RAISECOM

www.raisecom.com

RAX721-A (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: 8610-82883305

Fax: 8610-82883056

Email: export@raisecom.com

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

Postal code: 100094

Notice

Preface

Objectives

This document introduces features and related configurations supported by the RAX721-A, including basic principles and configuration procedures of IP routing, clock synchronization, Ethernet, multicast, QoS, OAM, security, and system configurations. In addition, this document provides related configuration examples. The appendix provides terms, acronyms, and abbreviations involved in this guide.

This document helps you master principles and configurations of the RAX721-A systematically, as well as networking with the RAX721-A.

Versions

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

Product name	Product version	Hardware version
RAX721-A	P100R001	A.00 or later

Conventions

Symbol conventions

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

Symbol	Description
	Indicate a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.
	Indicate a potentially hazardous situation that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.
	Provide additional information to emphasize or supplement important points of the main text.

Symbol	Description
	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`.
Book Antiqua	Heading 1, Heading 2, Heading 3, and Block are in Book Antiqua.

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.

Configuration mode prompt conventions

Convention	Description
/*	Indicate the interface ID/slot ID. For example, "Raisecom(config-eth/1)" indicates Ethernet interface 1 and "Raisecom(config-slot/4)" indicates slot 4.
/*/*	The first "/*" indicates the slot ID and the second "/*" indicates the interface ID. For example, "Raisecom(config-eth/1/1)" indicates Ethernet interface 1 of slot 1.

Interface type and value range conventions

Convention	Description
interface-type	Interface type: • vlan: VLAN interface • loopback: Loopback interface • tunnel: Tunnel interface • tengigabitethernet or gigaethernet: Layer 2 physical interface/Layer 3 physical interface/sub-interface • fastethernet: out-of-band network management interface • port-channel: Trunk interface/sub-interface
interface-number	Interface ID based on the device model and interface type: • vlan: 1–4094 • loopback: 1–32 • tunnel: 1/1/1–1/1/40000 • tengigabitethernet or gigaethernet *unit/slot/port*: 1/1/1–1/1/4 or 1/2/1–1/2/24 (Layer 2/Layer 3 physical interface) • tengigabitethernet or gigaethernet *unit/slot/port.sub-interface*: 1/1/1.1–1/1/1.4094 or 1/1/2.1–1/1/2.4094 and so on (sub-interface) • fastethernet: 1/0/1 • port-channel: 1–16

Interface configuration mode conventions

In screen outputs described in this document, we use `Raisecom(config-port)` to indicate that we have entered interface configuration mode.

However, based on the interface type, the actual screen outputs are in the form of `Raisecom(config-`*interface-type interface-number*`)`. The *interface-type* and *interface-number* parameters indicate the interface type and interface ID. For details about interface types and interface IDs, see interface type and value range conventions.

Actual screen outputs are shown as below.

Screen outputs in configuration modes of interfaces	Description
`Raisecom(config-fastethernet`*unit/slot/port*`)#`	Entered out-of-band interface configuration mode. The interface ID is *unit/slot/port*, such as Raisecom(config-fastethernet1/0/1)#.
`Raisecom(config-gigaethernet`*unit/slot/port*`)#`	Entered Gigabit Ethernet interface configuration mode. The interface ID is *unit/slot/port*, such as Raisecom(config-gigaethernet1/2/1)#.
`Raisecom(config-gigaethernet`*unit/slot/port.sub*`)#`	Entered Gigabit Ethernet sub-interface configuration mode. The interface ID is *unit/slot/port.sub*, such as Raisecom(config-gigaethernet1/2/1.1)#.
`Raisecom(config-tengigabitethernet`*unit/slot/port*`)#`	Entered 10 Gbit/s Ethernet interface configuration mode. The interface ID is *unit/slot/port*, such as Raisecom(config-gigaethernet1/2/1)#.
`Raisecom(config-tengigabitethernet`*unit/slot/port.sub*`)#`	Entered 10 Gbit/s Ethernet sub-interface configuration mode. The interface ID is *unit/slot/port.sub*, such as Raisecom(config-gigaethernet1/2/1.1)#.
`Raisecom(config-vlan`*port*`)#`	Entered VLAN interface configuration mode. The interface ID is an integer, such as Raisecom(config-vlan1)#.
`Raisecom(config-port-channel`*port*`)#`	Entered Trunk interface configuration mode. The interface ID is an integer, such as Raisecom(config-port-channel1)#.
`Raisecom(config-port-channel`*port.sub*`)#`	Entered Trunk sub-interface configuration mode. The interface ID is *port.sub*, such as Raisecom(config-port-channel1.1)#.
`Raisecom(config-tunnel`*unit/slot/port*`)#`	Entered Tunnel interface configuration mode. The interface ID is *unit/slot/port*, such as Raisecom(config-tunnel1/1/1)#.
`Raisecom(config-loopback`*port*`)#`	Entered Loopback interface configuration mode. The interface ID is an integer, such as Raisecom(config-loopback1)#.

Change history

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

Issue 02 (2021-12-31)

Second commercial release

Issue 01 (2020-06-12)

Initial commercial release

Contents

Figures

1 Basic configurations

This chapter describes basic information and configuration procedures of the RAX721-A, as well as related configuration examples, including following sections:

- CLI
- Connecting device and log
- Backup and upgrade
- Device management
- Configuring RMON

1.1 CLI

1.1.1 Overview

The Command Line Interface (CLI) is a medium for you to communicate with the RAX721-A. You can configure, monitor, and manage the RAX721-A through the CLI.

You can log in to the RAX721-A through the terminal equipment or through a computer that runs the terminal emulation program. Enter commands at the system prompt.

The CLI supports the following features:

- Configure the RAX721-A locally through the Console interface.
- Configure the RAX721-A locally or remotely through Telnet/Secure Shell v2 (SSHv2).
- Commands are classified into different levels. You can execute the commands that correspond to your level only.
- The commands available to you depend on which mode you are currently in.
- Shortcut keys can be used to execute commands.
- Check or execute a historical command by checking command history. The last 20 historical commands can be saved on the RAX721-A.
- Enter a question mark (?) at the system prompt to obtain online help.
- The RAX721-A supports multiple intelligent analysis methods, such as fuzzy match and context association.

1.1.2 Levels

The RAX721-A classifies commands into 16 levels in a descending order:

- 0–4: checking level. You can execute basic commands, such as clear and history, for clearing system information and showing command history.
- 5–10: monitoring level. You can execute commands, such as show, for system maintenance.
- 11–14: configuration level. You can execute commands for configuring services, such as Virtual Local Area Network (VLAN) and Internet Protocol (IP) routing.
- 15: management level. You can execute commands for system running.

1.1.3 Modes

Entering user EXEC mode through user name

The command mode is an environment where a command is executed. A command can be executed in one or multiple certain modes. The commands available to you depend on which mode you are currently in.

After connecting the RAX721-A, if the RAX721-A adopts default configurations, a Login prompt will be displayed. Enter the default user name (raisecom) and password (raisecom) to enter the user EXEC mode, where the following command is displayed:

```
Raisecom>
```

Entering privileged EXEC mode through Enable command

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

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

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

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

Note

- The CLI prompt Raisecom is a default host name. You can modify it by executing the hostname *string* command in privileged EXEC mode.

- Commands executed in global configuration mode can also be executed in other modes. The functions vary on command modes.
- You can enter the exit or quit command to return to the upper command mode. However, in privileged EXEC mode, you need to execute the disable command to return to user EXEC mode. In address family configuration mode, you need to execute the exit-address-family command to return to BGP configuration mode.
- You can enter the end command to return to privileged EXEC mode from any modes but user EXEC mode and privileged EXEC mode.

Command modes supported by the RAX721-A are listed in the following table.

Mode	Entry	Prompt
User EXEC	Log in to the RAX721-A, and then enter the correct user name and password.	`Raisecom>`
Privileged EXEC	In user EXEC mode, use the **enable** command and correct password.	`Raisecom#`
Global configuration	In privileged EXEC mode, use the **config** command.	`Raisecom(config)#`
Interface configuration	In global configuration mode, use the **interface fastethernet** 1/0/1 command.	`Raisecom(config-fastethernet1/0/1)#`
	In global configuration mode, use the **interface gigaethernet** *unit/slot/port* command.	`Raisecom(config-gigaethernetunit/slot/port)#`
	In global configuration mode, use the **interface tengigabitethernet** *unit/slot/port* command.	`Raisecom(config-tengigaethernetunit/slot/port)#`
Sub-interface configuration	In global configuration mode, use the **interface gigaethernet** *unit/slot/port.sub-interface* command.	`Raisecom(config-gigaethernetsubif)#`
VLAN interface configuration	In global configuration mode, use the **interface vlan** *vlan-id* command.	`Raisecom(config-vlanif)#`
Tunnel interface configuration	In global configuration mode, use the **interface tunnel** *tunnel-id* command.	`Raisecom(config-tunnel)#`
Loopback interface configuration	In global configuration mode, use the **interface loopback** *interface-number* command.	`Raisecom(config-loopback)#`
VRF configuration	In global configuration mode, use the **ip vrf** *vrf-name* command.	`Raisecom(config-vrf)#`
Route mapping configuration	In global configuration mode, use the **route-map** *map-name* { **permit** | **deny** } *number* command.	`Raisecom(config-route-map)#`
OSPF configuration	In global configuration mode, use the **router ospf** *process-id* [**router-id** *router-id*] command.	`Raisecom(config-router-ospf)#`

Mode	Entry	Prompt
OSPFv3 configuration	In global configuration mode, use the **ipv6 router ospf** *process-id* [**vrf** *vrf-name*] command.	`Raisecom(config-ospf6)#`
BGP configuration	In global configuration mode, use the **router bgp** [*as-id*] command.	`Raisecom(config-router)#`
BGP VPNv4 address family configuration	In BGP configuration mode, use the **address-family vpnv4** [**unicast**] command.	`Raisecom(config-router-af)#`
BGP VPN instance IPv4 unicast address family configuration	In BGP configuration mode, use the **address-family ipv4 vrf** *vrf-name* command.	`Raisecom(config-router-af)#`
VLAN configuration	In global configuration mode, use the **vlan** *vlan-id* command.	`Raisecom(config-vlan)#`
Basic IP ACL configuration	In global configuration mode, use the **access-list** *acl-number* command. The *acl-number* parameter ranges from 1000 to 1999.	`Raisecom(config-acl-ipv4-basic)#`
Extended IP ACL configuration	In global configuration mode, use the **access-list** *acl-number* command. The *acl-number* parameter ranges from 2000 to 2999.	`Raisecom(config-acl-ipv4-advanced)#`
MAC ACL configuration	In global configuration mode, use the **access-list** *acl-number* command. The *acl-number* parameter ranges from 3000 to 3999.	`Raisecom(config-acl-mac)#`
User ACL configuration	In global configuration mode, use the **access-list** *acl-number* command. The *acl-number* parameter ranges from 5000 to 5999.	`Raisecom(config-acl-map)#`
cos-remark configuration	In global configuration mode, use the **mls qos mapping cos-remark** *profile-id* command.	`Raisecom(cos-remark)#`
cos-to-pri configuration	In global configuration mode, use the **mls qos mapping cos-to-local-priority** *profile-id* command.	`Raisecom(cos-to-pri)#`
dscp-mutation configuration	In global configuration mode, use the **mls qos mapping dscp-mutation** *profile-id* command.	`Raisecom(dscp-mutation)#`
dscp-to-pri configuration	In global configuration mode, use the **mls qos mapping dscp-to-local-priority** *profile-id* command.	`Raisecom(dscp-to-pri)#`

Mode	Entry	Prompt
exp-to-pri configuration	In global configuration mode, use the **mls qos mapping exp-to-local-priority** *profile-id* command.	`Raisecom(exp-to-pri)#`
pri-to-exp configuration	In global configuration mode, use the **mls qos mapping local-priority-to-exp** *profile-id* command.	`Raisecom(pri-to-exp)#`
WRED profile configuration	In global configuration mode, use the **mls qos wred profile** *profile-id* command.	`Raisecom(wred)#`
Flow profile configuration	In global configuration mode, use the **mls qos flow-queue profile** command.	`Raisecom(flow-queue)#`
CMAP configuration	In global configuration mode, use the **class-map** *class-map-name* command.	`Raisecom(config-cmap)#`
Traffic monitoring profile configuration	In global configuration mode, use the **mls qos policer-profile** *policer-name* [**single**] command.	`Raisecom(traffic-policer)#`
PMAP configuration	In global configuration mode, use the **policy-map** *policy-map-name* command.	`Raisecom(config-pmap)#`
Traffic policy bound with traffic classification configuration	In PMAP configuration mode, use the **class-map** *class-map-name* command.	`Raisecom(config-pmap-c)#`
Service instance configuration	In global configuration mode, use the **service** *instance-name* **level** *md-level* command.	`Raisecom(config-service)#`
BFD session configuration	In global configuration mode, use the **bfd** *session-id* command.	`Raisecom(config-bfd-session)#`
	In global configuration mode, use the **bfd** *session-id* **bind peer-ip** *ip-address* [**vrf-name** *vrf-name*] command.	
	In global configuration mode, use the **bfd** *session-id* **bind peer-ip** *ip-address* **interface gigaethernet** *interface-number* command.	
	In global configuration mode, use the **bfd** *session-id* **bind ldp-lsp peer-ip** *ip-address ip-mask* command.	
	In global configuration mode, use the **bfd** *session-id* **bind mpls interface tunnel** *tunnel-if* **cr-lsp** command.	

Mode	Entry	Prompt
	In global configuration mode, use the **bfd** *session-id* **bind pw** *vc-id peer-ip* [**pw-ttl** *ttl*] command.	

1.1.4 Shortcut keys

The RAX721-A supports the following shortcut keys.

Shortcut key	Description
Up arrow (↑)	The previous command is displayed. If no previous command is available, no change is shown on the screen after you press the key.
Down arrow (↓)	The next command is displayed. If no previous command is available, no change is shown on the screen after you press the key.
Left arrow (←)	Move the cursor back one character. If the cursor is in front of the command, no change is shown on the screen after you press the key.
Right arrow (→)	Move the cursor forward one character. If the cursor is behind the command, no change is shown on the screen after you press the key.
Backspace	Erase the character to the left of the cursor. If the cursor is in front of the command, no change is shown on the screen after you press the key.
Tab	When you press it after entering an incomplete keyword, the system automatically executes some commands: • If the incomplete keyword matches a unique complete keyword, the unique complete keyword replaces the incomplete keyword, with the cursor forward a space from the unique complete keyword. • If the incomplete keyword matches more complete keywords, you can press the **Tab** key to alternate the matched complete keywords. • If the incomplete keyword matches no complete key word, you can press the **Tab** key to wrap, and then error information is displayed.
Ctrl+**A**.	Move the cursor to the beginning of the command line.
Ctrl+D or the **Delete**	Delete the character at the cursor.
Ctrl+**E**	Move the cursor to the end of the command line.
Ctrl+**K**	Delete all characters from the cursor to the end of the command line.

Shortcut key	Description
Ctrl+**X**	Delete all characters from the cursor to the beginning of the command line.
Ctrl+**Z**	Return to privileged EXEC mode from the current mode (excluding user EXEC mode).

1.1.5 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 available for each command mode.

```
Raisecom>?
```

The output is displayed 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
  show     Show running system information
  terminal Configure terminal
```

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

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

The output is displayed as below:

```
access-list      Access list
acl              Access control list
alarm            Alarm
arp              ARP table information
banner           banner
bfd              Bidirectional Forwarding Detection
```

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

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

The output is displayed as below:

```
<1-1024>  Tunnel interface number
```

Incomplete help

You can acquire incomplete help under following three conditions:

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

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

The output is displayed as below:

```
cfm         Connectivity fault management protocol
class-map    Set class map
clear       Clear screen
command-log  Log the command to the file
cpu         Configure cpu parameters
create       Create static VLAN
cspf        Cspf capability
```

- After you enter a command, press the 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(config)#show li?
```

The output is displayed as below:

```
license         license
link-aggregation  Link aggregation
```

- After you enter a partial command name and press the Tab, the full form of the keyword is displayed if there is a unique match command. Otherwise, after you press the Tab, different keywords will be displayed circularly and you can select one as required.

Error messages

The following table lists error messages that you may encounter while configure the RAX721-A on the CLI.

Error message	Description
% Incomplete command.	The input command is incomplete.
Error input in the position market by '^'	The keyword marked with "^" is invalid or does not exist.

1.2 Connecting device and logging in

1.2.1 Connecting device

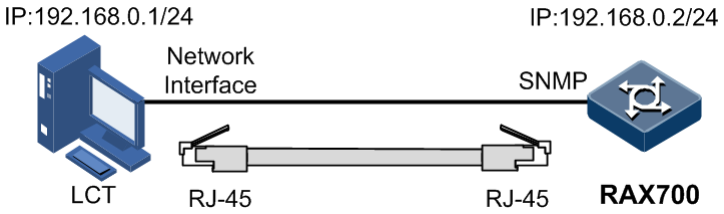
Users can log in to the device for configuration management through direct connection and network connection.

Direct connection

- Direction connection through a network cable

As shown in Figure 1-1, directly connect the SNMP interface on the device to the network interface on the computer with a network cable, configure the device IP address and the computer IP address on the same network segment, and then start the terminal maintenance software on the computer to log in to the device for configuration management.

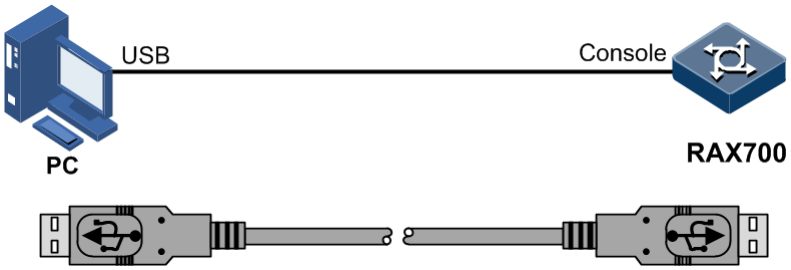
Figure 1-1 Direct connection



- Direct connection through a USB cable

As shown in Figure 1-2, use a USB cable to directly connect the Console interface on the device to the USB interface on the computer, start the terminal maintenance software on the computer, configure the serial port parameters, and log in to the device for configuration management. There is no need for configuring an IP address for this scenario.

Figure 1-2 USB connection

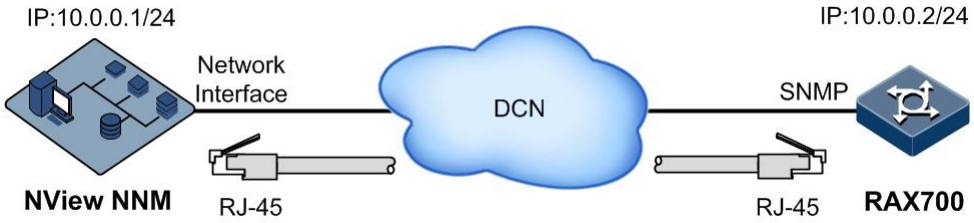


Network connection

The device supports out-of-band network management.

As shown in Figure 1-3, the device is connected to the DCN through the SNMP interface NEG, and the computer accesses the device management IP address through the DCN to configure and manage the device. Keep the route between the computer and the device available (the computer and device should be able to ping through each other) and then start the terminal maintenance software on the computer to log in to the device.

