you have configured a new root bridge, the backup bridge will recover from the root bridge. If you have configured multiple backup bridges for a spanning tree instance, once the root bridge stops working, MSTP will choose the backup root bridge with the smallest bridge ID (composed by system priority and MAC address) as the root bridge.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |
| 2 | `Raisecom(config)#spanning-tree [ instance` *instance-id* `] root { primary \| secondary }` | Configure the device as the root bridge or backup root bridge.<br>You can use the **no panning-tree** [ **instance** *instance-id* ] **root** command to restore default configurations. |

**Caution**

We recommend that you had better not modify the system priority of any device in the network if you adopt the mode of assigning the root bridge directly; otherwise, the assigned root bridge or backup root bridge may be invalid.

**Note**

- You can make sure the effective instance of a root bridge or backup root bridge through the instance-id parameter. If the value of the instance-id is 0 or this parameter is omitted, the current device will be designated as the root bridge or backup root bridge of CIST.
- The device root types in instances are independent mutually, that is, they not only can be the root bridge or backup root bridge of one instance, but also the root bridge or backup root bridge of other spanning tree instances. However, in the same spanning tree instance, the same device cannot be used as both root bridge and backup root bridge simultaneously.
- You cannot assign two or more root bridges for one spanning tree instance, but can assign multiple backup bridges for one spanning tree. Generally, we recommend you to assign one root bridge and multiple backup root bridges for one spanning tree.

## 6.3.6 Configuring system priority and port priority

Whether a port is selected as the root port depends on its priority if the path cost to the root bridge is identical. The smaller the port priority is, the more preferentially the port is selected as the root port. A port may have different priorities and play different roles in different instances.

The device Bridge ID decides whether it can be selected as the root of a spanning tree. Configure a smaller priority to get a smaller device Bridge ID and reach the purpose to designate some device as the root of a spanning tree. If the priority is identical, the device with smaller MAC address will be selected as the root.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |
| 2 | `Raisecom(config)#spanning-tree [ instance` *instance-id* `] priority` *priority-value* | Configure the system priority.<br>You can use the **no spanning-tree** [ **instance** *instance-id* ] **priority** command to restore default configurations. |

| Step | Command | Description |
|---|---|---|
| 3 | Raisecom(config)#**interface** { **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-id* | Enter physical interface configuration mode. |
| 4 | Raisecom(config-if-*-*:*)#**spanning-tree** [ **instance** *instance-id* ] **priority** *priority-value* | Configure the port priority.<br>You can use the **no spanning-tree** [ **instance** *instance-id* ] **priority** command to restore default configurations. |

**Note**

The priority must be a multiple of 4096, such as 0, 4096, and 8192, and the default value is 32768.

## 6.3.7 Configuring switching network diameter

Network diameter refers to the number of nodes on the path with the most devices in a switching network. In MSTP, the network diameter is valid only to CIST, but not to the MSTI. In the same domain, no matter how many nodes in a path, it is considered as just one node to calculate. Actually, the network diameter should be defined as the number of domains in the path crossing the most domains. The network diameter is 1 if there is only one domain in the whole network.

The maximum number of hops of the MST domain is used to indicate the scale of the domain, while the network diameter is used to indicate the scale of the whole network. The bigger the network diameter is, the bigger the network scale is.

Similar to maximum number of hops of the MST domain, the configuration takes effect only when the configured device serves as the CIST root device. When you configure the network diameter parameters, the MSTP will set Hello Time, Forward Delay, and Max Age to an optimal value automatically through calculation.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**spanning-tree bridge-diameter** *bridge-diameter-value* | Configure the switching network diameter.<br>You can use the **no spanning-tree bridge-diameter** command to restore default configurations. |

## 6.3.8 Configuring internal port path cost

When selecting the root port and designated port, the smaller the port path cost is, the easier it is selected as the root port or designated port. Internal port path cost is mutually independent in different instances.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**interface** { **gigabitethernet** \| **gigabitethernet** } *slot-id/port-id* | Enter physical interface configuration mode. |
| 3 | Raisecom(config-if-*-*:*)#**spanning-tree** [ **instance** *instance-id* ] **inter-path-cost** *cost-value* | Configure the internal port path cost for a spanning tree instance.<br>You can use the **no spanning-tree** [ **instance** *instance-id* ] **inter-path-cost** command to restore default configurations. |

## 6.3.9 Configuring external port path cost

External path cost is the path cost from the device to CIST root device, and the external path cost in the same domain is the same.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**interface** { **gigabitethernet** \| **gigabitethernet** } *slot-id/port-id* | Enter physical interface configuration mode. |
| 3 | Raisecom(config-if-*-*:*)#**spanning-tree extern-path-cost** *cost-value* | Configure the external port path cost.<br>You can use the **no spanning-tree extern-path-cost** command to restore default configurations. |

## 6.3.10 Configuring port maximum Tx rate

The maximum Tx rate refers to the maximum number of BPDUs allowed to be transmitted by MSTP in each Hello Time. In a Hello Time period, the number of Tx packets cannot exceed transit-limit+1 to avoid network oscillation from causing the frequent change of network topology, which makes the device transmit BPDUs frequently. This parameter is a relative value with no unit. The bigger the parameter is configured, the more packets are permitted to be transmitted in a Hello Time, the more device resource it consumes. The configuration takes effect on the root device only.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**spanning-tree transit-limit** *value* | Configure the port maximum Tx rate.<br>You can use the **no spanning-tree transit-limit** command to restore default configurations. |

## 6.3.11 Configuring MSTP timers

There are three MSTP timers:

- Hello Time timer: the interval of the device to send bridge configuration information (BPDU) regularly to detect whether the link fails or not. The device sends hello packets to other devices around every Hello Time to check if there is any failure in the link. The default value is 2s, and you can adjust the interval according to network conditions. Reduce the interval when the network link changes frequently to enhance the robustness of STP; on the contrary, increasing interval value will reduce the system CPU resource occupation rate for STP.
- Forward Delay timer: the time parameter to ensure safe status transition of the device. Link fault initiates the network to recalculate spanning tree, but the new configuration recalculated cannot be transmitted to the whole network immediately. There may be temporary loop if the new root port and designated port start transmitting data at once. This protocol adopts a status transition mechanism: before the root port and designated port start forwarding data, it experiences a medium status (learning status), after a Forward Delay, it enters the forwarding status. The delay guarantees the new configuration to be transmitted through whole network. You can adjust the delay according to actual conditions, that is, reduce it when the network topology changes infrequently and increase it otherwise.
- Max Age timer: the bridge configuration information used by STP has a life time, which is used to judge whether the configuration information is outdated. The device will discard outdated information and STP will recalculate spanning tree. Too small age value may cause frequent recalculation of spanning tree, while too big age value will make STP not adapt to the network topology change timely.

All devices in the whole switching network adopt the three time parameters on the CIST root device, so only the configuration on the root device is valid.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |
| 2 | `Raisecom(config)#spanning-tree hello-time` *value* | Configure the Hello Time timer.<br>You can use the **no spanning-tree hello-time** command to restore default configurations. |
| 3 | `Raisecom(config)#spanning-tree forward-delay` *value* | Configure the Forward Delay timer.<br>You can use the **no spanning-tree forward-delay** command to restore default configurations. |
| 4 | `Raisecom(config)#spanning-tree max-age` *value* | Configure the Max Age timer.<br>You can use the **no spanning-tree max-age** command to restore default configurations. |

**Note**

The values of Forward Delay and Max Age will change after you modify the value of Hello Time. The formula is as below:

- Max Age = (4 + network diameter/2) × Hello Time + network diameter − 1 − ((Hello Time + 1)/2) × ((network diameter + 1)/2), and if the Max Age < 6, the MaxAge = 6; if the MaxAge > 40, the Max Age = 40.
- If ((Hello Time + 1) × network diameter)/2 = 0, the Forward Delay = 2 × Hello Time + ((HelloTime + 1) × network diameter)/2; otherwise, the ForwardDelay = 2 × Hello Time + ((HelloTime + 1)* network diameter)/2 + 1; and if the ForwardDelay < 4, the Forward Delay = 4; if the Forward Delay > 30, the Forward Delay = 30.

In addition, the value of Forward Delay will change after you modify the value of Max Age. The formula is as below:

- If 3/4 × Max Age < 4, the Forward Delay = 4.
- If 3/4 × Max Age > 30, the Forward Delay = 30.
- Otherwise, the Forward Delay = 3/4 × HelloTime.

Return operation fails and the system will prompt error information when the configured value exceeds the range between 6 ≤ Max Age ≤ 40 and Max Age ≥ 2 × Hello Time + 1.

Return operation fails and the system will prompt error information when the configured value exceeds the range between 4 ≤ Forward Delay ≤ 30 and Forward Delay ≥ Max Age/2 + 1.

## 6.3.12 Configuring edge port

Edge port refers to the port neither connects to any devices directly nor connects to any device indirectly via network.

Configuring the edge port can change the port to the forwarding status quickly without any wait time. For the Ethernet port connected to the user terminal directly, you can configure it as the edge port to make it change to forwarding status quickly.

Configure the ISCOM5508-GP as below.

| 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-*-*:*)#**spanning-tree edged-port** { **auto** \| **force-true** \| **force-false** } | Configure edge port properties. |

## 6.3.13 Configuring link type

The two ports connected by a point-to-point link can change to the forwarding status quickly by transmitting synchronous packets, thus reducing unnecessary forwarding delay. By default, the MSTP configure the port link type according to the duplex mode. The full-duplex port is considered as a point-to-point link; half-duplex port is considered as a shared link.

You can configure the current Ethernet port to connect a point-to-point link by force, but the system will fail if the link is not a point-to-point one. Generally, we recommend you to configure this item in automatical status. In this case, the system will automatically detect whether the port is connected to a point-to-point link.

Configure the ISCOM5508-GP as below.

| 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-*-*:*)#**spanning-tree link-type** { **point-to-point** \| **shared** \| **auto** } | Configure the port link type.<br>You can use the **no spanning-tree link-type** command to restore default configurations. |

## 6.3.14 Configuring root port protection

When a bridge receives the packet with a higher priority, the bridge will be reselected. Reselection affects the network connectivity and consumes CPU resources. For the network enabled with the MSTP function, if someone sends the BPDU with a higher priority to attack the network, the network becomes unstable due to the continuous selection. Generally, the priority of each bridge has already been configured in the stage of network planning. The nearer to the edge the bridge is, the lower priority it has. So downlink ports cannot receive packets with priorities higher than the bridge priority (except the bridge reselection on the MSTP network caused by wrong connection of a device with a higher priority or hostile attacks). For these downlink ports, you can enable root port protection to refuse to deal with packets with priorities higher than the bridge priority and block the port for a period if it receives the packet with a higher priority, in order to prevent the attack source from damaging the upper layer link.

Configure the ISCOM5508-GP as below.

| 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-*-*:*)#**spanning-tree rootguard** | Configure root port protection.<br>You can use the **no spanning-tree rootguard** command to disable this function. |

## 6.3.15 Configuring port loop protection

Spanning tree provides two functions: loop protection and link backup. Loop protection requires carving up the network topology into the tree structure. There must be redundant links in the topology to perform link backup. Spanning tree can avoid loops by blocking the redundant links and enable link backup by enabling redundant links when the link breaks down.

Spanning tree modules exchange packets periodically. The link is considered to fail if it has not received packets in a period. Then a new link will be reselected and the backup port is enabled. In actual network applications, the packets cannot be received may not because of link failure; then at this time, enabling the backup port may lead to loop.

The purpose of loop protection is to keep the port in its original status without reselection when it cannot receive packets in a period. You should note that loop protection and link backup is mutually exclusive, that is, the trade-off of loop protection is disabling link backup.

Configure the ISCOM5508-GP as below.

| 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-*-*:*)#**spanning-tree loopguard** | Configure port loop protection.<br>You can use the **no spanning-tree loopguard** command to disable this function. |

## 6.3.16 Performing mcheck operation

There are two working modes for ports on the device supporting the MSTP function: STP compatible mode and MSTP mode. Suppose the port of a MSTP device in a switching network is connected to a device running STP, the port will change to work in STP compatible mode automatically. But the port cannot change to work in MSTP mode if the STP device is removed, i.e. the port still works in STP compatible mode. You can perform the mcheck operation to force the port to work in MSTP mode. Of course, if the port receives new STP packets again, it will return to STP compatible mode.

Configure the ISCOM5508-GP as below.

| 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-*-*:*)#**spanning-tree mcheck** | Perform the mcheck operation to forcibly return the port to MSTP mode. |

## 6.3.17 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show spanning-tree** [ **instance** *instance-id* ] [ **detail** ] | Show spanning tree configurations. |
| 2 | Raisecom#**show interface** { **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-id* **spanning-tree** [ **instance** *instance-id* ] [ **detail** ] | Show spanning tree configurations on the interface. |
| 3 | Raisecom#**show spanning-tree region-configuration** | Show MST domain configurations. |

| No. | Command | Description |
|---|---|---|
| 4 | Raisecom#**show spanning-tree region-operation** | Show MST domain operation information. |

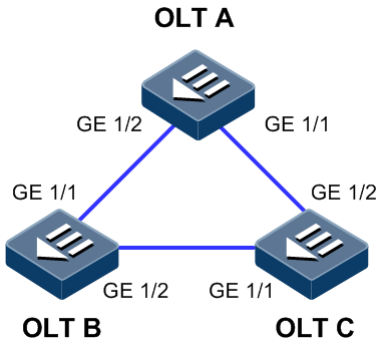
# 6.4 Configuration examples

## 6.4.1 Example for configuring STP

### Networking requirements

As shown in Figure 6-6, three devices OLT A, OLT B, and OLT C form a ring network. To solve the loop problem in a physical link ring, you need to enable STP on the three devices, and configure the priority of OLT A as 0 and the cost from OLT B to OLT A as 10.

Figure 6-6 STP networking




### Configuration steps

Step 1 Enable STP on OLT A.

```
Raisecom#config
Raisecom(config)#spanning-tree
Raisecom(config)#spanning-tree mode stp
```

Step 2 Configure port mode for OLT A.

```
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:1)#exit
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:2)#exit
```

Step 3 Configure the OLT A spanning tree priority and port path cost.

```
Raisecom(config)#spanning-tree priority 0
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#spanning-tree extern-path-cost 10
Raisecom(config-if-gigabitethernet-1:2)#exit
```

Configurations of OLT B and OLT C are identical with those of OLT A, so refer to OLT A configurations for related configuration.

## Checking results

Show the bridge status.

- OLT A

```
Raisecom#show spanning-tree
MSTP Admin State: Enable
Protocol Mode: STP
BridgeId:    Mac 000E.5E7B.C557  Priority 0
Root:       Mac 000E.5E7B.C557  Priority 0   RootCost 0
Operational:  HelloTime 2, ForwardDelay 15, MaxAge 20
Configured:   HelloTime 2, ForwardDelay 15, MaxAge 20 TransmitLimit 3
```

- OLT B

```
Raisecom#show spanning-tree
MSTP Admin State: Enable
Protocol Mode: STP
BridgeId:    Mac 000E.5E83.ABD1  Priority 32768
Root:       Mac 000E.5E7B.C557  Priority 0   RootCost 10
Operational:  HelloTime 2, ForwardDelay 15, MaxAge 20
Configured:   HelloTime 2, ForwardDelay 15, MaxAge 20 TransmitLimit 3
```

- OLT C

```
Raisecom#show spanning-tree
MSTP Admin State: Enable
Protocol Mode: STP
BridgeId:    Mac 000E.5E83.ABD5  Priority 32768
Root:       Mac 000E.5E7B.C557  Priority 0   RootCost 20000
Operational:  HelloTime 2, ForwardDelay 15, MaxAge 20
Configured:   HelloTime 2, ForwardDelay 15, MaxAge 20 TransmitLimit 3
```

Show the port status.

- OLT A

```
Raisecom#show interface gigabitethernet 1/1-2 spanning-tree
Port ID: gigabitethernet1/1
PortEnable: admin: enable
oper: enable
Rootguard: disable
Loopguard: disable
ExternPathCost:10
Partner MSTP Mode: stp
Bpdus send:   279 (TCN<0>   Config<279> RST<0> MST<0>)
Bpdus received:13 (TCN<13>   Config<0> RST<0> MST<0>)
State:forwarding Role:designated     Priority:128   Cost: 20000
Root:       Mac 000E.5E7B.C557 Priority 0   RootCost 0
DesignatedBridge: Mac 000E.5E7B.C557 Priority 0   DesignatedPort 32777

Port ID: gigabitethernet1/2
PortEnable: admin: enable
oper: enable
Rootguard: disable
Loopguard: disable
ExternPathCost:20000
Partner MSTP Mode: stp
Bpdus send:   279 (TCN<0>   Config<279> RST<0> MST<0>)
Bpdus received:6 (TCN<6>   Config<0> RST<0> MST<0>)
State:forwarding Role:designated     Priority:128   Cost: 20000
Root:       Mac 000E.5E7B.C557 Priority 0   RootCost 0
DesignatedBridge: Mac 000E.5E7B.C557 Priority 0   DesignatedPort 32778
```

- OLT B

```
Raisecom#show interface gigabitethernet 1/1-2 spanning-tree
Port ID: gigabitethernet1/1
PortEnable: admin: enable
oper: enable
Rootguard: disable
Loopguard: disable
ExternPathCost:10
Partner MSTP Mode: stp
Bpdus send:   357 (TCN<0>   Config<357> RST<0> MST<0>)
Bpdus received:13 (TCN<12>   Config<1> RST<0> MST<0>)
State:forwarding Role:designated     Priority:128   Cost: 20000
Root:       Mac 000E.5E7B.C557 Priority 0   RootCost 10
DesignatedBridge: Mac 000E.5E7B.C558 Priority 0   DesignatedPort 32777

Port ID: gigabitethernet1/2
PortEnable: admin: enable
oper: enable
Rootguard: disable
Loopguard: disable
ExternPathCost:20000
```

```
Partner MSTP Mode: stp
Bpdus send:    36  (TCN<13>    Config<23>  RST<0>  MST<0>)
Bpdus received:335  (TCN<0>    Config<335>  RST<0>  MST<0>)
State:forwarding  Role:root     Priority:128    Cost: 20000
Root:        Mac 000E.5E7B.C557  Priority 0    RootCost 20000
DesignatedBridge: Mac 000E.5E83.ABD1  Priority 32768    DesignatedPort
32777
```

- OLT C

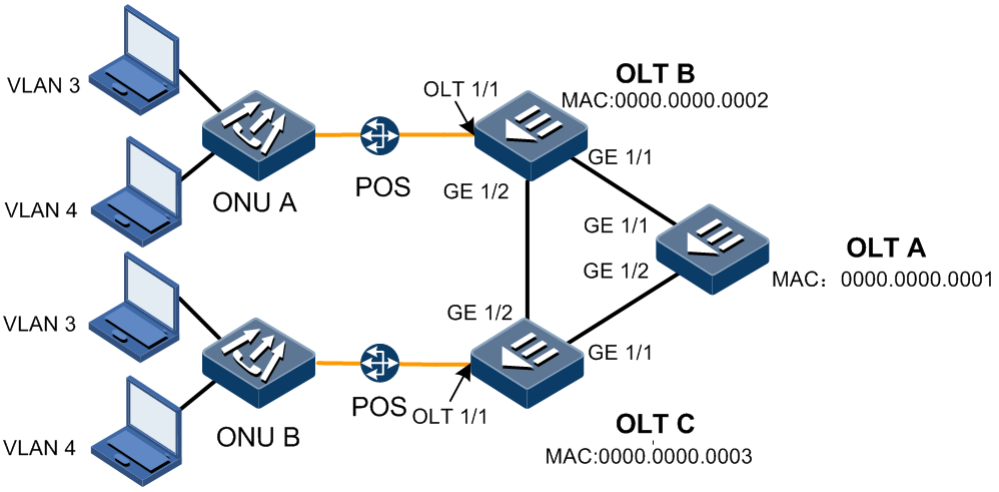
```
Raisecom#show interface gigabitethernet 1/1-2 spanning-tree
Port ID: gigabitethernet1/1
PortEnable: admin: enable
oper: enable
Rootguard:  disable
Loopguard:  disable
ExternPathCost:20000
Partner MSTP Mode: stp
Bpdus send:    22  (TCN<12>    Config<10>  RST<0>  MST<0>)
Bpdus received:390  (TCN<0>    Config<390>  RST<0>  MST<0>)
State:blocking  Role:non-designated     Priority:128    Cost: 20000
Root:        Mac 000E.5E7B.C557  Priority 0    RootCost 20000
DesignatedBridge: Mac 000E.5E83.ABD1  Priority 32768    DesignatedPort
32777

Port ID: gigabitethernet1/2
PortEnable: admin: enable
oper: enable
Rootguard:  disable
Loopguard:  disable
ExternPathCost:20000
Partner MSTP Mode: stp
Bpdus send:    38  (TCN<6>    Config<32>  RST<0>  MST<0>)
Bpdus received:368  (TCN<0>    Config<368>  RST<0>  MST<0>)
State:forwarding  Role:root     Priority:128    Cost: 20000
Root:        Mac 000E.5E7B.C557  Priority 0    RootCost 0
DesignatedBridge: Mac 000E.5E7B.C557  Priority 0    DesignatedPort 32778
```

## 6.4.2 Example for configuring MSTP

### Networking requirements

As shown in Figure 6-7, three devices OLT A, B, C form a ring network and run the MSTP protocol with a domain name aaa. OLT B and OLT C connect with two PCs respectively which belong to VLAN 3 and VLAN 4 respectively. Instance 3 associates with VLAN 3 and instance 4 associates with VLAN 4. You can configure the path cost for instance 3 of OLT B to forward two VLAN packets in two paths respectively, in which way to realize loop protection and load sharing.

Figure 6-7 MSTP networking




## Configuration steps

Step 1 Create VLAN 3 and VLAN 4 on three OLT devices respectively and activate them.

Configure OLT A.

```
Raisecom#config
Raisecom(config)#create vlan 3-4 active
Raisecom(config)#end
```

Configure OLT B.

```
Raisecom#config
Raisecom(config)#create vlan 3-4 active
Raisecom(config)#end
```

Configure OLT C.

```
Raisecom#config
Raisecom(config)#create vlan 3-4 active
Raisecom(config)#end
```

Step 2 Uplink ports GE 1/1 and GE 1/2 of OLT A, OLT B, and OLT C work in Trunk mode to allow all VLANs to pass. Downlink ports OLT 1/1 of OLT B and OLT C work in Trunk mode to allow VLAN 3 and VLAN 4 to pass.

Configure OLT A.

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

```
Raisecom(config-if-gigabitethernet-1:1)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:1)#exit
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:2)#exit
```

Configure OLT B.

```
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:1)#exit
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:2)#exit
Raisecom(config)#interface gpon-olt 1/1
Raisecom(config-if-gpon-olt-1:1)#switchport mode trunk
Raisecom(config-if-gpon-olt-1:1)#switchport trunk allowed vlan 3,4
Raisecom(config-if-gpon-olt-1:1)#exit
```

Configure OLT C.

```
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:1)#exit
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:2)#exit
Raisecom(config)#interface gpon-olt 1/1
Raisecom(config-if-gpon-olt-1:1)#switchport mode trunk
Raisecom(config-if-gpon-olt-1:1)#switchport trunk allowed vlan 3,4
```

Step 3 Configure OLT A, OLT B, and OLT C to MSTP mode and enable STP. Enter MSTP configuration mode and configure the domain name as aaa, the revision version as 0, instance 3 mapping VLAN 3, and instance 4 mapping VLAN 4.

Configure OLT A.

```
Raisecom(config)#spanning-tree mode mstp
Raisecom(config)#spanning-tree
Raisecom(config)#spanning-tree region-Command
Raisecom(config-region)#name aaa
Raisecom(config-region)#revision-level 0
Raisecom(config-region)#instance 3 vlan 3
Raisecom(config-region)#instance 4 vlan 4
Raisecom(config-region)#exit
```

Configure OLT B.

```
Raisecom(config)#spanning-tree mode mstp
Raisecom(config)#spanning-tree
Raisecom(config)#spanning-tree region-Command
Raisecom(config-region)#name aaa
Raisecom(config-region)#revision-level 0
Raisecom(config-region)#instance 3 vlan 3
Raisecom(config-region)#instance 4 vlan 4
Raisecom(config-region)#exit
```

Configure OLT C.

```
Raisecom(config)#spanning-tree mode mstp
Raisecom(config)#spanning-tree
Raisecom(config)#spanning-tree region-Command
Raisecom(config-region)#name aaa
Raisecom(config-region)#revision-level 0
Raisecom(config-region)#instance 3 vlan 3
Raisecom(config-region)#instance 4 vlan 4
Raisecom(config-region)#exit
```

Step 4 On OLT B, modify the internal path cost of port GE 1/1 in spanning tree instance 3 as 500000.

```
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#spanning-tree instance 3 inter-
path-cost 500000
```

## Checking results

Show MST domain configurations.

```
Raisecom#show spanning-tree region-operation
Operational:
-----------------------------------------------
Name: aaa
Revision level: 0       Instances running: 3
Digest: 0x024E1CF7E14D5DBBD9F8E059D2C683AA
Instance     Vlans Mapped
--------     ----------------------
0          1,2,5-4094
3          3
4          4
```

Show information about MSTI 3.