Figure 1-3 Out-of-band network management



1.2.2 Accessing device through Console interface

Note

The Console interface of the RAX721-A is a Universal Serial Bus (USB) A-shaped female interface, which is translated into a Universal Asynchronous Receiver/Transmitter (UART) in the device.

The Console interface is an interface for directly configuring and managing the device, which is connected to the USB interface on the PC that runs the maintenance terminal software through a USB cable. You can configure and manage the RAX721-A through this interface. This management method does not involve network communication.

You must log in to the RAX721-A through the Console interface under the following 2 conditions:

- The RAX721-A is powered on for the first time.
- You cannot log in to the RAX721-A through Telnet.

To log in to the RAX721-A through the Console interface, follow these steps:

Note

Before logging in to the RAX721-A through the USB interface, install the driver for translating the USB interface into the UART interface to the PC.

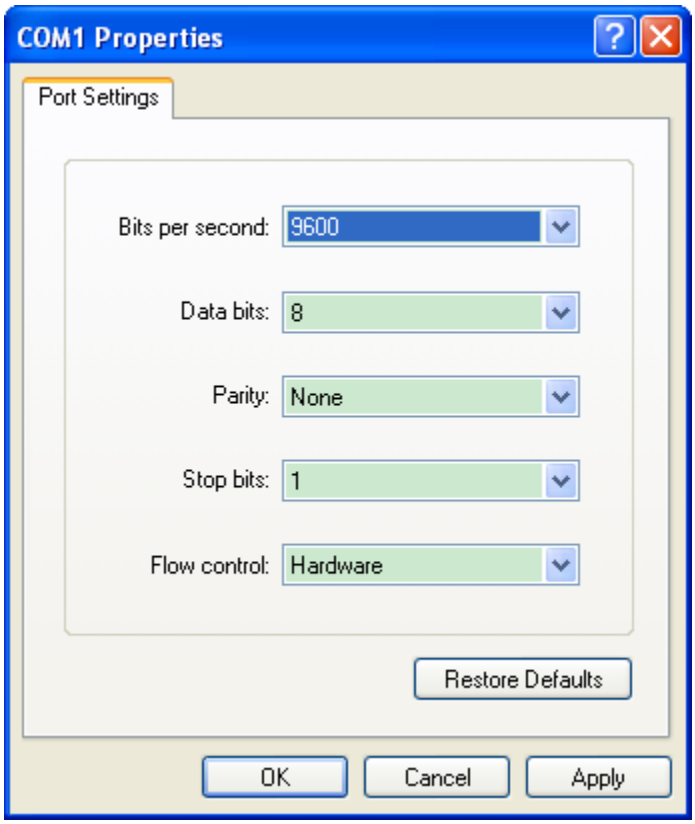
Step 1 Use an USB configuration cable to connect the Console interface of the RAX721-A with the USB interface of the PC.

Step 2 Run the terminal maintenance program on the PC, such as Hyper Terminal on Microsoft Windows XP. Enter the connection name at the Connection Description dialog box and then click **OK**.

Step 3 Select COM N (N refers to the COM interface ID into which the USB interface is translated.) at the Connect To dialog box and then click **OK**.

Step 4 Configure parameters as shown in Figure 1-4 and then click **OK**

Figure 1-4 Configuring parameters for Hyper Terminal



Step 5 Enter the configuration interface and then enter the user name and password to log in to the RAX721-A. By default, both the user name and password are set to raisecom.

Note

Hyper Terminal is not available on Windows Vista or Windows 7 Operating System (OS). For these OSs, download Hyper Terminal package and install it.

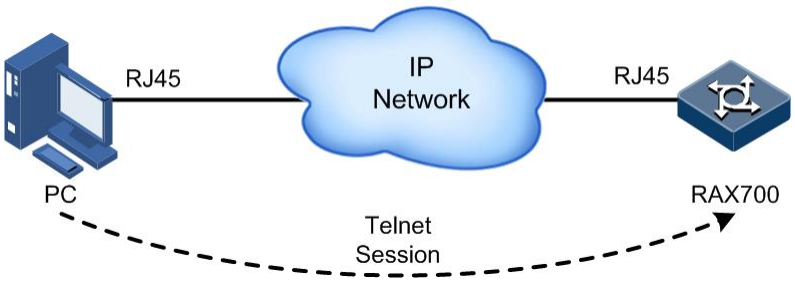
1.2.3 Accessing device through Telnet

Through Telnet, you can remotely log in to the RAX721-A through a PC and then log into other devices on the network through Telnet. In this way, it is not necessary to prepare a PC for each RAX721-A.

The RAX721-A provides the following Telnet services:

- Telnet Server: as shown in Figure 1-5, connect the PC and the RAX700 and start the terminal maintenance software on the PC. After selecting proper parameters, you can log in to the RAX700 for configuration and management.

Figure 1-5 Working as the Telnet server



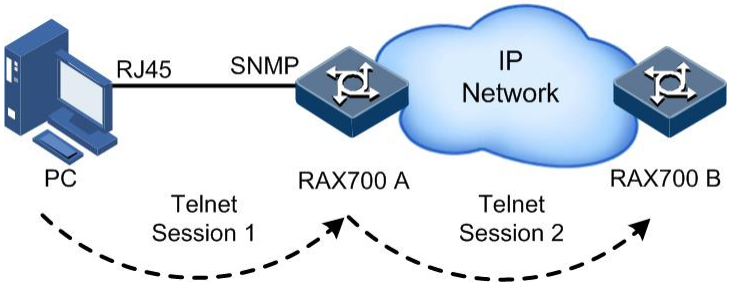
Note

For logging in to the RAX721-A through Telnet for the first time, you must log in to the RAX721-A through the Console interface and configure the IP address of the SNMP interface.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface fastethernet 1/0/1`	Enter SNMP interface configuration mode.
3	`Raisecom(config-fastethernet1/0/1)#ip address` *ip-address* `[` *ip-mask* `]` `Raisecom(config-fastethernet1/0/1)#exit`	Configure the IP address of the SNMP interface and return to global configuration mode. By default, it is 192.168.4.28.
4	`Raisecom(config)#telnet-server accept` *interface-type interface-list*	(Optional) configure the interface that supports Telnet.
5	`Raisecom(config)#telnet-server close terminal-telnet` *session-number*	(Optional) close the specified Telnet session.
6	`Raisecom(config)#telnet-server max-session` *session-number*	(Optional) configure the maximum number of Telnet sessions supported by the RAX721-A. By default, it is 10.
7	`Raisecom(config)#telnet-server access-list` *acl-number*	Configure Telnet server based on ACL.

- Telnet Client: after connecting the RAX721-A through the terminal emulation program running on the PC, you can log in to another device by entering the telnet command and then configure and manage the device. As shown in Figure 1-6, RAX700 A works as Telnet Server and Telnet Client.

Figure 1-6 Working as the Telnet client



Step	Command	Description
1	Raisecom#**telnet** *ip-address* [**port** port-id] [**source-ip** *ip-address*] [**vrf** *vrf-name*]	Log in to another device through Telnet.

1.2.4 Accessing device through SSHv2

Telnet is an authentication mode that is lack of security. In addition, it adopts Transmission Control Protocol (TCP) to transmit the password and data in clear text. It will cause malicious attack, such as Deny of Service (DoS), IP address spoofing, and route spoofing because only Telnet service is provided. With more attention is put on network security, the traditional modes (Telnet and FTP) for transmitting the password and data in clear text are not accepted gradually.

Secure Shell (SSH) is a protocol, which is used to provide secure remote login and other security network services in an insecure network. When you log in to a device in an insecure network environment, SSH will encrypt the data automatically when you transmit these data. When data is transmitted to the destination, the SSH will decrypt the data automatically. Therefore, SSH can provide secure information assurance. SSH can prevent devices from being attacked by clear text password intercepting and middleman, as well as prevent Domain Name Server (DNS) spoofing and IP spoofing. Because the transmitted data is compressed, the SSH can provide the greater transmission speed.

SSH adopts the client-server mode. The SSH server receives requests from SSH clients and then begin to authenticate them. After successful authentication, SSH connection is established. Therefore, you can log in to the SSH server through the SSH client. The authentication is a series of key processing actions performed between the server and client.

At present, SSH has a new version of SSHv2. The RAX721-A supports SSHv2.

Before accessing the RAX721-A through SSHv2, you must log in to the RAX721-A through the Console interface and enable SSH service.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**generate ssh-key** *length*	Generate local SSHv2 key pair and designate its length.
3	Raisecom(config)#**ssh2 server**	Start the SSHv2 server.
4	Raisecom(config)#**ssh2 server authentication** { **password** | **rsa-key** }	(Optional) configure SSHv2 authentication method.

Step	Command	Description
5	Raisecom(config)#**ssh2 server authentication-timeout** *period*	(Optional) configure SSHv2 authentication timeout. The RAX721-A refuses to authenticate and open the connection when client authentication time exceeds the upper threshold.
6	Raisecom(config)#**ssh2 server authentication-retries** *times*	(Optional) configure the allowable times for SSHv2 authentication failure. The RAX721-A refuses to authenticate and open the connection when client authentication failure times exceed the upper threshold.
7	Raisecom(config)#**ssh2 server port** *port-id*	(Optional) configure the SSHv2 listening port ID. **Note** When configuring the SSHv2 listening port ID, the input parameter cannot take effect immediately without rebooting the SSHv2 service.
8	Raisecom(config)#**show ssh2** { **server** | **session** }	(Optional) show information about the SSHv2 server or the session end.
9	Raisecom(config)#**show ssh2 public-key** [**authentication**]	(Optional) show the public key for SSHv2 authentication on the device and the client.

1.3 Backup and upgrade

1.3.1 Introduction

The RAX721-A uses the file system to manage system files. The file system is used to create, delete, and modify files and directories.

System files refer to files required for operating the RAX721-A, including the BootROM file, License file, Paf file, patch file, log file, configuration file, and system software. Based on the download location, these files are saved to the memory of the NXU card or service card.

System file

System files refer to the software and files required for operating the RAX721-A, including the BootROM file, system configuration file, system startup file and FPGA file. These files are saved to the memory of the RAX721-A.

File management includes backup, update, load and deletion of files.

The system supports dual-system software, offering primary and backup systems.

System Bootrom file

The system Bootrom file (BootROM software) is used to boot the device. After the device is powered on, the BootROM software is running to initialize the RAX721-A. You can upgrade the BootROM software if a new version is available.

System startup file

The system startup file (with the .z suffix) is used to start and operate the RAX721-A, support normal operating, and implement functions.

You can upgrade the system startup file if a new version is available. In addition, to prevent a system fault, you can back up the system startup file.

The RAX721-A supports 2 sets of system startup software simultaneously, providing primary and secondary switching between dual systems.

PAF file

PAF is used to control functions and specifications of the device. The PAF file defines all specification parameters supported by the device, such as, local and remote zero-configuration mode. It is able to confirm specifications supported by the device according to the parameter range. The following examples show several important parameter ranges:

- ZERO_CONFIG_MODE_CLIENT: the value 0 indicates disabling remote zero-configuration while the value 1 indicates enabling remote zero-configuration.
- ZERO_CONFIG_MODE_CLIENT: if ZERO_CONFIG_MODE_CLIENT=1, the value 0 indicates disabling China Telecom zero-configuration while the value 1 indicates enabling China Telecom zero-configuration. The zero-configuration scheme for China Telecom is to request the IP address on the first uplink interface.
- ZERO_CONFIG_MANAGE_VLAN: the value 0 indicates that the VLAN management is not configured. All VLANs are covered when the IP address is automatically obtained.

After configuring parameters is complete, you could download parameters to the device through the **download** command and reboot the RAX721-A through the **reboot** command. Then the RAX721-A will take effect.

Other functions of the PAF file are as below:

- Support customizing the default IP address of the NMS interface.
- Support the naming convention of the product version, such as "product version.paf" for the PAF file.

System configuration file

The system configuration file (with the .conf suffix) is configuration items to be loaded when the device is booted at this time or next time.

After being powered on, the RAX721-A reads the configuration file from the memory for initialization. If there is no configuration file in the memory, the RAX721-A will use the default configuration file.

Configuration parameters in the configuration file are divided into the following 2 types:

- Configuration parameters used for initialization are startup configurations.
- Configuration parameters used when a device is running properly are running configurations.

You can modify running configurations through CLI. To make these modified running configurations as startup configurations when the RAX721-A is powered on next time, you should save running configurations to the memory (by using the **write** command) as a configuration file.

Operations on the system configuration file include loading, upgrading, backing up, and deleting the system configuration file.

Backup

Backup means saving system files by copying them from the device memory and save them into the server memory to recover files if the RAX721-A fails. By doing so, the RAX721-A will run normally as before. The pervious system file should be restored under the following conditions:

- System files are lost or damaged due to the device fault.
- The device fails due to failure in system upgrade.

The RAX721-A supports backing up system configuration files, system startup files, and system log files.

Upgrade

After features are added or known bugs are fixed, a new software version will be released. Then you can upgrade the software.

The RAX721-A supports 2 upgrade modes:

- FTP upgrade in BootROM mode
- FTP/TFTP upgrade in system configuration mode

1.3.2 Backing up system

You need to establish a FTP/TFTP environment before backing up system files. Generally, you can use a PC to serve as the FTP/TFTP server and the RAX721-A as the client, with the basic requirements as below:

- Connect the RAX721-A to the PC through the SNMP interface.
- Configure the IP address of the PC to interconnect with the RAX721-A.

IPv4-based network

Step	Command	Description
1	Raisecom#**upload** { **running-config** | **startup-config** | **backup-config** } { **ftp** *ip-address username password* | **ftp-active** *ip-address username password* | **tftp** *ip-address* } [**source** *source-address*] *filename*	Upload the system bootstrap files and system configuration files to the backup server.
2	Raisecom#**upload** { **accident-logfile** | **command-logfile** | **alarm-logfile** | **running-logfile** | **all-logfile** } { **ftp** *ip-address username password* | **ftp-active** *ip-address username password* | **tftp** *ip-address* } [**source** *source-address*] *filename*	Back up the log file to the server.

IPv6-based network

Step	Command	Description
1	Raisecom#**upload** { **running-config** | **startup-config** | **backup-config** } { **ftp** *ipv6-address username password* | **ftp-active** *ipv6-address username password* | **tftp** *ipv6-address* } [**source** *source-address*] *filename*	Upload the system bootstrap file and system configuration file to the backup server.
2	Raisecom#**upload** { **accident-logfile** | **command-logfile** | **alarm-logfile** | **running-logfile** | **all-logfile** } { **ftp** *ipv6-address username password* | **ftp-active** *ipv6-address username password* | **tftp** *ipv6-address* } [**source** *source-address*] *filename*	Back up the log system file to the server.

1.3.3 Upgrading system

Upgrading files in privileged EXEC mode

You need to establish a FTP/TFTP environment before upgrading system files. Generally, you can use a PC to serve as the FTP/TFTP server and the RAX721-A to be the client, with the basic requirements as below:

- Connect the RAX721-A to the PC through the SNMP interface.
- Configure the IP address of the PC to interconnect with the RAX721-A.

Step	Command	Description
1	Raisecom#**download** { **system1** | **system2** | **bootstrap** | **cpld** | **startup-config** | **backup-config** | **paf** | **file** } { **ftp** *ip-address username password* | **ftp-active** *ip-address username password* | **tftp** *ip-address* } [**source** *source-address*]*filename* [**dir**]	In IPv4-based networks, download system files through FTP or TFTP.
2	Raisecom#**download** { **system1** | **system2** | **bootstrap** | **cpld** | **startup-config** | **backup-config** | **paf** | **file** } { **ftp** *ipv6-address username password* | **ftp-active** *ipv6-address username password* |**tftp** *ipv6-address* } [**source** *source-address*] *filename* [**dir**]	In IPv6-based networks, download system files through FTP or TFTP.
3	Raisecom#**boot next-startup** { **system1** | **system2** }	Specify the next bootstrap file for the device. The device supports dual-system software, offering primary and backup systems.
4	Raisecom#**reboot** [**now**] [**in** *minutes*]	Restart the device. The device will automatically load the downloaded system startup file.
5	Raisecom#**show version**	Show the device version.

Upgrading files in BootROM mode

Under the following conditions, you need to upgrade system software through BootROM mode.

- First startup
- System file damage
- Startup failure

You need to establish a FTP environment before upgrading system software in BootROM mode. Generally, you can use a PC to serve as the FTP server and the RAX721-A to be the client, with the basic requirements as below:

- Connect the RAX721-A to the FTP server through SNMP interface.
- Configure the FTP server to make it available.

Step	Operation
1	Log in to the device through the Console interface as an administrator and enter privileged EXEC mode, and then use the **reboot** command to restart the device. Raisecom#**reboot** Raisecom#reboot Please input 'yes' to confirm:yes 1970-01-01,08:02:42 [ros-scrnBg_0]System-4-SYSTEM_REBOOT:22 Reboot!!! 1970-01-01,08:02:54 [ros-scrnBg_0]System-4-SYSTEM_REBOOT:22 Reboot!!! booting... soc_pcie_hw_init : port->reg_base = 0x18012000 , its value = 0x1 PCIe port 0 in RC mode pos is 172 ==>PCIE: LINKSTA reg 0xbe val 0x1001 ********** port 0 is not active!! ********** GPIO:init Raisecom boot loader bootrom version 1.0.0 Raisecom Technology CO., LTD. Compiled Base Ethernet MAC address: 00:00:01:02:03:04 Press Ctrl+D to enter bootrom menu: 3 MBOOT MENU V1.1 1: Boot system from flash 2: Select default boot system 3: Update system from tftp 4: Update mboot from tftp 5: Update fpga from tftp 0: Reboot Press Up/Dwon or Number to move,Enter your choice: 3 Index Name Size ---------- 1* system1.z_9.0.0.20200420 27994264 2 system2.z_9.0.0.20200420 27994264 Current selected version is 1 Please select a version to overwrite: Raisecom#rebootinput number error. sys - Download system image and update to flash
2	Enter the following information according to the prompt: Current selected version is 2

Step	Operation
	Please select a version to overwrite: 2 Local IP Address[192.168.4.28]:192.168.4.28 Server IP Address[192.168.4.172]:192.168.4.174 Filename [system.bin]:system1.z_9.0.0.20200420
3	After the downloading is completed, load the downloaded system software according to the prompt and start the new software version.

1.3.4 Checking configurations

No.	Command	Description
1	Raisecom#**show version**	Show version information.
2	Raisecom#**show running-config**	Show current system configurations.
3	Raisecom#**show startup-config**	Show initial configuration files.

1.4 Device management

1.4.1 Introduction

Simple Network Management Protocol (SNMP) is designed by the Internet Engineering Task Force (IETF) to solve problems in managing network devices connected to the Internet. Through SNMP, a NMS 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 is someone being managed in the SNMP network while the NMS is the manager for the SNMP network. The Agent and NMS communicate with each other by sending SNMP packets through UDP.

The RAX721-A communicates with the NView NNM system through SNMP packets. Raisecom Nview NNM system can provide friendly Human Machine Interface (HMI) to facilitate network management. The following functions can be implemented through it:

- Send request packets to the RAX721-A.
- Receive reply packets and Trap packets from the RAX721-A, and show result.

The Agent is a program installed in the RAX721-A, implementing the following functions:

- Receive/reply request packets from Nview NNM system
- Read/write packets and generate response packets according to the packets type, then return the result to Nview NNM system

Define trigger condition according to protocol modules, enter/exit from system or reboot device when conditions are satisfied; the replying module sends Trap packets to NView NNM system through Agent to report current status of device.

An Agent can be configured with several versions concurrently, and different versions communicate with different NMSs. However, the SNMP version of the NMS must be consistent with that of the connected agent so that they can intercommunicate properly.

Protocol versions

Till now, SNMP has three versions: v1, v2c, and v3, described as below.

- SNMPv1 uses community name authentication mechanism. The community name, a string defined by an agent, acts like a password. The NMS can visit the agent only by specifying its community name correctly. If the community name carried in a SNMP packet is not authenticated by the RAX721-A, the packet will be dropped.
- Compatible with SNMPv1, SNMPv2c also uses community name authentication mechanism. SNMPv2c supports more operation types, data types, and error codes, and thus better identifying errors.
- SNMPv3 uses User-based Security Model (USM) and View-based Access Control Model (VACM) security mechanism. You can configure whether USM authentication is enabled and whether encryption is enabled to provide higher security. USM authentication mechanism is used to authenticate the senders so that illegal users will not be able to access them. Encryption is to encrypt packets transmitted between the NMS and agents, thus preventing interception.

The RAX721-A supports SNMPv1, SNMPv2c, and SNMPv3.

MIB

Management Information Base (MIB) is the collection of all objects managed by NMS. It defines attributes for the managed objects:

- Name
- Access right
- 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 RAX721-A.

MIB stores information in a tree structure, with unnamed root on the top. Nodes of the tree are the managed objects, which take a unique path starting from root (OID) for identification. SNMP protocol packets can access network devices by checking the nodes in MIB tree directory.

The RAX721-A supports standard MIB and Raisecom-customized MIB.

1.4.2 Preparing for configurations

Scenario

To log in to the RAX721-A through the NMS, you should first configure SNMP basic functions.

Prerequisite

- Configure the IP addresses on the SNMP interface.
- Configure static router to link RAX721-A and NMS through the router.

1.4.3 Confiurating SNMP basic functions

For SNMP v3, SNMP v1 or SNMP v2c, you should configure them respectively:

Configure SNMP v3 on the target device as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server access** *group-name* [**read** *view-name*] [**write** *view-name*] [**notify** *view-name*][**context** *context-name* { **exact** | **prefix** }] **usm** { **noauthnopriv** | **authnopriv** | **authpriv** }	Create and configure the SNMP access groups.
3	Raisecom(config)#**snmp-server group** *name* **user** *user* **usm**	(Optional) configure the mapping between users and access groups.
4	Raisecom(config)#**snmp-server contact** *syscontact*	(Optional) configure the ID and contact of network administrators.
5	Raisecom(config)#**snmp-server host** { *ip-address* | *ipv6-address* } **version 3** { **noauthnopriv** | **authnopriv** | **authpriv** } *user-name* [**udpport** *udpport*]	Configure the IP address of the SNMP target host.
6	Raisecom(config)#**snmp-server location** *sysLocation*	(Optional) specify the location for placing the RAX721-A.
7	Raisecom(config)#**snmp-server user** *user-name* [**remote** *engine-id*] **authentication** { **md5** | **sha** } *key-word* [**privacy** *privkey-value*]	Create a SNMP user name and configure the authentication algorithm, authentication password, and encryption password.
8	Raisecom(config)#**snmp-server user** *user-name* [**remote** *engine-id*] **authkey** { **md5** | **sha** } *authkey-word* [**privkey** *privkey-value*]	Add a SNMP user and specify the authentication algorithm, authentication password, and encryption password.
9	Raisecom(config)#**snmp-server view** *view-name oid-tree* [*mask*] { **included** | **excluded** }	Configure SNMP view.

Configure SNMP v1 or v2c on the target device as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server community** *name* [**view** *view*] { **ro** | **rw** }	Create a community name and configure its corresponding view and access priority.
3	Raisecom(config)#**snmp-server contact** *contact*	(Optional) configure the ID and contact of network administrators.
4	Raisecom(config)#**snmp-server host** { *ip-address* | *ipv6-address* } **version** { 1 | 2c } *community-string* [**udpport** *port-id*]	Configure the IP address of the SNMP target host.
5	Raisecom(config)#**snmp-server location** *location*	(Optional) specify the location for placing the RAX721-A.

1.4.4 Configuring Trap

Note

Configuration steps in SNMP v1, v2c and v3 are the same except the configuration of the target host. Choose it as required.

A Trap is used by the RAX721-A to send unrequested information to the NView NNM system automatically, which is used to report some critical events.

Finish the following tasks before configuring Trap:

- Configure SNMP basic functions. SNMP v3 requires configuring the user name and SNMP view.
- Configure routing protocols, and ensure routing between the RAX721-A and the NView NNM system is available.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#**ip address** *ip-address vlan-id*	Configure the IP address of the RAX721-A.
4	Raisecom(config-port)#**ipv6 address** *ipv6-address/prefix-length* [**eui-64**]	Configure the IPv6 address of the interface.
5	Raisecom(config-port)#**exit**	Exit Layer 3 physical interface configuration mode. Enter global configuration mode.
6	Raisecom(config)#**snmp-server host** { *ip-address* | *ipv6-address* } **version 3** { **noauthnopriv** | **authnopriv** | **authpriv** } *name* [**udpport** *udpport*]	(Optional) configure the SNMPv3 Trap target host.
7	Raisecom(config)#**snmp-server host** { *ip-address* | *ipv6-address* } **version** { **1** | **2c** } *name* [**udpport** *udpport*]	(Optional) configure the SNMP v1 and SNMP v2c Trap target host.

1.4.5 Checking configurations

No.	Command	Description
1	Raisecom#**show snmp access**	Show configurations of the SNMP access group.
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 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.

1.5 Configuring RMON

1.5.1 Introduction

Remote Network Monitoring (RMON) is a standard stipulated by IETF (Internet Engineering Task Force) for network data monitoring through different network Agent and NMS. RMON is derived from SNMP. Compared with SNMP, RMON can monitor remote devices more actively and more effectively, network administrators can track the network, network segment or device malfunction more quickly. This approach reduces the data flows between NMS and Agent, makes it possible to manage large networks simply and powerfully, and makes up the limitations of SNMP in the ever-growing distributed Internet.

RMON implements 4 function groups: statistics group, history group, alarm group, and event group.

- Statistics group: gather statistics on each interface, including number of received packets and packet size distribution statistics.
- History group: similar with the statistics group, but it only collects statistics in an assigned detection period.
- Alarm group: monitor an assigned MIB object, configure the upper and lower thresholds in an assigned time interval, and trigger an event if the monitored object exceeds the threshold.
- Event group: cooperating with the alarm group, when alarm triggers an event, it records the event, such as sending Trap or writing it into the log, and so on.

1.5.2 Preparing for configurations

Scenario

RMON helps monitor and gather statistics about network traffics.

Compared with SNMP, RMON is a more high-efficient monitoring method. After you specify an alarm threshold, the RAX721-A actively sends alarms when the threshold is exceeded without obtaining variable information. This helps reduce traffic of Central Office (CO) and managed devices and facilitates network management.

Prerequisite

The route between the RAX721-A and the NView NNM system is reachable.

1.5.3 Configuring RMON alarm group

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**rmon alarm** *alarm-id mibvar* [**interval** *second*] { **absolute** | **delta** } **rising-threshold** *rising-num* [*rising-event*] **falling-threshold** *falling-num* [*falling-event*] [**owner** *owner-name*]	Configure related parameters of the RMON alarm group.

1.5.4 Configuring RMON event group

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**rmon event** *event-id* [**log**] [**trap**] [**description** *string*] [**owner***owner-name*]	Configure related parameters of the RMON event group.

1.5.5 Configuring RMON statistics

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**rmon statistics** { *interface-type interface-number* | **ip** *if-number* }[**owner** *owner-name*]	Enable RMON statistics on an interface and configure related parameters. By default, RMON statistics on all interfaces is enabled.

1.5.6 Configuring RMON history statistics

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**rmon history** { *interface-type interface-number* | **ip** *if-number* }[**shortinterval** *period*] [**longinterval** *period*] [**buckets** *buckets-number*] [**owner***string*]	Enable RMON history statistics on an interface and configure related parameters. By default, RMON history statistics on all interfaces is disabled.

1.5.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show rmon**	Show RMON configurations.
2	Raisecom#**show rmon alarms**	Show information about the RMON alarm group.
3	Raisecom#**show rmon events**	Show information about the RMON event group.
4	Raisecom#**show rmon statisttics**	Show information about the RMON statistics group.
5	Raisecom#**show rmon history** *interface-type interface-number*	Show information about the RMON history group.

2 System management

This chapter describes principles and configuration procedures of system management, including following sections:

- User management
- Fan management
- Saving configurations
- Time management
- Log management
- File management
- Alarm management
- Key chain management

2.1 User management

When you start the RAX721-A for the first time, connect the PC through Console interface to the device, input the initial user name and password in Hyper Terminal to log in to and configure the RAX721-A.

By default, both the user name and password are raisecom.

If there is not any privilege restriction, any remote can log in to the RAX721-A through Telnet, when the Simple Network Management Protocol (SNMP) interface or other service interfaces of device are configured with IP addresses. This is unsafe to the RAX721-A and network. Creating user and setting password and privilege help to manage the login users and ensure network and device security.

2.1.1 Configuring user management

Step	Command	Description
1	`Raisecom#user name` *user-name* `password` *password*	Create or modify the user name and password. You can delete a created user through the **no username** command.

Step	Command	Description
2	Raisecom#**user name** *user-name* **privilege** *privilege-level*	Configure the level and privilege of the user.

2.1.2 Checking configurations

No.	Command	Description
1	Raisecom#**show user** { **active** [**onlineid** *online-id*] | **table** [**detail** | **username** *username*]	Show user information.

2.2 Fan management

When the device is placed in a hot environment, the high temperature will affect the heat dissipation performance of the device. At this time, you need to configure fan monitoring so that the fan of the device can automatically make adjustments according to the ambient temperature to maintain the normal operation of the device.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**fan-monitor mode** { **auto** | **enforce** }	Configure the working mode of the fan, including automatic mode and forced mode.
3	Raisecom(config)#**fan-monitor enforce level** *level-id*	Configure the fan rotating level in forced working mode.
4	Raisecom(config)#**fan-monitor trap send enable**	Enable fan monitoring.
5	Raisecom(config)#**fan-monitor temperature-scale** *temperature1 temperature2 temperature3*	Configure the critical temperature corresponding to the rotating level.
6	Raisecom#**show fan-monitor information**	Show the running information about the fan.
7	Raisecom#**show fan-monitor status**	Show the fan status.

2.3 Saving configurations

No.	Command	Description
1	Raisecom#**write**	Saving current configurations

No.	Command	Description
2	Raisecom#**auto-write enable** Raisecom#**auto-write interval** *minutes*	(Optional) enable auto-saving of configurations.

2.4 Time management

2.4.1 Configuring time and time zone

To ensure that the RAX721-A can cooperate with other devices, you need to configure system time and time zone precisely for the RAX721-A.

Step	Command	Description
1	Raisecom#**clock display** { **default** | **utc** }	Configure the system clock display mode. By default, the system clock display mode is **default**.
2	Raisecom#**clock set** *hour minute second year month day*	Configure the system time. By default, the system start time is 08:00:00, Jan 1, 1970.
3	Raisecom#**clock timezone** { **+** | **-** } *hour minute*	Configure the system time zone. By default, it is GMT+8:00.

2.4.2 Configuring DST

Daylight Saving Time (DST) is set locally to save energy. About 110 countries around the world apply DST in summer, but vary in details. Thus, you need to consider detailed DST rules locally before configuration.

Step	Command	Description
1	Raisecom#**clock summer-time enable**	Enable DST on the RAX721-A. By default, DST is disabled.
2	Raisecom#**clock summer-time recurring** { *start-week* | **last** } { **sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat** } *start-month start-hour start-minute* { *end-week* | **last** } { **sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat** } *end-month end-hour end-minute offset-min*	Configure the start time, end time, and offset of DST.

Note

- For example, if DST starts from 02:00 A.M. second Monday of April to 02:00 a.m. second Monday of September, the clock is adjusted forward 60 minutes. Thus, the

period between 02:00 and 03:00 second Monday of April does not exist. Configuring time during this period will fail.

- DST in the Southern Hemisphere is opposite to that in the Northern Hemisphere. It is from September this year to April next year. If the starting month is later than the ending month, the system judges that it is located in the Southern Hemisphere.

2.4.3 Configuring NTP/SNTP

Configuring NTP/SNTP basic functions

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ntp server** { *ip-address* | *ipv6-address* } [**version** *version-number*] [**keyid** *key-id*]	(Optional) configure the NTP server address for the client working in server/client mode.
3	Raisecom(config)#**ntp peer** { *ip-address* | *ipv6-address* } [**version** *version-number*] [**keyid** *key-id*]	(Optional) configure the NTP peer address for the device working in peer mode.
4	Raisecom(config)#**sntp server** { *ip-address* | *ipv6-address* } **version** { **v1** | **v2** | **v3** | **v4** }	Configure the IP address of the SNTP server for the device working in SNTP client mode.
5	Raisecom(config)#**ntp refclock-master** *ip-address* [*stratum*]	Configure the local device as the NTP master clock, namely, the reference clock. By default, the local device is not a reference clock source.

Configuring NTP identity authentication

In networks with high security requirements, authentication is required when using NTP. After identity verification is enabled, the NTP client only synchronizes with the verified server to ensure the security of the network. The NTP client will authenticate the server only when authentication is enabled. If authentication is not enabled, the client will not perform authentication even if the server carries key information, and will directly synchronize the time with the server.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ntp authenticate enable**	Enable NTP server/client authentication.
3	Raisecom(config)#**ntp authentication-keyid** *key-id* **md5** *password*	Configure the authentication key ID and key value of the NTP server/client.

Step	Command	Description
4	Raisecom(config)#**ntp trusted-keyid** *key-id*	Configure the authentication key ID of the NTP server/client to a trusted ID. **Note** The NTP client will verify the server only when authentication is enabled, and the client will only synchronize with the server that provides the trusted key.

Note

- If the device is configured as the NTP reference clock source, the configuration of the NTP server or NTP peer fails and cannot be synchronized by other devices. If the NTP server or peer is configured, the device will fail to be configured as a clock reference source.
- SNTP and NTP are mutually exclusive. If the SNTP server address is configured on the device, NTP cannot be configured for the device, and vice versa.

2.4.4 Checking configurations

No.	Command	Description
1	Raisecom#**show clock** [**summer-time recurring**]	Show configurations of the system time, time zone, and DST.
2	Raisecom#**show sntp**	Show SNTP obtaining time and whether configurations are correct.
3	Raisecom#**show ntp status**	Show NTP configurations.
4	Raisecom#**show ntp associations** [**detail**]	Show NTP connections.
5	Raisecom#**show ntp authentication**	Show information about NTP security.

2.5 Log management

2.5.1 Basic configurations of log management

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**logging on**	Enable global system log. By default, global system log is enabled.

Step	Command	Description
3	Raisecom(config)#**logging rate-limit** *number*	Configure the rate limiting value of logs. By default, it is 0. It means that no rate is configured on logs.
4	Raisecom(config)#**logging sequence-number**	Configure the log to display the sequence number. By default, the sequence number is not displayed.
5	Raisecom(config)#**logging buginf** [**high** | **low** | **none** | **normal**]	Configure the level of the Debug information. By default, it is **none**.

2.5.2 Configuring log discriminator

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**logging discriminator** *number* { **facility** | **mnemonics** | **msg-body** } { **none** | { **drops** | **includes** } *string* }	Configure the log discriminator.
3	Raisecom(config)#**logging** { **buffered** | **console** | **file** | **trap** } **discriminator** *number*	Associate the log buffer, Console log, log file, and Trap with the log discriminator.

2.5.3 Configuring log storage

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**logging buffered size** *size*	Configure the size of the log buffer. By default, it is 4 kBytes.
3	Raisecom(config)#**logging file**	Save logs to the log file.
4	Raisecom(config)#**logging** [**host** *ip-address*] **facility** { **alert** | **audit** | **auth** | **clock** | **cron** | **daemon** | **ftp** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **ntp** | **security** | **syslog** | **user** | **uucp** }	Configure the facility type of logs in the log host. By default, it is local7.
5	Raisecom(config)#**logging history**	Save logs to the historical log table.
6	Raisecom(config)#**logging history size** *size*	Configure the size of the historical log table. By default, it is 1.

2.5.4 Checking configurations

No.	Command	Description
1	Raisecom#**show logging**	Show system log configurations.
2	Raisecom#**show logging buffer**	Show buffer parameters of the system log.
3	Raisecom#**show logging discriminator**	Show configurations of log discriminator.
4	Raisecom#**show logging file**	Show log files.
5	Raisecom#**show logging history**	Show information about the historical log table.

2.5.5 Maintenance

No.	Command	Description
1	Raisecom(config)#**clear logging buffer**	Clear contents from the log buffer.
2	Raisecom(config)#**clear logging statistics**	Show log statistics in the buffer.

2.6 File management

2.6.1 Managing system files

No.	Command	Description
1	Raisecom#**erase** [*file-name* | **backup-config**]	Delete files from the memory. **Caution** Use this command with caution.
2	Raisecom#**dir**	Show system files.
3	Raisecom#**show startup**	Show system startup files.

2.7 Alarm management

An alarm refers to information generated by the system based on module failures when a fault is generated on the RAX721-A or some working condition changes.

The alarm is used to report some urgent and important events and notify them to the network administrator promptly, which provides strong support for monitoring device operation and diagnosing faults.

The alarm is stored in the alarm buffer. If the NView NNM system is configured, the alarm will be sent to it through SNMP. The information sent to the NView NNM system is called Trap.

Alarm classification

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 port Down alarm
- Recovery alarm: alarms generated when device failure or abnormal function returns to normal, such as port 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 4 types according to functions:

- 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 2 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 or restored.
  - History alarm table: consists of restored alarms and records the cleared and auto-restored alarms.
- 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 RAX721-A, including CLI terminal and NView NNM system.

Related concepts

Related concepts about alarm management are displayed as below:

- Alarm inhibition

The RAX721-A only records root-cause alarms but incidental alarms when enabling alarm inhibition. For example, the generation of alarm A will inevitably produce alarm B, then alarm B is inhibited and does not appear in the alarm buffer when enabling alarm inhibition. By enabling alarm inhibition, the RAX721-A can effectively reduce the number of alarms.

The root-cause alarm and all other incidental alarms will be recorded on the RAX721-A when alarm inhibition is disabled.

- Alarm auto-report

Auto-report refers that an alarm will be reported to the NView NNM system automatically with its generation and the NView NNM system does not need to query or synchronize alarms actively.

You can set auto-report to some alarm, some alarm source, or the specified alarm from specified alarm source.

The alarm source refers to an entity that generates related alarms, such as interfaces, devices, or cards.

- Alarm monitoring

Alarm monitoring is used to process alarms generated by modules:

  - When alarm monitoring is enabled, the alarm module will receive alarms generated by modules, and process them according to configurations of the alarm module, such as recording alarm in the alarm buffer, etc.
  - When alarm monitoring is disabled, the alarm module will discard alarms generated by modules without follow-up treatment. In addition, alarms will not be recorded on the RAX721-A.