- OLT A

```
Raisecom#show spanning-tree instance 3
MSTP Admin State: Enable
Protocol Mode: MSTP
MST ID: 3
------------------------------------------------------------
BridgeId:    Mac 0000.0000.0001  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost 0
PortId  PortState   PortRole   PathCost  PortPriority  LinkType   TrunkPort
------------------------------------------------------------------------
gigabitethernet1/1      forwarding  designated 20000    128         point-
to-point  no
gigabitethernet1/2      forwarding  designated 20000    128         point-
to-point  no
```

- OLT B

```
Raisecom#show spanning-tree instance 3
MSTP Admin State: Enable
Protocol Mode: MSTP
MST ID: 3
------------------------------------------------------------
BridgeId:    Mac 0000.0000.0002  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost
500000
PortId  PortState   PortRole   PathCost  PortPriority  LinkType   TrunkPort
------------------------------------------------------------------------
gigabitethernet1/1      discarding  alternate  500000    128         point-
to-point  no
gigabitethernet1/2      forwarding  root       20000    128         point-
to-point  no
gpon-olt1/1      forwarding  designated 20000    128         point-to-point
no
```

- OLT C

```
Raisecom#show spanning-tree instance 3
MSTP Admin State: Enable
Protocol Mode: MSTP
MST ID: 3
------------------------------------------------------------
BridgeId:    Mac 0000.0000.0003  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost 20000
PortId  PortState   PortRole   PathCost  PortPriority  LinkType   TrunkPort
```

```
------------------------------------------------------------------------
gigabitethernet1/1      forwarding  root        20000    128         point-
to-point  no
gigabitethernet1/2      forwarding  designated 20000    128         point-
to-point  no
gpon-olt1/1      forwarding  designated 20000    128         point-to-point
no
```

Show information about MSTI 4.

- OLT A

```
Raisecom#show spanning-tree instance 4
MSTP Admin State: Enable
Protocol Mode: MSTP
MST ID: 4
------------------------------------------------------------
BridgeId:    Mac 0000.0000.0001  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost 0
PortId  PortState   PortRole   PathCost  PortPriority  LinkType   TrunkPort
------------------------------------------------------------------------
gigabitethernet1/1      forwarding  designated 20000    128         point-
to-point  no
gigabitethernet1/2      forwarding  designated 20000    128         point-
to-point  no
```

- OLT B

```
Raisecom#show spanning-tree instance 4
MSTP Admin State: Enable
Protocol Mode: MSTP
MST ID: 4
------------------------------------------------------------
BridgeId:    Mac 0000.0000.0002  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost 20000
PortId  PortState   PortRole   PathCost  PortPriority  LinkType   TrunkPort
------------------------------------------------------------------------
gigabitethernet1/1      forwarding  root      200000    128         point-
to-point  no
gigabitethernet1/2      forwarding  designated 20000    128        point-
to-point  no
gpon-olt1/1            forwarding  designated   20000    128         point-
to-point  no
```

- OLT C

```
Raisecom#show spanning-tree instance 4
MSTP Admin State: Enable
```

```
Protocol Mode: MSTP
MST ID: 4
------------------------------------------------------------
BridgeId:    Mac 0000.0000.0003  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost 20000
PortId  PortState   PortRole   PathCost  PortPriority  LinkType  TrunkPort
------------------------------------------------------------------------
gigabitethernet1/1      forwarding  root       20000    128         point-
to-point  no
gigabitethernet1/2      discarding  alternate  200000    128         point-
to-point  no
gpon-olt1/1             forwarding  designated   20000    128         point-
to-point  no
```

# 7 Configuring routing

This chapter introduces the routing feature and configure process of the ISCOM5508-GP, and provides related configuration examples, including the following sections:

- Overview of route
- Configuring ARP
- Configuring static route
- Configuring VRRP
- Configuration examples

## 7.1 Overview of route

### 7.1.1 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, you must learn the physical address of the destination host. It means that you 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 relationship between IP addresses and MAC addresses, helping translate IP addresses into MAC addresses.

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

- Static ARP entry: static 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 ISCOM5508-GP.
  - Dynamic ARP entries are aged when the aging time is exceeded, if dynamic ARP entries are not used.

The ISCOM5508-GP supports **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 relationship between its IP address and its MAC address into the ARP request packet. Device B learns this mapping relationship 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.

# 7.2 Configuring ARP

## 7.2.1 Preparing for configurations

### Scenario

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

In general, ARP address entries are maintained by devices dynamically. The device searches the mapping relationship 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 cheat.

### Prerequisite

N/A

## 7.2.2 Default configurations

Default configurations of ARP on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Static ARP entries | N/A |
| Dynamic ARP learning mode | learn-all |

## 7.2.3 Configuring static ARP entries

**Caution**

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

Configure the ISCOM5508-GP as below.

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

| Step | Command | Description |
|---|---|---|
| 3 | Raisecom(config)#**arp aging-time** *time* | Configure the aging time of dynamic ARP entries.<br>You can use the **no arp aging-time** command to restore default configurations. |

### 7.2.4 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show arp** | Show all ARP entries. |
| 2 | Raisecom#**show arp static** | Show static ARP entries. |
| 3 | Raisecom#**show arp** *ip-address* | Show ARP entries with specified IP address. |
| 4 | Raisecom#**show arp interface vlanif** *vlan-id* | Show ARP entries on specified VLAN interface. |
| 5 | Raisecom#**show arp summary** | Show ARP table statistics. |

## 7.3 Configuring static route

### 7.3.1 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.

### 7.3.2 Configuring static route

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**ip routing** | Enable routing.<br>You can use the **no ip routing** command to disable this function. |
| 3 | Raisecom(config)#**router id** *id* | Configure the router ID.<br>You can use the **no router id** command to delete the configuration. |

| Step | Command | Description |
|---|---|---|
| 4 | Raisecom(config)#**ip route** *ip-address mask nexthopip* [ **distance***value* ] [ **description** *description* ] [ **tag** *tag-id* ] | Configure the static route.<br>You can use the **no ip route** *ip-address mask nexthopip* command to delete the configuration. |
| 5 | Raisecom(config)#**ip route static distance** *value* | (Optional) configure the management distance of the static route.<br>You can use the **no ip route static distance** command to restore default configurations. |

### 7.3.3 Checking configurations

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show ip route** [ **detail** ] | Show routing details. |
| 2 | Raisecom#**show ip route** *ip-address* [ *ip-mask* ] [ **longer-prefixes** ] [ **detail** ] | Show routing information to a specified IP address. |
| 3 | Raisecom#**show ip route** start-*ip-address ip-mask end-ip-address ip-mask* [ **detail** ] | Show routing information in a specified address range. |
| 4 | Raisecom#**show ip route protocol** { **static** \| **direct** \| **ospf** } | Show routing information about a specified protocol. |
| 5 | Raisecom#**show ip route statistics** | Show routing statistics. |
| 6 | Raisecom#**show ip route protocol** { **direct** \| **static** \| **ospf** \| **rip** } | Show configurations of the routing protocol. |
| 7 | Raisecom#**show router id** | Show the router ID. |

## 7.4 Configuring VRRP

### 7.4.1 Preparing for configurations

#### Scenario

Virtual Router Redundancy Protocol (VRRP) is a fault-tolerant protocol.

In general, all hosts in the network are configured with a default route. Packets, whose destination address is not in the network segment, are sent through the default router. Therefore, hosts can communicate with the external network. However, if the default router fails, hosts will fail to communicate with the external network and a single-point fault occurs. VRRP can resolve this problem. VRRP is designed for the Local Area Network with multicast or broadcast capability (such as Ethernet).

### Prerequisite

Configure the IP address of the Layer 3 interface.

## 7.4.2 Default configurations

Default configurations of VRRP on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| VRRP alarm | Enable |
| VRRP | Enable |
| VRRP backup group | N/A |

## 7.4.3 Configuring VRRP

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**vrrp ping** | (Optional) enable VRRP. |
| 3 | Raisecom(config)#**vrrp trap** | (Optional) enable VRRP alarm. |
| 4 | Raisecom(config)#**interface vlanif** *vlan-id* | Enter VLAN interface configuration mode. |
| 5 | Raisecom(config-vlanif-*)#**vrrp** *id* **description** *text* | Configure descriptions about the VRRP backup group.<br>You can use the **no vrrp** *id* **description** *text* command to delete the configuration. |
| 6 | Raisecom(config-vlanif-*)#**vrrp** *id* { **enable** \| **disable** } | Enable/Disable the VRRP backup group. |
| 7 | Raisecom(config-vlanif-*)#**vrrp** *id* **ip** *ip-address* | Configure the IP address of the VRRP backup group.<br>You can use the **no vrrp** *id* **ip** *ip-address* command to delete the configuration. |
| 8 | Raisecom(config-vlanif-*)#**vrrp** *id* **preempt** [ **delay-time** *time* ] | Configure VRRP preemption and delay time.<br>You can use the **no vrrp** *id* **preempt** [ **delay-time** *time* ] command to delete the configuration. |
| 9 | Raisecom(config-vlanif-*)#**vrrp** *id* **priority** value | Configure the VRRP priority.<br>You can use the **no vrrp** *id* **priority** *value* command to delete the configuration. |
| 10 | Raisecom(config-vlanif-*)#**vrrp** *id* **timer advertise-interval** *time* | Configure the timer for sending VRRP notification packets.<br>You can use the **no vrrp** *id* **timer advertise-interval** *time* command to delete the configuration. |

| Step | Command | Description |
|---|---|---|
| 11 | Raisecom(config-vlanif-*)#**vrrp** *id* **track interface vlanif** *vlan-id* [ **reduced** *value* ] | Check VRRP. |

### 7.4.4 Checking configurations

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show vrrp** | Show VRRP configurations. |

## 7.5 Configuration examples

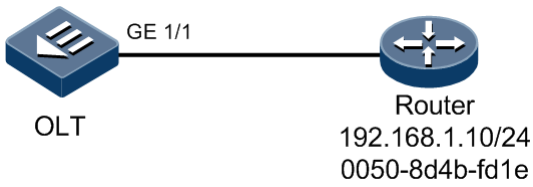
### 7.5.1 Example for configuring ARP

#### Networking requirements

As shown in Figure 7-1, the OLT device connects the host, and connects the upper layer router through the interface GE 1/1. The IP address of the router is 192.168.1.10/24, and the MAC address is 0050.8d4b.fd1e.

You need to configure corresponding static ARP entries on the OLT to increase the communication security between the OLT and router.

Figure 7-1 ARP networking




#### Configuration steps

Add a static ARP entry.

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

#### Checking results

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

```
Raisecom#show arp

ARP mode: Learn all
IP Address      Mac Address      Interface        Type     Age(s)
--------------------------------------------------------------------------
192.168.1.10     0050.8d4b.fd1e   ip1  static   3

Total:  1
Static: 1
Dynamic:0
```

# 8 Configuring DHCP

This chapter introduces the DHCP feature and configuration process of the ISCOM5508-GP, and provides related configuration examples, including the following sections:

- Overview of DHCP
- Configuring DHCP Snooping
- Configuring DHCP Relay
- Configuring DHCP Option 82
- Configuration examples

## 8.1 Overview of DHCP

With development of Internet, it is more complex to manage IP addresses in the network.

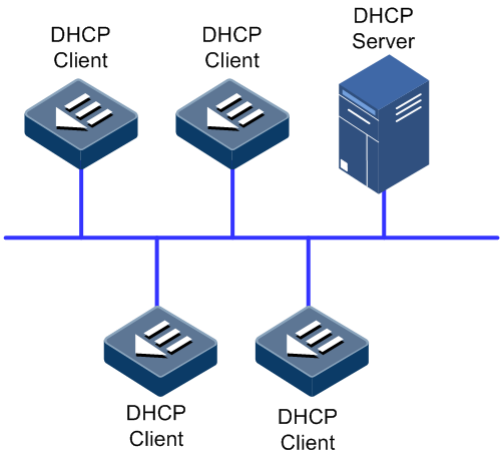
- The number of PCs in the network increases dramatically, which consumes a lot of human resources to manually configure and modify their IP addresses.
- There are multiple laptops in the network, whose IP addresses are frequently changed. The administrator must modify IP configurations frequently.
- To improve IP management efficiency, the administrator must perform centralized management on IP addresses.

Dynamic Host Configuration Protocol (DHCP) can be used to solve the above problems. DHCP can automatically allocate IP addresses for all clients in the network. It helps reduce workload of the administration, realizing centralized management of IP addresses.

DHCP works in a Client/Server mode. The Client sends an IP request to the Server. The Server provides an IP address and related configurations for the Client, once receiving the IP request.

A typical DHCP application contains at least a SHCP server and multiple DHCP clients (including PCs and laptops), as shown in Figure 8-1.

Figure 8-1 Typical application of DHCP




## Working principles of DHCP

The DHCP server provides IP configurations for a DHCP client by flowing the below steps:

- IP request: a DHCP client broadcasts a DHCP Discover packet to query DHCP servers of the network segment for acquiring an IP address and related configurations.
- IP offer: all DHCP servers in the network segment broadcast a DHCP Offer packet after receiving the DHCP Discover packet. The DHCP Offer packet contains an IP address and related configurations provided for the DHCP client. In addition, the packet contains the identifier of the DHCP server.
- IP selection: the DHCP client selects one IP as its IP address after receiving DHCP Offer packet(s). At the same time, the DHCP client broadcasts a DHCP Request packet to tell other DHCP servers the selected configurations and ask other DHCP servers to withdraw their configurations.
- IP acknowledgement: the DHCP server sends a DHCP Ack packet for acknowledgement after receiving the DHCP Request packet.

Then, the DHCP server implements allocating an IP address and related configurations for the DHCP client.

## DHCP lease renewal

After a DHCP client obtains an IP address from the DHCP server, it cannot use this IP address permanently. The IP address has a fixed usage period, which is called a lease. The lease interval can be assigned by users. If the DHCP client uses the IP address and related configurations permanently, it must ask the DHCP server to renew the lease for the client. The DHCP renewal process is shown as below.

- When 50% lease expires, the DHCP client sends a DHCP Request packet to the DHCP server for renewing the lease. If success, the lease becomes a complete one. Otherwise, a DHCP Request is sent again when 87.5% lease expires.
- When 87.5% lease expires, the DHCP client sends another DHCP Request packet to the DHCP server for renewing the lease. If success, the lease becomes a complete one. Otherwise, lease renewal fails. In addition, the IP address and related configurations are withdrawn.

### Scenarios of DHCP

In general, the DHCP server allocates IP addresses in the following scenarios:

- It is the heavy workload for manually configuring IP addresses in a large network.
- The number of PCs is greater than the number of available IP addresses in a network. The administrator cannot assign a fixed IP address to each PC. In addition, the number of PCs accessing the network is limited.
- A few PCs need a fixed IP address in the network.

## 8.1.2 DHCP packet

Figure 8-2 shows the DHCP packet structure.

Figure 8-2 DHCP packet structure

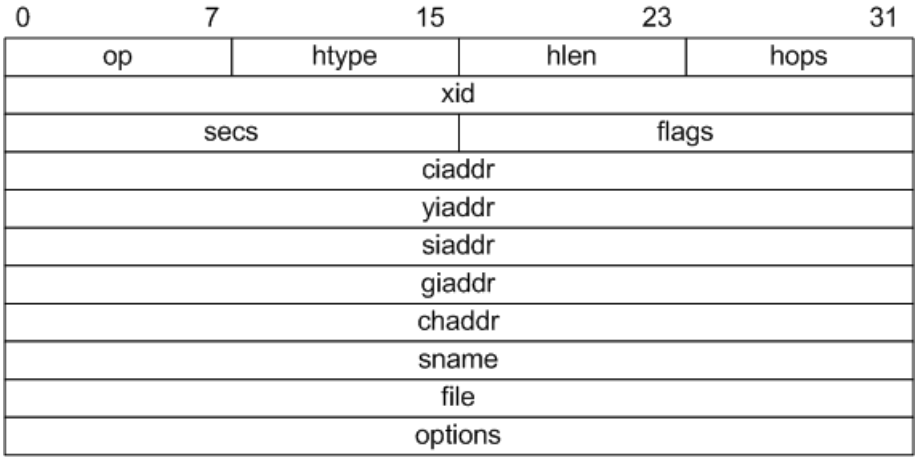



Table 8-1 lists meanings of fields in the DHCP packet.

Table 8-1 Meanings of fields in the DHCP packet

| Name | Length (B) | Description |
|---|---|---|
| op | 1 | Packet type<br>• 1: request packet<br>• 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<br>The value is added by 1 once 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. |
| secs | 2 | Time elapsed since the DHCP client initiates a DHCP request. At present, it is not used and is set to 0. |

| Name | Length (B) | Description |
|---|---|---|
| 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<br>• 0: unicast<br>• 1: broadcast<br>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 route information of 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). |

## 8.1.3 DHCP Snooping

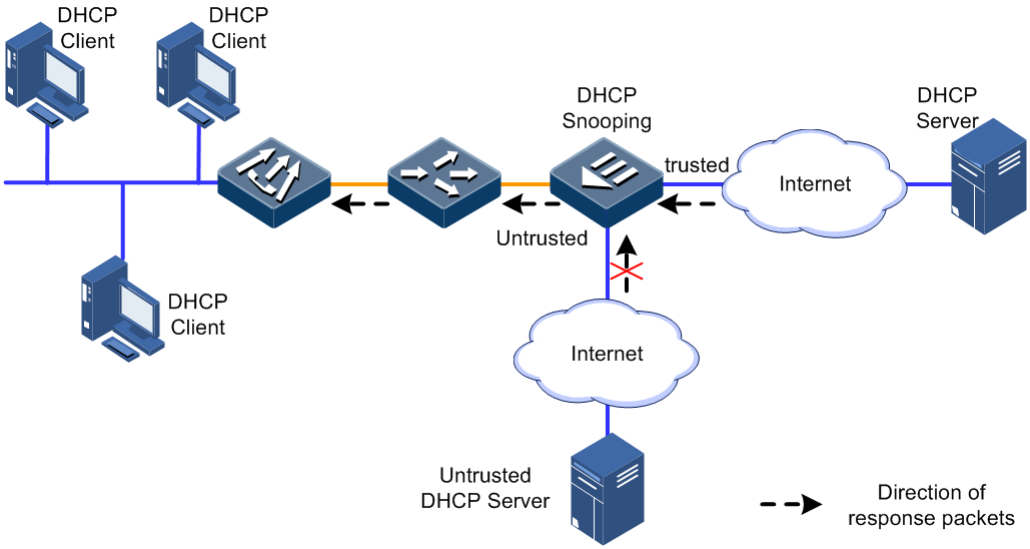
### Overview of DHCP Snooping

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

- Ensuring 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 8-3. To ensure DHCP clients obtain IP addresses from a legal DHCP server, the DHCP Snooping mechanism allows configuring ports as trusted ports or untrusted ports. Trusted ports can forward received DHCP packets properly while untrusted ports will discard packets from DHCP servers.

Figure 8-3 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 ports, including MAC addresses of DHCP clients, obtained IP addresses, ports connected to DHCP clients, and VLAN information of these ports. With this information, the DHCP Snooping can realize 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 a port by dynamically obtaining DHCP Snooping entries. It helps prevent illegal packets from passing through the port.

### 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 realize security and accounting control of DHCP clients.

If the ISCOM5508-GP is enabled with DHCP Snooping supporting Option, it takes the following two actions when receiving a DHCP packet.

- When the ISCOM5508-GP 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 ISCOM5508-GP 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.

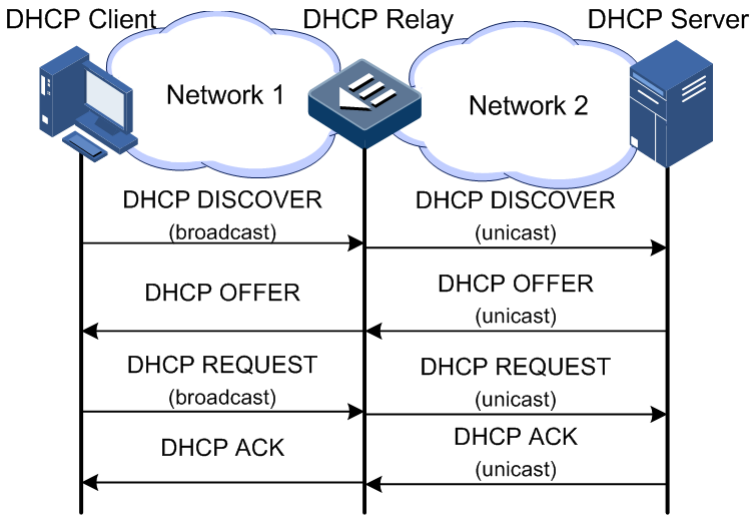
## 8.1.4 DHCP Relay

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 8-4 shows the working principle of DHCP Relay.

Figure 8-4 Working principle of DHCP Relay




As shown in Figure 8-4, 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.

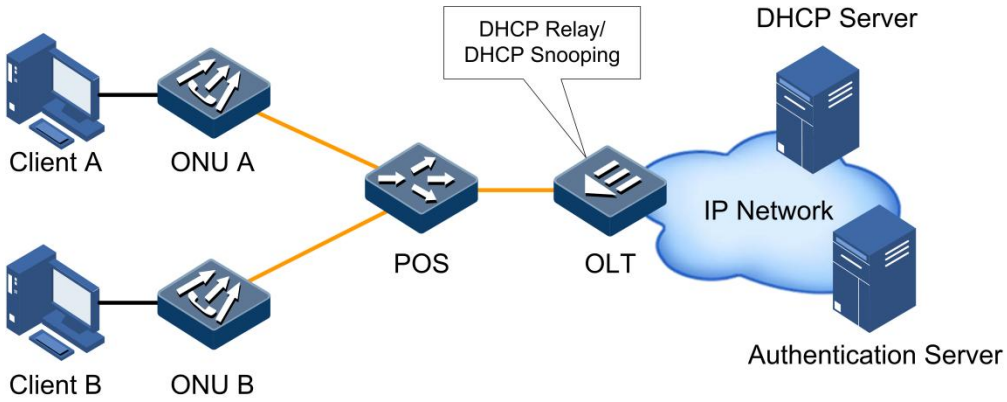
## 8.1.5 DHCP Option 82

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 8-5 Working principle of DHCP Option 82



As shown in Figure 8-5, the working process of DHCP Option 82 is as below.

Step 1 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 2 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 3 After the authentication server authenticates the client's legality, it sends an authentication response packet to the client, informing the client's authority.

Step 4 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 5 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 ISCOM5508-GP can perform policy route based on the source IP address. Therefore, users with different IP addresses have various routing rules and authorities.

# 8.2 Configuring DHCP Snooping

## 8.2.1 Preparing for configurations

### Scenario

DHCP Snooping is a DHCP security feature, being used to guarantee the DHCP client to get IP addresses 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 ISCOM5508-GP 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.
- Interface DHCP Snooping can take effect only after global DHCP Snooping is enabled. So you need to enable global DHCP Snooping before configuring interface DHCP Snooping.

## 8.2.2 Default configurations

Default configurations of DHCP Snooping on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Global DHCP Snooping | Disable |
| Interface DHCP Snooping | Enable |
| Interface DHCP Snooping trust status | Untrusted |
| DHCP Option 82 | Unsupported |

## 8.2.3 Configuring global DHCP Snooping

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#{ **ip** \| **ipv6** } **dhcp snooping** | Enable global DHCP Snooping.<br>You can use the **no ip dhcp snooping** command to disable this function. |

## 8.2.4 Configuring interface DHCP Snooping

Configure the ISCOM5508-GP as below.

| 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-*-*:*)#{ **ip**\| **ipv6** } **dhcp snooping** | Enable interface DHCP Snooping.<br>You can use the **no ip dhcp snooping** command to disable this function. |

## 8.2.5 Configuring interface DHCP Snooping trust

Configure the ISCOM5508-GP as below.

| 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. |

| Step | Command | Description |
|---|---|---|
| 3 | Raisecom(config-if-*-*:*)#{ **ip** \| **ipv6** } **dhcp snooping trust** | Enable interface trust.<br>You can use the **no ip dhcp snooping trust** command to disable this function. |

Generally, you need to make sure that the device connected interface at the legal DHCP server side is in trusted status, while the interface at the DHCP client side is in untrusted status.

## 8.2.6 (Optional) configuring DHCP Snooping supporting Option 82

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**ip dhcp information option** [ **schedule-list** *list-number* ] | Configure DHCP Snooping supporting Option 82.<br>You can use the **no ip dhcp information option** [ **schedule-list** *list-number* ] command to disable this function. |

If the device is enabled with DHCP Snooping without being configured with the DHCP Snooping supporting Option 82 function, the device will do nothing to Option 82 fields in the packets. For packets without Option 82 fields, the device also does not perform insertion operation.

## 8.2.7 Checking configurations

Use the following commands to check configuration results.

| 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. |

# 8.3 Configuring DHCP Relay

## 8.3.1 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.
- Interface DHCP Relay can take effect only after global DHCP Relay is enabled. So you need to enable global DHCP Relay before configuring interface DHCP Relay.

## 8.3.2 Default configurations

Default configurations of DHCP Relay on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Global DHCP Relay | Disable |
| Interface DHCP Relay | Enable |
| DHCP Relay interface destination IP address | N/A |
| ONU DHCP Relay interface destination IP address | N/A |
| Interface DHCP Relay trust status | Untrusted |
| DHCP Option 82 | Unsupported |
| Processing policy of request packets containing Option 82 field | Replace |

## 8.3.3 Configuring global DHCP Relay

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |
| 2 | `Raisecom(config)#ip dhcp relay` | Enable global DHCP Relay.<br>You can use the **no ip dhcp relay** command to disable this function. |

## 8.3.4 Configuring interface destination IP address

Configure the ISCOM5508-GP 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 dhcp relay** | Configure DHCP Relay on the VLAN interface,<br>You can use the **no ip dhcp relay** command to disable DHCP Relay. |
| 4 | Raisecom(config-vlanif-*)#**ip dhcp relay target-ip** *ip-address* | (Optional) configure the destination IP address of the VLAN interface. |

**Note**

When the DHCP client connects the DHCP server through multiple DHCP relays, we recommend that the number of DHCP relays does not exceed 4.

## 8.3.5 Configuring interface DHCP Relay trust

Configure the ISCOM5508-GP as below.

| 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-*-*:*)#**ip dhcp relay information trusted** | Configure DHCP Relay to trust interfaces.<br>You can use the **no ip dhcp relay informaiton trusted** command to restore default configurations. |

**Note**

Interface trust can take effect only when DHCP Relay supports DHCP Option 82.

## 8.3.6 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show ip dhcp relay** | Show DHCP Relay configurations. |
| 2 | Raisecom#**show ip dhcp relay statistics** | Show DHCP Relay statistics. |

# 8.4 Configuring DHCP Option 82

## 8.4.1 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.

**Note**

- Before configuring DHCP Option 82, you need to enable customized DHCP Option 82 firstly.
- To enable customized DHCP Option 82, see section 8.2.6 (Optional) configuring DHCP Snooping supporting Option 82.

## 8.4.2 Default configurations

Default configurations of DHCP Option 82 on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Global DHCP Option 82 | Disable |
| Global DHCP Option attach-string | N/A |
| Global remote-id | switch-mac |
| Interface circuit-id | N/A |
| Processing policy of DHCP packets containing Option 82 field | transparent |

## 8.4.3 Configuring DHCP Option 82

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |
| 2 | `Raisecom(config)#ip dhcp information option` | Enable DHCP Option 82 on the OLT.<br>You can use the **no ip dhcp information option** command to disable this function. |

## 8.4.4 Configuring global DHCP Option remote-id

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**ip dhcp information option remote-id** { **switch-mac** \| **client-mac** \| **switch-mac-string** \| **client-mac-string** \| **hostname** \| **string** *string* } | Configure the Remote ID of Option 82.<br>You can use the **no ip dhcp information option remote-id** command to restore default configurations. |

## 8.4.5 Configuring interface DHCP Option circuit-id

Configure the ISCOM5508-GP as below.

| 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-*-*:*)#**ip dhcp information option circuit-id** *string* | Configure the Circuit ID of Option 82.<br>You can use the **no ip dhcp information option circuit-id** command to restore default configurations. |

## 8.4.6 Configuring Option 82 packet processing policy

Configure the ISCOM5508-GP as below.

| 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-*-*:*)#**ip dhcp information option overwrite-policy** { **drop** \| **transparent** } | Configure the processing policy to the DHCP request packet containing Option 82 on the interface.<br>You can use the **no ip dhcp information option overwrite-policy** command to restore default configurations. |
| 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.<br>You can use the **no ip dhcp information option overwrite-policy** command to restore default configurations. |

## 8.4.7 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | `Raisecom#show ip dhcp information option` | Show DHCP Option configurations. |

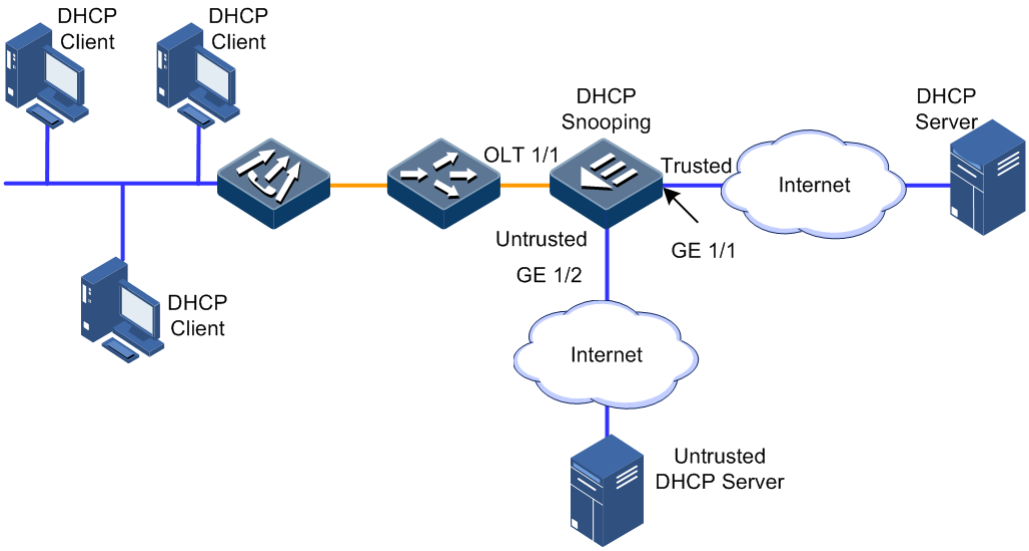
# 8.5 Configuration examples

## 8.5.1 Example for configuring DHCP Snooping

### Networking requirements

As shown in Figure 8-6, the OLT, which works as a DHCP Snooping device, needs to ensure that the DHCP client can obtain IP addresses from a legal DHCP server. In addition, the OLT supports DHCP Option 82 to manage the DHCP client. Configure the filling information of the Circuit ID sub-option on interface OLT 1/1 as raisecom, and filling information of the Remote ID sub-option as user 01.

Figure 8-6 DHCP Snooping networking




### Configuration steps

Step 1 Configure global DHCP Snooping.

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

Step 2 Configure the trusted interface.

```
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#ip dhcp snooping trust
Raisecom(config-if-gigabitethernet-1:1)#exit
```

Step 3 Configure supporting DHCP Option82 and configure the Option 82 field.

```
Raisecom(config)#ip dhcp information option
Raisecom(config)#ip dhcp information option remote-id string user01
Raisecom(config)#interface gpon-olt 1/1
Raisecom(config-if-gpon-olt-1:1)#ip dhcp information option circuit-id
raisecom
```

### Checking results

Use the **show ip dhcp information option** command to show DHCP client configurations.

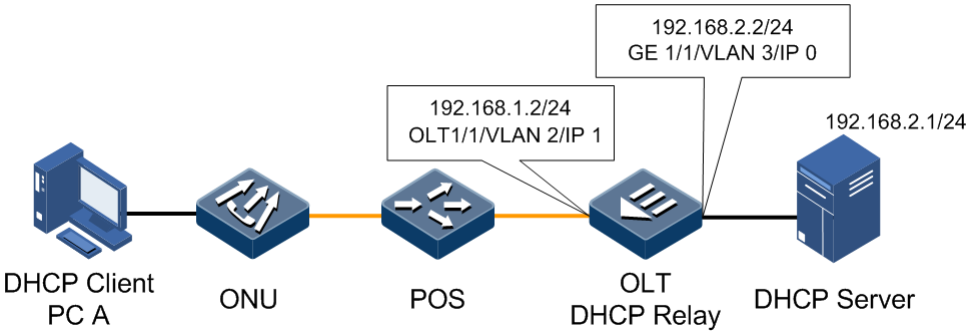
```
Raisecom#show ip dhcp information option
DHCP Option Config Information
Option 82: Enabled
Remote-ID Mode: string
Remote-ID String: user01
Port                    Op82Policy        CircuitId
-----------------------------------------------------------
igabitethernet1/1       replace           --
gpon-olt1/1              replace           raisecom
```

## 8.5.2 Example for configuring DHCP Relay

### Networking requirements

As shown in Figure 8-7, 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 8-7 DHCP Relay networking




## Configuration steps

Step 1 Configure global DHCP Relay.

```
Raisecom#config
Raisecom(config)#ip dhcp relay
```

Step 2 Configure the destination IP address of IP interface 1.

```
Raisecom(config)#ip dhcp relay interface vlanif 1 target-ip 192.168.2.1
```

Step 3 Configure supporting DHCP Option82.

```
Raisecom(config)#ip dhcp information option
```

Step 4 Configure interface GE 1/1 as the DHCP Relay trust interface.

```
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#ip dhcp relay information trusted
```

## Checking results

Use the **show ip dhcp relay** command to show DHCP Relay configurations.

```
Raisecom#show ip dhcp relay
IP Interface    Enabled Status    Target IP Address
 ------------------------------------------------
     0           Enabled           --
     1           Enabled           --
     2           Enabled           --
```

```
3           Enabled           --
4           Enabled           --
5           Enabled       192.168.2.1
6           Enabled           --
7           Enabled           --
8           Enabled           --
9           Enabled           --
10          Enabled           --
11          Enabled           --
12          Enabled           --
13          Enabled           --
14          Enabled           --
```

# 9 Configuring QoS

This chapter introduces the QoS feature and configuration process of the ISCOM5508-GP, and provides related configuration examples, including the following sections:

- Overview of QoS
- Configuring traffic classification
- Configuring traffic monitoring
- Configuring congestion management
- Configuring congestion avoidance
- Configuring traffic shaping
- Configuring traffic policy
- Configuration examples

## 9.1 Overview of QoS

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 to transmit packets 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 the whole network runs high-efficiently.

### 9.1.1 Priority trust

Priority trust refers 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.

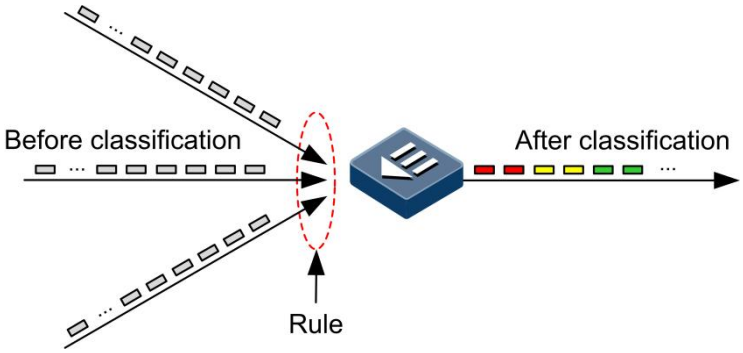
The ISCOM5508-GP supports port-based priority trust. The priorities are divided into priority based on Differentiated Services Code Point (DSCP) of IPv4 packets, priority based on Class of Service (CoS) of VLAN packets, and priority based on Traffic Class (TC) of IPv6 packets.

## 9.1.2 Traffic classification

Traffic classification is a process that recognizes specified packets according to some certain rule. All resulting packets can be treated differently to differentiate the service implied to users.

The ISCOM5508-GP 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 9-1 shows the traffic classification process.

Figure 9-1 Traffic classification process




### ToS priority and DSCP priority

Figure 9-2 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 9-3 shows structures of ToS and DSCP priority packets.

Figure 9-2 IP packet header structure

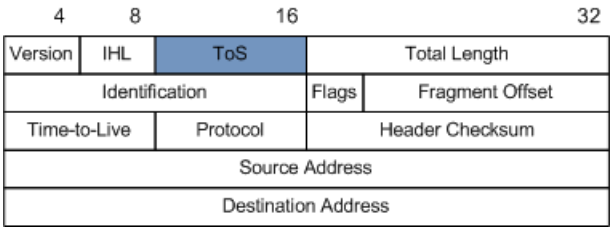
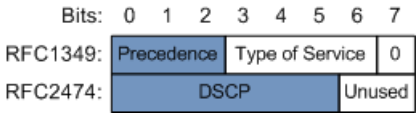


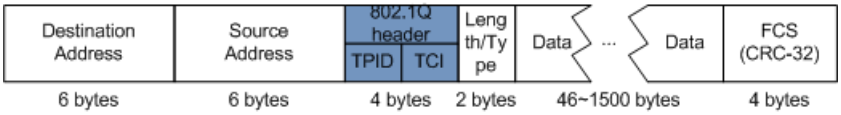

Figure 9-3 Structures of ToS priority and DSCP priority packets




### CoS priority

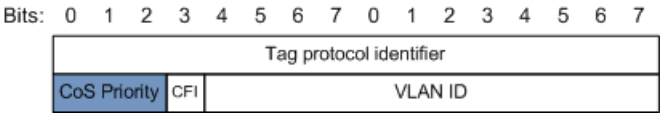
IEEE802.1Q-based VLAN packets are a modification of Ethernet packets. A 4-bit 802.1Q header is added between the source MAC address and protocol type, as shown in Figure 9-4. The 802.1Q header consists a 2-bit Tag Protocol Identifier (TPID, valuing 0x8100) filed and a 2-bit Tag Control Information (TCI) field.

Figure 9-4 VLAN packet structure




The first 3 bits of TCI field represent the CoS priority, which ranges from 0 to 7, as shown in Figure 9-5. The bigger the number is, the higher the CoS priority is. CoS priority is used for ensuring service quality in Layer 2 network.

Figure 9-5 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, is 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.

## 9.1.3 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 that a packet is not forwarded according to the mapping relationship 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.

## 9.1.4 Priority mapping

Priority mapping refers to sending packets to different queues with different local priorities according to configured mapping relationship 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.

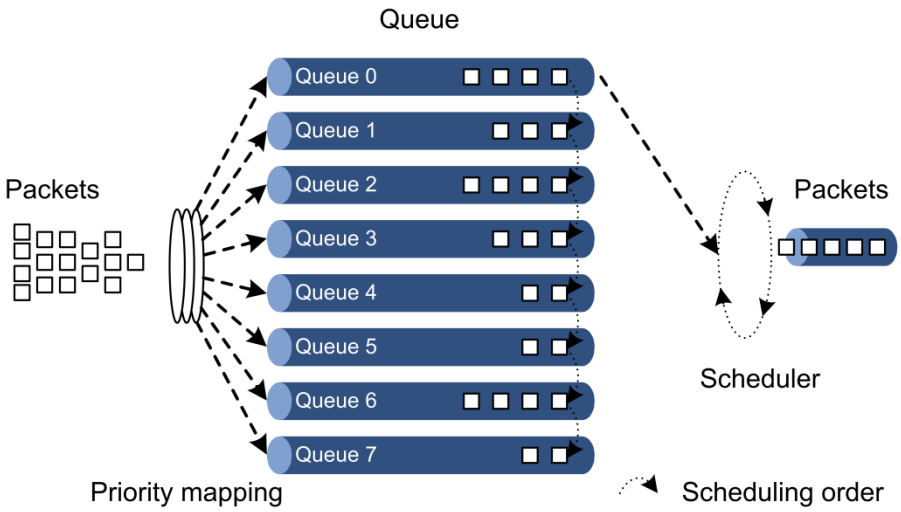
## 9.1.5 Congestion management

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 ISCOM5508-GP include Strict Priority (SP), Weight Round Robin (WRR), Deficit Round Robin (DRR), SP+WRR, and SP+DRR. All scheduling algorithms are designed for addressing specified traffic problems. And they have different effects on bandwidth distribution, delay, and jitter.

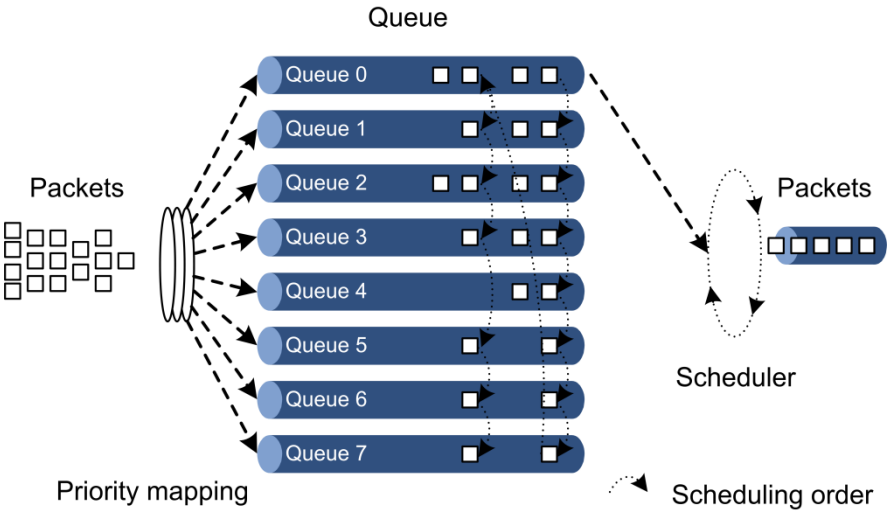
- SP: the device strictly schedules packets in a descending order of priority. Packets with lower priority cannot be scheduled until packets with higher priority are scheduled, as shown in Figure 9-6.

Figure 9-6 SP scheduling



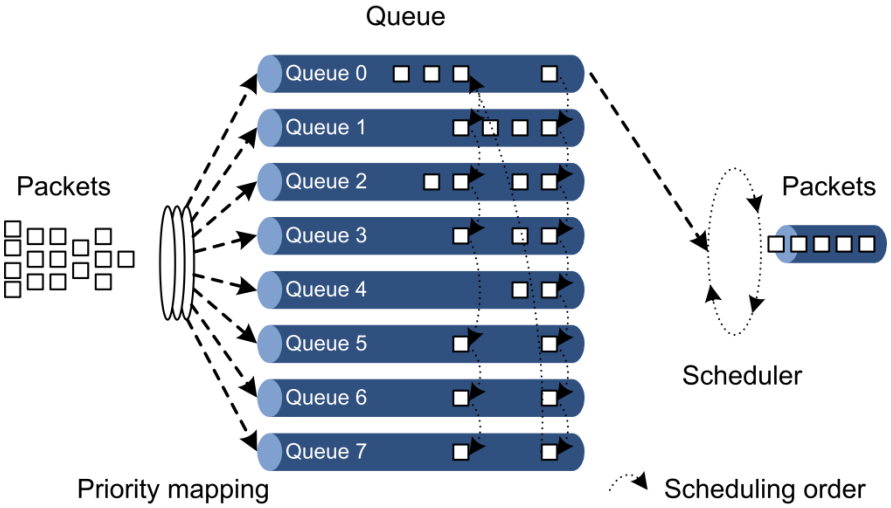

- WRR: on the basis of scheduling packets in a polling manner according to the priority, the device schedules packets according to the weight of the queue, as shown in Figure 9-7.

Figure 9-7 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 9-8.

Figure 9-8 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 queues where SP scheduling/WRR scheduling is performed.
- SP+DRR: a scheduling mode combining the SP scheduling and the DRR scheduling together. In this mode, queues on a port are divided into 2 groups. You can specify the queues where SP scheduling/DRR scheduling is performed.

# 9.2 Configuring traffic classification

## 9.2.1 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

## 9.2.2 Default configurations

### Priority trust

Default configurations of priority trust are as below.

| Function | Default value |
|---|---|
| Priority trust type | CoS |
| Interface default priority | 0 |

### Priority mapping

Mapping among the CoS priority, local priority, and queue 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 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 |

## 9.2.3 Configuring priority trust

Configure the ISCOM5508-GP as below.

| 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 trust dscp` | Configure trusting the DSCP field.<br>You can use the **no mls qos trust** command to restore default configurations.<br>**Note**<br>For IPv4 packets, this command refers to trusting the DSCP field. For IPv6 packets, this command refers to trusting the Traffic Class field.<br>By default, interfaces on the device trust the CoS priority. Therefore, when you need to configure trusting the CoS priority, use the **no** form of this command to restore default configurations. |
| 4 | `Raisecom(config-if-gigabitethernet-*:*)#mls qos priority value` | Configure the default priority of the interface.<br>You can use the **no mls qos priority** command to restore default configurations.<br>**Note**<br>For packets without the 802.1p field, use the default priority. |

## 9.2.4 Configuring priority mapping

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |

| Step | Command | Description |
|---|---|---|
| 2 | Raisecom(config)#**mls qos mapping cos** *cos-value* **to localpriority** *local-priority* | (Optional) configure mapping between the CoS priority and local priority.<br>You can use the **no mls qos mapping cos** command to restore default configurations. |
| 3 | Raisecom(config)#**mls qos mapping dscp** *dscp-value* **to localpriority** *local-priority* | (Optional) configure mapping between the DSCP priority and local priority.<br>You can use the **no mls qos mapping dscp** command to restore default configurations. |
| 4 | Raisecom(config)#**mls qos mapping localpriority** *local-priority* **to queue** *queue-id* | (Optional) configure mapping between the local priority and queue.<br>You can use the **no mls qos mapping localpriority** command to restore default configurations. |

### 9.2.5 Checking configurations

Use the following commands to check configuration results.

| 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 interface trust mode, queue scheduling mode, and default CoS value. |
| 2 | Raisecom#**show mls qos mapping cos** | Show mapping between the CoS priority and local priority. |
| 3 | Raisecom#**show mls qos mapping dscp** | Show mapping between the DSCP priority and local priority. |
| 4 | Raisecom#**show mls qos mapping local-priority** | Show mapping between the local priority and queue. |

## 9.3 Configuring traffic monitoring

### 9.3.1 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 method for traffic measurement 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. In addition, there are two algorithm modes for the token bucket: color-blind and color-sensitive. So there are six algorithm modes in total:

- Single-rate single-token bucket (color-blind and color-sensitive)
- Single-rate dual-token bucket (color-blind and color-sensitive)
- Dual-rate dual-token bucket (color-blind and color-sensitive)

### Prerequisite

N/A

## 9.3.2 Default configurations

N/A

## 9.3.3 Configuring rate limiting

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 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 to take 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 to take when the rate exceeds the threshold (dual-token bucket monitoring) |

When you configure the PIR parameter, the rate limiting policer works in dual-token bucket mode. Otherwise, it works in single-token bucket mode.

## 9.3.4 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show mls qos policer** [ *policer-id* ] | Show configurations of the rate limiting policer. |

# 9.4 Configuring congestion management

## 9.4.1 Preparing for configurations

### Scenario

Congestion management refers to allocating and controlling bandwidth when the network is congested. Congestion management adopts the queue technology to buffer 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

## 9.4.2 Default configurations

### Scheduling mode

Default configurations of the queue scheduling mode are as below.

| Function | Default value |
|---|---|
| Queue scheduling mode | SP |

### Queue weight

Default weights of WDRR and WRR queues on the ISCOM5508-GPare 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 |

## 9.4.3 Configuring SP scheduling

Configure the ISCOM5508-GP as below.

| 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 queue scheduler sp` | Configure the queue scheduling mode to SP.<br>You can use the **no mls qos queue scheduler** command to restore default configurations. |

## 9.4.4 Configuring WRR scheduling

Configure the ISCOM5508-GP as below.

| 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 queue scheduler wrr** | Configure the queue scheduling mode to WRR.<br>You can use the **no mls qos queue scheduler** command to restore default configurations. |
| 4 | Raisecom(config-if-*-*:*)#**mls qos queue wrr** *value0 value1 value2 value3 value4 value5 value6 value7* | Configure the weight of each queue in WRR scheduling mode. |

## 9.4.5 Configuring WDRR scheduling

Configure the ISCOM5508-GP as below.

| 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 queue scheduler wdrr** | Configure the queue scheduling mode to WDRR.<br>You can use the **no mls qos queue scheduler** command to restore default configurations. |
| 4 | Raisecom(config-if-*-*:*)#**mls qos queue wdrr** *value0 value1 value2 value3 value4 value5 value6 value7* | Configure the weight of each queue in WDRR scheduling mode. |

## 9.4.6 Checking configurations

Use the following commands to check configuration results.

| 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 interface trust mode, queue scheduling mode, and default CoS value. |
| 2 | Raisecom#**show interface** { **gigabitethernet** \| **ten-gigabitethernet** \| **gpon-olt** } *slot-id/port-id* **mls qos queue** | Show configurations of queue weights. |

# 9.5 Configuring congestion avoidance

## 9.5.1 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, for TCP packets, if a number of packets are dropped, it 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

## 9.5.2 Default configurations

N/A

## 9.5.3 Configuring WRED scheduling

Configure the ISCOM5508-GP as below.

| 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. |

## 9.5.4 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show interface** { **gigabitethernet** \| **ten-gigabitethernet** \| **gpon-olt** } *slot-id/port-id* **mls qos queue wred** | Show WRED configurations. |

# 9.6 Configuring traffic shaping

## 9.6.1 Preparing for configurations

### Scenario

Traffic shaping aims to eliminate the burst traffic to make it output smoothly. Traffic shaping is usually used on the egress interface.

Similar to traffic monitoring, traffic shaping also adopts the token bucket to measure traffic. Different from traffic monitoring, traffic shaping 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

## 9.6.2 Default configurations

Default configurations of traffic shaping are as below.

| 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 |

## 9.6.3 Configuring traffic shaping

Configure the ISCOM5508-GP as below.

| 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. |

### 9.6.4 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show interface** { **gigabitethernet** \| **ten-gigabitethernet** \| **gpon-olt** } *slot-id/port-id* **mls qos queue shaping** | Show configurations of traffic shaping. |

## 9.7 Configuring traffic policy

### 9.7.1 Preparing for configurations

#### Scenario

After traffic classification, you need to perform different operations on packets of different types, for example, redirect some specified traffic to other physical interfaces.

#### Prerequisite

N/A

### 9.7.2 Default configurations

N/A

### 9.7.3 Configuring traffic policy

Configure the ISCOM5508-GP as below.