You can perform alarm monitoring on some alarm, alarm source, or specified alarm from specified alarm source.

- Alarm inverse

Alarm inverse (taking alarms of the interface for examples) refers that the reported alarm status of the interface is opposite to the actual alarm status. The interface will not report an alarm if it is unused but it will report alarms if it is used. If the interface returns to the unused status, the reported alarm will be cleared. There are 3 alarm inverse modes available:

  - Non-inverse mode: alarms are reported normally
  - Manual inverse mode: in this mode, whatever the current alarm status of the interface is, the reported alarm status of the interface is changed to the one opposite to the actual alarm status. It means that the interface reports the related recovery alarm if there is an alarm and reports an alarm if there is no alarm.
  - Auto inverse mode: in this mode, if there is no alarm to be inversed, operations are configured successfully but not take effect. If there is an alarm to be inversed, operations are configured successfully. The related recovery alarm is reported and the interface will enter the inverse mode, which means status of all reported alarms is opposite to the real one. After the alarm is completed, the interface enters the non-inverse mode automatically and reports alarms properly.

- Alarm delay

Alarm delay refers that the device will record alarms and report them to the NView NNM system after a delay but not immediately when alarms generate. Delay for recording and reporting alarms are identical.

By default, an alarm is reported 5s later after it is generated and an alarm is cleared 5s later after it is finished.

- Alarm storage mode

Alarm storage mode refers to how to record new generated alarms when the alarm buffer is full. There are two ways:

  - stop: stop mode, when the alarm buffer is full, new generated alarms will be discarded without recording.
  - loop: loop mode, when the alarm buffer is full, the new generated alarms will replace old alarm information and take rolling records.

For the RAX721-A, the current alarm table can record up to 1000 alarms and the historical alarm table can record up to 500 alarms. Use the configured alarm storage mode to deal with newly-generated alarms when the alarm table is full.

- Alarm clearance

Clear the current alarm, which means deleting current alarms from the current alarm table. The cleared alarms will be saved to the historical alarm table.

- Viewing alarms

The administrator can view alarms and monitor alarms directly on the RAX721-A. If the RAX721-A is configured with the NView NNM system, the administrator can monitor alarms on the NView NNM system.

2.7.1 Configuring alarm inhibition

The RAX721-A only records root-cause alarms but incidental alarms when enabling alarm inhibition. For example, the generation of alarm A will inevitably produce alarm B, then alarm B is inhibited and does not appear in the alarm buffer or record the log information when enabling alarm inhibition. By enabling alarm inhibition, the RAX721-A can effectively reduce the number of alarms. The root-cause alarm and all other incidental alarms will be recorded on the RAX721-A when alarm inhibition is disabled.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#alarm inhibit enable`	Enable alarm inhibition. By default, it is enabled.
3	`Raisecom(config)#alarm correlation-inhibit enable`	Enable correlation inhabitation.

2.7.2 Configuring alarm delay

The alarm delay can be divided into alarm generation delay and alarm clearance delay.

- Alarm generation delay refers to the delay after an alarm is generated.
- Alarm clearance delay refers to the delay after an alarm is finished.

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

Step	Command	Description
2	Raisecom(config)#**alarm active delay** *second*	Configure the alarm generation delay. By default, it is 0s.
3	Raisecom(config)#**alarm clear delay** *second*	Configure the alarm clearance delay. By default, it is 0s.

2.7.3 Configuring alarm storage modes

Alarm storage modes are modes for Network Elements (NEs) storing alarms, which can be divided into loop and stop modes.

- In stop alarm storage mode, if there is no more capacity for alarms stored by NEs, newly-reported alarms will be discarded.
- In loop alarm storage mode, if there is no more capacity for alarms stored by NEs, newly-reported alarms will overwrite the old ones and will be stored at the initial position of the memory.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**alarm active storage-mode** { **loop** | **stop** }	Configure the alarm storage mode. By default, it is stop.

2.7.4 Configuring alarm clearance

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**alarm clear type** *module_name*	Clear alarms of a specified functional module.

2.7.5 Configuring alarm report

Auto-report refers that the device will automatically report an alarm to the NView NNM system when the alarm is generated, without querying or synchronizing the alarm. Trap is the information sent by the device to the NView NNM system. Trap is used to report some emergent and critical events (for example, the managed device is restarted).

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

Step	Command	Description
2	Raisecom(config)#**alarm auto-report** *interface-type interface-number* **enable**	Enable alarm auto-report based on various types of interfaces, including Ethernet interface, sub-interface, loopback interface, and link aggregation interface. By default, it is enabled.
3	Raisecom(config)#**alarm auto-report type** *module_name* [*group-name*] [*interface-type interface-number*] **enable**	Enable alarm auto-report for a function module. By default, it is enabled.
4	Raisecom(config)#**alarm auto-report all enable**	Enable alarm auto-report for all alarm. By default, it is enabled.

2.7.6 Configuring alarm inverse

Alarm inverse refers to that the actual alarms are shielded when the interface is disabled or without services. In other words, the interface does not report an alarm when there is an alarm but reports an alarm when there is no alarm.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**alarm inverse** *interface-type interface-number* { **auto** | **manual** | **none** }	Configure the alarm inverse mode.

2.7.7 Configuring alarm monitoring

Alarm monitoring is used to process alarms generated by interfaces or functional modules.

- After alarm monitoring is enabled, the alarm module will receive alarms generated by all modules and process them based on configurations of the alarm module, such as, saving alarms to the alarm buffer.
- After alarm monitoring is disabled, the alarm module will discard alarms generated by all modules without processing them. These alarms will not be record to the device.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**alarm monitor** *interface-type interface-number* **enable**	Enable alarm monitoring based on various types of interfaces, including Ethernet interface, sub-interface, loopback interface, VLAN interface, and link aggregation interface. By default, it is enabled.
3	Raisecom(config)#**alarm monitor** *module_name* [*group-name*] [*interface-type interface-number*] **enable**	Enable alarm monitoring based on functional module. By default, it is enabled.

Step	Command	Description
4	Raisecom(config)#**alarm monitor all enable**	Enable alarm monitoring for all alarms. By default, it is enabled.

2.7.8 Configuring alarm output

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**alarm syslog enable**	Enable alarm output to syslog. By default, it is enabled.

2.7.9 Checking configurations

No.	Command	Description
1	Raisecom#**show alarm active** [*module_name* | **severity** *severity*]	Show currently active alarms.
2	Raisecom#**show alarm cleared** [*module_name* | **severity** *severity*]	Show historical alarms.
3	Raisecom#**show alarm management** [*module_name*]	Show alarm management configurations.
4	Raisecom#**show alarm management statistics**	Show alarm statistics.
5	Raisecom#**show alarm log**	Show alarm logs.

2.8 Key chain management

2.8.1 Introduction

For the sake of security, the authentication information of the application layer needs to be continuously changed on the network. The authentication algorithm and the shared security key together can be used to determine whether information is tampered when it is transmitted on an unsecured network. When this authentication method is used to authenticate data, it is necessary to share the security key and authentication algorithm between the data sender and the receiver. And the key cannot be transmitted on the network.

If each application layer protocol maintains a set of authentication rules (including authentication algorithms and keys), a large number of applications will use the same authentication method. This will cause the authentication information to be copied and changed. Similarly, if each application uses a fixed authentication key, each change requires the manual intervention of the administrator, which is complicated and cumbersome. In addition, it is very difficult to change the password of all routers without packet loss.

Therefore, the system needs to be able to centrally manage all authentication processes and change authentication algorithms and keys without excessive manual intervention. Key-chain achieves this function.

Key-chain provides authentication for all application layer protocols and can dynamically change the password chain without packet loss.

2.8.2 Configuring key chain

No.	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**key-chain** *key-chain-name*	Create a key chain and enter Keychain configuration mode.
3	Raisecom(config-keychain)#**accept-tolerance** { *time-value* | **infinite** }	Configure the receiving-tolerance time.
4	Raisecom(config-keychain)#**key** *key-id* **key-string** [**0** | **7**] *keystring*	Configure the key and password string.
5	Raisecom(config-keychain)#**key** *key-id* **send-lifetime** *start-time* { **duration** *duration-time* | *end-time* | **infinite** }	Configure the key sending liftetime.
6	Raisecom(config-keychain)#**key** *key-id* **accept-lifetime** *start-time* { **duration** *duration-time* | *end-time* | **infinite** }	Configure the key receiving lifetime.

2.8.3 Checking configurations

No.	Command	Description
1	Raisecom#**show key-chain**	Show key configurations and statistics.
2	Raisecom#**show key-chain** *key-chain-name* **key** *key-id*	Show configurations and statistics of a specified key.

3 Zero-configuration

This chapter describes principles and configuration procedures of interface management, including following sections:

- Configuring CO zero-configuration
- Checking configurations

3.1 Configuring CO zero-configuration

3.1.1 Preparing for configurations

Scenario

- When the CO device connects with remote devices, the RAX721-A can discover these remote devices by using the extended OAM protocol and configure the management IP address, management VLAN, and default route for them. Therefore, the NView NNM system can quickly manage remote devices through the public IP address and global interface ID of the RAX721-A without being configured manually.
- When the CO RAX721-A and remote devices are connected directly/indirectly, both the CO and remote devices can provide zero-configuration through Dynamic Host Configuration Protocol (DHCP).

Prerequisite

- The RAX721-A is a CO device.
- The CO zero-configuration server is connected to the NView NNM system and remote devices properly.
- Perform the following operations on the CO device based on extended OAM protocol:
  - Create and activate the management VLAN.
  - Manually enable the OAM active mode on the interface.

3.1.2 Configuring zero-configuration Server based on extended OAM

The IP RAN local device assigns private IP addresses for remote devices through extended OAM zero-configuration, ensuring that routes are available between the local and remote devices. To implement NMS path protection, the remote device is connected to the local device through dual uplinks.

Configuring management VLAN

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#create vlan` *vlan-id* `active`	Create and activate a VLAN.
3	`Raisecom(config)#oam mng-vlan` *vlan-id*	Configure the remote management VLAN of zero-configuration. By default, it is VLAN 0. **Note** After configuring the management VLAN through this command, do not modify the switching property of downlink interfaces of the CO device. Otherwise, it may cause the remote device to be out of management.
4	`Raisecom(config)#interface` *interface-type interface-number*	Enter interface configuration mode.
5	`Raisecom(config-port)#oam enable`	Enable OAM. By default, the interface is enabled with OAM.
6	`Raisecom(config-port)#oam active`	Configure the OAM active mode of the interface.

Configuring ACL

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#access-list` *acl-number*	Create an ACL and enter ACL configuration mode.
3	`Raisecom(config-acl-ipv4-advanced)#rule [` *rule-id* `] permit ip` *source-ip-address source-ip-mask* `any`	Configure the ACL rules. Packets with source IP addresses meeting the ACL rule will be reported to the CPU.
	`Raisecom(config-acl-ipv4-advanced)#exit`	Exit ACL configuration mode.

Configuirng traffic classification rules

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#**class-map** *class-map-name* **match all**	Create a traffic classifier and enter CMAP configuration mode.
3	Raisecom(config-cmap)#**match access-list** *acl-number* Raisecom(config-cmap)#**exit**	Define traffic classification which should match the ACL filtering rules.
4	Raisecom(config)#**policy-map** *policy-map-name*	Create a traffic policy and enter PMAP configuration mode.
5	Raisecom(config-pmap)#**class-map** *class-map-name*	Add a traffic classification policy to the traffic policy and enter traffic policy configuration mode which binds with traffic classification.
6	Raisecom(config-pmap-c)#**forward-to-cpu** Raisecom(config-pmap-c)#**exit** Raisecom(config-pmap)#**exit**	Forward the traffic to the CPU.

Applying traffic classification to interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical interface configuration mode. The interface is an uplink interface, for connecting the public network.
3	Raisecom(config-port)#**switchport mode trunk**	Configure the interface to Trunk mode.
4	Raisecom(config-port)#**switchport trunk allowed vlan** *vlan-id* [**confirm**]	Configure the VLANs allowed to pass in Trunk mode.
5	Raisecom(config-port)#**oam active**	Configure the OAM active mode.
6	Raisecom(config-port)#**service-policy ingress** *policy-map-name*	Apply the traffic classification rule in the ingress direction of the interface.

Configuring address pool and gateway

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

Step	Command	Description
2	Raisecom(config)#**ip oam server pool** *pool-name*	Configure the address pool of the OAM property and enter address pool configuration mode.
3	Raisecom(config-pool)#**address** *start-ip-address end-ip-address* **mask** { *mask-address* | *mask-length* }	Configure the IP address range and subnet mask of the address pool.
4	Raisecom(config-pool)#**gateway** *ip-address*	Configure the gateway of the address pool.
	Raisecom(config-pool)#**exit**	Exit address pool configuration mode.
5	Raisecom(config)#**interface vlan** *vlan-id*	Enter VLAN interface configuration mode. The VLAN ID is pre-activated.
6	Raisecom(config-vlanif)#**ip address** *ip-address* [*ip-mask*] [**sub**]	Configure the IP address of the VLAN interface, which is the IP address of the configured gateway of the address pool.

Configuring NAT

Network Address Translation (NAT) is used to convert the private management IP address of the remote device to the public IP address. Through zero-configuration, the remote device obtains a private IP address from the CO device. NAT can be used to translate the private IP address into the public IP address of the management network and distinguish different remote devices in a form of public IP address+global interface ID. Network management information transmitted between remote devices and the NView NNM system is forwarded through the public IP address. Therefore, you should configure the public IP address and related management VLAN of the CO device.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface fastethernet** *interface-number*	Enter network management interface configuration mode. The network management interface of the device is used to connect the network management server, which is also called the public network interface.
3	Raisecom(config-port)#**nat outbound** *acl-number*	Configure NAT. The ACL is created in the previous step.

(Optional) releasing IP address

When replacing a remote device that has applied for a management IP address, to prevent the IP address resource from being occupied for a long time, you need to manuallt configure the lease information about the IP address on the central office server.

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#**oam address** *ip-address* **release**	Release the specified IP address.

3.1.3 Configuring zero-configuration server based on DHCP

Configuring ACL

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**access-list** *acl-number*	Create an ACL and enter ACL configuration mode.
3	Raisecom(config-acl-ipv4-advanced)#**rule** [*rule-id*] **permit ip** *source-ip-address source-ip-mask* **any**	Configure the ACL filtering rule. The packets with the source IP address matching the ACL filtering rule will be reported to the CPU.
	Raisecom(config-acl-ipv4-advanced)#**exit**	Exit ACL configuration mode.

Configuring traffic classification rules

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**class-map** *class-map-name* **match all**	Create a traffic classifier and enter CMAP configuration mode.
3	Raisecom(config-cmap)#**match access-list** *acl-number* Raisecom(config-cmap)#**exit**	Define traffic classification which should match the ACL filtering rules.
4	Raisecom(config)#**policy-map** *policy-map-name*	Create a traffic policy and enter PMAP configuration mode.
5	Raisecom(config-pmap)#**class-map** *class-map-name*	Add a traffic classification policy to the traffic policy and enter traffic policy configuration mode which binds with traffic classification.
6	Raisecom(config-pmap-c)#**forward-to-cpu** Raisecom(config-pmap-c)#**exit** Raisecom(config-pmap)#**exit**	Forward the traffic to the CPU.

Configuring DHCP server interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-tyep interface-number*	Enter uplink physical layer interface configuration mode. The interface is a DHCP gateway interface. The types of interface supported can be a VLAN interface, sub-interface, and physical interface.
	Raisecom(config-port)#**no portswitch**	Switch the interface mode to Layer 3 router mode.
	Raisecom(config-port)#**encapsulation dot1Q** *vlan-id*	(Optional) when the DHCP gateway uses a sub-interface, configure the single-layer VLAN encapsulated by the Ethernet sub-interface. Configure the interface IP address.
3	Raisecom(config-port)#**ip address** *ip-address*	Configure the interface IP address. The address is consistent with the address of the address pool gateway.
4	Raisecom(config-port)#**service-policy ingress** *policy-map-name*	Apply the traffic classification rule to the ingress direction of the interface. Only physical layer interfaces support traffic classification rules.
5	Raisecom(config-port)#**ip dhcp server**	Enable DHCP Server on the interface. By default, the device is not enabled with DHCP Server.
	Raisecom(config-port)#**exit**	Exit interface configuration mode.

Configuring DHCP server address pool

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp server pool** *pool-name*	Configure the address pool of the DHCP property and enter address pool configuration mode.
3	Raisecom(config-pool)#**address** *start-ip-address end-ip-address* **mask** { *mask-address* | *mask-length* }	Configure the IP address range and subnet mask of the address pool.
4	Raisecom(config-pool)#**gateway** *ip-address*	Configure the default gateway of the address pool. The gateway is identical to the private IP address of the management IP address assigned to the remote device by the local device.
5	Raisecom(config-pool)#**lease expired** { *minute* | **infinite** }	(Optional) configure the lease of the address pool. By default, it is 30min.

Step	Command	Description
6	Raisecom(config-pool)#**option 60** *vendor-string*	(Optional) configure information carried by Option60.
7	Raisecom(config-pool)#**option 43** [**sub-option** *option-id*] { **hex** | **ascii** } *string*	(Optional) configure information about Option43.
8	Raisecom(config-pool)#**trap server-ip** *ip-address*	(Optional) configure the IP address of the SNMP server (NView NNM system) to which the Trap is sent.
9	Raisecom(config-pool)#**tftp-server** *ip-address*	(Optional) configure the TFTP server related to the address pool.
10	Raisecom(config-pool)#**exit**	Exit address pool configuration mode.

Note

- If the zero-configuration server assigns management IP addresses to remote devices based on Layer 3 physical interface, the network management information exchanged between CO and remote devices is untagged packets.
- If the zero-configuration server assigns management IP addresses to remote devices based on sub-interface or VLAN interface, the network management information exchanged between CO and remote devices is Tagged packets with the management VLAN ID.

Configuring NAT

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter network management interface configuration mode.
3	Raisecom(config-port)#**nat outbound** *acl-number*	Configure NAT.

(Optional) releasing IP address

When changing a remote device, which has applied for a management IP address, to prevent the IP address from being occupied for a long time, you should manually release the IP address on the CO server.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp address** *ip-address* **release**	Release the specified IP address. This command is used to release the lease table and NAT table of the CO device only without influencing the IP address of the remote device.

(Optional) configuring lease file management

The RAX721-A supports saving and synchronizing the lease file automatically, as well as deleting the lease file.

When changing the CO zero-configuration server, you can upload assigned IP addresses in a form of lease to the TFTP/FTP server (such as a PC) for backup. After changing the CO device, you can download the backup lease file to the local device to confirm that these assigned IP addresses are not lost.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp lease save**	Save the lease file.
3	Raisecom(config)#**ip dhcp lease erase**	(Optional) delete the lease file from the DHCP server.
4	Raisecom(config)#**ip dhcp address release** [**pool** *pool-name*]	Release lease of specified address pool.
5	Raisecom(config)#**ip dhcp address** *ip-address* **release**	Release lease of the specified IP address.
6	Raisecom(config)#**exit**	Exit global configuration mode.
7	Raisecom#**upload dhcpLease** { **ftp** *ip-address username password filename* | **tftp** *ip-address filename* }	Upload the lease file to the PC through TFTP/FTP.
8	Raisecom#**download dhcpLease** { **ftp** *ip-address username password filename* | **tftp** *ip-address filename* }	Download the lease file from the PC through TFTP/FTP.