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

| Step | Command | Description |
|---|---|---|
| 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. |
| 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* } | Remark the data traffic.<br>**Note**<br>Remarking the data traffic complies with the backward effective principle. |
| 5 | Raisecom(config-*-acl-*-rule-*)#**redirect-to interface** { **gigabitethernet** \| **ten-gigabitethernet** \| **gpon-olt** } *slot-id/port-id* | Redirect the data traffic to other interfaces. |
| 6 | Raisecom(config-*-acl-*-rule-*)#**mirror-to interface** { **gigabitethernet** \| **ten-gigabitethernet** \| **gpon-olt** } *slot-id/port-id* | Mirror the data traffic to other interfaces. |
| 7 | Raisecom(config-*-acl-*-rule-*)#**policer** *policer-id* | Bind the rate limiting policer to limit the rate of data traffic. |

## 9.7.4 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show mls qos policer** | Show rate limiting configurations |

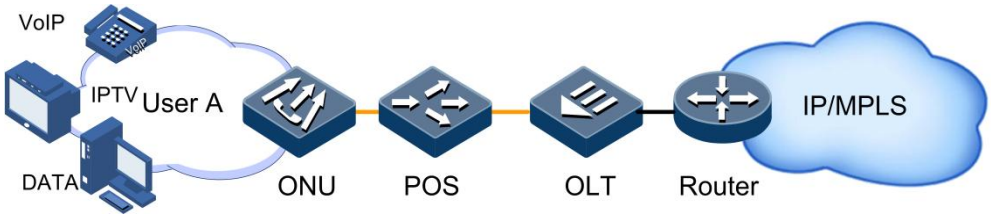
# 9.8 Configuration examples

## 9.8.1 Example for configuring rate limiting

### Networking requirements

As shown in Figure 9-9, User A belongs to VLAN 2 and connects to the OLT through an ONU. According to users' requirements, provide a bandwidth of 25 Mbit/s for User A. The burst traffic is 100 Bytes. Excessive traffic is dropped.

Figure 9-9 Configuring rate limiting based on traffic policy




## Configuration steps

Step 1 Create rate limiting rules.

```
Raisecom#config
Raisecom(config)#mls qos single-policer 1 cir 25000 cbs 100 red drop
green drop
```

Step 2 Bind the filter rule to the policy.

```
Raisecom(config)#l2-access-list 1
Raisecom(config-l2-acl-1)#rule 1
Raisecom(config-l2-acl-1-rule-1)#policer 1
Raisecom(config-l2-acl-1-rule-1)#set vlan 2
Raisecom(config-l2-acl-1-rule-1)#exit
Raisecom(config-l2-acl-1)#exit
```

Step 3 Apply the ACL to the ISCOM5508-GP.

```
Raisecom(config)#filter l2-access-list 1
```

## Checking results

Show rate limiting configurations.

```
Raisecom#show mls qos policer 1
ID    Type      Rate   Burst  Exceed Action  New DSCP  Ref. Times
------------------------------------------------------------------
1     single    25000  100    drop          --
```

# 9.8.2 Example for configuring queue scheduling

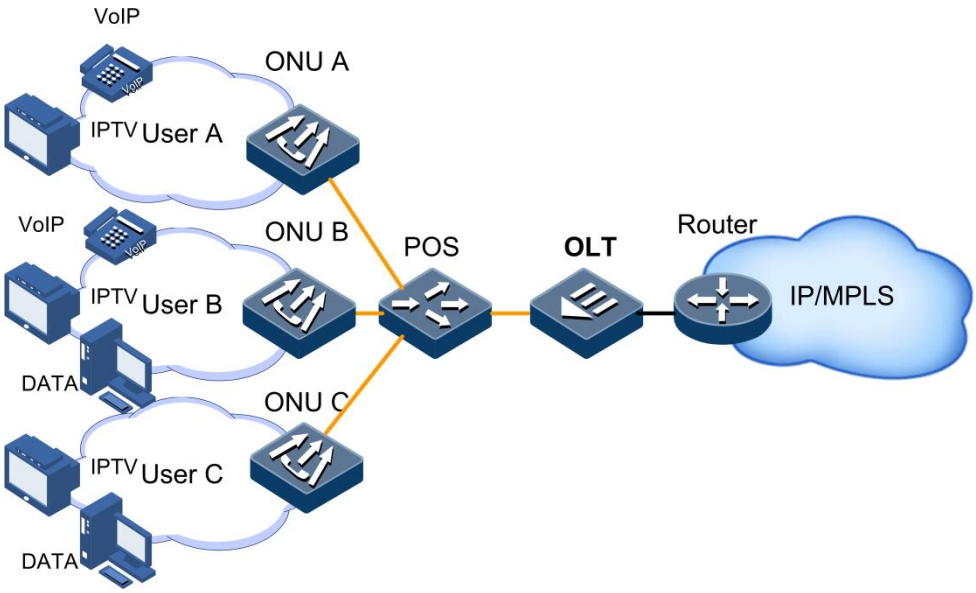
## Networking requirements

As shown in Figure 9-10, 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 9-10 Configuring queue scheduling




## Configuration steps

Step 1 Configure interface priority trust.

```
Raisecom#config
Raisecom(config)#interface gpon-olt 1/1
Raisecom(config-if-gpon-olt-1:1)#no mls qos trust dscp
Raisecom(config-if-gpon-olt-1:1)#exit
```

Step 2 Configure mapping between the CoS priority and local priority.

```
Raisecom(config)#mls qos mapping cos 5 to localpriority 6
Raisecom(config)#mls qos mapping cos 4 to localpriority 5
Raisecom(config)#mls qos mapping cos 2 to localpriority 2
```

Step 3 Configure SP+WRR scheduling.

```
Raisecom(config)#interface gpon-olt 1/1
Raisecom(config-if-gpon-olt-1:1)#mls qos queue scheduler wdrr
Raisecom(config-if-gpon-olt-1:1)#mls qos queue wdrr 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
```

# 10 Configuring system security

This chapter introduces the system security feature and configuration process of the ISCOM5508-GP, and provides related configuration examples, including the following sections:

- Overview of system security
- Configuring ACL
- Configuring RADIUS
- Configuring TACACS+
- Configuring storm control
- Configuring interface isolation
- Maintenance
- Configuration examples

## 10.1 Overview of system security

### 10.1.1 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.

### 10.1.2 RADIUS

Remote Authentication Dial In User Service (RADIUS) is a standard communication protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for remote users.

RADIUS works in client/server mode. Network devices are clients of the RADIUS server. RADIUS server is responsible for receiving users' connection requests, authenticating uses, and replying configurations required by all clients to provide services for users. This mode can control users accessing devices and network to improve network security.

clients and the RADIUS server communicate with each other through the shared key. The shared key is not transmitted through the network. In addition, any user password needs to be encapsulated when it is transmitted through clients and RADIUS. This helps prevent getting the user password by sniffing unsecure network.

RADIUS accounting is designed for RADIUS authenticated users. When a user logs in to the device, the device sends an accounting packet to the RADIUS accounting server to begin accounting. During login, the device sends accounting update packets to the RADIUS accounting server. When the user exits from the device, no accounting packet is sent to the RADIUS accounting server. These packets contain the login time. With these packets, the RADIUS accounting server can record the access time and operation of each user.

## 10.1.3 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 interface, providing higher transmission reliability. RADIUS uses a UDP interface.
- 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.

## 10.1.4 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 occurring when broadcast packets increase sharply on the network. Therefore, it makes sure that unicast packets can be properly forwarded.

## 10.1.5 Interface isolation

Interface isolation adopts the isolation group method to realize data isolation among multiple interfaces on the device, thus enhancing network access security.

# 10.2 Configuring ACL

## 10.2.1 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 corresponding packets to pass according to the configured policy.

ACL can be divided into the following types.

- IP ACL: according to the source or destination address, used TCP or UDP port ID, and other data packet attributes carried by the IP head to formulate classification rules.
- IPv6 ACL: according to the source or destination address, used TCP or UDP port ID, and other data packet attributes carried by the IP head to formulate classification rules.
- Layer 2 ACL: 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 head to formulate classification rules.
- Hybrid ACL: according to information about the IP head and Layer 2 frame head to formulate classification rules. This type of ACL mixes characteristics of IP ACL and Layer 2 ACL.
- IPv6 hybrid ACL: according to information about the IPv6 head and Layer 2 frame head to formulate classification rules. This type of ACL mixes characteristics of IPv6 ACL and Layer 2 ACL.
- User ACL: formulate classification rules from the user's perspective.

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

## 10.2.2 Default configurations

N/A

## 10.2.3 Configuring IP ACL

### Configuring IPv4 ACL

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |

| Step | Command | Description |
|---|---|---|
| 2 | Raisecom(config)#**ip-access-list** *list-number* | Create an IPv4 ACL and enter IPv4 ACL configuration mode.<br>You can use the **no ip-access-list** { **all** \| l*ist-numb*er } 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 number of the IPv4 ACL sub-rule. |
| 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 priority. |
| 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. |
| 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. |

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

Configure the ISCOM5508-GP as below.

| 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.<br>You can use the **no ipv6-access-list** { **all** \| l*ist-numb*er } command to delete the ACL. |
| 3 | Raisecom(config-ipv6-acl-*)#**description** *desc-string* | (Optional) configure descriptions of the IPv6 ACL. |
| 4 | Raisecom(config-ipv6-acl-*)#**rule** *rule-number* | Configure the number of the IPv6 ACL sub-rule. |
| 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-address/prefix-length* | Configure the source IP address of the IPv6 ACL 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-num* | Configure the IPv6 ACL sub-rule matching with IP upper protocol type. |

| Step | Command | Description |
|---|---|---|
| 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** *1ab1e-num* | Configure matching the IPv6 ACL sub-rule with the flow label of the IPv6 packet. |
| 13 | Raisecom(config-ip-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. |

## 10.2.4 Configuring Layer 2 ACL

Configure the ISCOM5508-GP as below.

| 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.<br>You can use the **no l2-access-list** *acl-numb*er command to delete the ACL. |
| 3 | Raisecom(config-l2-acl-*)#**description** *desc-string* | (Optional) configure descriptions of the Layer 2 ACL. |
| 4 | Raisecom(config-l2-acl-*)#**rule** *rule-number* | 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. |
| 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. |

| Step | Command | Description |
|---|---|---|
| 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** \| **ipv6** \| **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. |

# 10.2.5 Configuring hybrid ACL

## Configuring IPv4 hybrid ACL

Configure the ISCOM5508-GP as below.

| 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.<br>You can use the **no hybrid-access-list** { **all** \| l*ist-numb*er } command to delete the ACL. |
| 3 | Raisecom(config-hybrid-acl-*)#**description** *desc-string* | (Optional) configure descriptions of the hybrid ACL. |
| 4 | Raisecom(config-hybrid-acl-*)#**rule** *rule-number* | Configure the number 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. |

| Step | Command | Description |
|---|---|---|
| 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** *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** \| **ipv6** \| **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 priority. |
| 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 matching the hybrid ACL sub-rule with 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. |

| Step | Command | Description |
|---|---|---|
| 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 matching the hybrid ACL sub-rule with the destination/source interface ID of the UDP packet. |

## Configuring IPv6 hybrid ACL

Configure the ISCOM5508-GP as below.

| 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 the hybrid ACL configuration mode.<br>You can use the **no ipv6-hybrid-access-list** { **all** \| l*ist-numbe*r } command to delete the ACL. |
| 3 | Raisecom(config-ipv6-hybrid-acl-*)#**description** *desc-string* | (Optional) configure descriptions of the IPv6 hybrid ACL. |
| 4 | Raisecom(config-ipv6-hybrid-acl-*)#**rule** *rule-number* | Configure the number of the IPv6 hybrid ACL sub-rule. |
| 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* | Configure matching the IPv6 hybrid ACL sub-rule with the source SVLAN ID. |
| 9 | Raisecom(config-ipv6-hybrid-acl-*-rule-*)#**match svlan-cos** *svlan-cos* | Configure matching the IPv6 hybrid ACL sub-rule with the 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. |
| 11 | Raisecom(config-ipv6-hybrid-acl-*-rule-*)#**match cvlan-cos** *cvlan-cos* | Configure matching the IPv6 hybrid ACL sub-rule with the CVLAN CoS. |

| Step | Command | Description |
|---|---|---|
| 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 Layer 2 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 Layer 2 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 the IPv6 hybrid ACL sub-rule matching with the user level of the IPv6 packet. |
| 17 | Raisecom(config-ipv6-hybrid-acl-*-rule-*)#**match ip protocol** *protocol-num* | Configure the IPv6 hybrid ACL sub-rule matching with 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 the IPv6 hybrid ACL sub-rule with the destination/source interface ID of the TCP packet. The packet type refers to the classical 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 sub-rule with the destination/source interface ID of the UDP packet. |

## 10.2.6 Configuring user ACL

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**user-access-list profile field** *field-id* **layer** { **l2** \| **l3** \| **l4** } **offset** *offset-value* | Configure customized ACL match objects. |

| Step | Command | Description |
|---|---|---|
| 3 | Raisecom(config)#**user-access-list** *list-number* | Create a customized ACL and enter user ACL configuration mode.<br>You can use the **no user-access-list** { **all** \| l*ist-numb*er } command to delete the ACL. |
| 4 | Raisecom(config-user-acl-*)#**description** *desc-string* | (Optional) configure descriptions of the user ACL.<br>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. |
| 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. |

## 10.2.7 Applying ACL

Configure the ISCOM5508-GP as below.

### Applying ACL based on the whole device

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**filter** { **l2-access-list** \| **ip-access-list** \| **ipv6-access-list** \| **hybrid-access-list** \| **ipv6-hybrid-access-list** \| **user-access-list** } *acl-num* [ **statistics** ] | Configure applying filtering rules based on the whole device. If you have configured the **statistics** parameter, the system takes statistics according to the filtering rules.<br>You can use the **no filter** *acl-num* command to delete the application relationship of the filtering rules. |

### Applying ACL based on uplink and downlink of the interface

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**filter** { **l2-access-list** \| **ip-access-list** \| **ipv6-access-list** \| **hybrid-access-list** \| **ipv6-hybrid-access-list** \| **user-access-list** } *acl-num* **egress interface** { **gpon-olt** \| **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-list* [ **statistics** ] | Configure applying ACL filtering rules based on the downlink of the interface. If you have configured the **statistics** parameter, the system takes statistics according to the filtering rules. |

| Step | Command | Description |
|---|---|---|
| 3 | Raisecom(config)#**filter** { **l2-access-list** \| **ip-access-list** \| **ipv6-access-list** \| **hybrid-access-list** \| **ipv6-hybrid-access-list** \| **user-access-list** } *acl-num* **ingress interface** { **gpon-olt** *slot-id/port-list* \| **gigabitethernet** *slot-id/port-list* \| **ten-gigabitethernet** *slot-id/port-list* \| **port-channel** *group-id* } [ **statistics** ] | Configure applying ACL filtering rules based on the uplink of the interface. If you have configured the **statistics** parameter, the system takes statistics according to the filtering rules. |

Applying ACL based on traffic from the 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** \| **ipv6-access-list** \| **hybrid-access-list** \| **ipv6-hybrid-access-list** \| **user-access-list** } *acl-num* **from interface** { **gpon-olt** \| **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-list* **to interface** { **gpon-olt** \| **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-list* [ **statistics** ] | Configure applying ACL filtering rules based on traffic from the ingress interface to egress interface. If you have configured the **statistics** parameter, the system takes statistics according to the filtering rules.<br>**Note**<br>When you use this command, the ingress and egress interfaces should be on the same card or sub-card. |

## 10.2.8 Checking configurations

Use the following commands to check configuration results.

| 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. |

| No. | Command | Description |
|---|---|---|
| 8 | Raisecom#**show interface vlanif ip-access-list** | Show ACL configurations on the VLAN interface. |
| 9 | Raisecom#**show filter** [ filter-*number* ] **statistics** | Show filter statistics. |

# 10.3 Configuring RADIUS

## 10.3.1 Preparing for configurations

### Scenario

You can deploy the RADIUS server on the network to perform authentication and accounting to control users to access to the ISCOM5508-GP and network. The ISCOM5508-GP 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

## 10.3.2 Default configurations

Default configurations of RADIUS on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| RADIUS accounting | Disable |
| IP address of RADIUS authentication server | 0.0.0.0 |
| UDP interface ID of RADIUS authentication server | 1812 |
| IP address of RADIUS accounting server | 0.0.0.0 |
| UDP interface ID of RADIUS accounting server | 1813 |
| Shared key used to communicate with the RADIUS accounting server | N/A |
| Processing policy upon accounting failure | online |
| Time to send accounting update packets | 0 |

## 10.3.3 Configuring RADIUS authentication

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**radius** [ **backup** ] *ip-address* [ **auth-port** *slot-id/port-id* ] | Specify the IPv4 address and interface ID of the RADIUS authentication server.<br>You can use the **backup** parameter to specify the backup RADIUS authentication server. |
| | Raisecom#**radius** [ **backup** ] *ipv6-address* [ **scopeid** *string* ] [ **auth-port** *slot-id/port-id* ] | Specify the IPv6 address and interface ID of the RADIUS authentication server.<br>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. |

## 10.3.4 Configuring RADIUS accounting

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**aaa accounting login enable** | Enable RADIUS accounting.<br>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 interface ID of the RADIUS accounting server.<br>You can use the **backup** parameter to specify the backup RADIUS accounting server. |
| | Raisecom#**radius** [ **backup** ] **accounting-server** *ipv6-address* [**scopeid** *string* ] [ **acct-port** *port-id* ] | Specify the IPv6 address and UDP interface ID of the RADIUS accounting server.<br>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 fail** { **online** \| **offline** } | Configure the processing policy upon accounting failure. |
| 5 | Raisecom#**aaa accounting update** *period* | Configure the period to send accounting update packets. If it is configured to 0, accounting update packets will not be sent.<br>**Note**<br>Through the accounting start packet, update packet, and end packet, the RADIUS accounting server records the access time and operations of each user. |

### 10.3.5 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | `Raisecom#show radius-server` | Show RADIUS server configurations. |
| 2 | `Raisecom#show aaa accounting` | Show RADIUS accounting server running conditions. |

## 10.4 Configuring TACACS+

### 10.4.1 Preparing for configurations

#### Scenario

You can deploy the TACACS+ server on the network to perform authentication and accounting to control users to access to the ISCOM5508-GP and network. TACACS+ is safer and more reliable than RADIUS. The ISCOM5508-GP 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

### 10.4.2 Default configurations

Default configurations of TACACS+ on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| IP address of TACACS+ authentication server | 0.0.0.0 |
| IP address of TACACS+ accounting server | 0.0.0.0 |
| Shared key | N/A |
| User login mode | local-user |
| Privileged login mode | local-user |

### 10.4.3 Configuring TACACS+

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**tacacs-server** [ **backup** ] *ip-address* | Specify the IPv4 address of the TACACS+ authentication server.<br>You can use the **backup** parameter to specify the backup TACACS+ authentication server. |
| | Raisecom#**tacacs-server** [ **backup** ] *ipv6-address* [**scopeid** *string* ] | (Optional) specify the IPv6 address of the TACACS+ authentication server.<br>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#**enable login tacacs-local** [ **server-no-response** ] | (Optional) configure login mode in privileged EXEC mode. |

## 10.4.4 Configuring TACACS+ accounting

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**tacacs** [ **backup** ] **accounting-server** *ip-address* | Specify the IPv4 address of the TACACS+ accounting server.<br>You can use the **backup** parameter to specify the backup TACACS+ accounting server. |
| | Raisecom#**tacacs** [ **backup** ] **accounting-server** *ipv6-address* [**scopeid** *string* ] | (Optional) specify the IPv6 address of the TACACS+ accounting server.<br>You can use the **backup** parameter to specify the backup TACACS+ accounting server. |

## 10.4.5 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show tacacs-server** | Show TACACS+ configurations. |

# 10.5 Configuring storm control

## 10.5.1 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.

## 10.5.2 Default configurations

Default configurations of storm control on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Broadcast storm control | Enable |
| Multicast storm control | Disable |
| DLF storm control | Disable |
| Storm control rate threshold | 1024 Kbit/s |
| Burst length | 512 KBytes |

## 10.5.3 Configuring storm control

Configure the ISCOM5508-GP as below.

| 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-*-*:*)#**storm-control** { **all** \| **broadcast** \| **dlf** \| **multicast** } | Enable storm control on broadcast, multicast, and DLF traffic. |

| Step | Command | Description |
|---|---|---|
| 4 | Raisecom(config-if-*-*:*)#**storm-control bps** *value burst* | (Optional) configure the rate threshold of storm control. |

### 10.5.4 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show** [ **interface** { **gpon-olt** \| **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-id* ] **storm-control** | Show storm control configurations. |

## 10.6 Configuring interface isolation

### 10.6.1 Preparing for configurations

#### Scenario

Interface isolation is a Layer 2 isolation mode, which adopts the isolate group to realize data isolation among multiple interfaces on the device. You can isolate different physical interfaces and interfaces in the same VLAN by creating create the isolate group to enhance safety of network access.

#### Prerequisite

N/A

### 10.6.2 Default configurations

Default configurations of interface isolation are as below.

| Function | Default value |
|---|---|
| Isolation group ID | 1 |
| Member interface in an isolation group | GPON interfaces 1–4 in slot 1 |

### 10.6.3 Configuring physical interface isolation

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**interface** { **gpon-olt** *slot-id/port-id* \| **gigabitethernet** *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.<br>You can use the **no isolate-group** *group-id* command to delete the isolation group or interfaces in the group. |

## 10.6.4 Configuring VLAN interface isolation

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**interface** { **gpon-olt** \| **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/olt-id* | Enter physical interface configuration mode. |
| 3 | Raisecom(config-if-*-*:*)#**vlan** *vlan-id* **isolate-group** *group-id* | Create the isolation group in the VLAN. If a specified isolation group exists, add interfaces to the group.<br>You can use the **no vlan** *vlan-id* **isolate-group** *group-id* command to delete the isolation group or interfaces in the group. |

## 10.6.5 Checking configurations

Use the following commands to check configuration results.

| 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. |

# 10.7 Maintenance

Maintain the ISCOM5508-GP as below.

| Command | Description |
|---|---|
| Raisecom(config)#**clear filter** [ *filter-number* ] **statistics** | Clear ACL filter statistics. |
| Raisecom(config)#**clear tacacs statistics** | Clear TACACS+ statistics. |

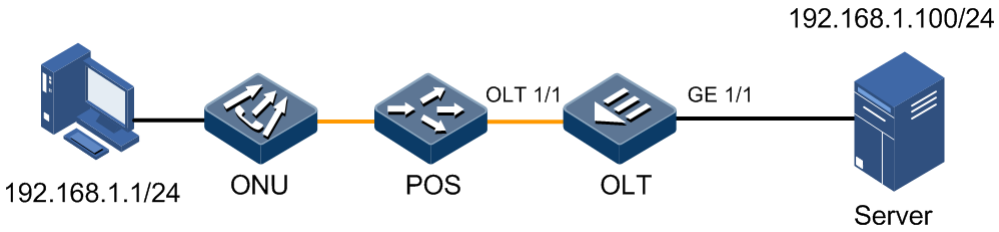
# 10.8 Configuration examples

## 10.8.1 Example for configuring ACL

### Networking requirements

As shown in Figure 10-1, to control users to access the server, you can configure ACL forbidding 192.168.1.1 to access the server 192.168.1.100.

Figure 10-1 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
1/1
```

### 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** to show filter configurations.

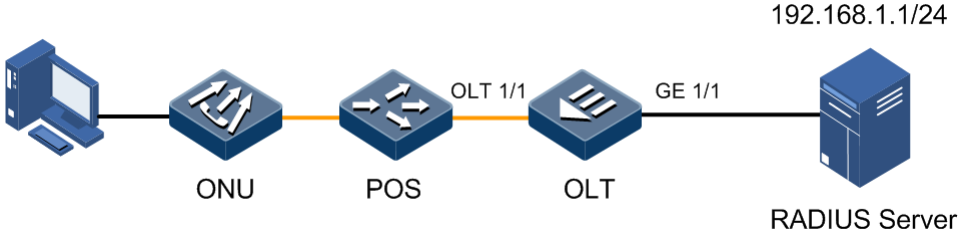
```
Raisecom#show filter
Filter ID : 1001
ACL ID      : 1
Hardware    : Yes
Egress Port  : gpon-olt 1/1
Ingress Port : gpon-olt 1/1
Statistics   : Disable
```

## 10.8.2 Example for configuring RADIUS

### Networking requirements

As shown in Figure 10-2, to control users to access the device, you need to deploy RADIUS authentication and accounting on the OLT to authenticate login users and record their operations. It is required that the interval to send update packets is 2min and the user is logged off when accounting fails.

Figure 10-2 RADIUS networking



## Configuration steps

Step 1 Configure RADIUS authenticating login users.

```
Raisecom#radius 192.168.1.1
Raisecom#radius-key raisecom
Raisecom#user login radius-user
```

Step 2 Configure RADIUS accounting login users.

```
Raisecom#aaa accounting login enable
Raisecom#radius accounting-server 192.168.1.1
Raisecom#radius accounting-server key raisecom
Raisecom#aaa accounting fail offline
Raisecom#aaa accounting update 120
```

## Checking results

Use the **show radius-server** to show RADIUS configurations.

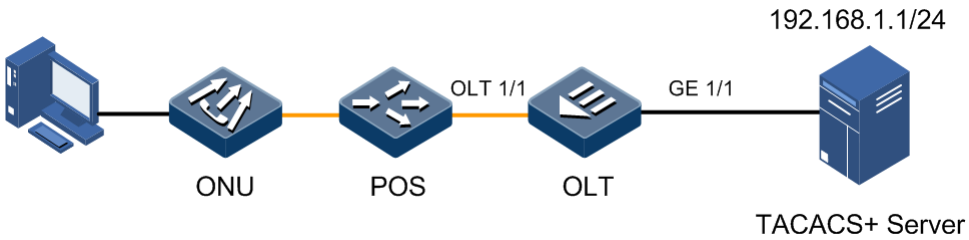
```
Raisecom#show radius-server
Authentication server IP:         192.168.1.1 port:1812
Backup authentication server IP:      0.0.0.0 port:1812
Authentication server key:     raisecom
Accounting server IP:            192.168.1.1 port:1813
Backup accounting server IP:          0.0.0.0 port:1813
Accounting server key:        raisecom
```

# 10.8.3 Example for configuring TACACS+

## Networking requirements

As shown in Figure 10-3, to control users to access the device, you need to deploy TACACS+ authentication on the OLT to authenticate login users.

Figure 10-3 TACACS+ networking



### Configuration steps

Configure TACACS+ authenticating 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** to show TACACS+ configurations.

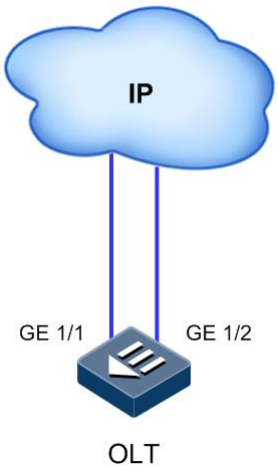
```
Raisecom#show tacacs-server
Server Address:                192.168.1.1
Backup server Address:          0.0.0.0
Sever Shared Key:              raisecom
Total Packet Sent:             0
Total Packet Recv:             0
Num of Error Packets:           0
Accounting server Address:       0.0.0.0
Backup Accounting server Address: 0.0.0.0
```

## 10.8.4 Example for configuring strom control

### Networking requirements

As shown in Figure 10-4, 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 length is 1024 KBytes.

Figure 10-4 Storm control networking



## Configuration steps

Configure storm control on the OLT.

```
Raisecom#config
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#storm-control broadcast
Raisecom(config-if-gigabitethernet-1:1)#storm-control dlf
Raisecom(config-if-gigabitethernet-1:1)#storm-control bps 2000 burst 1024
Raisecom(config-if-gigabitethernet-1:1)#exit
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#storm-control broadcast
Raisecom(config-if-gigabitethernet-1:2)#storm-control dlf
Raisecom(config-if-gigabitethernet-1:2)#storm-control bps 2000 burst 1024
```

## Checking results

Use the **show storm-control** to show storm control configurations.

```
Raisecom#show storm-control
Port         Broadcast     Multicast     DLF_Unicast    Threshold
-------------------------------------------------------------------------
gigabitethernet1/1   enable     disable   enable  2000Kb/s Burst 1024 KB
gigabitethernet1/2   enable     disable   enable  2000Kb/s Burst 1024 KB
```

# 11 Configuring link security

This chapter introduces the link security feature and configuration process of the ISCOM5508-GP, and provides related configuration examples, including the following sections:

- Overview of link security
- Configuring link aggregation
- Configuring failover
- Configuring RRPS
- Configuring loopback detection
- Configuring interface backup
- Maintenance
- Configuration examples

## 11.1 Overview of link security

### 11.1.1 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. In addition to effectively improving reliability on links between devices, link aggregation helps gain higher bandwidth without upgrading hardware.

#### Manual link aggregation

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.

#### Static LACP link aggregation

Link Aggregation Control Protocol (LACP) is a protocol based on IEEE802.3ad. With LACP, the device communicates with the peer through the Link Aggregation Control Protocol Data Unit (LACPDU). After LACP is enabled on an interface, the interface sends a LACPDU to

inform the peer of its system LACP priority, system MAC address, interface LACP priority, interface ID, and operation key.

After receiving the LACPDU, the peer compares its information with that received by other interfaces to choose an interface can be set to selected status. Therefore, both ends reach a consensus on the interface status (selected). The operation key is a configuration combination automatically generated based on configurations of the interface, such as the rate, duplex mode, and Up/Down status. In a LAG, interfaces in the selected status share the identical operation key.

## 11.1.2 Failover

Failover provides an interface linkage scheme to extend the range of link backup. By monitoring uplinks and synchronizing downlinks, the downlink devices can be informed of faults of uplink devices immediately to trigger switching, thus preventing traffic loss because downlink devices are not informed of uplink failures.

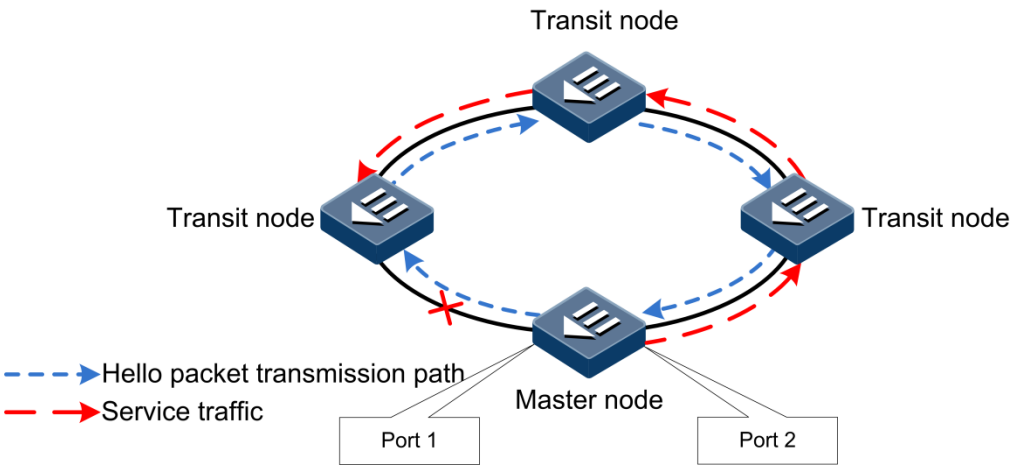
## 11.1.3 RRPS

With the development of Ethernet to the MAN, voice and video multicast service has come up with higher requirements on the Ethernet redundancy protection and fault recovery time. The fault recovery convergence time of the original STP mechanism is at the second level, which is far from meeting requirements on the fault recovery time in the MAN.

Raisecom Ring Protection Switching (RRPS) technology is RAISECOM independent research and development protocol, which can ensure that there is no data loop in the Ethernet ring through blocking some interface on the ring. RRPS solves the problems of weak protection and taking too long to recover faults of the traditional data network. RRPS, in theory, can provide 50ms rapid protection features.

As shown in Figure 11-1, the network consists of a master node, multiple transit nodes, and control VLAN. Configure Port 1 and Port 2 on the master node. Generally, the master node sends Hello packets periodically through Port 1. If the master node receives the Hello packet from Port 2, the Ethernet ring is in normal status and you should logically block Port 1 immediately.

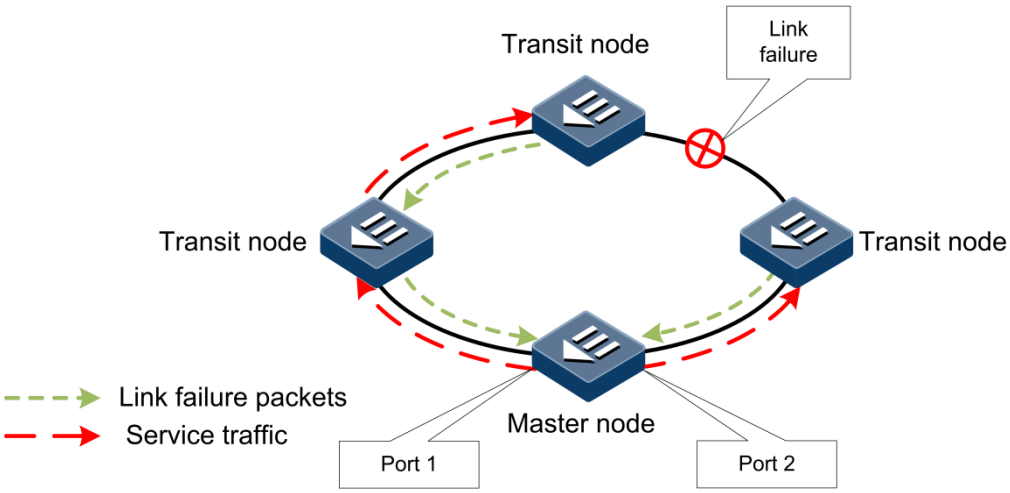
Figure 11-1 Ethernet ring in normal status




Once the link fails (such as, link interruption), the failure adjacent node or interface will check the fault immediately and send link failure packets to the master node. If the master node receives the link failure packet, the Ethernet ring is in fault status and you should

unblock Port 1 immediately. At the same time, the master node sends packets to inform other transit nodes of link failure to make them change transmission direction. Data traffic will be switched to normal link after transit nodes update the forwarding table. As shown in Figure 11-2.

Figure 11-2 Ethernet ring in switching status




## 11.1.4 Loopback detection

Loopback detection aims to solve problems caused by loops on the network, and improve the self-checking ability, fault tolerance, and robustness of the network.

The process of loopback detection is as below:

- Each interface of the device sends the loopback-detection packet periodically (the interval is configurable and by default it is 4s).
- The device checks the source MAC address of the received loopback detection packet, if the source MAC address is identical to the MAC address of the device, it is believed that a loop is generated on some interface of the device.
  - If the Tx interface ID is identical to Rx interface ID, shut down the interface.
  - If the Tx interface ID is not identical to Rx interface ID, shut down the interface with a bigger ID, and leave the interface with a smaller ID in Up status.

## 11.1.5 Interface backup

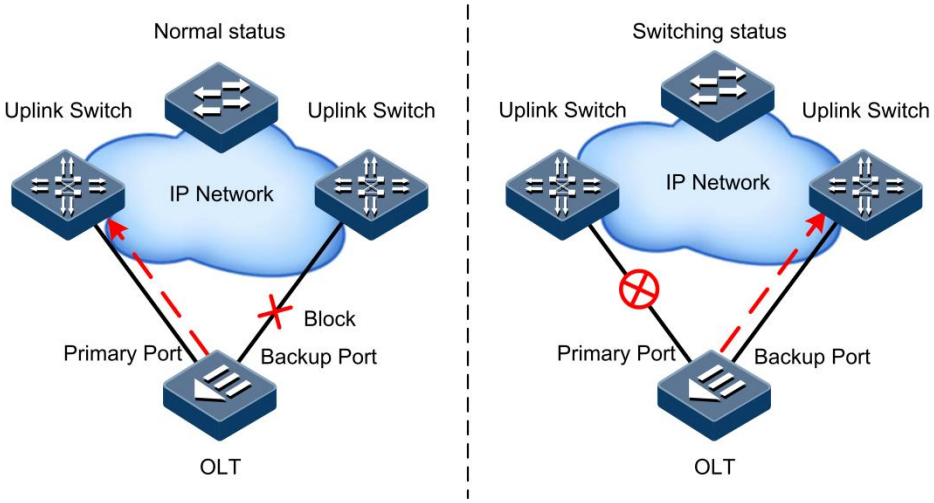
Interface backup is another solution of STP. When STP is disabled, you can realize basic link redundancy by manually configuring interface backup.

Interface backup is realized by configuring the interface backup group. Each interface backup group contains a primary interface and a backup interface. The principle of interface backup is as below:

- When the device is in normal status, all services are forwarded through the primary interface.
- When the link on the primary interface fails, services are switched to the backup interface for forwarding automatically.

Figure 11-3 shows the principle of interface backup.

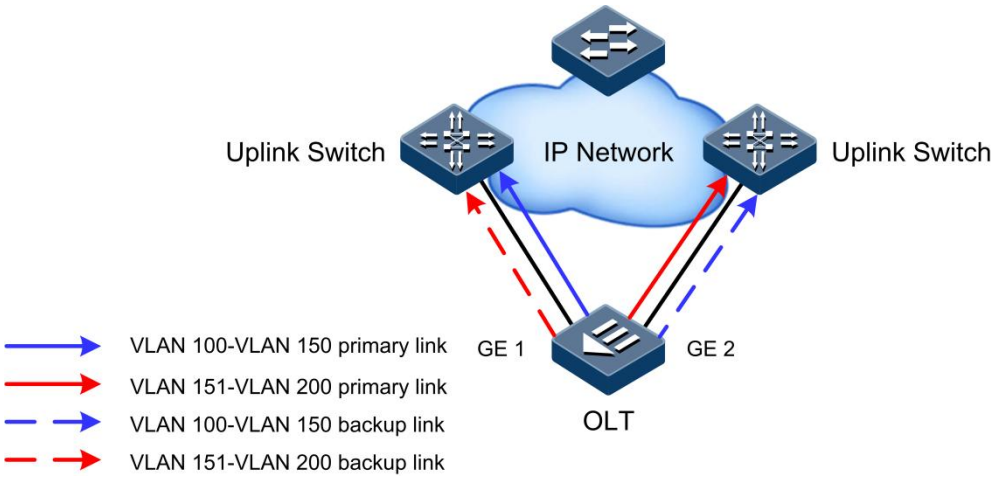
Figure 11-3 Principle of interface backup




## VLAN-based interface backup

Through applying interface backup on the VLAN, you can make two interfaces forward data simultaneously in different VLANs. As shown in Figure 11-4, through creating VLANs and adding interfaces to the VLAN, you can realize VLAN-based interface backup.

Figure 11-4 Principle of VLAN-based interface backup




In different VLANs, the interface forwarding status is shown as below:

- Under normal conditions, configure the ISCOM5508-GP in VLANs 100–150. GE 1 is the primary interface and GE 2 is the backup interface. In VLANs 151–200, GE 2 is the primary interface and GE 1 is the backup interface. Therefore, GE 1 forwards traffic of VLANs 1–100, and GE 2 forwards traffic of VLANs 101–200.
- When GE 1 fails, GE 2 forwards traffic of VLANs 100–150.
- When GE 1 restores normally and keeps Up for a period (restore-delay), GE 1 forwards traffic of VLANs 100–150, and GE 2 forwards traffic of VLANs 151–200.

VLAN-based interface backup can be used for load balancing. Moreover, it does not depend on configurations of uplink devices, thus facilitating users' operation.

# 11.2 Configuring link aggregation

## Scenario

When needing to provide higher bandwidth and reliability for a link between two devices, you can configure the 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.

# 11.2.2 Default configurations

Default configurations of link aggregation on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Link aggregation | Enable |
| LACP link aggregation | Enable |
| LAG | N/A |
| Load balancing mode | sxordmac |
| LACP system priority | 32768 |

# 11.2.3 Configuring manual link aggregation

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**interface port-channel** *group-id* | Create a LAG and enter LAG 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** { **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-list* | Add interfaces to the LAG in batch.<br>You can use the **no interface** { **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-list* command to delete the interface from the LAG. |

| Step | Command | Description |
|---|---|---|
| | Raisecom(config-port-channel-*)#**exit**<br>Raisecom(config)#**interface** { **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-id*<br>Raisecom(config-if-*-*:*)#**port-channel** *group-id* | Add an interface to the LAG.<br>You can use the **no port-channel** *group-id* command to delete the interface from the LAG. |

**Note**

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: port STP enabling/disabling status, link attributes connected to the port (point-to-point or not), port path cost, STP priority, packet Tx rate limiting, loopback protection, root protection, edge port or not.
- QoS: traffic monitoring, traffic shaping, rate limiting, SP queue, WRR queue scheduling, 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.

## 11.2.4 Configuring static LACP link aggregation

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**lacp system-priority** *system-priority* | (Optional) configure the LACP system priority.<br>You can use the **no lacp system-priority** command to restore default configurations.<br>**Note**<br>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. |

| Step | Command | Description |
|---|---|---|
| 4 | Raisecom(config-port-channel-*)#**port-channel mode lacp-static** | Configure the static LACP LAG. |
| 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** { **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-list* | Add interfaces to the LAG in batch.<br>You can use the **no interface** { **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-list* command to delete the interface from the LAG. |
| | Raisecom(config-port-channel-*)#**exit**<br>Raisecom(config)#**interface** { **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-list*<br>Raisecom(config-if-*-*:*)#**port-channel** *group-id* | Add an interface to the LAG.<br>You can use the **no port-channel** *group-id* command to delete the interface from the LAG. |

**Note**

- Interfaces in a static LACP LAG can be in active or standby status. Both active and standby interfaces can receive/send LACP packets, but standby interfaces cannot forward client packets.
- The system selects a default interface based on the following conditions in order: whether its neighbour is discovered, maximum interface rate, highest interface LACP priority (the smaller the value is, the higher the priority is), and smallest interface ID. The default interface is in active status. Interfaces, which have the same rate, peer device, and operation key with the default interface, are also in active status. Other interfaces are in standby status.

## 11.2.5 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show lacp system** | Show system LACP configurations. |
| 2 | Raisecom#**show lacp neighbor** | Show neighbor LACP information, including flag, interface priority, device ID, Age, operation key, interface ID, and status of the interface state machine. |
| 3 | Raisecom#**show lacp internal** | Show local LACP interface configurations. |
| 4 | Raisecom#**show lacp statistics** | Show interface LACP statistics, including total number of received/sent LACP packets, the number of received/sent Marker packets, the number of received/sent Marker Response packets, the number of errored packets. |
| 5 | Raisecom#**show port-channel** [ *group-id* ] | Show LAG configurations. |

# 11.3 Configuring failover

## Scenario

When the uplink fails, if downlink devices are not informed of the link failure, traffic will be interrupted because it cannot be switched to the backup link.

Through failover, uplink and downlink interfaces of the transit device are added to a failover group, and the uplink interface is monitored in real time. Once all uplink interfaces fail, all downlink interfaces are set to Down status. When at least one uplink interface recovers, all downlink interfaces recover to Up status. Therefore, faults of uplink devices can be transmitted to the downlink devices immediately. Uplink interfaces are not influenced when downlink interfaces fail.

## Prerequisite

Connect the interface, configure its physical parameters, and make it Up at the physical layer.

# 11.3.2 Default configurations

N/A

# 11.3.3 Configuring failover

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**link-state-tracking group** *group-number* | Create a failover group.<br>You can use the **no link-state-tracking group** *group-number* command to delete the failover group. |
| 3 | Raisecom(config)#**link-state-tracking group** *group-number* { **enable** \| **disable** } | Enable/Disable the failover group. |
| 4 | Raisecom(config)#**interface** { **gigabitethernet** *slot-id/port-id* \| **ten-gigabitethernet** *slot-id/port-id* \| **gpon-olt** *slot-id/port-id* \| **port-channel** *group-id* } | Enter physical interface configuration mode. |
| 5 | Raisecom(config-if-*-*:*)#**link-state-tracking group** *group-number* { **downstream** \| **upstream**} | Configure the failover group to which the interface belongs and the interface type.<br>**Note**<br>An interface can belong to one failover group only and the interface can only be an uplink or downlink interface. |

One failover group can contain several uplink interfaces. Failover will not be performed when at least one uplink interface is Up. Only when all uplink interfaces are Down, failover occurs.

## 11.3.4 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | `Raisecom#show link-state-tracking group [ group-number ]` | Show failover group configurations and status. Using this command does not display information about the failover group which has been created but is not enabled and has no member interface. |

# 11.4 Configuring RRPS

### Scenario

As a metro Ethernet technology, RRPS solves the problems of weak protection and taking too long to recover faults of the traditional data network. RRPS, in theory, can provide 50ms rapid protection features and is compatible with traditional Ethernet protocol, and is an important technology option and solution for metro broadband access network optimization and transformation.

RRPS technology is Raisecom independent research and development protocol, which achieves the elimination of ring network loopback, fault protection switching, and automatic fault recovery function through simple configuration, and makes the fault protection switching time less than 50ms.

### Prerequisite

N/A

## 11.4.2 Default configurations

Default configurations of RRPS on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| RRPS status | Disable |
| Interval to send Hello packets | 1s |
| Fault recovery delay | 5s |
| Bridge priority | 1 |
| Ring interface aging time | 15s |

| Function | Default value |
|---|---|
| Ring protocol packet VLAN | 2 |
| Ring description | Ethernet ring *ring-id* |

**Caution**

For all devices on a ring, we recommend that configurations of the fault recovery time, interval to send Hello packets, ring protocol packet VLAN, and aging time of the ring interface are consistent with those of master node.

## 11.4.3 Creating Ethernet ring

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**create ethernet ring** *ring-id* | Create an Ethernet ring.<br>Use the **no ethernet ring** *ring-id* command to delete the Ethernet ring. |
| 3 | Raisecom(config)#**ethernet ring** *ring-id* { **enable** \| **disable** } | Enable/Disable the Ethernet ring. |
| 4 | Raisecom(config)#**interface** { **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-id* | Enter physical interface configuration mode. |
| 5 | Raisecom(config-if-*-*:*)#**ethernet ring** *ring-id* { **primary** \| **secondary** } | Create the primary/secondary interface for the Ethernet ring. |

## 11.4.4 Configuring basic functions of Ethernet ring

**Note**

Master node selection: at the beginning, all nodes consider themselves as the master node, one of two interfaces is blocked, so no data loop on the ring; when two interfaces on the ring node receive the same Hello packet for many times, the node considers that the ring topology is stable and can be selected as the master node. Other nodes will enable the blocked interface. Generally, there is only one master node, which ensures that only one interface is blocked, and connectivity of nodes on the ring is proper.

Configure the ISCOM5508-GP as below.

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

| Step | Command | Description |
|---|---|---|
| 2 | Raisecom(config)#**ethernet ring** *ring-id* **hello-time** *hello-time* | (Optional) configure the interval to send Hello packets on the Ethernet ring.<br>Use the **no ethernet ring** *ring-id* **hello-time** *hello-time* command to restore default configurations.<br>**Note**<br>The interval to send Hello packets on the Ethernet ring should be less than half of the aging time of the ring interface. |
| 3 | Raisecom(config)#**ethernet ring** *ring-id* **restore-delay** *delay-time* | (Optional) configure the fault recovery delay on the Ethernet ring. When the fault recovers, the original working link restores to work after the delay expires.<br>You can use the **no ethernet ring** *ring-id* **restore-delay** *delay-time* command to restore default configurations. |
| 4 | Raisecom(config)#**ethernet ring** *ring-id* **priority** *priority* | (Optional) configure the bridge priority on the Ethernet ring.<br>You can use the **no ethernet ring** *ring-id* **priority** *priority* command to restore default configurations. |
| 5 | Raisecom(config)#**ethernet ring** *ring-id* **description** *string* | (Optional) configure ring descriptions.<br>You can use the **no ethernet ring** *ring-id* **description** command to restore default configurations. |
| 6 | Raisecom(config)#**ethernet ring** *ring-id* **hold-time** *hold-time* | (Optional) configure the aging time of the Ethernet ring interface.<br>You can use the **no ethernet ring** *ring-id* **hold-time** command to restore default configurations.<br>**Note**<br>If the Ethernet ring interface has not received a Hello packet in the aging time, age this interface. If the interface on a node is in blocked status, it will enable the temporarily blocked interface to ensure the normal communication of all nodes on the Ethernet ring. |
| 7 | Raisecom(config)#**ethernet ring** *ring-id* **protocol-vlan** *vlan-id* | (Optional) configure the Ethernet ring protocol VLAN.<br>You can use the **no ethernet ring** *ring-id* **protocol-vlan** command to restore default configurations. |
| 8 | Raisecom(config)#**ethernet ring upstream-group** { *group-list* } | (Optional) configure the uplink interface group on the Ethernet ring.<br>You can use the **no ethernet ring upstream-group** command to restore default configurations. |

- The uplink interface group works with failover, and supports dual homming topology applications.
- The uplink interface group ID is corresponding to the failover group ID.

## 11.4.5 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show ethernet ring** [ *ring-id* ] | Show information about the Ethernet ring. |
| 2 | Raisecom#**show ethernet ring port** | Show information about the Ethernet ring interface. |
| 3 | Raisecom#**show ethernet ring port statistic** | Show Ethernet ring interface statistics. |

## 11.4.6 Maintenance

Maintain the ISCOM5508-GP as below.

| Command | Description |
|---|---|
| Raisecom(config)#**clear ethernet ring** *ring-id* **statistics** | Clear Ethernet ring interface statistics. |

# 11.5 Configuring loopback detection

## 11.5.1 Preparing for configurations

### Scenario

On the network, hosts or Layer 2 devices connected downlink to all access devices may form loopback intentionally or involuntarily. Enabling loopback detection on the downlink interface of the access device can avoid the network congestion formed by unlimited data traffic caused by loopback on the downlink interface. Once the loopback 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.

## 11.5.2 Default configurations

Default configurations of loopback detection on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Global loopback detection status | Disable |
| Interface loopback detection status | Disable |
| Loopback detection VLAN | VLAN 1 |
| MAC address of loopback detection packet | FFFF.FFFF.FFFF |
| Loopback detection period | 4s |
| Loopback 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) |

## 11.5.3 Configuring loopback detection

**Note**

- Loopback detection and STP are exclusive, only one can be enabled at one time.
- Loopback detection cannot be enabled on both ends of the directly-connected device simultaneously; otherwise, interfaces at both ends will be blocked.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |
| 2 | `Raisecom(config)#loopback-detection` | Enable global loopback detection.<br>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 loopback detection packet.<br>You can use the **no loopback-detection destination-address** command to restore default configurations. |
| 4 | `Raisecom(config)#loopback-detection down-time { second \| infinite }` | (Optional) configure the shutdown time of the loopback interface.<br>You can use the **no loopback-detection down-time** command to restore default configurations. |
| 5 | `Raisecom(config)#loopback-detection hello-time` *second* | (Optional) configure the loopback detection period.<br>You can use the **no loopback-detection hello-time** command to restore default configurations. |

| Step | Command | Description |
|---|---|---|
| 6 | Raisecom(config)#**loopback-detection vlan** *vlan-id* | (Optional) configure the loopback detection VLAN.<br>You can use the **no loopback-detection vlan** command to restore default configurations. |
| 7 | Raisecom(config)#**interface** { **gigabitethernet** \| **ten-gigabitethernet** \| **gpon-olt** } *slot-id/port-id* | Enter physical interface configuration mode. |
| 8 | Raisecom(config-if-*-*:*)#**loopback-detection** | Enable interface loopback detection.<br>You can use the **no loopback-detection** command to disable this function. |
| 9 | Raisecom(config-if-*-*:*)#**loopback-detection** { **exloop** \| **loop** } { **discarding** \| **trap-only** } | Configure the action of the interface upon receiving the loopback detection packet. |
| 10 | Raisecom(config-if-*-*:*)#**no loopback-detection discarding** | (Optional) enable the blocked interface manually. |

## 11.5.4 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show** [**interface** { **gigabitethernet** \| **ten-gigabitethernet** \| **gpon-olt** } *slot-id/port-id* ] **loopback-detection** [ **statistics** ] | Show loopback detection configurations and statistics. |

# 11.6 Configuring interface backup

## 11.6.1 Preparing for configurations

### Scenario

Interface backup is another solution of STP. When STP is disabled, you can realize basic link redundancy by manually configuring interface backup.

### Prerequisite

Loopback detection and STP are exclusive, only one can be enabled at one time. So disable STP before configuring interface backup.

## 11.6.2 Default configurations

Default configurations of interface backup on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Interface backup group | N/A |
| Interface recovery | Enable |
| Interface recovery delay | 15s |
| Interface backup group VLAN | 1–4094 |

## 11.6.3 Creating interface backup group

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |
| 2 | `Raisecom(config)#create port-backup group` *group-id* | Create an interface backup group.<br>You can use the **no create backup-port group** *group-id* command to delete the configuration. |
| 3 | `Raisecom(config)#port-backup group` *group-id* { `enable` \| `disable` } | Enable/disable the interface backup group.<br>**Note**<br>The following two reasons may lead to enabling interface backup group failure:<br>The interface backup group does not exist.<br>The primary/backup interface is not configured in the interface backup group. |

## 11.6.4 Configuring interface backup group

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |
| 2 | `Raisecom(config)#port-backup group` *group-id* `vlanlist` *vlan-list* | Configure interface backup group VLAN.<br>You can use the **no port-backup group** *group-id* **vlanlist** command to restore default configurations. |
| 3 | `Raisecom(config)#interface` { `gigabitethernet` \| `ten-gigabitethernet` \| `gpon-olt` } *slot-id/port-id* | Enter physical interface configuration mode. |
| 4 | `Raisecom(config-if-*-*:*)#port-backup group` *group-id* { `primary-port` \| `backup-port` } | Configure the primary interface and backup interface.<br>You can use the **no port-backup group** *group-id* { **primary-port** \| **backup-port** } command to delete the configuration. |

| Step | Command | Description |
|---|---|---|
| 5 | Raisecom(config-if-*-*:*)#**port-backup group** *group-id* **restore-mode** { **enable** \| **disable** } | Enable/Disable interface recovery. |
| 6 | Raisecom(config-if-*-*:*)#**port-backup group** *group-id* **restore-delay** *time* | Configure the interface recovery delay.<br>You can use the **no port-backup group** *group-id* **restore-delay** command to restore default configurations. |

## 11.6.5 Configuring Force Switch

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**port-backup group** *group-id* **force-switch** | Configure FS on the interface backup group.<br>**Note**<br>When FS is configured on the interface backup group, the system configures the primary interface to blocked status and the backup interface to forwarding status without considering the current status of the primary/backup interface.<br>When FS is disabled on the interface backup group, the system configures the primary interface to forwarding status and the backup interface to blocked status without considering the current status of the primary/backup interface. |

## 11.6.6 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show port-backup group** [ *group-id* ] | Show interface backup configurations. |

# 11.7 Maintenance

Maintain the ISCOM5508-GP as below.

| Command | Description |
|---|---|
| `Raisecom(config)#clear ethernet ring ring-id statistics` | Clear protection ring statistics. |

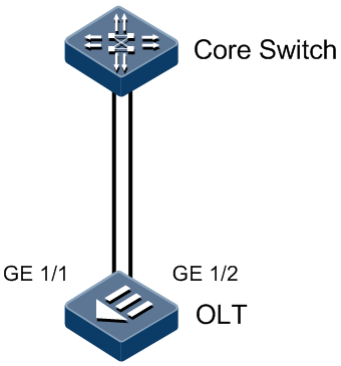
# 11.8 Configuration examples

## 11.8.1 Example for configuring manual link aggregation

### Networking requirements

As shown in Figure 11-5, to improve link reliability between the OLT and uplink aggregation switch, you can configure manual link aggregation on the OLT. Add GE 1/1 and GE 1/2 to the LAG to form a single logical interface. The LAG performs load balancing according to the source MAC address.

Figure 11-5 Manual link aggregation networking




### Configuration steps

Step 1 Create a manual LAG and the group ID is 1.