Configuring DHCP Relay

If the zero-configuration server and the remote device are in the same network segment, the remote device can obtain the IP address from the DHCP Server. Otherwise, the remote device can obtain the IP address from the DHCP Server through the device, which is enabled with DHCP Relay. The zero-configuration server can assign IP addresses to remote devices in different network segments.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp relay**	Configure global DHCP Relay.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 3 physical interface configuration mode.  The Layer 3 physical interface needs to be configured with the IP address.

Step	Command	Description
4	Raisecom(config-port)#**ip dhcp relay**	Enable DHCP Relay. Enable DHCP Relay on the interfaces connecting DHCP Server and DHCP Client.
5	Raisecom(config-port)#**ip dhcp relay target-ip** *ip-address*	Configure the destination IP address. The IP address can be either the IP address of DHCP Server or that of DHCP Relay.

3.2 Checking configurations

No.	Command	Description
1	Raisecom(config)#**show ip dhcp server**	Show configurations of interfaces of the DHCP server.
2	Raisecom(config)#**show ip dhcp server lease**	Show assigned IP addresses and information about remote devices.
3	Raisecom(config)#**show ip server pool** [*pool-name*]	Show configurations of the DHCP or OAM address pool.
4	Raisecom(config)#**show ip dhcp server statistics**	Show statistics of the DHCP server.
5	Raisecom(config)#**show ip dhcp static-bind**	Show static binding information about the IP address in the address pool and the MAC address.
6	Raisecom(config)#**show oam zero config**	Show configurations of directly-connected zero-configurations.
7	Raisecom(config)#**show remote config-info all**	Show configurations of remote devices in directly-connected zero-configuration server mode.
8	Raisecom(config)#**show ip dhcp relay**	Show configurations of DHCP Relay.
9	Raisecom(config)#**show debugging ospf dcn_info** [**self**]	Show NE information collected about the CO OSPF DCN zero-configuration server.
10	Raisecom(config)#**show nat session** [**file**] [**count**]	Show NAT entries of the CO OSPF DCN zero-configuration server.
11	Raisecom(config)#**show nat outbound**	Check the ACL information bound when NAT is performed in the outbound direction of the interface.
12	Raisecom(config)#**show nat netstack-rule** [**dnat** | **snat**]	Show the protocol stack rules for NAT.

4 Interface management

This chapter describes principles and configuration procedures of interface management, including following sections:

- Basic configurations of interface
- Configuring Ethernet interface
- Configuring Ethernet sub-interface
- Configuring VLAN interface
- Configuring optical module DDM
- Configuring loopback interface
- Configuring out-of-band network management interface
- Checking configurations

4.1 Basic configurations of interface

4.1.1 Configuring basic information of interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**no portswitch**	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#**ip address** *ip-address* [*ip-mask*] [**sub**]	Configure the primary and secondary IP addresses, as well as subnet mask of the Layer 3 physical interface.
4	Raisecom(config-port)#**description** *string*	Configure interface descriptions.
5	Raisecom(config-port)#**portswitch**	Switch interface configuration mode. Switch the interface to Layer 2 physical interface configuration mode, namely, the switching mode.
6	Raisecom(config-port)#**shutdown**	(Optional) shut down the interface.

4.1.2 Configuring interface working mode

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#**mode** { **l2** | **l3** }	Configure Layer 3 physical interface working mode. • L2: access L2VPN. • L3: access L3VPN.

4.1.3 Configuring Jumboframe on interface

When exchanging high-throughput data, such as transmitting files, the Ethernet interface may receive the Jumbo frame, whose size is greater than the standard Ethernet frame size. The system will directly discard Jumbo frames. If you configure to allow Jumbo frames to pass, the system will continue to process them, when the size of these Jumbo frames is greater than the standard size but in specified value range.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**jumboframe** *frame-size*	Configure the interface to allow Jumbo frames to pass. By default, it is 9600 Bytes.

4.1.4 Configuring MTU of interface

The Maximum Transmission Unit (MTU) is the largest bytes of packets that can be transmitted in a physical network. After you configure the RAX721-A to allow Jumbo frames to pass, the IP layer will compare the MTU with the size of the packet to be sent. If the size of the packet is greater than the MTU, the IP layer will fragment the packet. The fragmented packet can be smaller than or equal to the MTU. When MTUs of two connected devices are configured inconsistently, these 2 devices fail to communicate with each other. In this case, you should adjust MTU configurations.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 3 physical interface configuration mode.
3	Raisecom(config-port)#**mtu** *size*	Configure the MTU of the interface. By default, it is 1500 bytes.

4.1.5 Configuring vibration suppression of interface

When working on the network, the interface of the device may be alternately up and down due to various reasons, such as physical signal interference and configuration error in link layer. Frequent alternation causes repetitive vibration of routing protocols and unfavorably impacts the device and the network and even cause the network and some devices unavailable.

You can configure the vibration suppression period to reduce the switching frequency of interface Up and Down.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**vibration-suppress peroid** *second*	Configure the suppression period of the interface. By default, the suppression period is 0s.

4.1.6 Configuring MAC address of interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**mac** *mac-address*	Configure the MAC address of the interface. **Caution** If different interfaces are configured with the same MAC address, conflicts will occur. Before configuration, plan the interface MAC address in advance.
4	Raisecom(config-port)#**shutdown** Raisecom(config-port)#**no shutdown**	Restart the interface to make the MAC address take effect.

4.2 Configuring Ethernet interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**tpid** { **8100** | **9100** | **88a8** }	Configure the TPID of the interface. By default, it is 0x8100.

Step	Command	Description
4	Raisecom(config-port)#**speed** { **auto** | **10** | **100** | **1000** | **10000** | **25000** | **40000** }	Configure the interface rate.
5	Raisecom(config-port)#**duplex** { **auto** | **full** | **half** }	Configure the interface duplex mode.

4.3 Configuring Ethernet sub-interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**no portswitch**	Enter interface configuration mode.
3	Raisecom(config-port)#**interface gigaethernet** *unit/slot/port.sub-interface*	In Layer 3 physical interface configuration mode, enter Ethernet sub-interface configuration mode.
4	Raisecom(config-subif)#**encapsulation dot1Q** *vlan-id*	Configure the single VLAN used for encapsulating the Ethernet sub-interface.
5	Raisecom(config-subif)#**encapsulation qinq svlan** s*vlan-id* **cvlan** c*vlan-id*	Configure the double VLAN Tag used for encapsulating the Ethernet sub-interface.
6	Raisecom(config-subif)#**mode** { **l2** | **l3** }	Configure the sub-interface mode for accessing L2VPN or L2VPN.
7	Raisecom(config-subif)#**vlan translate** [**svlan** { **untag** | *vlan-id* }] [**cvlan** { **untag** | *vlan-id* }]	In L2VPN mode, configure VLAN mapping on the Ethernet sub-interface.

4.4 Configuring VLAN interface

The prerequisite is that the related VLAN ID is created.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface vlan** *vlan-id*	Enter VLAN interface configuration mode.
3	Raisecom(config-vlanif)#**ip address** *ip-address* [*ip-mask*] [**sub**]	Configure the primary and secondary IP addresses, and the subnet mask of the VLAN interface.

4.5 Configuring optical module DDM

4.5.1 Preparing for configurations

Scenario

Optical module DDM provides a method to detect SFP performance parameters. You can predict the service life of optical module, isolate system fault, and check its compatibility during installation by analyzing monitoring data.

Prerequisite

N/A

4.5.2 Enabling optical module DDM

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**transceiver ddm enable**	Enable optical module DDM. By default, it is disabled.

4.5.3 Checking configurations

No.	Command	Description
1	Raisecom#**show transceiver** [*interface-type interface-number* **history** { **15m** | **24h** }]	Show history information about optical module DDM.
2	Raisecom#**show transceiver ddm** *interface-type interface-list* [**detail**]	Show information about optical module DDM.
3	Raisecom#**show transceiver information** *interface-type interface-number*	Show information about optical module DDM.
4	Raisecom#**show transceiver threshold-violations** *interface-type interface-number*	Show transceiver threshold violations.
5	Raisecom#**show transceiver ddm brief**	Show brief information about optical module DDM.
6	Raisecom#**show transceiver ddm poll-interval**	Show information about optical module DDM at the poll interval.

4.6 Configuring loopback interface

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface loopback` *interface-number*	Enter loopback interface configuration mode.
3	`Raisecom(config-port)#ip address` *ip-address* `[` *ip-mask* `] [ sub ]`	Configure the primary and secondary IP addresses, and the subnet mask of the loopback interface.

4.7 Configuring out-of-band network management interface

4.7.1 Preparing for configurations

Scenario

The out-of-band DCN network management channel is provided by the out-of-band management interface, and the out-of-band network management is provided based on SNMP /UDP. The out-of-band management interface is located on the MCC of the device and uses the RJ45 interface. Management through out-of-band DCN has the following characteristics:

- Does not occupy service bandwidths.
- Does not affect the network management channel when the service channel and physical line are interrupted.
- Depend on a separate DCN.

Prerequisite

The network management IP address of the device is planned.

4.7.2 Configuring IP address of out-of-band network management interface

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface fastethernet 1/0/1`	Enter out-of-band network management interface configuration mode.
3	`Raisecom(config-port)#ip address` *ip-address* `[` *ip-mask* `] [ sub ]`	Configure the IP address of the out-of-band network management interface.

4.8 Checking configurations

No.	Command	Description
1	Raisecom#**show interface** [**rang**] [*interface-type interface-number*] [**configuration**] [**statistics**]	Show interface configurations, status, and statistics.

5 Ethernet

This chapter describes principles and configuration procedures of Ethernet, including following sections:

- Configuring VLAN
- Configuring MAC address table
- Configuring QinQ
- Configuring LLDP
- Configuring loop detection
- Configuring L2CP
- Configuring STP
- Configuring RSTP/MSTP
- Configuring MRSTP
- Configuring Super VLAN
- Configuring PVLAN
- Configuring GARP/GVRP
- Configuring port security MAC

5.1 Configuring VLAN

5.1.1 Preparing for configurations

Scenario

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

- Small LAN: on one Layer 2 device, the LAN is carved up to several VLANs. Hosts that connect to the device are carved up by VLANs. So hosts in the same VLAN can communicate, but hosts between different VLANs cannot communicate. For example, the financial department needs to be separated from other departments and they cannot access each other. In general, the port connected to the host is in Access mode.
- Big LAN or enterprise network: multiple Layer 2 devices connect to multiple hosts and these devices are concatenated. Packets take VLAN Tag for forwarding. Ports of multiple

devices, which have identical VLAN, can communicate, but hosts between different VLANs cannot communicate. This mode is used for enterprises that have many people and need a lot of hosts, and the people and hosts are in the same department but different positions. Hosts in one department can access each other, so you have to partition VLANs on multiple devices. Layer-3 devices like a router are required if you want to communicate among different VLANs. The concatenated ports among devices are in Trunk mode.

Prerequisite

N/A

5.1.2 Configuring VLAN properties

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**create vlan** *vlan-list* **active**	Create a VLAN. By default, there is no VLAN and the interface is not added to any VLAN.
3	Raisecom(config)#**vlan** *vlan-id*	Enter VLAN configuration mode.
4	Raisecom(config-vlan)#**name** *vlan-name* Raisecom(config-vlan)#**exit**	(Optional) configure the VLAN name.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
6	Raisecom(config-port)#**portswitch**	Switch the interface to work in Layer 2 mode.
7	Raisecom(config-port)#**switchport mode** { **access** | **trunk** }	Configure the current interface as the Access/Trunk interface. By default, all interfaces are Access interfaces.
8	Raisecom(config-port)#**switchport reject-frame** { **tagged** | **untagged** }	Configure the types of frames denied by the interface.

Note

- VLANs that are created by using the vlan *vlan-id* command are in active status.
- All configurations of a VLAN cannot take effect until the VLAN is activated.

5.1.3 Configuring VLANs based on Access interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**portswitch**	Switch the interface to work in Layer 2 mode.

Step	Command	Description
4	Raisecom(config-port)#**switchport mode access**	Configure the interface mode to Access.
5	Raisecom(config-port)#**switchport access vlan** *vlan-id*	Configure the interface Access VLAN.
6	Raisecom(config-port)#**switchport access egress-allowed vlan** { **all** | *vlan-list* } [**confirm**]	Configure the VLAN list available for the Access interface.
7	Raisecom(config-port)#**switchport reject-frame** { **untagged** | **tagged** }	(Optional) configure the untagged packets or tagged packets denied by the interface.

5.1.4 Configuring VLANs based on Trunk interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**portswitch**	Switch the interface to work in Layer 2 mode.
4	Raisecom(config-port)#**switchport mode trunk**	Configure the interface mode to Trunk.
5	Raisecom(config-port)#**switchport trunk native vlan** *vlan-id*	Configure the interface Native VLAN.
6	Raisecom(config-port)#**switchport trunk allowed vlan** { **all** | *vlan-list* } [**confirm**]	(Optional) configure the VLAN list available for the Trunk interface.
7	Raisecom(config-port)#**switchport trunk untagged vlan** { **all** | *vlan-list* } [**confirm**]	(Optional) configure the Untagged VLAN list available for the Trunk interface.
8	Raisecom(config-port)#**switchport reject-frame** { **untagged** | **tagged** }	(Optional) configure the untagged packets or tagged packets denied by the interface.

Note

- The Trunk interface permits Native VLAN packets to pass regardless of configurations for Trunk Allowed VLAN list and Trunk Untagged VLAN list on the interface. And forwarded packets do not carry VLAN TAG.
- When configuring a Native VLAN, the system will automatically create and activate a VLAN if you do not create the VLAN in advance.
- The interface permits Trunk Allowed VLAN packets passing. If the VLAN is a Trunk Untagged VLAN, the VLAN TAG of the packet is removed on the egress interface. Otherwise, the packet is not modified.

- If the configured Native VLAN is not the default VLAN and there is no default VLAN in the VLAN list on the Trunk interface, the interface will not allow packets in the default VLAN to pass.
- When configuring a Trunk Untag VLAN list, the system automatically adds all Untagged VLAN to the Trunk allowed VLAN.
- Trunk allowed VLAN list and Trunk Untagged VLAN list are valid for the static VLAN only.

5.1.5 Configuring VLAN based on MAC address

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mac-vlan** *mac-address* **vlan** *vlan-id* [**priority** *value*]	Associate the MAC address with the VLAN.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#**mac-vlan enable**	Enable MAC-VLAN.

Caution

- When the MAC address is a multicast MAC address, all 0s or all Fs, the configuration fails.
- If the association between the created MAC address and the VLAN conflicts with the existing association (for example, the same MAC address is associated with different VLANs), the configuration fails.

5.1.6 Configuring VLAN based on IP subnet

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip-subnet-vlan** *ip-address* [*ip-mask*] **vlan** *vlan-id* [**priority** *value*]	Associate the VLAN with the IP subnet address.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#**ip-subnet-vlan enable**	Enable VLAN partition based on IP subnet.

Caution

- When the IP address or mask is invalid, the configuration fails.
- If the association between the created IP subnet and the VLAN conflicts with the existing association (for example, the same subnet is associated with different VLANs), the configuration fails.

5.1.7 Configuring VLAN based on protocol

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**protocol-vlan** *protocol-index* { **ipv4** | **ipv6** | **ethertype** *protocol-id* }	Configure the association rules between the protocol VLAN and Ethernet packets.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#**switchport protocol-vlan** *protocol-index* **vlan** *vlan-id*	Configure the association rules between the protocol VLAN and the interface.

5.1.8 Checking configurations

No.	Command	Description
1	Raisecom#**show vlan** [*vlan-list* | **static** | **dynamic**] [**detail**]	Show configurations and status of all VLANs or specified VLANs.
2	Raisecom#**show switchport interface** *interface-type interface-number*	Show switching configurations on the interface.
3	Raisecom#**show vlan precedence**	Show VLAN priority of the MAC-VLAN and IP subnet.
4	Raisecom#**show mac-vlan** { **all** | **vlan** *vlan-id* }	Show MAC VLAN configurations.
5	Raisecom#**show ip-subnet-vlan** { **all** | **vlan** *vlan-id* }	Show VLAN configurations of the IP subnet.
6	Raisecom#**show protocol-vlan all**	Show configurations of all VLANs.
7	Raisecom#**show protocol-vlan interface** *interface-type interface-number*	Show VLAN configurations on the interface.

5.2 Configuring MAC address table

5.2.1 Preparing for configurations

Scenario

When configuring the MAC address table, you can configure static MAC addresses for fixed and important devices to prevent illegal users from accessing the network from other locations.

To avoid saving too many dynamic MAC addresses to the MAC address table and exhausting resources of the MAC address table, you need to configure the aging time of dynamic MAC addresses to ensure upgrading dynamic MAC addresses effectively.

Prerequisite

N/A

5.2.2 Configuring static MAC address table

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

2	`Raisecom(config)#mac-address static unicast mac-address vlan vlan-id interface-type interface-number`
	`Raisecom(config)#mac-address static unicast mac-address vsi vsi-name interface-type interface-number`
	`Raisecom(config)#mac-address static unicast mac-address vsi vsi-name vc-id vc-id peer ip-address`
		Add a static unicast MAC address to the MAC address table.
		Note
		It must be a unicast MAC address. The local MAC address, multicast address, all-F, and all-0 MAC addresses cannot be set to the static MAC address.

5.2.3 Configuring dynamic MAC address table

Commands for steps 2, 3, and 4 are used to configure dynamic MAC address limit in interface configuration mode. Commands for steps 5–10 and 11–12 are used to configure dynamic MAC address limit in VLAN configuration mode and VSI configuration mode respectively.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface interface-type interface-number`	Enter interface configuration mode.
3	`Raisecom(config-port)#mac-address learning enable`	Enable MAC address learning. By default, MAC address learning is enabled.
4	`Raisecom(config-port)#mac-address threshold threshold-value`	(Optional) configure dynamic MAC address limit. By default, no dynamic MAC address limit is configured.
5	`Raisecom(config)#vlan vlan-id`	Enter VLAN configuration mode.
6	`Raisecom(config-vlan)#mac-address learning enable` `Raisecom(config-vlan)#exit`	Enable MAC address learning. By default, MAC address learning is enabled.
7	`Raisecom(config)#mac-address aging-time second`	(Optional) configure the aging time of the MAC address. By default, it is 300s.

Step	Command	Description
8	Raisecom(config-port)#mac-address **move-restrain enable** Raisecom(config-port)#**exit**	(Optional) configure suppression over MAC address flapping. By default, it is disabled.
9	Raisecom(config)#**vlan** *vlan-id*	(Optional) enter VLAN configuration mode.
10	Raisecom(config-vlan)#**mac-address threshold** *threshold-value*	(Optional) configure dynamic MAC address limit. By default, no dynamic MAC address limit is configured.

5.2.4 Configuring blackhole MAC address

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mac-address blackhole** *mac-address* { **vlan** *vlan-id* | **vsi** *vsi-name* }	Create the blackhole MAC address. By default, no blackhole MAC address is configured.