```
Rraisecom#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 gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#port-channel 1
Raisecom(config-if-gigabitethernet-1:1)#exit
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#port-channel 1
Raisecom(config-if-gigabitethernet-1:2)#exit
```

### Checking results

Use the **show port-channel** command to show global configurations of manual link aggregation.

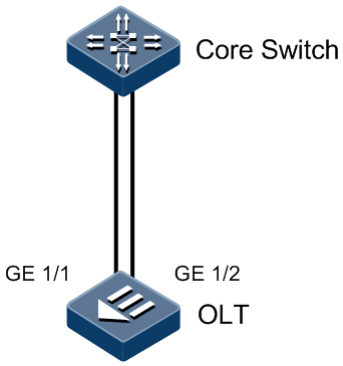
```
Raisecom#show port-channel 1
Port-channel ID : 1
   Mode            : Manual
   Load-sharing Mode : smac
   Member ports     : gigabitethernet 1/1,2
   Efficient ports   :
```

## 11.8.2 Example for configuring static LACP link aggregation

### Networking requirements

As shown in Figure 11-6, to improve link reliability between the OLT and uplink aggregation switch, you can configure static LACP link aggregation on the OLT. Add GE 1/1 and GE 1/2 to the LAG. GE 1/1 works as the primary link, and GE 1/2 works as the backup link.

Figure 11-6 Static LACP link aggregation networking




### Configuration steps

Step 1 Create a static LACP LAG.

```
Rraisecom#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 gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#port-channel 1
Raisecom(config-if-gigabitethernet-1:1)#exit
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#port-channel 1
Raisecom(config-if-gigabitethernet-1:2)#exit
```

Step 3 Configure the priority of GE 1/ to make the GE 1/1 as the primary link and GE 1/2 as the backup link.

```
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigaethgigabitethernet-1:1)#lacp port-priority 10000
Raisecom(config-if-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 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 peer 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
```

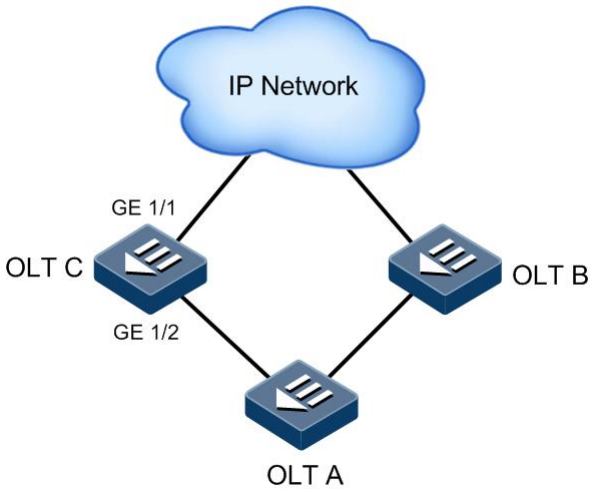
```
1/2    down     FA    32768      0x1        0x1        0x4d
```

## 11.8.3 Example for configuring failover

### Networking requirements

As shown in Figure 11-7, OLT C/OLT A is one of dual homing devices. Configure failover on OLT C to ensure that OLT A can detect the link failure quickly and switch to the backup link when the uplink of OLT C fails.

Figure 11-7 Failover networking




### Configuration steps

Step 1 Create and enable the failover group.

```
Raisecom#config
Raisecom(config)#link-state-tracking group 1
```

Step 2 Configure the uplink interface of the failover group.

```
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#link-state-tracking group 1
upstream
Raisecom(config-if-gigabitethernet-1:1)#exit
```

Step 3 Configure the downlink interface of the failover group.

```
Raisecom(config)#interface gigabitethernet 1/2
```

```
Raisecom(config-if-gigabitethernet-1:2)#link-state-tracking group 1
downstream
```

### Checking results

Use the **show link-state-tracking group** command to show failover configurations.

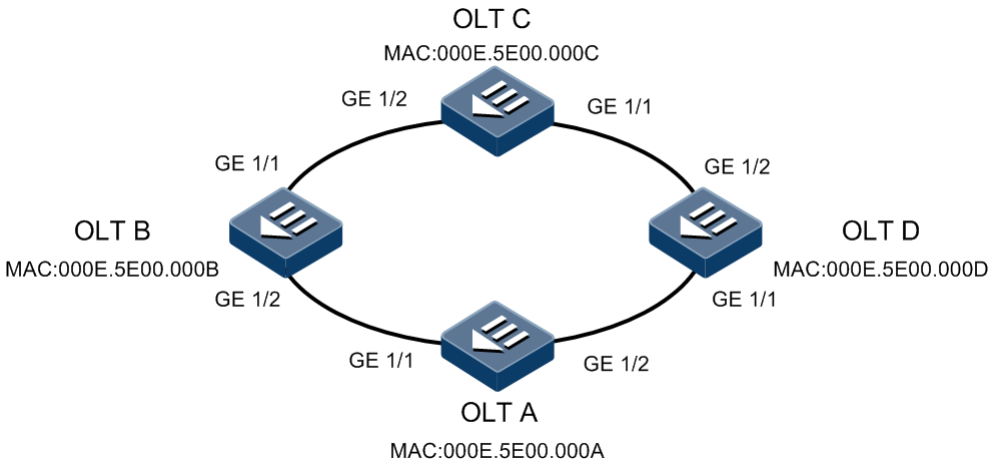
```
Raisecom#show link-state-tracking group 1
Link State Tracking Group: 1 (Enable)
Status:  Failover
Upstream Interfaces:
gigabitethernet 1/1(Up)
Downstream Interfaces:
gigabitethernet1/2(Up)
```

## 11.8.4 Example for configuring Ethernet ring

### Networking requirements

As shown in Figure 11-8, four OLTs form a ring network. Configure the Ethernet ring feature to achieve elimination of ring network loopback, fault protection switching, and automatic fault recovery. OLT A is the master node.

Figure 11-8 Ethernet ring networking




### Configuration steps

Configurations on four OLTs are identical. Take OLT A for example.

Step 1 Configure the Ethernet ring on OLT A.

```
Raisecom#config
Raisecom(config)#create ethernet ring 1
```

```
Raisecom(config)#ethernet ring 1 enable
```

Step 2 Configure the interface mode for OLT A and interface allowing the Ethernet ring protocol VLAN to pass.

```
Raisecom#config
Raisecom(config)#interface gigabitethernet 1/1
Raisecom(config-if-gigabitethernet-1:1)#ethernet ring 1 primary
Raisecom(config-if-gigabitethernet-1:1)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:1)#switchport trunk allowed vlan 2
Raisecom(config-if-gigabitethernet-1:1)#exit
Raisecom(config)#interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#ethernet ring 1 secondary
Raisecom(config-if-gigabitethernet-1:2)#switchport mode trunk
Raisecom(config-if-gigabitethernet-1:2)#switchport trunk allowed vlan 2
Raisecom(config-if-gigabitethernet-1:2)#exit
```

## Checking results

Use the **show ethernet ring** to show Ethernet ring configurations.

```
Raisecom#show ethernet ring
Ethernet Ring Upstream-Group:--
Ethernet Ring 1:
Ring Admin:         Enable
Ring State:         Unenclosed
Bridge State:       Block
Ring state duration:  0 days, 0 hours, 0 minutes, 55 seconds
Bridge Priority:     1
Bridge MAC:         000E.5E00.000A
Ring DB State:      Block
Ring DB Priority:    1
Ring DB:           000E.5E00.000A
Hello Time:         1
Restore delay:      5
Hold Time:          15
Protocol Vlan:      2
```

Use the **show ethernet ring port** to show Ethernet ring interface status.

```
Raisecom#show ethernet ring port
Ethernet Ring 1:
Primary Port:         1/1
Port Active State:     Active
State:               Block
Peer State:           None
Switch counts:        5
```

```
Current state duration: 0 days, 0 hours, 2 minutes, 28 seconds
Peer Ring Node:
1   --2:000E.5E00.000B:1--
2   --2:000E.5E00.000C:1--
3   --2:000E.5E00.000D:1–
Secondary Port:       1/2
Port Active State:     Active
State:               Forward
Peer State:           None
Switch counts:        6
Current state duration: 0 days, 0 hours, 2 minutes, 28 seconds
Peer Ring Node:
1   --1:000E.5E00.000D:2--
2   --1:000E.5E00.000C:2--
3   --1:000E.5E00.000B:2–
```

**Caution**

Before configuring Ethernet ring, you must configure the interface allowing the protocol VLAN to pass. By default, the protocol VLAN of the OLT is VLAN 2.

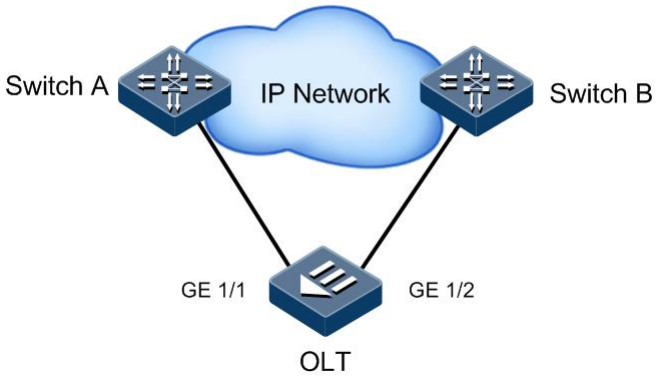
## 11.8.5 Example for configuring interface backup

### Networking requirements

As shown in Figure 11-9, 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 backup group 2, including interfaces GE 1/1 and GE 1/2. GE 1/1 is the primary interface of VLANs 100–150. GE 1/2 is the backup interface of VLANs 100–150.
- Create interface backup group 2, including GE 1/1 and GE 1/2. GE 1/2 is the primary interface of VLANs 151–200. GE 1/1 is the backup interface of VLANs 151–200.

Figure 11-9 Interface backup networking



## Configuration steps

Step 1 Create an interface backup group 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 1 backup-port
Raisecom(config-if-gigabitethernet-1:1)#exit
Raisecom(config)interface gigabitethernet 1/2
Raisecom(config-if-gigabitethernet-1:2)#port-backup group 1 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 interface backup
Group Id: 1
Primary Port(State): gigabitethernet1/1(Forwarding)
Backup Port(State) : gigabitethernet1/2(Discarding)
Vlanlist         : 100-150
Restore delay     : 15
Restore mode      : enable
switch state      : no force
switch count      : 0
---------------------------------------------
Group Id: 2
```

```
Primary Port(State): gigabitethernet1/2(Forwarding)
Backup Port(State) : gigabitethernet1/1(Discarding)
Vlanlist          : 151-200
Restore delay     : 15
Restore mode      : enable
switch state      : no force
switch count      : 0
----------------------------------------------
```

# 12 Configuring system management

This chapter introduces the basic principle and configuration process of the system management and maintenance feature of the ISCOM5508-GP, and provides related configuration examples, including the following sections:

- Overview of system management
- Configuring SNMP
- Configuring RMON
- Configuring optical module DDM
- Configuring Layer 2 protocol transparent transmission
- Configuring Watchdog
- Configuring system log
- Configuring port mirroring
- Configuring link detection
- Configuring LLDP
- Configuring system monitoring
- Configuring alarm and event management
- BCMP
- Maintenance
- Configuration examples

## 12.1 Overview of system management

### 12.1.1 SNMP

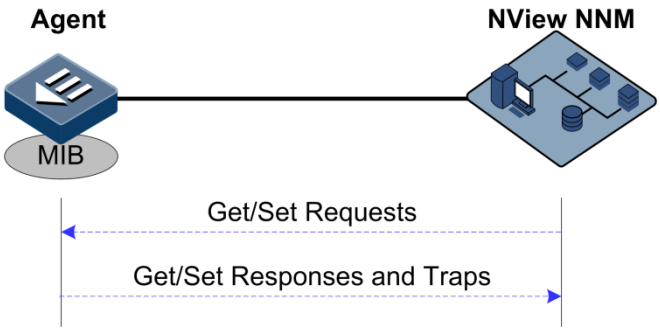
Simple Network Management Protocol (SNMP) is designed by the Internet Engineering Task Force (IETF) to resolve problems in managing network devices connected to the Internet. Through SNMP, a network management system can manage all network devices that support SNMP, including monitoring network status, 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 12-1.

Figure 12-1 Working mechanism of SNMP




Raisecom NView NNM system can provide friendly Human Machine Interface (HMI) to facilitate network management. The below functions can be realized 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 trigger conditions according to protocol modules, enter/exit from system or reboot device when conditions are satisfied; reply module sends Trap packets to NView NNM system via 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.

- SNMP v1 uses community name authentication mechanism. The community name, a string defined by an agent, acts like a secret. 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 ISCOM5508-GP, the message will be dropped.

- Compatible with SNMP v1, SNMP v2c also uses community name authentication mechanism. SNMP V2c supports more operation types, data types, and error codes, and thus better identifying errors.
- SNMP v3 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 store information in a tree structure, its root is on the top, without name. Nodes of the tree are the managed objects, which take a uniquely path starting from root (OID) for identification. SNMP packets can access network devices by checking the nodes in MIB tree directory.

## 12.1.2 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, as well as 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

## 12.1.3 System log

The system log refers 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 process. 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.

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 is an example of system log sent to the host:

```
07-01-201311:31:28Local0.Debug20.0.0.6JAN 01 10:22:15 ISCOM5508: CONFIG-
7-CONFIG:USER " raisecom " Run " logging on "
07-01-200811:27:41Local0.Debug20.0.0.6JAN 01 10:18:30 ISCOM5508: 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 12-1.

Table 12-1 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. Such as, when the information is configured with the level 3 (or the severity is errors), the information whose level ranges from 0 to 3,that is, the severity ranges 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 ISCOM5508-GP, 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 12-2 lists alarm fields.

Table 12-2 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 12-3.

Table 12-3 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) |

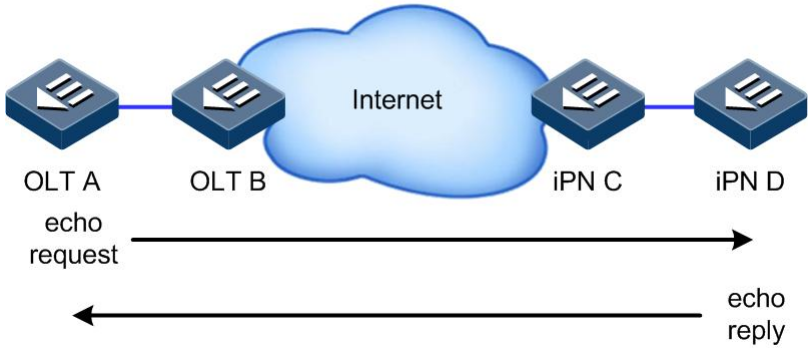
## 12.1.4 Ping

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 12-2 shows the working principle of Ping

Figure 12-2 Working principle of Ping




## 12.1.5 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.

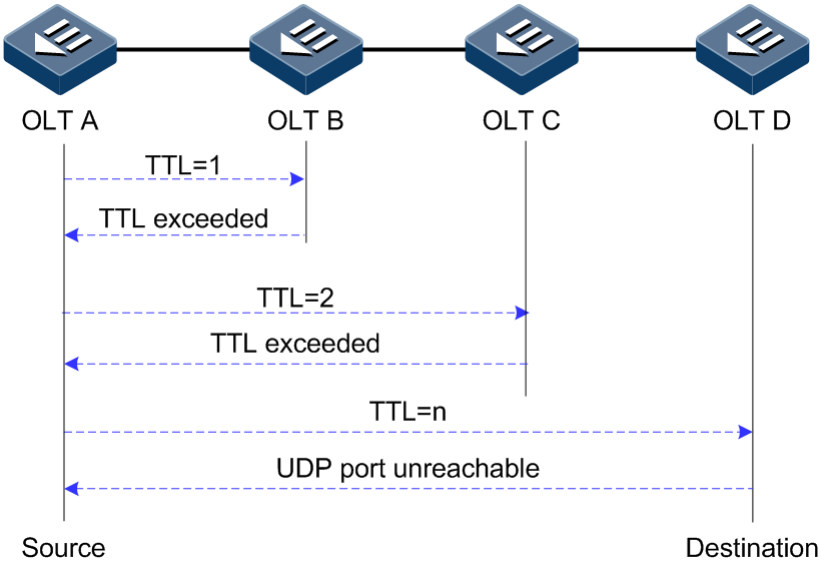
The following shows how Traceroute works:

- 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 be used, the destination host will send the 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 12-3 shows the working principle of Traceroute.

Figure 12-3 Working principle of Traceroute




## 12.1.6 LLDP

With the enlargement of network scale and increase of network devices, the network topology becomes more and more complex and network management becomes very 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 to the 3rd layer and cannot make sure the interfaces connect to other devices.

Link Layer Discovery Protocol (LLDP) is based on IEEE 802.1ab standard. Network management system 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 neighbour. It also saves the information from neighbour as standard Management Information Base (MIB) for network management system querying and judging link communication.

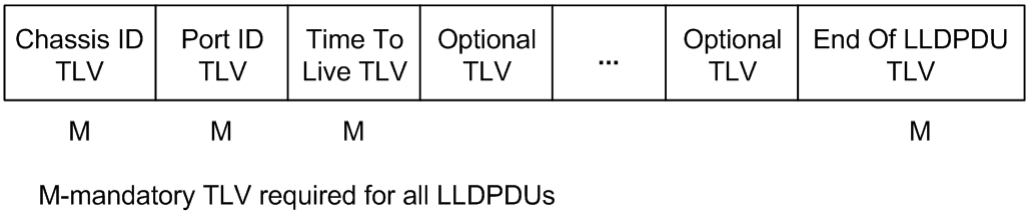
### Basic concepts

The LLDP packet is the Ethernet packet encapsulated LLDPDU in the data unit.

LLDPDU is a data unit of LLDP packet. The device encapsulates local information in TLV before forming LLDPDU, and then several TLVs fit together into one LLDPDU, which will be encapsulated in Ethernet data for transmission.

As shown in Figure 12-4, a LLDPDU consists of multiple TLVs, of which four are mandatory and others are optional.

Figure 12-4 Structure of LLDPDU



TLV: the unit to make up a LLDPDU, which refers to the unit describing the type, length and information of the object.

As shown in Figure 12-5, each TLV indicates a piece of information about the local device, such as device ID, interface ID, related Chassis ID TLV, and Port ID TLV fixed TLV.

Figure 12-5 Structure of TLV

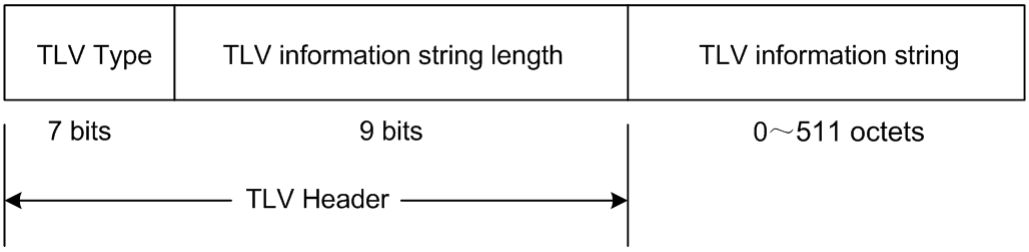



Table 12-4 lists the TLV types. At present, only types 0–8 are used.

Table 12-4 TLV type

| TLV type | Description | Mandatory or optional |
|---|---|---|
| 0 | End Of LLDPDU, indicating end of the LLDP packet | Mandatory |
| 1 | Chassis Id, indicating the MAC address of the Tx device | Mandatory |
| 2 | Port Id, indicating the Tx port of the LLDP packet | Mandatory |
| 3 | Time To Live, indicating the aging time of the local information on the neighbor device | Mandatory |
| 4 | Port Description, indicating descriptions of the Ethernet interface | Optional |
| 5 | System Name, indicating the name of the device | Optional |
| 6 | System Description, indicating descriptions of the system | Optional |
| 7 | System Capabilities, indicating the main function of the system and used options | Optional |
| 8 | Management Address | Optional |

## Working principle of LLDP

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

The process of packet exchange is as below:

- When the local device sends the LLDPDU, it gets system information required by TLV from NView NNM system and gets configuration information from LLDP MIB to generate TLV and form LLDPDU to transmit to the peer.
- The peer receives LLDPDU and analyzes TLV information. If there is any change, the information will be updated in neighbor MIB table of LLDP and notifies the NView NNM system.

The Time To Live (TTL) of local device information in the neighbour node can be adjusted by modifying the parameter values of aging coefficient. Send LLDP packets to the neighbour node, the neighbour node will adjust the aging time of its neighbour node (Tx end) after receiving LLDP packets. The aging time formula, TTL = Min {65535, (interval × hold-multiplier)}:

- Interval refers to the time period to send LLDP packets from the device to the neighbor node.
- Hold-multiplier refers to the aging coefficient of the device information on the neighbor node.

## 12.1.7 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 high-efficiently.

The difference of 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 not reported to the NMS nor recorded in the history event table. Event masking will not stop until you disable it manually.

# 12.2 Configuring SNMP

## 12.2.1 Default configurations

Default configurations of SNMP on the ISCOM5508-GP 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 | | | |

## 12.2.2 Configuring basic functions of SNMP v1/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.

SNMP v1/v2c uses the community name authentication scheme. SNMP packets which are inconsistent with the community name will be discarded.

Configure the ISCOM5508-GP as below.

| 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. |

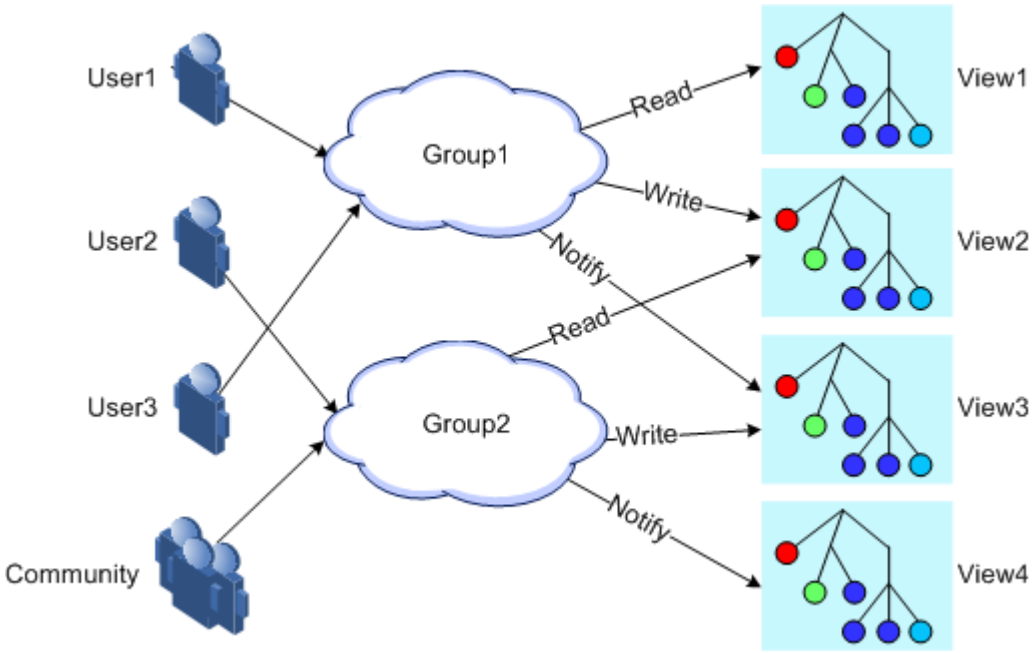
## 12.2.3 Configuring basic functions of SNMP v3

SNMP v3 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 12-6, the network management station uses SNMP v3 to access the ISCOM5508-GP 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 12-6 Authentication mechanism of SNMP V3




Configure the ISCOM5508-GP as below.

| 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 SNMP v3 access group. |
| 7 | Raisecom(config)#**snmp-server group** *group-name* **user** *username* { **v1sm** \| **v2csm** \| **usm** } | Configure mapping between the user and access group. |

## 12.2.4 Configuring other information of SNMP

Configure other information of SNMP, including:

- Identification and contact of administrators
- Physical location of the ISCOM5508-GP

SNMP v1, v2c, and v3 are in support of the above configuration.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**snmp-server contact** *contact* | (Optional) configure identification and contact of administrators.<br>**Note**<br>For example, user 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. |

## 12.2.5 Configuring Trap

**Note**

Except for the destination host configuration, Trap configurations of SNMP v1, 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 SNMP v1 and v2c, configure the community name; if using SNMP v3, configure the user name and SNMP view.
- Configure the routing protocol, and ensure that the route between the ISCOM5508-GP and NMS is reachable.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**snmp-server host** *ip-address* **version** { **1** \| **2c** } *name* [ **udpport** *value* ] | (Optional) configure the IPv4 Trap/Notification target host based on SNMP v1/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 SNMP v3. |
| 4 | Raisecom(config)#**snmp-server host ipv6** *ipv6-address* [**scopeid** *string* ] **version** { **1** \| **2c** } *name* [ **udpport** *value* ] | (Optional) configure the IPv6 Trap/Notification target host based on SNMP v1/v2. |
| 5 | Raisecom(config)#**snmp-server host ipv6** *ipv6-address* [ **scopeid** *string* ] **version 3** { **noauthnopriv** \| **authnopriv** } *name* [ **udpport** *value* ] | (Optional) configure the IPv6 Trap/Notification target host based on SNMP v3. |

| Step | Command | Description |
|---|---|---|
| 6 | Raisecom(config)#**snmp-server enable traps** | Enable the OLT to send Trap.<br>You can use the **no snmp-server enable traps** command to disable this function. |
| 7 | Raisecom(config)#**snmp-server keepalive-trap** { **enable** \| **disable** \| **pause** } | Enable/Disable/Pause to send KeepAlive Trap. |
| 8 | Raisecom(config)#**snmp-server keepalive-trap interval** *period* | Configure the interval to send KeepAlive Trap from the device to the SNMP NMS.<br>You can use the **no snmp-server keepalive-trap interval** command to restore default configurations. |

### 12.2.6 Checking configurations

Use the following commands to check configuration results.

| 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. |

## 12.3 Configuring RMON

### 12.3.1 Default configurations

Default configurations of RMON on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Statistics group | Enable |
| Historical statistics group | Disable |
| Alarm group | N/A |

| Function | Default value |
|---|---|
| Event group | N/A |

## 12.3.2 Configuring RMON statistics

RMON statistics is used to take statistics on an interface, including the number of Tx/Rx packets, undersized/oversized packets, collision, CRC and errors, discarded packets, length of Rx packets, fragments, broadcast packets, multicast packets, and unicast packets.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |
| 2 | `Raisecom(config)#rmon statistics { ip` *if-number* `\| port-list` *port-list* `} [ owner` *owner-name* `]` | Enable RMON statistics on an interface and configure related parameters.<br>You can use the **no rmon statistics** { **port-list** *port-list* \| **ip** *if-num* } command to disable this function. |

## 12.3.3 Configuring RMON historical statistics

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |
| 2 | `Raisecom(config)#rmon history { ip` *if-number* `\| port-list` *port-list* `} [ shortinterval` *period* `] [ longinterval` *period* `] [ buckets` *number* `] [ owner` *owner-name* `]` | Enable RMON historical statistics on an interface and configure related parameters.<br>You can use the **no rmon history** { **ip** *if-number* \| **port-list** *port-list* } command to disable the historical statistics group.<br>**Note**<br>When the historical statistics group is disabled on the interface, the system will not take statistics on the interface and historical statistics will be cleared. |

## 12.3.4 Configuring RMON alarm group

You can monitor a MIB variable (mibvar) by setting a RMON alarm group instance (*alarm-id*). An alarm event is generated when the value of the monitored data exceeds the defined threshold. Related information is recorded in the log or Trap is sent to the NView NNM system according to the definition of alarm events.

Note

- The monitored MIB variable must be real, and the data type is correct. If the variable does not exist or the value type is incorrect, return ERROR. For the successfully configured alarm, if the variable cannot be collected later, close the alarm. Reset it if you need to monitor the variable again.
- Disabling the statistics feature on the interface refers to not taking statistics on the interface instead of not take statistics any more.

By default, the event ID to trigger an event is 0, which indicates no event is triggered. If the number is not set to 0 and there is no event configured in the event group, the event is not successfully triggered when the monitored variable is abnormal. The event cannot be successfully triggered unless the event is created.

The alarm will be triggered as long as the upper or lower threshold of the event in the event table is matched. The alarm is not generated even when alarm conditions are matched if the event related to the upper/lower threshold (*rising-event-id* or *falling-event-id*) is not configured in the event table.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |
| 2 | `Raisecom(config)#rmon alarm` *alarm-id mibvar* `[ interval` *period* `] { delta \| absolute } rising-threshold` *value* `[` *event* `] falling-threshold` *value* `[` *event* `] [ owner` *owner-name* `]` | Add alarm instances to the RMON alarm group and configure related parameters.<br>You can use the **no rmon alarm** *alarm-id* command to delete the alarm group. |

## 12.3.5 Configuring RMON event group

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |
| 2 | `Raisecom(config)#rmon event` *event-id* `[ log ] [ trap ] [ description` *string* `] [ owner` *owner-name* `]` | Add events to the RMON event group and configure processing modes of events.<br>You can use the **no rmon event** *event-id* command to delete the event group. |

## 12.3.6 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | `Raisecom#show rmon alarms` | Show information about the RMON alarm group. |
| 2 | `Raisecom#show rmon events` | Show information about the RMON event group. |

| No. | Command | Description |
|---|---|---|
| 3 | Raisecom#**show rmon statistics** [ **ip** *if-number* \| **port** *port-id* ] | Show information about the RMON statistics group. |
| 4 | Raisecom#**show rmon history** [ **ip** *if-number* \| **port** *port-id* ] | Show information about the RMON historical statistics group. |

# 12.4 Configuring optical module DDM

## 12.4.1 Default configurations

Default configurations of optical module DDM on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Global optical module DDM | Enable (unconfigurable) |
| Global optical module DDM Trap | Enable (unconfigurable) |
| Optical module DDM on the interface | Disable |
| Optical module DDM Trap on the interface | Enable |

## 12.4.2 Configuring optical module DDM

Configure the ISCOM5508-GP as below.

| 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-*-*:*)#**transceiver ddm** { **enable** \| **disable** } | Enable/Disable optical module DDM. |
| 4 | Raisecom(config-if-*-*:*)#**snmp trap transceiver** { **enable** \| **disable** } | (Optional) enable/disable optical module DDM Trap on the interface. |

## 12.4.3 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show transceiver** | Show the global and interface status of the optical module measurement and diagnosis. |

| No. | Command | Description |
|---|---|---|
| 2 | Raisecom#**show interface gpon-olt** *slot-id/olt-id* **transceiver rx-onu-power** | Show information about the uplink average optical power of the ONU received by the optical module under the GPON interface. |
| 3 | Raisecom#**show interface** { **gpon-olt** \| **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-id* **ddm** [ **detail** ] | Show the current performance, alarm status, and alarm threshold of the optical module. |
| 4 | Raisecom#**show interface** { **gpon-olt** \| **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-id* **ddm history** [ **fifteen-minutes** \| **twenty-four-hours** ] | Show historical performance parameters of the optical module. |
| 5 | Raisecom#**show interface** { **gpon-olt** \| **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-id* **ddm information** | Show optical module status. |
| 6 | Raisecom#**show interface** { **gpon-olt** \| **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-id* **ddm threshold-violation** | Show the time from the last violation of the optical module to the present and corresponding violation value. |

# 12.5 Configuring Layer 2 protocol transparent transmission

## 12.5.1 Preparing for configurations

### Scenario

In the ISP network, destination multicast addresses for some Layer 2 protocol packets cannot be forwarded. The Layer 2 protocol transparent transmission is configured to make the Layer 2 protocol packet of the user network traverse the ISP network and to realize the Layer 2 protocol to run in the same user network at different locations. With the Layer 2 protocol transparent transmission, you can modify the multicast addresses for Layer 2 protocol packets for forwarding them across the ISP. In addition, you can decapsulate the modified multicast address to the original one on the egress interface. Therefore, the same user network at different locations can run the same Layer 2 protocol.

### Prerequisite

Configure physical parameters of the interface and make it Up at the physical layer.

## 12.5.2 Default configurations

Default configurations of Layer 2 protocol transparent transmission are as below.

| Function | Default value |
|---|---|
| Layer 2 protocol transparent transmission | Disable |
| Destination MAC address of transparent transmission packets | 010e.5e00.0003 |

| Function | Default value |
|---|---|
| CoS of transparent transmission packets | 5 |
| Specified VLAN of transparent transmission packets | N/A |
| Specified interface of transparent transmission packets | N/A |
| Interface disabling threshold of transparent transmission packets | N/A |

## 12.5.3 Configuring Layer 2 protocol transparent transmission

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |
| 2 | `Raisecom(config)#relay` | Enable Layer 2 protocol transparent transmission.<br>You can use the **no relay** command to disable this function. |
| 3 | `Raisecom(config)#relay destination-address` *mac-address* | (Optional) configure the destination MAC address of transparent transmission packets.<br>You can use the **no relay destination-address** command to restore default configurations. |
| 4 | `Raisecom(config)#relay cos` *cos-value* | (Optional) configure the CoS value of transparent transmission packets.<br>You can use the **no relay cos** command to restore default configurations. |
| 5 | `Raisecom(config)#interface { gigabitethernet \| gpon-olt }` *slot-id/port-id* | Enter physical interface configuration mode. |
| 6 | `Raisecom(config-if-*-*:*)#relay egress-port interface { gigabitethernet \| gpon-olt }` *slot-id/port-id* | Specify the egress interface of transparent transmission packets.<br>You can use the **no relay egress interface** command to restore default configurations. |
| 7 | `Raisecom(config-if-*-*:*)#relay vlan` *vlan-id* | Configure the specified VLAN of transparent transmission packets.<br>You can use the **no relay vlan** command to restore default configurations. |
| 8 | `Raisecom(config-if-*-*:*)#relay { all \| stp }` | Configure the type of transparent transmission packets on the interface.<br>You can use the **no relay** { **all** \| **stp** } command to restore default configurations. |

### 12.5.4 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show relay** | Show configurations of Layer 2 protocol transparent transmission. |
| 2 | Raisecom#**show interface** { **gigabitethernet** \| **ten-gigabitethernet** \| **gpon-olt** } *slot-id/port-id* **relay** | Show configurations of Layer 2 protocol transparent transmission on the interface. |
| 3 | Raisecom#**show interface** { **gigabitethernet** \| **ten-gigabitethernet** \| **gpon-olt** } *slot-id/port-id* **relay statistics** | Show statistics of transparent transmission packets. |

### 12.5.5 Maintenance

Maintain the ISCOM5508-GP as below.

| Command | Description |
|---|---|
| Raisecom(config)#**clear interface** { **gigabitethernet** \| **ten-gigabitethernet** \| **gpon-olt** } *slot-id/port-id* **relay statistics** | Clear statistics of Layer 2 protocol transparent transmission. |

## 12.6 Configuring Watchdog

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**watchdog** { **enable** \| **disable** } | Enable/Disable Watchdog. |

## 12.7 Configuring system log

### 12.7.1 Default configurations

Default configurations of system log on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| System log | Enable |

| Function | Default value |
|---|---|
| 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 |

## 12.7.2 Configuring basic information about system log

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**logging on** | Enable system log.<br>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. |

## 12.7.3 Configuring output direction of system log

Configure the ISCOM5508-GP as below.

| 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** \| **ipv6** } **address** ip-address **facility** { **local0** \| **local1** \| **local2** \| **local3** \| **local4** \| **local5** \| **local6** \| **local7** } **severity** [ *log-level* \| **alerts** \| **critical** \| **debugging** \| **emergencies** \| **errors** \| **informational** \| **notifications** \| **warnings** ] | (Optional) output system log to the log host. |
| | 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. |

### 12.7.4 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show logging** | Show system log configurations. |
| 2 | Raisecom#**show logging host** | Show information about the system log host. |
| 3 | Raisecom#**show logging history** | Show information about system log buffer. |
| 4 | Raisecom#**show logging statistics** | Show statistics of system log. |

## 12.8 Configuring port mirroring

### 12.8.1 Default configurations

N/A

### 12.8.2 Configuring port mirroring

Configure the ISCOM5508-GP as below.

| 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** { **gigabitethernet** \| **ten-gigabitethernet** \| **gpon-olt** } *slot-id/port-id* | Enter physical interface configuration mode. |
| 4 | Raisecom(config-if-*-*/*)#**mirror monitor-port** *uni-id* | (Optional) configure the monitor port.<br>You can use the **no mirror monitor-port** command to delete the monitor port.<br>**Note**<br>The GPON interface cannot be configured as the monitor port, and it can only be configured as the source port. The Ethernet interface can be configured as the monitor port or mirroring source port. |
| 5 | Raisecom(config-if-*-*/*)#**mirror source-port** { **both** \| **egress** \| **ingress** } | (Optional) configure the mirroring source port.<br>You can use **no mirror source-port** command to restore default configurations. |

### 12.8.3 Checking configurations

Use the following commands to check configuration results.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**show mirror** | Show configurations of port mirroring. |

## 12.9 Configuring link detection

### 12.9.1 Ping

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**ping** *ip-address* [ **count** *num* ] [ **size** *size* ][ **waittime** *timout* ] | Test whether the IPv4 remote host is reachable. |
| 2 | Raisecom#**ping ipv6** *ipv6-address* [ **count** *num* ] [ **size** *size* ] [ **waittime** *timout* ] | 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 Ping is complete or press **Ctrl**+**C** to interrupt Ping.

### 12.9.2 Traceroute

**Note**

Configure the IP address and default gateway for the ISCOM5508-GP before using the Traceroute function.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**traceroute** *ip-address* [ **firstttl** *fitst-ttl* ] [ **maxttl** *max-ttl* ] [ **port** *slot-id/port-id* ] [ **waittime** *period*] [ **count** *count* ] | Test the IPv4 network connectivity using the **traceroute** command and show the network nodes passed through by the packet. |
| 2 | Raisecom#**traceroute ipv6** *ipv6-address* [ **firstttl** *fitst-ttl* ] [ **maxttl** *max-ttl* ] [ **port** *slot-id/port-id* ] [ **waittime** *period*] [ **count** *count* ] | Test the IPv6 network connectivity using the **traceroute** command and show the network nodes passed through by the packet. |

# 12.10 Configuring LLDP

## 12.10.1 Default configurations

Default configurations of LLDP on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Global LLDP | Disable |
| Interface LLDP | Enable |
| Delay Tx timer | 2s |
| Period Tx timer | 30s |
| Aging coefficient | 4 |
| Restart timer | 2s |
| LLDP alarm | Enable |
| Alarm notification timer | 5s |

## 12.10.2 Configuring global LLDP

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |
| 2 | `Raisecom(config)#lldp { enable \| disable }` | Enable/Disable global LLDP. |
| 3 | `Raisecom(config)#lldp message-transmission interval` *period* | (Optional) configure the period Tx timer of LLDP packets.<br>You can use the **no lldp message-transmission** command to restore default configurations. |
| 4 | `Raisecom(config)#lldp message-transmission delay` *period* | (Optional) configure delay Tx timer of LLDP packets.<br>You can use the **no lldp message-transmission delay** command to restore default configurations. |
| 5 | `Raisecom(config)#lldp message-transmission hold-multiplier` *hold-multiplier* | (Optional) configure the aging coefficient of LLDP packets.<br>You can use the **no lldp message-transmission hold-multiplier** command to restore default configurations. |
| 6 | `Raisecom(config)#lldp restart-delay` *period* | (Optional) configure the restart timer. When global LLDP is disabled, you can re-enable it only after the time configured by the restart timer.<br>You can use the **no lldp restart-delay** command to restore default configurations. |

**Caution**

- After global LLDP is disabled, you cannot re-enable it immediately. Global LLDP cannot be enabled unless the restart timer times out. Because disabling or enabling operations will trigger logout and login of Tx and Rx packets, when disabling the LLDP function, the device will send the Shutdown packet, LLDP can be logged out after each interface completes sending the packet, that is, say, there is a delay after LLDP logout. If enabling LLDP again before the delayed logout, LLDP will be logged out in delayed logout, which will make the configuration different from the actual situation.
- When you configure the delay Tx timer and period Tx timer, the value of the delay Tx timer cannot exceed one quarter of that of the period Tx timer.

## 12.10.3 Configuring interface LLDP

Configure the ISCOM5508-GP as below.

| 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-*-*:*)#lldp { enable \| disable }` | Enable/Disable interface LLDP. |

## 12.10.4 Configuring LLDP alarm

Enable LLDP alarm notification to send the topology update alarm to the NView NNM system when the network changes.

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | `Raisecom#config` | Enter global configuration mode. |
| 2 | `Raisecom(config)#snmp trap lldp { enable \| disable }` | Enable/Disable the LLDP alarm. |
| 3 | `Raisecom(config)#lldp trap-interval period` | (Optional) configure the period Tx time of LLDP Trap. |

**Note**

After enabling the LLDP alarm function, the device will send Trap when it detects neighbor aging, new neighbor, and neighbor information changing.

## 12.10.5 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show lldp local config** | Show LLDP local configurations. |
| 2 | Raisecom#**show lldp local system-data** | Show local LLDP status. |
| 3 | Raisecom#**show interface** { **gpon-olt** \| **gigabitethernet** \| **ten-gigabitethernet** } *slot-id/port-id* **lldp local system-data** | Show configurations of the LLDP interface. |
| 4 | Raisecom#**show lldp remote** [ **detail** ] | Show LLDP local neighbor information. |
| 5 | Raisecom#**show interface** { **gigabitethernet** \| **ten-gigabitethernet** \| **gpon-olt** } *slot-id/port-id* **lldp remote** [ **detail** ] | Show LLDP interface neighbor information. |
| 6 | Raisecom#**show lldp statistic** | Show LLDP local packet statistics. |
| 7 | Raisecom#**show interface** { **gigabitethernet** \| **ten-gigabitethernet** \| **gpon-olt** ] *slot-id/port-id* **lldp statistic** | Show LLDP interface packet statistics. |

# 12.11 Configuring system monitoring

## 12.11.1 Default configurations

Default configurations of system monitoring on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Temperature monitoring | Enable |
| Power monitoring | Enable |
| Fan monitoring | Enable |
| CPU utilization threshold Trap | Disable |
| CPU alarm rising threshold | 80 |
| CPU alarm falling threshold | 30 |
| Available memory utilization threshold Trap | Disable |
| Memory monitoring alarm threshold | 1 |

## 12.11.2 Configuring temperature monitoring

Configure the ISCOM5508-GP as below.

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

| Step | Command | Description |
|---|---|---|
| 2 | Raisecom(config)#**shelf temperature-threshold** *threshold-value* | Configure the temperature alarm threshold. When the temperature of the device exceeds the threshold, the alarm is reported. |

## 12.11.3 Configuring fan monitoring

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**fan speed mode** { **auto** \| **manual** } | Configure the fan control mode. |
| 3 | Raisecom(config)#**fan speed manual** *grade* | (Optional) configure the fan speed grade. |

**Note**

You need to configure the fan control mode to manual mode before configuring the fan speed grade.

## 12.11.4 Configuring CPU monitoring

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**cpu threshold-trap** | Configure the CPU utilization threshold Trap feature. |
| 3 | Raisecom(config)#**cpu rising-threshold** *threshold* | Configure the CPU alarm rising threshold. |
| 4 | Raisecom(config)#**cpu falling-threshold** *threshold* | Configure the CPU alarm falling threshold. |
| 5 | Raisecom(config)#**cpu threshold-interval** *threshold* | Configure the CPU utilization monitoring period. |

## 12.11.5 Configuring memory monitoring

Configure the ISCOM5508-GP as below.

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

| Step | Command | Description |
|---|---|---|
| 2 | Raisecom(config)#**memory avail-trap slot** *slot-list* | Configure the available memory utilization threshold Trap feature. |
| 3 | Raisecom(config)#**memory avail-threshold** *threshold* **slot** *slot-list* | Configure the memory monitoring alarm threshold. |

## 12.11.6 Checking configurations

Use the following commands to check configuration results.

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show fan** | Show the fan status and configurations. |
| 2 | Raisecom#**show power** | Show power information, including power type, related threshold configurations, input and output voltage, related alarm status, and power version. |
| 3 | Raisecom#**show device** | Show information about the device, including temperature, temperature alarm threshold, power, and fan. |
| 4 | Raisecom#**show card-power** [ **slot** *slot-id* ] | Show voltage information of all cards in the slots (except for the power card and fan), including card voltage status and card voltage. |
| 5 | Raisecom#**show card-temperature** [ **slot** *slot-id* ] | Show temperature of all cards in the slots. |
| 6 | Raisecom#**show cpu-utilization** [ **slot** *slot-list* ] [ **dynamic** ] | Show CPU utilization of cards in the specified slot. |
| 7 | Raisecom#**show process sorted** { **normal-priority** \| **process-name** } | Show the status of each task. |
| 8 | Raisecom#**show process cpu** [ **sorted** { **1min** / **10min** / **5sec** / **invoked** } ] | Show the running status of each task. |
| 9 | Raisecom#**show process** *taskname* | Show detailed running status of a specified task. |
| 10 | Raisecom#**show process dead** | Show information about the dead task. |
| 11 | Raisecom#**show memory** | Show utilization of the system memory. This command is applicable to cartridge device only. |
| 12 | Raisecom#**show memory** [ **slot** *slot-list* ] | Show memory utilization of cards in the specified slot. This command is applicable to rack-mount device. |
| 13 | Raisecom#**show abnormal-reboot** [ **slot** *slot-list* ] | Show information about abnormal start. |
| 14 | Raisecom#**show abnormal-reboot last** [ **slot** *slot-list* ] | Show the status of the last abnormal start. |

| No. | Command | Description |
|---|---|---|
| 15 | Raisecom#**show abnormal-reboot last wait-info [slot** *slot-list* **]** | Show wait information about the last abnormal start. |

# 12.12 Configuring alarm and event management

## 12.12.1 Default configurations

Default configurations of alarm and event management on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| Alarm Trap | Enable |
| Event Trap | Enable |
| Alarm delay | Disable |
| Alarm delay interval | 10s |
| Timed alarm masking interval | 3600s |

## 12.12.2 Configuring alarm management

The alarm management feature on the ISCOM5508-GP includes alarm reporting, alarm masking, and alarm delay.

### Configuring alarm reporting

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**alarm traps** { **enable** \| **disable** } | 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. |

### 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.

Configure the ISCOM5508-GP as below.

| 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.<br>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.<br>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** { **gigabitethernet** \| **gpon-olt** } *slot-id/port-id* [ **alarm-id** *alarm-id* ] | Configure alarm masking on the alarm source of the OLT interfaces.<br>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 gpon-onu** *slot-id/olt-id/onu-id* [ **alarm-id** *alarm-id* ] | Configure alarm masking on the alarm source of the ONU.<br>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 ONU are masked. |
| 3 | Raisecom(config)#**alarm inhibit** { **dev** \| **slot** \| **port** \| **onu** \| **uni** } **alarm-id** *alarm-id* | Configure alarm masking based on the 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.<br>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 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.<br>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. |

| Step | Command | Description |
|---|---|---|
| | Raisecom(config)#**alarm inhibit time** [ **range** ] **interface** { **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.<br>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. |
| 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 the alarm ID. |
| 6 | Raisecom(config)#**alarm inhibit interval** *time* | (Optional) configure the interval of timed alarm masking. |

## Configuring alarm filtering

Configure the ISCOM5508-GP as below.

| 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.<br>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.<br>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. |
| 4 | Raisecom(config)#**alarm filter** [ **range** ] **interface** { **gigabitethernet** \| **ten-gigabitethernet** \| **gpon-olt** } *slot-id/port-id* [ **alarm-id** *alarm-id* ] | Configure alarm filtering on the alarm source of the OLT interfaces.<br>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** { **dev** \| **slot** \| **port** \| **onu** \| **uni** } **alarm-id** *alarm-id* | Configure alarm filtering based on the alarm ID. |

## 12.12.3 Configuring event management

Configure the ISCOM5508-GP as below.

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configuration mode. |
| 2 | Raisecom(config)#**event traps** { **enable** \| **disable** } | Enable/Disable the event Trap feature. |
| 3 | Raisecom(config)#**event inhibit dev** [ **event-id** *event-id* ] | Configure event masking on the event source of the whole device.<br>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.<br>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 are masked. |
| 5 | Raisecom(config)#**event inhibit** [ **range** ] **interface** { **gigabitethernet** \| **gpon-olt** } *slot-id/port-id* [ **event-id** *event-id* ] | Configure event masking on the event source of the OLT interfaces.<br>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 the event ID. |

## 12.12.4 Checking configurations

Use the following commands to check configuration results.

| 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 detailed information about alarms. |
| 5 | Raisecom#**show event inhibit** | Show event masking configurations. |

| No. | Command | Description |
|---|---|---|
| 6 | Raisecom#**show event event-id** *event-id* | Show detailed information about events. |

# 12.13 BCMP

## 12.13.1 Default configurations

Default configurations of BCMP on the ISCOM5508-GP are as below.

| Function | Default value |
|---|---|
| IP address of the BCMP server | 0.0.0.0 |
| UDP port of the BCMP server | 5000 |
| UDP port of the BCMP Proxy | 5001 |

## 12.13.2 Configuring BCMP

| Step | Command | Description |
|---|---|---|
| 1 | Raisecom#**config** | Enter global configurations. |
| 2 | Raisecom(config)#**bcmp server ip-address** *ip-address* | Configure the IP address of the BCMP server. |
| 3 | Raisecom(config)#**bcmp server udp-port** *port-id* | Configure the UDP port ID of the BCMP server. |
| 4 | Raisecom(config)#**bcmp proxy udp-port** *port-id* | Configure the UDP port ID of the BCMP Proxy. |

## 12.13.3 Checking configurations

| No. | Command | Description |
|---|---|---|
| 1 | Raisecom#**show bcmp information** | Show BCMP configurations. |

# 12.14 Maintenance

Maintain the ISCOM5508-GP as below.

| Command | Description |
|---|---|
| Raisecom(config)#**clear lldp statistic** [ **port-list** *slot-id/port-list* ] | Clear LLDP statistics. |
| Raisecom(config)#**clear lldp remote-table** [ **port-list** *slot-id/port-list* ] | Clear LLDP neighbor information. |
| Raisecom(config)#**clear logging history** | Clear log records in the buffer. |

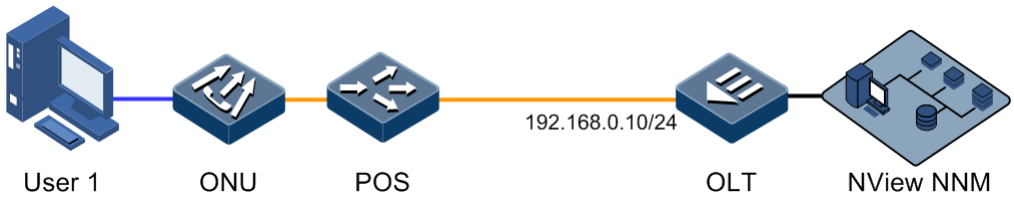
# 12.15 Configuration examples

## 12.15.1 Example for configuring SNMP

### Networking requirements

As shown in Figure 12-7, 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 guestgroup access group 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 12-7 SNMP v3 networking




### Configuration steps

Step 1 Configure the IP address.