5.2.5 Filtering unknown L2 multicast packets

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mac-address multicast drop-unknown** { **reserved-address** | **vlan** *vlan-list* }	Configure the mode of MAC address table multicast filtering to discard packets. • If **reserved-address** is selected, it indicates whether the discarded packets contain reserved addresses. • If **vlan** *vlan-list* is selected, it means filtering based on VLAN.

5.2.6 Checking configurations

No.	Command	Description
1	Raisecom#**show mac-address count** [**vlan** *vlan-id*] [*interface-type interface-number*]	Show the number of MAD address entries.
	Raisecom#**show mac-address count vsi** *vsi-name* [*interface-type interface-number*]	
	Raisecom#**show mac-address count vsi** *vsi-name* [**vc-id** *vc-id* **peer** *ip-address*]	
2	Raisecom#**show mac-address** { **all** | **static** | **dynamic** } [**vlan** *vlan-id*] [*interface-type interface-number*]	Show MAC address entries.

No.	Command	Description
	Raisecom#**show mac-address** { **all** | **static** | **dynamic** } **vsi** *vsi-name* [*interface-type interface-number*]	
	Raisecom#**show mac-address** { **all** | **static** | **dynamic** } **vsi** *vsi-name* [**vc-id** *vc-id* **peer** *ip-address*]	
	Raisecom#**show mac-address** *mac-address* [**vlan** *vlan-id* | **vsi** *vsi-name*]	
	Raisecom#**show mac-address blackhole** [**vlan** *vlan-id* | **vsi** *vsi-name*]	
3	Raisecom#**show mac-address learning vlan**	Show automatic learning status of the MAC address table.
	Raisecom#**show mac-address learning** [*interface-type interface-number*]	
4	Raisecom#**show mac-address multicast** [**vlan** *vlan-id*] [**count**]	Show the L2 multicast table.

5.2.7 Maintenance

No.	Command	Description
1	Raisecom(config)#**clear mac-address dynamic**	Clear MAC addresses.
	Raisecom(config)#**clear mac-address dynamic** [**vlan** *vlan-id*] [*interface-type interface-number*]	
	Raisecom(config)#**clear mac-address dynamic vsi** *vsi-name* [*interface-type interface-number*]	
	Raisecom(config)#**clear mac-address dynamic vsi** *vsi-name* [**vc-id** *vc-id* **peer** *ip-address*]	
	Raisecom(config)#**clear mac-address dynamic** *mac-address* [**vlan** *vlan-id* | **vsi** *vsi-name*]	

5.3 Configuring QinQ

5.3.1 Preparing for configurations

Scenario

With basic QinQ, you can add outer VLAN Tag and freely plan your own private VLAN ID. Therefore, the data between devices on both ends of the Internet Service Provider (ISP) network can be transparently transmitted, without conflicting with the VLAN ID in the ISP network.

QinQ-based VLAN mapping can meet the following conditions:

- N:1 VLAN mapping
- Single-to-double VLAN mapping

- 2:2 VLAN mapping
- Double-to-single VLAN mapping
- Untagged packets can be converted into single VLAN or double VLAN

Prerequisite

- Connect interfaces and configure physical parameters of interfaces. Make the physical layer Up.
- Create a VLAN.

5.3.2 Configuring basic QinQ

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**portswitch**	Enter Layer 2 interface configuration mode.
3	Raisecom(config-port)#**dot1q-tunnel**	Enable basic QinQ on the interface.
4	Raisecom(config-port)#**dot1q-tunnel cos override**	Enable CoS priority overriding on the interface.
5	Raisecom(config-port)#switchport **reject-frame** { **tagged** | **untagged** }	Configure the type of packets denied by the interface.

Note

When using the basic QinQ function of an interface, you must configure the interface attributes of the interface, that is, specify the interface type as Access or Trunk, and configure the default VLAN of the interface.

5.3.3 Configuring selective QinQ

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**portswitch**	Enter Layer 2 interface configuration mode.
3	Raisecom(config-port)#**switchport vlan-mapping-miss discard**	Configure the interface to discard tagged messages that cannot match selective QinQ or VLAN translation rules.

Step	Command	Description
4	Raisecom(config-port)#**switchport vlan-mapping both priority-tagged** [**cos** *cos-value*] **add-outer** *outer-vlan-id* [**cos** *cos-value*] [**remove** | **translate** *vlan-id*]	Add SVLAN to the packet configuration matching the specified priority, you can specify the CoS value of SVLAN, and you can modify or remove CVLAN at the same time.
5	Raisecom(config-port)#**switchport vlan-mapping both cvlan** *custom-vlan-id* [**cos** *cos-value*] **add-outer** *outer-vlan-id* [**cos** *cos-value*] { **remove** | **translate** *vlan-id* }	Add SVLAN to the packet configuration matching CVLAN+CoS, you can specify the SVLAN CoS value, and you can modify or remove CVLAN at the same time.
6	Raisecom(config-port)#**switchport vlan-mapping both inner** *inner-vlan-list* **add-outer** *outer-vlan-id* [**cos** *cos-value*]	Add SVLAN based on CVLAN list configuration, you can add the specified SVLAN CoS value.
7	Raisecom(config-port)#**switchport qinq default-cvlan** *vlan-id*	Configure the default CVLAN for the interface.
	Raisecom(config-port)#**switchport vlan-mapping both untag add-outer** *outer-vlan-id* [**cos** *cos-value*]	Add SVLAN based on default CVLAN. You can add the specified SVLAN CoS value.
8	Raisecom(config-port)#**switchport vlan-mapping both outer** *outer-vlan-id* **inner** *inner-vlan-id* **translate outer** *outer-vlan-id* **inner** *inner-vlan-id* [**cos** *cos-value*]	Configure VLAN mapping rules based on SVLAN and CVLAN, and add the specified SVLAN CoS value.
9	Raisecom(config-port)#**switchport vlan-mapping both outer** *outer-vlan-id* **translate** *outer-vlan-id* [**cos** *cos-value*]	Configure VLAN mapping rules based on SVLAN, and add the specified SVLAN CoS value.
10	Raisecom(config-port)#**switchport vlan-mapping both** *vlan-list* **translate** *vlan-id*	Configure N:1 VLAN mapping rules.

5.3.4 Checking configurations

No.	Command	Description
1	Raisecom#**show dot1q-tunnel** [**interface** *interface-type interface-number*]	Show configurations of basic QinQ.
2	Raisecom#**show vlan-mapping both interface** *interface-type interface-number*	Show VLAN mapping rules on the interface.

5.4 Configuring LLDP

5.4.1 Preparing for configurations

Scenario

When you obtain connection information between devices through the NView NNM system for topology discovery, you need to enable LLDP on the RAX721-A. Therefore, the RAX721-A can notify its information to the neighbors mutually, and store neighbor information to facilitate the NView NNM system querying information.

Prerequisite

N/A

5.4.2 Enabling global LLDP

Caution

After global LLDP is disabled, you cannot re-enable it immediately. Global LLDP cannot be enabled unless the restart timer times out.

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

5.4.3 Enabling interface LLDP

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

5.4.4 Configuring LLDP basic functions

Caution

When configuring the delivery delay timer and the delivery period timer, set the value of the delivery delay timer to be smaller than or equal to one quarter of the value of the delivery period timer.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**lldp message-transmission interval** *second*	(Optional) configure the delivery period timer of the LLDP packet. By default, it is 30s.
3	Raisecom(config)#**lldp message-transmission delay** *second*	(Optional) configure the delivery delay timer of the LLDP packet. By default, it is 2s.
4	Raisecom(config)#**lldp message-transmission hold-multiplier** *coefficient*	(Optional) configure the aging coefficient of the LLDP packet. By default, it is 4.
5	Raisecom(config)#**lldp restart-delay** *second*	(Optional) configure the restart timer. After global LLDP is disabled, it cannot be enabled unless the restart timer times out. By default, it is 2s.

5.4.5 Configuring LLDP to send TLV packets

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**lldp tlv-select basic-tlv** { **all** | **port-description** | **system-capability** | **system-description** | **system-name** }	Configure the basic TLV packets which are allowed to be sent.
4	Raisecom(config-port)#**lldp tlv-select dot1-tlv** { **all** | **port-vlan-id** | **protocol-identity** | **vlan-name** [*vlan-id*] | **protocol-vlan-id** *vlan-id* }	Configure the 802.1 TLV packets which are allowed to be advertised.
5	Raisecom(config-port)#**lldp tlv-select dot3-tlv** { **all** | **link-aggregation** | **mac-physic** | **max-frame-size** | **power** }	Configure the 802.3 TLV packets which are allowed to be advertised.
6	Raisecom(config-port)#**lldp tlv-select med-tlv** { **all** | **apability** | **inventory** | **location-id** { **civic-address** *device-type country-code ca-type ca-value* | **elin-address** *tel-number* } | **network-policy** }	Configure the multimedia extended TLV packets which are allowed to be advertised.

5.4.6 Configuring LLDP Trap

When the network changes, you need to enable LLDP Trap to send topology update traps to the NView NNM system immediately.

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

Step	Command	Description
2	Raisecom(config)#**lldp trap-interval** *second*	(Optional) configure the LLDP Trap delivery period timer. By default, it is 5s.

Note

After enabled with LLDP Trap, the RAX721-A will send Traps after detecting aged neighbors, newly-added neighbors, and changed neighbor information.

5.4.7 Checking configurations

No.	Command	Description
1	Raisecom#**show lldp local config**	Show LLDP local configurations.
2	Raisecom#**show lldp local system-data** [*interface-type interface-number*]	Show LLDP local system information.
3	Raisecom#**show lldp remote** [*interface-type interface-number*] [**detail**]	Show LLDP neighbor information.
4	Raisecom#**show lldp statistic** [*interface-type interface-number*]	Show LLDP packet statistics.
5	Raisecom#**show lldp tlv-select** [*interface-type interface-number*]	Configure the selectable TLV packets sent by the interface.

5.5 Configuring loop detection

5.5.1 Preparing for configurations

Scenario

In the network, hosts or Layer 2 devices connected to access devices may form a loopback intentionally or involuntary. Enable loop detection on downlink interfaces of all access devices to avoid the network congestion generated by unlimited copies of data traffic. Once a loop is detected on a port, the interface will be blocked.

Prerequisite

Configure physical parameters on an interface and make the physical layer Up.

5.5.2 Configuring loop detection

Note

- Loop detection and STP are mutually exclusive. They cannot be enabled simultaneously.

- For directly connected devices, you cannot enable loop detection on both ends simultaneously. Otherwise, interfaces of these 2 devices are blocked.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**portswitch** Raisecom(config-port)#**mold l2**	Configure the interface to a switching interface or a Layer 3 interface working in L2 mode.
4	Raisecom(config-port)#**loopback-detection** [**pkt-vlan** { **untag** | *vlan-id* }] [**log-interval** *minutes*] [**hello-time** *second*] [**restore-time** *second*] [**action** { **block** | **trap-only** | **shutdown** }]	Enable loop detection on a required interface. You can simultaneously configure the VLAN of the transmitted packet (optional), hello period (optional), restore time (optional), and loopback action.
5	Raisecom(config-port)#**loopback-detection manual restore**	Manually release the interface blocked because of the detected loop.

5.5.3 Checking configurations

No.	Command	Description
1	Raisecom#**show loopback-detection** [*interface-type interface-list*] [**detail**]	Show configurations of loop detection on interfaces.

5.5.4 Maintenance

Command	Description
Raisecom(config)#**clear loopback-detection statistic** [*interface-type interface-list*]	Clear statistics of loop detection.

5.6 Configuring L2CP

5.6.1 Preparing for configurations

Scenario

You can configure the mode for process processing Layer 2 control packets of the customer network on the access device within MAN according to the services provided by carriers. This configuration is done on the network-side interface of the customer.

Prerequisite

N/A

5.6.2 Configuring L2CP to transparently transmit MAC address

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**l2cp-process tunnel destination-address** *mac-address*	(Optional) configure the MAC address of the transparently transmitted packets.
3	Raisecom(config)#**l2cp-process usr-define** *define-id* { **ethertype** *type-value* | **mac-address** *mac-address* [**ethertype** *type-value*] | **name** *name* }	(Optional) configure the customized parameters of the transparently transmitted packets.

5.6.3 Configuring L2CP profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**l2cp-process profile** *profile-number*	Create a L2CP profile and enter L2CP profile mode.
3	Raisecom(config-l2cp-profile)#**name** *string*	(Optional) add profile descriptions.
4	Raisecom(config-l2cp-profile)#**protocol** { **oam** | **stp** | **dot1x** | **lacp** | **lldp** | **cdp** | **vtp** | **pvst** |**all** } **action** { **tunnel** | **drop** | **peer** }	(Optional) configure the processing action for L2CP packets.
5	Raisecom(config-l2cp-profile)#**tunnel vlan** *vlan-id*	(Optional) configure the specified VLAN of transparent transmission.
6	Raisecom(config-l2cp-profile)# **port** *interface-type interface-number*	(Optional) configure the specified egress interface of transparent transmission.
7	Raisecom(config-l2cp-profile)#**tunnel type mac**	(Optional) configure the tunnel type of transparent transmission.
8	Raisecom(config-l2cp-profile)#**usr-define** *define-id* **action** { **tunnel** | **peer** | **drop** }	Configure the action type of user-defined protocols.

5.6.4 Applying L2CP profile to interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.

Step	Command	Description
3	Raisecom(config-port)# **l2cp-process profile** *profile-number*	Apply the L2CP profile to the interface.

5.6.5 Checking configurations

No.	Command	Description
1	Raisecom#**show l2cp-process profile** [*profile-number*]	Check the created L2CP profile.
2	Raisecom#**show l2cp-process** [*interface-type interface-number*]	Show L2CP-related configurations on the interface.
3	Raisecom#**show l2cp-process** [**tunnel statistics**] [*interface-type interface-number*]	Show L2CP packet statistics on the interface.

5.6.6 Maintenance

Command	Description
Raisecom(config)#**clear l2cp-process tunnel statistic** [*interface-type interface-number*]	Clear L2CP packet statistics on the interface.

5.7 Configuring STP

5.7.1 Preparing for configurations

Scenario

In a big LAN, multiple devices are concatenated for accessing each other among hosts. They need to be enabled with STP to avoid MAC address learning fault, and broadcast storm and network down caused by quick copy and transmission of data frame due to loops. STP calculation can block one interface in a broken loop and ensure that there is only one path from the data flow to the destination host, which is also the best path.

Prerequisite

Before configuring STP, you need to configure the physical parameters of the interface so that the physical layer status of the interface is Up.

5.7.2 Enabling STP

No.	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**	Enable STP.

5.7.3 Configuring STP parameters

Configure STP parameters for the RAX721-A as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**spanning-tree priority** *priority-value*	(Optional) configure the device priority.
3	Raisecom(config)#**spanning-tree root** { **primary** | **secondary** }	(Optional) configure the RAX721-A as the root or backup device.
4	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**spanning-tree priority** *priority-value* Raisecom(config-port)#**exit**	(Optional) configure the device interface priority.
5	Raisecom(config)#**spanning-tree hello-time** *value*	(Optional) configure the Hello Time.
6	Raisecom(config)#**spanning-tree transit-limit** *value*	(Optional) configure the maximum number of BPDU packets allowed to be sent within the Hello Time.
7	Raisecom(config)#**spanning-tree forward-delay** *value*	(Optional) configure the forward delay.
8	Raisecom(config)#**spanning-tree max-age** *value*	(Optional) configure the maximum age.

5.7.4 Checking configurations

No.	Command	Description
1	Raisecom#**show spanning-tree**	Show basic configurations of STP.
2	Raisecom#**show spanning-tree** *interface-type interface-number*	Show STP configurations on the interface.

5.7.5 Maintenance

Command	Description
`Raisecom(config-port)#spanning-tree clear statistics`	Clear statistics about interface spanning tree.

5.8 Configuring RSTP/MSTP

5.8.1 Preparing for configurations

Scenario

In big LAN or residential region aggregation, the aggregation devices form a ring for link backup, to avoid loops and meanwhile realize service load balancing. MSTP can select a different and unique forwarding path for each one or a group of VLANs.

Prerequisite

Configure interface physical parameters to make it Up.

5.8.2 Enabling MSTP

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`	Enable STP.

5.8.3 Configuring MST domain and its maximum number of hops

You can configure domain information about the RAX721-A when it is running in MSTP mode. The device MST domain is decided by domain name, VLAN mapping table and configuration of MSTP revision level. You can configure the current device in a specific MST domain through the following configurations.

MST domain scale is restricted by the maximum number of hops. Starting from the root bridge of spanning tree in the domain, the configuration message (BPDU) reduces 1 hop count every time it passes a device. The RAX721-A discards the configuration message whose number of hops is 0. The device exceeding the maximum number of hops cannot join spanning tree calculation, thus restricting the MST domain scale.

Configure MSTP domain and its maximum number of hops for the RAX721-A as below.

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

Step	Command	Description
2	Raisecom(config)#**spanning-tree region-configuration**	Enter MST domain configuration mode.
3	Raisecom(config-region)#**name** *name*	Configure MST domain name.
4	Raisecom(config-region)#**revision-level** *level-value*	Configure the revision level for MST domain. By default, it is 0.
5	Raisecom(config-region)#**instance** *instance-id* **vlan** *vlan-list* Raisecom(config-region)#**exit**	Configure mapping from the MST domain VLAN to the instance.
6	Raisecom(config)#**spanning-tree max-hops** *hops-value*	Configure the maximum number of hops for the MST domain.

Note

Only when the configured device is the domain root can the configured maximum number of hops be used as the maximum number of hops for MST domain; other non-domain root cannot be configured this item.

5.8.4 Configuring root/backup bridge

Two methods for MSTP root selection are as below:

- Configure the device priority to confirm STP root bridge or backup bridge though STP calculation.
- Assign the MSTP root directly with this command.

When the root bridge is faulty or powered off, the backup bridge can replace the root bridge and become a related instance. In this case, if a new root bridge is assigned, the backup bridge will not become the root bridge. If several backup bridges for a spanning tree are configured, when the root bridge stops working, MSTP will choose the backup root with the smallest MAC address as the new root bridge.

Caution

We do not recommend modifying the priority of any device on the network if you directly assign the root bridge; otherwise, the assigned root bridge or backup bridge may be invalid.

Configure root bridge or backup bridge for the RAX721-A 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 RAX721-A as the root bridge or backup bridge for a STP instance.

- You can confirm the effective instance of the root bridge or backup bridge through the **instance** *instance-id* command. The current device will be assigned as the root bridge or backup bridge of CIST if instance-id is 0 or parameter **instance** *instance-id* is omitted.
- The root types of the device in different instances are independent, that is, they not only can be the root bridge or the backup bridge of one instance, but also the root bridge or backup bridge of other spanning tree instances. However, in the same spanning tree instance, the same device cannot be used as the root bridge and backup bridge at the same time.
- You cannot assign two or more root bridges for one spanning tree instance, but can assign several backup bridges for one spanning tree. Generally, we recommend assigning one root bridge and several backup bridges for one spanning tree.

5.8.5 Configuring device interface and system priority

Whether the interface is selected as the root interface depends on the interface priority. Under the same condition, the interface with smaller priority will be selected as the root interface. An interface may have different priorities and play different roles in different instances.

The Bridge ID decides whether the RAX721-A can be selected as the root of the spanning tree. Configuring smaller priority helps obtain a smaller Bridge ID to achieve the goal of designating certain device as the root. If the priority of two RAX721-A devices are identical, the RAX721-A with smaller MAC address will be selected as the root.

Similar to configuring root and backup root, priority is independent in different instances. You can confirm the priority instance through the **instance** *instance-id* parameter. Configure the bridge priority for CIST if instance-id is 0 or the **instance** *instance-id* parameter is omitted.

Configure interface priority and system priority for the RAX721-A as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#spanning-tree [ instance` *instance-id* `] priority` *priority-value* `Raisecom(config-port)#exit`	Configure the interface priority for a STP instance.
4	`Raisecom(config)#spanning-tree [ instance` *instance-id* `] priority` *priority-value*	Configure the system priority for a STP instance.

The priority must be multiples of 4096, such as 0, 4096, and 8192. It is 32768 by default.

5.8.6 Configuring network diameter for switching network

The network diameter indicates the number of nodes on the path that has the most devices on a switching network. In MSTP, the network diameter is valid only to the CIST, and invalid to the MSTI instance. Regardless of the number of nodes in a path in one domain, it is considered as just one node. 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 MST domain is used to measure the domain scale, while the network diameter is a parameter to measure the whole network scale. The bigger the network diameter is, the bigger the network scale is.

Similar to the maximum number of hops of MST domain, only when the RAX721-A is configured as the CIST root device can this configuration take effect. MSTP will automatically configure the Hello Time, Forward Delay and Max Age parameters to a privileged value through calculation when you configure the network diameter.

Configure the network diameter for the switching network as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#spanning-tree bridge-diameter` *bridge-diameter-value*	Configure the network diameter for the switching network.

5.8.7 Configuring internal path cost of interfaces

When selecting the root interface and designated interface, the smaller the interface path cost is, the easier it is to be selected as the root interface or designated interface. Inner path costs of interface are independent in different instances. You can configure the internal path cost for an instance through the **instance** *instance-id* parameter. Configure the internal path cost of the interface for the CIST if instance-id is 0 or the **instance** *instance-id* parameter is omitted.

By default, interface cost often depends on the physical features:

- 10 Mbit/s: 2000000
- 100 Mbit/s: 200000
- 1000 Mbit/s: 20000
- 10 Gbit/s: 2000

Configure the internal path cost for the RAX721-A as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#spanning-tree [ instance` *instance-id* `] inter-path-cost` *cost-value*	Configure the internal path cost of the interface.

5.8.8 Configuring external path cost of interfaces

The external path cost is the cost from the device to the CIST root, which is equal in the same domain.

Configure the external path cost for the RAX721-A as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#spanning-tree extern-path-cost` *cost-value*	Configure the external path cost of interfaces.

5.8.9 Configuring maximum transmission rate on interface

The maximum transmission rate on an interface means the maximum number of transmitted BPDUs allowed by MSTP in each Hello Time. This parameter is a relative value and of no unit. The greater the parameter is configured, the more packets are allowed to be transmitted in a Hello Time, the more device resources it takes up. Similar with the time parameter, only the configurations on the root device can take effect.

Configure maximum transmission rate on the interface for the RAX721-A as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#spanning-tree transit-limit` *value*	Configure the maximum transmission rate on the interface.

5.8.10 Configuring MSTP timer

- Hello Time: the interval for the RAX721-A to send BPDUs. It is used to detect whether a link fails on the RAX721-A. The RAX721-A sends hello packets to other devices around in Hello Time to check if there is fault in the link. The default value is 2s. You can adjust the interval value according to network condition. You can reduce the interval when network link changes frequently to enhance the stability of STP. However, increasing the interval reduces CPU utilization rate for STP.
- Forward Delay: the time parameter to ensure the safe transit of device status. Link fault causes the network to recalculate spanning tree, but the new configuration message recalculated cannot be transmitted to the whole network immediately. There may be temporary loop if the new root interface and designated interface start transmitting data at once. This protocol adopts a status migration system: before the root interface and designated interface start forwarding data, it needs a medium status (learning status); after a Forward Delay, it enters forwarding status. The delay guarantees the new configuration message to be transmitted through the whole network. You can adjust the delay according to actual condition. That is, you can reduce it when the network topology changes infrequently and increase it under opposite conditions.

- Max Age: the bridge configurations used by STP have a life time that is used to judge whether the configurations are outdated. The RAX721-A will discard outdated configurations and STP will recalculate spanning tree. The default value is 20s. if the value is too small, it may cause frequent recalculation of the spanning tree. If the value is too larger, it will make STP unable to adapt to the network topology change timely.

All devices in the entire switching network use the three time parameters on the CIST root device, so only the configuration on the root device takes effect.

Configure the MSTP timer for the RAX721-A as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**spanning-tree hello-time** *value*	Configure the Hello Time.
3	Raisecom(config)#**spanning-tree forward-delay** *value*	Configure the Forward Delay.
4	Raisecom(config)#**spanning-tree max-age** *value*	Configure the Max Age.

5.8.11 Configuring edge interface

The edge interface indicates that the interface neither directly connects to any devices nor indirectly connects to any device via the network where the interface is located.

If you configure the interface to an edge interface, its status can change into the forwarding status quickly without any waiting time. You can configure the Ethernet interface connected to the user client as an edge interface to fast change into the forwarding status.

When an interface is configured to edge interface auto detection (auto), the attributes of the edge interface are determined by the actual situation. When an interface is configured to an edge interface (force-true), the actual operating value of the interface becomes a non-edge interface after receiving the BPDU. When an interface is configured to a non-edge interface (force-false), similarly, regardless of whether it is an edge or non-edge interface, the interface will remain a non-edge interface until the configuration changes.

By default, all interfaces on the RAX721-A are configured in auto-detection attribute.

Configure the edge interface for the RAX721-A as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**spanning-tree edged-port** { **auto** | **force-true** | **force-false** }	Configure attributes of the edge interface.

5.8.12 Configuring link type

Two interfaces connected by a point-to-point link can quickly transit to the forwarding status by transmitting synchronization packets. By default, MSTP configures the link type of

interfaces according to duplex mode. The full duplex interface is considered as the point-to-point link, and the half duplex interface is considered as the shared link.

You can manually configure the current Ethernet interface to connect to a point-to-point link, but the system will fail if the link is not point to point. Generally, we recommend configuring this item to auto status and the system will automatically detect whether the interface is connected to a point-to-point link.

Configure the link type for the RAX721-A as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#spanning-tree link-type { auto | point-to-point | shared }`	Configure the link type for the interface.

5.8.13 Configuring root interface protection

The bridge will re-elect a root interface when it receives a packet with higher priority, which influents network connectivity and also consumes CPU resources. For the MSTP network, if someone sends BPDUs with higher priority, the network may become unstable for the continuous election.

Generally, the priority of each bridge has already been configured in network planning phase. The nearer a bridge is to the edge, the lower the bridge priority is. Therefore, the downlink interface cannot receive the packets with priority higher than that of the bridge unless someone maliciously attacks. For these interfaces, you can enable rootguard to refuse to process packets with priority higher than bridge priority and block the interface for a period to prevent damaging the upper layer link by other attacks from attacking sources.

Configure root interface protection for the RAX721-A as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#spanning-tree rootguard { enable | disable }`	Configure root interface protection.

5.8.14 Configuring interface loopguard

The spanning tree has two functions: loopguard and link backup. Loopguard requires carving up the network topology into tree structure. There must be redundant links in the topology if link backup is required. Spanning tree can avoid loops by blocking the redundant link and enable link backup function by opening redundant links when the link breaks down.

The spanning tree module exchanges packets periodically, and it is considered that the link fails if it has not received a packet in a period. It will then select a new link and enable the

backup interface. In actual networking, the cause to failure in receiving packets may not be the link fault. In this case, enabling the backup interface may generate loops.

Loopguard is used to keep the original interface status when it cannot receive packet in a period.

Loopguard conflicts with link backup. That is, loopguard is implemented at the cost of disabling link backup.

Configure interface loop protection for the RAX721-A as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**spanning-tree loopguard** { **enable** | **disable** }	Configure interface loopguard attributes.

5.8.15 Executing mcheck operation

Interface on the MSTP device has two working modes: STP compatible mode and MSTP mode. Suppose the interface of the MSTP device in a switch network is connected to the RAX721-A running STP, the interface will change to work in STP compatible mode automatically. The interface cannot change to work in MSTP mode if the RAX721-A running STP is removed, but the interface still works in STP compatible mode. You can execute the mcheck operation to force the interface to work in MSTP mode. If the interface receives new STP packets again, it will return to STP compatible mode.

Execute mcheck operation for the RAX721-A as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**spanning-tree mcheck**	Execute the mcheck operation to force the interface back to the MSTP mode.

5.8.16 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show spanning-tree**	Show basic configurations of STP.

No.	Command	Description
2	Raisecom#**show spanning-tree** [**instance** *instance-id*] **port-list** *port-list* [**detail**]	Show configurations of spanning tree on the interface.
3	Raisecom#**show spanning-tree region-operation**	Show configurations of the MST domain.

5.9 Configuring MRSTP

5.9.1 Preparing for configurations

Scenario

When device A connects upstream to device B, if device B has a higher priority, it will be elected as the root bridge. However, if device A is connected downstream to multiple ring networks and only STP/RSTP can run in the ring network. At this time, device A is expected to be designated as the root bridge of multiple ring network devices, all traffic is forwarded through device A, while device A can still select device B as the root bridge.

Prerequisite

N/A

5.9.2 Enabling MRSTP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**spanning-tree enable**	Enable global STP.
3	Raisecom(config)#**spanning-treemode mrstp**	Configure the spanning tree operation mode to MRSTP.
4	Raisecom(config)#**spanning-tree mrstp** *pro-id*	Create a MRSTP process.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode or aggregation group interface configuration mode.
6	Raisecom(config-port)#**spanning-tree mrstp** *pro-id*	Bind the interface to the specified process.

5.9.3 Configuring MRSTP parameter

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

Step	Command	Description
2	Raisecom(config)#**spanning-tree mrstp** *pro-id* **priority** *priority*	(Optional) configure priority of the specified process.
3	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**spanning-tree priority** *priority-value*	(Optional) configure the device interface priority.
4	Raisecom(config)#**spanning-tree hello-time** *value*	(Optional) configure the value of HelloTime.
5	Raisecom(config)#**spanning-tree transit-limit** *value*	(Optional) configure the maximum number of BPDU packets allowed to be sent within the Hello Time.
6	Raisecom(config)#**spanning-tree forward-delay** *value*	(Optional) configure the value of Forward Delay.
7	Raisecom(config)#**spanning-tree max-age** *value*	(Optional) configure the MaxAge.

5.9.4 Checking configurations

No.	Command	Description
1	Raisecom#**show spanning-tree mrstp** *pro-id*	Show basic information about MRSTP.

5.10 Configuring Super VLAN

5.10.1 Preparing for configurations

Scenario

With super VLAN, hosts that are connected to the same switch but belong to different VLANs can communicate on Layer 3 by using the IP address of Layer 3 interface of the super VLAN as the default gateway.

Prerequisite

- After being configured, the super VLAN cannot contain any member interfaces. If a VLAN has member interfaces, it cannot be configured with attributes of super VLAN.
- Create a VLAN to be added to the super VLAN, and activate it. If the physical interface is taken as a Layer 3 interface by default, configure it as a Layer 2 interface.

5.10.2 Configuring Super VLAN

Configure the super VLAN for the RAX721-A as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**create vlan** *vlan-id* **active** Raisecom(config)#**vlan** *vlan-id*	Create a VLAN, and enter VLAN configuration mode.
3	Raisecom(config-vlan)#**supervlan**	Configure the VLAN as a super VLAN.
4	Raisecom(config-vlan)#**subvlan** [**add** | **remove**] *subvlan-list*	Configure sub-VLANs of the super VLAN.
5	Raisecom(config-vlan)#**exit**	Exit VLAN configuration mode.
6	Raisecom(config)#**interface vlan** *vlan-id*	Enter VLAN interface configuration mode.
7	Raisecom(config-vlan)#**arp local-proxy enable**	Enable local ARP proxy of the super VLAN.

Note

- After the interface of the super VLAN is configured, configure its IP address. The VLAN belonging to the super VLAN is a sub-VLAN.
- After being configured as a super VLAN, a VLAN cannot be configured with the VLAN interface and IP address.

5.10.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show supervlan** [*vlan-list*]	Show configurations of super VLAN and sub-VLANs.
2	Raisecom#**show ip interface brief**	Show configurations of the IP address of the super VLAN.

5.11 Configuring PVLAN

5.11.1 Preparing for configurations

Scenario

PVLAN, used on an enterprise Intranet, allows devices inside the PVLAN to communicate with the default gateway only rather than the Intranet.

Prerequisite

- Create a static VLAN
- Activate it.

5.11.2 Configuring PVLAN type

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**private-vlan** { **primary vlan** *vlan-id* | **isolated vlan** *vlan-id* | **community vlan** *vlan-list* }	Configure the PVLAN type.

Caution

- Up to 32 primary VLANs and 2048 secondary VLANs are allowed.
- If the VLAN is associated, its PVLAN type cannot be modified nor deleted.

5.11.3 Configuring PVLAN association

Configure PVLAN association for the RAX721-A as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**private-vlan** { **primary vlan** *vlan-id* | **isolated vlan** *vlan-id* | **community vlan** *vlan-list* }	Configure the PVLAN type.
3	Raisecom(config)#**private-vlan association** *primary-vlan-id* [**add** | **remove**] *secondary-vlan-list*	Associate the primary VLAN and secondary VLANs. You can use the **no private-vlan association** *primary-vlan-id* command to delete the association between the primary VLAN and secondary VLANs under the specified primary VLAN.

Caution

- Before configuring VLAN association, create a VLAN and activate it, configure the PVLAN type, configure the primary VLAN and secondary VLANs, and choose the correct association type. Otherwise, VLAN association cannot be configured.
- The primary VLAN and secondary VLANs cannot be configured to the default VLAN. If VLAN2 is a cluster VLAN, it cannot be configured to PVLAN.
- A secondary VLAN can be added to only one PVLAN.
- A primary VLAN can be associated with only one isolated VLAN, or up to 64 secondary VLANs.

5.11.4 Configuring PVLAN mode on interface

The VLAN of the RAX721-A supports Access interface mode and Trunk interface mode, and the PVLAN supports promiscuous interface mode and host interface mode.

Caution

- The promiscuous interface mode and host interface mode support configuring association or mapping under the condition that PVLAN association or mapping already exists, otherwise the configuration will fail.
- When an interface is configured to the host interface mode or promiscuous interface mode without being associated with or mapped into a primary VLAN or secondary VLAN, the interface only allows untagged packets to enter.
- IGMP runs on the primary VLAN only. The VLANs that the data flow passes in the uplink and downlink of the PVLAN are different, so you cannot configure IGMP Snooping to implement multicast. Instead, you need to configure IGMP MVR.

Configure the PVLAN mode on the interface for the RAX721-A as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical interface configuration mode.
3	Raisecom(config-tengigabitethernet1/1/*)#**switchport mode private-vlan** { **host**| **promiscuous** }	Configure the PVLAN mode on the interface.
4	Raisecom(config-tengigabitethernet1/1/*)#**exit**	Return to global configuration mode.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
6	Raisecom(config-tengigabitethernet1/1/*)#s**witchport private-vlan host-association** *primary-vlan-id secondary-vlan-id*	Associate the primary VLAN and secondary VLANs on the host interface. You can use the **no switchport private-vlan host-association** command to delete the association between the primary VLAN and secondary VLANs on the host interface.
7	Raisecom(config-tengigabitethernet1/1/*)#**switchport private-vlan mapping** *primary-vlan-id* [**add** | **remove**] *secondary-vlan-list*	Associate the primary VLAN and secondary VLANs on the promiscuous interface. You can use the **no switchport private-vlan mapping** command to delete the association between the primary VLAN and secondary VLANs on the promiscuous interface.

5.11.5 Checking configuration

No.	Command	Description
1	Raisecom#**show vlan private-vlan**	Show PVLAN configurations.
2	Raisecom#**show switchport interface** *interface-type interface-number*	Show configurations of interface VLAN attributes.
3	Raisecom#**show vlan** [*vlan-list* | **static** | **dynamic**] [**detail**]	Show configurations of VLAN attributes.

5.12 Configuring GARP/GVRP

5.12.1 Configuring GARP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-num*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**garp timer** { **join** | **leave** | **leaveall** } *time-value*	Configure the GARP timer.

Caution

- The value of the Join timer must be less than half the value of the Leave timer.
- The value of the Leave timer must be greater than 2 times the value of theJoin timer and less than the value of the LeaveAll timer.
- The value of the LeaveAll timer must be greater than that of the Leave timer.
- In actual networking, we recommend that the values of the Join timer, Leave timer, and LeaveAll timer be 3000, 15000, and 20000 (in units of 10ms).

5.12.2 Configuring GVRP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**gvrp enable**	Enable global GVRP.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#**switchport mode trunk**	Configure the interface to Trunk mode.
5	Raisecom(config-port)#**gvrp registration** { **fixed** | **forbidden** | **normal** }	(Optional) configure the GVRP registration mode.

Step	Command	Description
6	Raisecom(config-port)#**gvrp enable**	Enable interface GVRP.

Caution

- You must configure the interface to Trunk mode before enabling interface GVRP.
- We do not recommend enabling GVRP on the member interfaces of the aggregation group.

5.12.3 Checking configurations

No.	Command	Description
1	Raisecom#**show garp** [*interface-type interface-number*]	Show configurations of the GARP timer.
2	Raisecom# **show garp** [*interface-type interface-number*] **statistics**	Show GARP statistics.
3	Raisecom#**show gvrp** [*interface-type interface-number*]	Show GVRP configurations.
4	Raisecom#**show gvrp** [*interface-type interface-number*] **statistics**	Show GVRP statistics.
5	Raisecom#**show gvrp local-vlan** *interface-type interface-number*	Show the local VLAN of GVRP.

5.12.4 Maintenance

Command	Description
Raisecom(config)#**clear gvrp** [*interface-type interface-number*] **statistics**	Clear GVRP statistics.

5.13 Configuring port security MAC

5.13.1 Configuring basic functions of port security MAC

Caution

- We do not recommend enabling port security MAC on member interfaces of the LAG.
- We do not recommend using the MAC address management function to configure static MAC addresses when port security MAC is enabled on the same interface.
- When the 802.1x interface adopts a MAC address-based authentication mode, port security MAC conflicts with 802.1x. We do not recommend configuring them concurrently.

- Port security MAC conflicts with interface/interface+VLAN-based MAC address limit. We do not recommend configuring them concurrently.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**switchport port-security**	Enable port security MAC.
4	Raisecom(config-port)#**switchport port-security maximum** *maximum*	(Optional) configure the maximum number of secure MAC addresses.
5	Raisecom(config-port)#**switchport port-security violation** { **protect** | **restrict** | **shutdown** }	(Optional) configure the port security MAC violation mode.
6	Raisecom(config-port)#**no port-security shutdown** Raisecom(config-port)#**exit**	(Optional) re-enable the interface which is shut down due to violating port security MAC.
7	Raisecom(config)#**port-security recovery-time** *second*	(Optional) configure the restoration time of port security MAC.

Note

- When the secure MAC violation policy is Shutdown, you can use this command to re-enable this interface which is shut down due to violating port security MAC.
- When the interface is Up, the configured secure MAC violation mode will remain valid.