```
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address 192.168.0.10 10
Raisecom(config-ip)#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 the access group and its name.

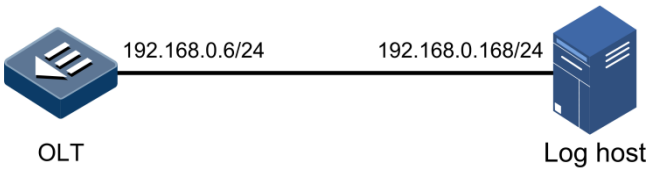
```
Raisecom#show snmp group
Index    UserName           SecModel       GroupName
------------------------------------------------------------
  0      none               usm            initialnone
  1      user1              usm            guestgroup
  2      md5nopriv          usm            initial
  3      shanopriv          usm            initial
```

## 12.15.2 Example for outputting system log to host

### Networking requirements

As shown in Figure 12-8, 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 12-8 Outputting system log to host




### Configuration steps

Step 1 Configure the IP address of the OLT.

```
Raisecom#config
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address 192.168.0.6 255.255.255.0 1
Raisecom(config-ip)#exit
```

Step 2 Configure 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.

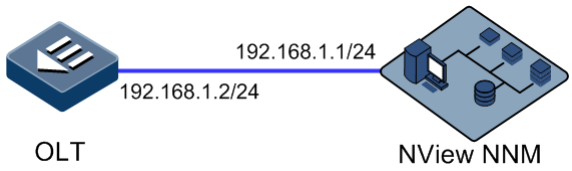
```
Raisecom#show logging
Syslog logging    : Enable
Rate-limited      : 10 messages per second
Logging time-stamp : Relative time-stamp
Console logging   : Enable
Conslole severity  : Notifications
Monitor logging   : Disable
Monitor severity   : Informational
History logging   : Enable
History severity   : Debugging
File logging      : Disable
File severity     : Informational
```

## 12.15.3 Example for configuring KeepAlive Trap

### Networking requirements

As shown in Figure 12-9, the IP address of the OLT is 192.168.1.2. The IP address of the SNMP v2c Trap target host is 192.168.1.1. The read-write community name is public. And the SNMP version is v2c. Configure the interval to send KeepAlive Trap from the OLT to the SNMP NMS as 120s and enable KeepAlive Trap.

Figure 12-9 KeepAlive networking




### Configuration steps

Step 1 Configure the management IP address of the OLT.

```
Raisecom#config
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address 192.168.1.2 255.255.255.0 1
Raisecom(config-ip)#exit
```

Step 2 Configure the IP address of the SNMP Trap target host.

```
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 show KeepAlive configurations.

```
Raisecom#show keepalive
Keepalive Admin State:Enable
Keepalive trap interval:120s
Keepalive trap count:1
```

# 13 Appendix

This chapter lists terms, acronyms, and abbreviations involved in this document.

- Terms
- Acronyms and abbreviations

## 13.1 Terms

**A**

| | |
|---|---|
| Advanced Encryption Standard (AES) | It is a kind of block encryption standard adopted by the United States to replace the DES. At present, it has become the most widely used standard in the field of symmetric key cryptography. |

**C**

| | |
|---|---|
| Connectivity Fault Management (CFM) | CFM is end-to-end service-level Ethernet OAM technology. This function is used to actively diagnose fault for Ethernet Virtual Connection (EVC) and provide cost-effective network maintenance solution via fault management function and improve network maintenance. |

**D**

| | |
|---|---|
| Denial of Service (DoS) | A common network or computer attack, which aims to make the network or computer fail to provide normal services |
| Dynamic ARP Inspection (DAI) | A security feature that can be used to verify the ARP datagram in the network. With DIA, 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 realize centralized management of IP addresses. |

**E**

| | |
|---|---|
| Ethernet Linear Protection Switching (ELPS) | An APS protocol based on ITU-T G.8031 Recommendation to protect an Ethernet link. It is an end-to-end protection technology, including two line protection modes: linear 1:1 protection switching and linear 1+1 protection switching. |
| Ethernet Over Coaxial (EoC) | EoC enables transmitting Ethernet signals on the coaxial cable. EoC supports coupling CATV signals and Ethernet data signals, and transmitting the hybrid signals to the user side through the CATV coaxial cable, and then demodulating signals through the CNU. EoC is the key technology to realize tri-networks integration (data, voice, and CATV networks) and bidirectional reconstruction of HFC networks. |
| Ethernet Ring Protection Switching (ERPS) | An APS (Automatic Protection Switching) protocol based on ITU-T G.8032 Recommendation to provide backup link protection and recovery switching for Ethernet traffic in a ring topology and at the same time ensuring that there are no loops formed at the Ethernet layer. |

**F**

| | |
|---|---|
| Failover | Provide a port association solution, extending link backup range. Transport fault of upper layer device quickly to downstream device by monitoring upstream link and synchronize downstream link, then trigger switching between master and standby device and avoid traffic loss. |
| Fiber to the Building (FTTB) | FTTB is based on perfection of broadband access method on the optical fiber network. Through FTTB and cable-to-household, broadband access can be realized. |
| Fiber to the Curb (FTTC) | Optical fiber is installed on the roadside within 1000 feet away from the Central Office to the households or offices. |
| Fiber to the Home (FTTH) | Namely, optical fiber is used to connect the household directly. FTTH not only helps gain greater bandwidth, but also increase transparency of data format, rate, wavelength, and protocol. Moreover, it is more adaptive to environment and power conditions, and simplifies the maintenance and installation. |
| Forward Error Correction (FEC) | It is a method to increase ODN power budget by adding Error Correcting Code (ECC). It supports longer transmission distance and larger splitting ratio. |

| | |
|---|---|
| Frequency Division Multiplexing (FDM) | It is a multiplexing technology which divides the carrier bandwidth into multiple sub-channels at different frequency bands. And each sub-channel can transmit one way of signals concurrently. |

**H**

| | |
|---|---|
| H.248 | It is a media gateway control protocol proposed by the 16th working group of ITU-T in 2000 based on the MGCP. H.248/MeGaCo protocol is the gateway control protocol used to connect the MGC and MG. It can be applied between the media gateway and soft switch, or soft switch and H.248/MeGaCo terminal. It is also an important protocol supported by soft switch. |
| HomePlug | HomePlug is a non-profit organization, which is established by 13 companies, such as, Panasonic, Intel, HP, and Sharp, in March, 2000. At present, HomePlug has developed into an enterprise alliance composed of 90 companies. The purpose of this organization is to unite leading enterprise in the field of applied electronics, consumer electronics, software, hardware, and retail, and so on to provide an open power-line Internet access specifications for various information appliances. |

**I**

| | |
|---|---|
| Institute of Electrical and Electronics Engineers (IEEE) | An international Institute of electrical and Electronics Engineers. It is one of the largest technical organizations. It has more than 360,000 members in 175 countries (up to 2005). |
| Internet Assigned Numbers Authority (IANA) | It is mainly used to assign and maintain the unique code and value in Internet technology standard (protocol), such as the IP address or multicast address. |
| Internet Engineering Task Force (IETF) | It is established in 1985. It is the most authoritative technology and standard organization, which develops and formulate specifications related to the Internet. |

**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. |

| | |
|---|---|
| Link Aggregation Control Protocol (LACP) | A protocol used for realizing link dynamic aggregation. LACP communicates with the peer by exchanging LACPDU. |

**M**

| | |
|---|---|
| Maintenance Association (MA) | MA, also called Service Instance, is part of a Maintenance Domain (MD). One MD can be divided into one MA or multiple MAs if required. One MA corresponds to one service and can be mapped to a VLAN. VLANs to which are mapped by different services cannot cross. |
| Maintenance associations End Point (MEP) | MEP is an edge node of a service instance. MEPs can be used to send and process CFM packets. The MA and the MD where MEP locates decide the VLAN and the level for packets received and sent by MEP. |
| Maintenance association Intermediate Point (MIP) | MIP is the internal node of a service instance, which is automatically created by the device. MIP cannot actively send CFM packets but can forward and respond to Link Trace Message (LTM) and LoopBack Message (LBM). |
| Maintenance Domain (MD) | MD is a network that runs the CFM function. It defines network range for OAM. MD can be identified with 8 levels (0–7). The bigger the number, the higher the level and the larger the MD range. Protocol packets in a lower-level MD will be discarded after entering into a higher-level MD. Protocol packets in a higher-level MD can transmit through a lower-level MD. In the same VLAN, Different MDs can be adjacent, embedded, but not crossed. |
| Maintenance Point (MP) | MEP and MIP are called as MP. |
| Mobile Backhaul | Solve communication problem from BTS to BSC for 2G, NodeB to RNC for 3G.<br>Mobile backhaul for 2G focuses on voice service, not request high bandwidth, implemented by TDM microwave or SDH/PDH device.<br>In 3G times, lots of data service as HSPA, HSPA+, etc concerning to IP service, voice is changing to IP as well, namely IP RAN, to solve problem of IP RAN mobile backhaul is solving whole network backhaul, satisfying both data backhaul and voice transportation over IP (clock synchronization). |

**N**

| | |
|---|---|
| Network Time Protocol (NTP) | A time synchronization protocol defined by RFC1305. It is used to synchronize time between distributed timer server and clients. NTP is used to perform clock synchronization on all devices in the network that support clock. Therefore, devices can provide different applications based on some time. In addition, NTP can ensure very high accuracy (about 10ms). |

**O**

| | |
|---|---|
| Optical Distribution Frame (ODF) | A distribution connection device between the fiber and a communication device. It is an important part of the optical transmission system. It is mainly used for fiber splicing, optical connector installation, fiber adjustment, additional pigtail storage, and fiber protection. |
| Optical Distribution Network (ODN) | The optical transmission channel between the OLT and ONU. |
| Open System Interconnection (OSI) | OSI, defined by the International Standard Organization (ISO), is a conceptual model that characterizes and standardizes the internal functions of a communication system by partitioning it into seven abstraction layers. The seven layers are physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and application layer. |
| Open Shortest Path First (OSPF) | An internal gateway dynamic routing protocol, which is used to decide the route in an Autonomous System (AS). |
| OLT backbone fiber protection (Type B) | Backbone fiber and OLT PON interface redundancy protection. |
| Orthogonal Frequency Division Multiplexing (OFDM) | OFDM is one kind of multi-carrier modulation. The purpose of OFDM is to divide the channel into multiple orthogonal sub-channels and transfer high-speed data signals into concurrent low-speed data flow, and then transmit these signals through each sub-channel after modulation. |

**P**

| | |
|---|---|
| PON full-protection (Type C) | Perform dual redundancy protection on OLT dual PON interface, ONU dual optical module, backbone fiber, optical splitter, and wiring fiber. |
| PON full-protection (Type D) | Perform dual redundancy protection on OLT dual PON interface, ONU dual PON interface, backbone fiber, optical splitter, and wiring fiber. |
| Point-to-point Protocol over Ethernet (PPPoE) | With PPPoE, the remote device can control and account each access user. |
| Precision Time Protocol (PTP) | IEEE 1588 v2 protocol is also called PTP (Precision Time Protocol), a high-precision time protocol for synchronization used in measurement and control systems residing on a local area network. Accuracy in the sub-microsecond range may be achieved with low-cost implementations. |

**Q**

| | |
|---|---|
| QinQ | QinQ is (also called Stacked VLAN or Double VLAN) extended from 802.1Q, defined by IEEE 802.1ad recommendation. Basic QinQ is a simple Layer 2 VPN tunnel technology, encapsulating outer VLAN Tag for client private packets at carrier access end, the packets take double VLAN Tag passing through trunk network (public network). In public network, packets only transmit according to outer VLAN Tag, the private VLAN Tag are transmitted as data in packets. |
| Quality of Service (QoS) | A commonly-used performance indicator of a telecommunication system or channel. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio. It functions to measure the quality of the transmission system and the effectiveness of the services, as well as the capability of a service provider to meet the demands of users. |

**R**

| | |
|---|---|
| Rapid Spanning Tree Protocol (RSTP) | RSTP is an extension of Spanning Tree Protocol, which realizes quick convergency of network topology. |
| Remote Authentication Dial In User Service (RADIUS) | A protocol used to authenticate and account users in the network. |

**S**

| | |
|---|---|
| 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. |
| Simple Network Time Protocol (SNTP) | SNTP is mainly used for synchronizing time of devices in the 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 protection link. |

| | |
|---|---|
| SyncE | A technology adopts Ethernet link codes recover clock, similar to SDH clock synchronization quality, SyncE provides frequency synchronization of high precision. Unlike traditional Ethernet just synchronize data packets at receiving node, SyncE implements real-time synchronization system for inner clock. |

**T**

| | |
|---|---|
| Time Division Multiplexing (TDM) | TDM is a method to transmit multiple digital data, voice, and video signals on the same communication medium through different channels or cross pulse in timeslots. |
| Time Division Multiple Access (TDMA) | TDMA divides time into periodical frames and each frame are subdivided into multiple timeslots, each of which will send signals to the base station independently. On the condition of fixed time and synchronization, the base station can receive signals of each mobile terminal from each timeslot orderly. Meantime, signals sent by the base station to the mobile terminals are transmitted through the specified timeslots in sequence. Each mobile terminal can receive signals in the specified timeslot only, so signals will be received in order from the common channel. |
| TR069 | It is a CPE WAN management protocol defined by DSL forum. It provides the general frame and protocol for management and configuration of home network devices on the next-generation network through remotely and concentratedly managing the gateway, router, and STB on the home network. |

**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 segment logically rather than physically, thus implementing virtual work groups which are based on Layer 2 isolation and do not affect each other. |
| Virtual Private Network (VPN) | It uses the Internet to establish a special data transmission channel to achieve secure, reliable, and remote data transmission. |
| Voice over Internet Protocol (VoIP) | VoIP can transfer analog voice signals into digital signals and transmit them through the IP network in packets. The biggest advantage of VoIP is that it can transmit voice, video, and data services at lower costs through the IP network. |

# 13.2 Acronyms and abbreviations

**3**

| | |
|---|---|
| 3G | 3rd-Generation |

| | |
|---|---|
| 3GPP | The 3rd Generation Partnership Project |
| 3GPP2 | 3rd Generation Partnership Project 2 |

**A**

| | |
|---|---|
| ACL | Access Control List |
| AES | Advanced Encryption Standard |
| APS | Automatic Protection Switching |
| ARP | Address Resolution Protocol |
| AS | Autonomous System |

**B**

| | |
|---|---|
| BGP | Border Gateway Protocol |
| BPDU | Bridge Protocol Data Unit |

**C**

| | |
|---|---|
| CATV | Community Antenna Television |
| CBAT | Coax Broadcast Access Terminal |
| CC | Continuity Check |
| CCM | Continuity Check Message |
| CCS | Common Channel Signalling |
| CDMA2000 | Code Division Multiple Access 2000 |
| CDR | Calling Detail Records |
| CFM | Connectivity Fault Management |
| CE | Customer Edge |
| CESoPSN | Structure-Aware TDM Circuit Emulation Service over Packet Switched Network |
| CFI | Canonical Format Indicator |
| CIDR | Classless Inter-Domain Routing |
| CIR | Committed Information Rate |
| CIST | Common Internal Spanning Tree |
| CLI | Command Line Interface |
| CMCI | CNU Management Control Interface |
| CNU | Coax Network Unit |

| | |
|---|---|
| CoS | Class of Service |
| CO | Central Office |
| CPE | Customer Premises Equipment |
| CSMA | Carrier Sense Multiple Access |
| CST | Common Spanning Tree |
| CWDM | Coarse Wavelength Division Multiplexing |

**D**

| | |
|---|---|
| DAI | Dynamic ARP Inspection |
| DBA | Dynamic Bandwidth Allocation |
| DCN | Data Communication Network |
| DHCP | Dynamic Host Configuration Protocol |
| DoS | Deny of Service |
| DRR | Deficit Round Robin |
| DSCP | Differentiated Services Code Point |
| DWDM | Dense Wavelength Division Multiplexing |

**E**

| | |
|---|---|
| EFM | Ethernet in the First Mile |
| ELPS | Ethernet Linear Protection Switching |
| EoC | Ethernet over Coaxial |
| EPON | Ethernet Passive Optical Network |
| ERPS | Ethernet Ring Protection Switching |
| ESD | Electro Static Discharge |
| EVC | Ethernet Virtual Connection |

**F**

| | |
|---|---|
| FDM | Frequency-division multiplexing |
| FDQAM | Frequency Diverse Quadrature Amplitude Modulation |
| FEC | Forward Error Correction |
| FIB | Forwarding Information Base |
| FIR | Fixed Information Rate |
| FTTB | Fiber to the Building |

| | |
|---|---|
| FTTC | Fiber to the Curb |
| FTTH | Fiber to the Home |
| FTP | File Transfer Protocol |
| FR | Frame Relay |

**G**

| | |
|---|---|
| GARP | Generic Attribute Registration Protocol |
| GE | Gigabit Ethernet |
| GPS | Global Positioning System |
| GPON | Gigabit-Capable PON |
| GUI | Graphic User Interface |
| GSM | Global System for Mobile Communications |
| GVRP | GARP VLAN Registration Protocol |

**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 | Internet Group Management Protocol |
| IGMP Snooping | Internet Group Management Protocol Snooping |
| IP | Internet Protocol |
| IPDV | IP Packet Delay Variation |
| IST | Internal Spanning Tree |
| ITU-T | International Telecommunications Union-Telecommunication Standardization Sector |
| IWF | Inter-working Function |

**L**

| | |
|---|---|
| LACP | Link Aggregation Control Protocol |

| | |
|---|---|
| LACPDU | Link Aggregation Control Protocol Data Unit |
| LBM | LoopBack Message |
| LBR | LoopBack Reply |
| LLID | Logical Link Identifier |
| LLDP | Link Layer Discovery Protocol |
| LLDPDU | Link Layer Discovery Protocol Data Unit |
| LSA | Link-State Advertisement |
| LTM | LinkTrace Message |
| LTR | LinkTrace Reply |

**M**

| | |
|---|---|
| MA | Maintenance Association |
| MAC | Medium Access Control |
| MD | Maintenance Domain |
| MEG | Maintenance Entity Group |
| MEP | Maintenance associations End Point |
| MGCP | Media Gateway Control Protocol |
| MIB | Management Information Base |
| MIP | Maintenance association Intermediate Point |
| MoCA | Multimedia over Coax Alliance |
| MP | Maintenance Point |
| MSTI | Multiple Spanning Tree Instance |
| MSTP | Multiple Spanning Tree Protocol |
| MTU | Maximum Transferred Unit |
| MVR | Multicast VLAN Registration |
| MPCP | Multi-Point Control Protocol |

**N**

| | |
|---|---|
| NAT | Network Address Translation |
| NMS | Network Management System |
| NNI | Network Node Interface |
| NView NNM | NView Network Node Management |
| NTP | Network Time Protocol |

**O**

| | |
|---|---|
| OAM | Operation, Administration and Management |
| ODF | Optical Distribution Frame |
| ODN | Optical Distribution Network |
| OFDM | Orthogonal Frequency Division Multiplexing |
| OLT | Optical Line Terminal |
| ONU | Optical Network Unit |
| OSI | Open System Interconnect |
| OSPF | Open Shortest Path First |

**P**

| | |
|---|---|
| P2P | Peer-to-Peer |
| P2MP | Point to Multipoint |
| PC | Personal Computer |
| PE | Provider Edge |
| PIB | Parameter Information Block |
| PIR | Peak Information Rate |
| PMD | Physical Medium Dependent |
| PoE | Power Over Ethernet |
| PPP | Point to Point Protocol |
| PPPoE | Point-to-Point Protocol over Ethernet |
| PTP | Precision Time Protocol |

**Q**

| | |
|---|---|
| QoS | Quality of Service |

**R**

| | |
|---|---|
| RADIUS | Remote Authentication Dial In User Service |
| RED | Random Early Detection |
| RF | Radio Frequency |
| RIP | Routing Information Protocol |
| RMON | Remote Network Monitoring |
| RMEP | Remote Maintenance association End Point |

| | |
|---|---|
| RNC | Radio Network Controller |
| RSTP | Rapid Spanning Tree Protocol |

**S**

| | |
|---|---|
| SAToP | Structure-Agnostic Time Division Multiplexing (TDM) over Packet |
| 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 |
| SST | Single Spanning Tree |
| STP | Spanning Tree Protocol |

**T**

| | |
|---|---|
| TACACS+ | Terminal Access Controller Access Control System |
| TC | Transparent Clock |
| TCI | Tag Control Information |
| TCP | Transmission Control Protocol |
| TD-SCDMA | Time Division-Synchronous Code Division Multiple Access |
| TDM | Time Division Multiplex |
| TDMA | Time Division Multiple Address |
| TDMoIP | Time Division Multiplexing over IP |
| TFTP | Trivial File Transfer Protocol |
| TLV | Type Length Value |
| ToS | Type of Service |
| TPID | Tag Protocol Identifier |

**U**

| | |
|---|---|
| URI | Uniform Resource Identifier |

**V**

| | |
|---|---|
| VLAN | Virtual Local Area Network |
| VID | VLAN Identifiter |
| VoIP | Voice over Internet Protocol |

**W**

| | |
|---|---|
| WCDMA | Wideband Code Division Multiple Access |
| WDM | Wavelength Division Multiplexing |
| WiFi | Wireless Fidelity |
| WRED | Weighted Random Early Detection |
| 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