5.13.2 Configuring static secure MAC address

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/port)#**switchport port-security**	Enable port security MAC.
4	Raisecom(config-gigaethernet1/1/port)#**switchport port-security mac-address** *mac-address* **vlan** *vlan-id*	Configure the static secure MAC address.

5.13.3 Configuring dynamic secure MAC address

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

Step	Command	Description
2	Raisecom(config)#**port-security aging-time** *period*	(Optional) configure the aging time of dynamic secure MAC addresses.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical interface configuration mode.
4	Raisecom(config-port)#**switchport port-security aging-type** { **absolute** | **inactivity** }	(Optional) configure the aging type of secure MAC addresses.
5	Raisecom(config-port)#**switchport port-security**	(Optional) enable port dynamic security MAC learning.
6	Raisecom(config-port)#**switchport port-security trap enable**	(Optional) enable port security MAC Trap.
7	Raisecom(config-port)#**switchport port-security trap period** *value*	(Optional) configure the period for sending Traps for port security MAC.

Note

The **switchport port-security** command can enable port security MAC and dynamic secure MAC learning at the same time.

5.13.4 Configuring sticky secure MAC address on interface

Caution

We do not recommend configuring sticky secure MAC addresses when port sticky security MAC is disabled. Otherwise, port Sticky security MAC may be abnormal.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/port)#**switchport port-security**	Enable port security MAC.
4	Raisecom(config-gigaethernet1/1/port)#**switchport port-security mac-address sticky**	Enable sticky secure MAC learning.
5	Raisecom(config-gigaethernet1/1/port)#**switchport port-security mac-address sticky** *mac-address* **vlan** *vlan-id*	(Optional) manually configure sticky secure MAC addresses.

Note

After sticky secure MAC address learning is enabled, dynamic secure MAC addresses will be converted into sticky secure MAC addresses; manually configured sticky secure MAC addresses will take effect.

5.13.5 Checking configurations

No.	Command	Description
1	Raisecom#**show port-security** [*interface-type interface-list*]	Show configurations of port security MAC.
2	Raisecom#**show port-security mac-address** [*interface-type interface-list*]	Show configurations of secure MAC address and secure MAC address learning.

5.13.6 Maintenance

Command	Description
Raisecom(config-gigaethernet1/1/port)#**clear port-security** { **all** | **configured** | **dynamic** | **sticky** }	Clear the secure MAC address of a specified type on a specified interface.

6 Clock synchronization

This chapter describes principles and configuration procedures of clock synchronization, as well as related configuration examples, including the following sections:

- Configuring PTP-based clock synchronization

6.1 Configuring PTP-based clock synchronization

6.1.1 Preparing for configurations

Scenario

Synchronous Ethernet only supports frequency synchronization instead of clock synchronization. However, mobile communication networks and power markets have strict requirements on the accuracy of clock synchronization. Therefore, PTP is adopted for time synchronization over the full-mesh network.

The RAX721-A only supports 1588 TC.

Prerequisite

N/A

6.1.2 Configuring PTP clock modes

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ptp enable`	Enable global PTP. By default, global PTP is disabled.
3	`Raisecom(config)#interface` *`interface-type interface-number`*	Enter the switch interface configuration mode.
4	`Raisecom(config-port)#portswitch`	Configure the interface to switch mode.

Step	Command	Description
5	Raisecom(config-port)#**switchport access vlan** *vlan-id*	Configure the interface VLAN.
6	Raisecom(config-port)#**ptp enable**	Enable PTP on the interface. By default, PTP on all interfaces is disabled.

6.1.3 Checking configurations

No.	Command	Description
1	Raisecom#**show ptp**	Show PTP information.

7 IP services

This chapter describes principles and configuration procedures of IP services, including following sections:

- Configuring IPv4
- Configuring IPv6
- Configuring ARP
- Configuring NDP
- Configuring ICMP
- Configuring VRF
- Configuring fault detection
- Configuring DHCPv4 Server
- Configuring DHCPv6 server
- Configuring DHCPv4 Client
- Configuring DHCPv6 client
- Configuring DHCPv4 Relay
- Configuring DHCPv6 relay
- Configuring DHCPv4 Snooping
- Configuring DHCPv6 Snooping
- Configuring DHCPv4/DHCPv6 Option

7.1 Configuring IPv4

7.1.1 Preparing for configurations

Scenario

Before configuring the IPv4 services, you need to configure the IPv4 address and the MTU on the interface.

Prerequisite

N/A

7.1.2 Configuring IPv4 address on interface

No.	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
	Raisecom(config-port)#**no portswitch**	Switch the interface to Layer 3 router mode.
3	Raisecom(config-port)#**ip address** *ip-address* [*ip-mask*] [**sub**]	Configure the IPv4 address of the interface. The interface type includes the Ethernet physical interface, Loopback interface, and VLAN interface.
4	Raisecom(config-port)#**ip address unnumbered** *interface-type interface-number*	(Optional) configure the interface to borrow the IP address of other interfaces.
5	Raisecom(config-port)#**mtu** *max-frame-length*	Configure the maximum transmission unit of the interface.

7.1.3 Configuring IPv4 PMTU

No.	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv4 pathmtu** *ip-address value*	Configure static PMTU entries.
3	Raisecom(config)#**ipv4 pathmtu enable**	Enable the IPv4 PMTU.
4	Raisecom(config)#**ipv4 pathmtu age** *age-time*	Configure the aging time of dynamic PMTU entries.

7.1.4 Checking configurations

No.	Command	Description
1	Raisecom#**show ip interface brief**	Show IP address configurations of the L3 interface.
2	Raisecom#**show ipv4 pathmtu** { *ip-address* | **all** | **dynamic** | **static** }	Show IPv4 PMTU configurations.

7.2 Configuring IPv6

7.2.1 Preparing for configurations

Scenario

With the rapid development of the network, IPv4 shows deficiencies gradually, and IPv6 has more advantages than IPv4. For example, IPv6 has a huge amount of address space, highly flexible message format, efficient routing and forwarding efficiency and so on. IPv6 can not only solve the problem of network address resource limitation, but also solve the problem of limited access to the Internet by various access devices.

Prerequisite

N/A

7.2.2 Configuring IPv6 address on interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
	Raisecom(config-port)#**no portswitch**	Switch the interface to Layer 3 router mode.
3	Raisecom(config-port)#**ipv6 address** *ipv6-address/prefix-length* [**eui-64**]	Configure the IPv6 address of the interface.
4	Raisecom(config-port)#**ipv6 address** *ipv6-address* **link-local**	Configure the IPv6 local link address of the interface.
5	Raisecom(config-port)#**ipv6 address auto**	Enable automatic configuration of IPv6 stateless address in interface mode.

7.2.3 Configuring IPv6 PMTU

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 pathmtu** *ipv6-address value*	Configure static PMTU entries.
3	Raisecom(config)#**ipv6 pathmtu enable**	Enable IPv6 PMTU.
4	Raisecom(config)#**ipv6 pathmtu age** *age-time*	Configure the aging time of dynamic PMTU entries.

7.2.4 Checking configurations

Step	Command	Description
1	Raisecom#**show ipv6 interface brief** [*interface-type interface-number*]	Show IPv6 address configurations of the L3 interface.
2	Raisecom#**show ipv6 address auto**	Show information about the IPv6 address prefix.
3	Raisecom#**show ipv6 pathmtu** { **all** | **dynamic** | **static** |*ipv6-address* }	Show information about the PMTU configured.

7.3 Configuring ARP

7.3.1 Preparing for configurations

Scenario

ARP is a protocol for resolving the IP address into Ethernet MAC address (or physical address).

Prerequisite

Configure the interface IPv4 address.

7.3.2 Configuring static ARP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**arp** *ip-address mac-address* [**vrf** *vrf-name*]	Configure static ARP.

7.3.3 Configuring dynamic ARP

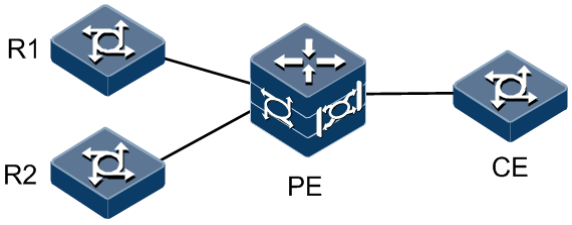
Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**arp mode** { **learn-all** | **learn-reply-only** }	Configure the ARP mode. By default, it learns the MAC address of all hosts.
3	Raisecom(config)#**arp aging-time** *time*	(Optional) configure the aging time of dynamic ARP. By default, the aging time is 1200 seconds.

Step	Command	Description
4	Raisecom(config)#**interface** *interface-type interface-number*	Enter the interface configuration mode.
5	Raisecom(config-port)#**arp learning** [**strict**] **enable**	Enable dynamic ARP learning on the interface. By default, dynamic ARP learning on the interface is enabled.
6	Raisecom(config-port)#**arp max-learning-num** *number*	Configure the maximum number of ARP entries dynamically learned by the interface. By default, the number of ARP entries dynamically learned by the interface is 50000.
7	Raisecom(config-port)#**gratuitous-arp-learning** {**enable** | **disable** }	Configure gratuitous ARP learning on the interface. By default, it is enabled.

7.3.4 Configuring proxy ARP

As shown in Figure 7-1, the PE device is configured with interface isolation, and R1 and R2 cannot communicate directly. After proxy ARP is enabled on the PE, when R1 sends an ARP request to R2, the PE will, on behalf of R2, send an ARP reply message carrying its own MAC address and R2 IP address to R1.

Figure 7-1 Proxy ARP application scenario



Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter the interface configuration mode.
3	Raisecom(config-port)#**arp proxy enable**	Enable proxy ARP on the interface. By default, it is disabled.

7.3.5 Clearing ARP entries

Step	Command	Description
1	Raisecom(config)#**clear arp** [**vrf** *vrf-name*] [*ip-address* | **interface** *interface-type interface-number*] [**static**]	Clear ARP entries.

7.3.6 Checking configurations

No.	Command	Description
1	Raisecom#**show arp** [**vrf** *vrf-name*] [*ip-address* | **interface** *interface-type interface-number* | **static**]	Show ARP information.

7.4 Configuring NDP

7.4.1 Preparing for configurations

Scenario

IPv6 implements address resolution and obtains the device MAC address through Neighbor Discovery Protocol (NDP), and generates related routing information.

There are two ways for the NDP to resolve neighbor node IPv6 addresses into link layer addresses.

- By manually configuring static neighbor entries
- Through the Neighbor Solicitation (NS) message and Neighbor Announcement (NA) message

Prerequisite

Configure the interface IPv6 address.

7.4.2 Configuring static NDP entries

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 neighbor** *ipv6-address mac-address* [**vrf** *vrf-name*]	Configure static neighbor entries.

7.4.3 Configuring dynamic NDP entries

Configuring times of sending NS messages for detecting duplicated addresses

Configure times of sending NS messages for detecting duplicated addresses for the RAX721-A as below.

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

Step	Command	Description
2	Raisecom(config)#**ipv6 nd dad attempts** *value*	Configure times of sending NS messages for detecting duplicated addresses.

When the RAX721-A obtains an IPv6 address, it uses the duplicated address detection function to determine whether the IPv6 address is already used by another device. After sending NS messages for certain specified times and receiving no response, it determines that the IPv6 address is not duplicated and thus can be used.

Configuring maximum number of NDPs allowed to be learnt

Configure the maximum number of NDPs allowed to be learnt on the Layer 3 interface for the RAX721-A as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 neighbor max-learning-num** *number*	Configure the maximum number of NDPs allowed to be learnt.

Configuring aging time of dynamic NDP entries

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 neighbor aging-time** *aging-time*	Configure the aging time of dynamic NDP.

Configuring RA message

Router Advertisement (RA) messages are NDP messages that are periodically sent by the device or for responding to the Router Solicitation (RS) messages in real time.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical interface configuration mode.
3	Raisecom(config-port)#**ipv6 nd ra repression**	Enable RA repression. By default, RA suppression is enabled.

Step	Command	Description
4	Raisecom(config-port)#**ipv6 nd ra interval** *interval*	Configure the interval for advertising RA messages.
5	Raisecom(config-port)#**ipv6 nd ra advlinkmtu** *mtu-value*	Configure the MTU information carried in the RA message.
6	Raisecom(config-port)#**ipv6 nd ra prefix** *ipv6-prefix-address/prefix-length valid-lifetime preferred-lifetime* **[no-autoconfig] [off-link]**	Configure the prefix information carried in the RA message.
7	Raisecom(config-port)#**ipv6 nd ra router-lifetime** *lifetime*	Configure the lifetime of the router in the RA message.
8	Raisecom(config-port)#**ipv6 nd ra hop-limit** *hopsvalue*	Configure the hop limits in the RA message.
9	Raisecom(config-port)#**ipv6 nd ra reachable-time** *time*	Configure the peer reachable time in the RA message.
10	Raisecom(config-port)#**ipv6 nd ra retrans-timer** *value*	Configure the retransmission timer in the RA message.
11	Raisecom(config-port)#**ipv6 nd ra managed-config-flag**	Configure the management address configuration flag in the RA message.
12	Raisecom(config-port)#**ipv6 nd ra other-config-flag** Raisecom(config-port)#**exit**	Configure other configuration flags in the RA message.

7.4.4 Configuring proxy NDP

When a host on a network sends an NS request to another host on the same network segment but not on the same network, the other party will not receive the NS request message. In this case, a device with proxy enabled needs to respond to the request, namely, responding to the NA message. This process is called ND Proxy.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**ipv6 nd proxy** { **enable** | **disable** }	Enable or disable ordinary ND Proxy.

7.5 Configuring ICMP

7.5.1 Configuring IPv4 ICMP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv4 icmp** { **type** *type-value* **code** *code-value* | **name** *icmp-name* | **all** } **send**	Enable ICMPv4 packet sending.
3	Raisecom(config)#**ipv4 icmp send-rate bucket** *bucket-size* **ratelimit** *interval*	Configure the limit of the sending rate for ICMPv4 packets.
4	Raisecom(config)#**ipv4 icmp** { **type** *type-value* **code** *code-value* | **name** *icmp-name* | **all** } **receive**	Enable ICMPv4 packet receiving.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
6	Raisecom(config-port)#**ipv4 icmp address-unreachable send**	Enable the function of sending ICMPv4 packets when the IP address is unavailable.
7	Raisecom(config-port)#**ipv4 icmp port-unreachable send**	Enable the function of sending ICMPv4 packets when the interface is unavailable.

7.5.2 Configuring IPv6 ICMP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 icmp send-rate bucket** *bucket-size* **ratelimit** *interval*	Configure the bucket size and rate limit of sending ICMPv6 error packets.
3	Raisecom(config)#**ipv6 icmp** { **type** *type-value* **code** *icmpv6-code* | **name** *icmpv6-name* | **all** } **send**	Enable the function of sending ICMPv6 packets.
4	Raisecom(config)#**ipv6 icmp** { **type** *type-value* **code** *icmpv6-code* | **name** *icmpv6-name* | **all** } **receive**	Enable the function of receiving ICMPv6 packets.
5	Raisecom(config)#**ipv6 icmp redirect send**	Enable the function of ICMPv6 packet redirection sending.
6	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
7	Raisecom(config-port)#**ipv6 icmp address-unreachable send**	Enable the function of sending ICMPv6 packets when the IPv6 address is unavailable.
8	Raisecom(config-port)#**ipv6 icmp port-unreachable send**	Enable the function of sending ICMPv6 packets when the IPv6 interface is unavailable.

Step	Command	Description
9	Raisecom(config-port)#**ipv6 icmp hop-limit-exceeded send**	Enable the function of sending ICMPv6 packets when the number of hops exceeds the threshold.

7.6 Configuring VRF

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip vrf** *vrf-name*	Create a VRF and enter VRF configuration mode.
3	Raisecom(config-vrf)#**rd** *rd*	Configure the VRF RD.
4	Raisecom(config-vrf)#**route-target** [**export** | **import** | **both**] *rt*	Configure the VRF RT.
5	Raisecom(config-vrf)#**tunnel-policy** *policy-name*	(Optional) configure the VRF tunnel policy and enter tunnel policy configuration mode.
6	Raisecom(config-tunnelpolicy)#**tunnel select-seq** { **lsp** | **cr-lsp** } *	(Optional) configure the tunnel priority.

7.7 Configuring fault detection

7.7.1 PING

PING IPv4 network

Step	Command	Description
1	Raisecom#**ping** [**vrf** *vpn-instance-name*] *ip-address* [**count** *count*] [**size** *size*] [**waittime** *period*] [**source** *ip-address*] [**df-bit**]	Use the **ping** command to test the connectivity of the IPv4 network.

Note

The RAX721-A cannot perform other operations in the process of Ping. It can perform other operations only when Ping is finished or Ping is interrupted by pressing **Ctrl**+**C**.

PING IPv6 network

Step	Command	Description
1	Raisecom#**ping** [**vrf** *vpn-instance-name*] **ipv6** *ipv6-address* [**count** *count*] [**size** *size*] [**waittime** *period*] [**source** *ipv6-address*]	Use the **ping** command to test the connectivity of the IPv6 network.

7.7.2 Traceroute

Traceroute IPv4 network

The interface is configured with an IPv4 address.

Step	Command	Description
1	Raisecom#**traceroute** [**vrf** *vpn-instance-name*] *ip-address* [**firstttl** *fitst-ttl*] [**maxttl** *max-ttl*] [**port** *port-number*] [**waittime** *period*] [**count** *times*] [**size** *size*]	Use the **traceroute** command to test the IPv4 network connectivity and view nodes passed by the packet. By default, the initial TTL is configured to 1; the maximum TTL is configured to 30; the interface ID is configured to 33433; the timeout is configured to 3s; the number of detection packets is configured to 3.

Traceroute IPv6 network

Step	Command	Description
1	Raisecom#**traceroute** [**vrf** *vpn-instance-name*] **ipv6** *ipv6-address* [**firstttl** *fitst-ttl*] [**maxttl** *max-ttl*] [**port** *port-number*] [**waittime** *period*] [**count** *times*] [**size** *size*]	Use the **traceroute** command to test the IPv6 network connectivity and view nodes passed by the packet. By default, the initial TTL is configured to 1; the maximum TTL is configured to 30; the interface ID is configured to 33433; the timeout is configured to 3s; the number of detection packets is configured to 3.

7.8 Configuring DHCPv4 Server

7.8.1 Preparing for configurations

Scenario

When the RAX721-A works as the DHCP v4 server, the DHCP v4 client can obtain the IP address from the server.

Prerequisite

The RAX721-A is not enabled with DHCP v4 Client. In addition, the DHCP v4 server works in common DHCP v4 server mode.

7.8.2 Creating and configuring IPv4 address pool

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp server pool** *pool-name*	Create the IPv4 address pool and enter address pool configuration mode.
3	Raisecom(config-pool)#**address** *start-ip-address end-ip-address* **mask** { *mask* | *mask-length* }	Configure the range of the IPv4 address pool.
4	Raisecom(config-pool)#**lease expired** { *minute* | **infinite** }	Configure the lease of the IPv4 address pool.
5	Raisecom(config-pool)#**dns-server** *ip-address* [**secondary**]	Configure the DNS of the IPv4 address pool.
6	Raisecom(config-pool)#**gateway** *ip-address*	Configure the default gateway of the IPv4 address pool.
7	Raisecom(config-pool)#**option 60** *vendor-string*	Configure information carried by Option 60.
8	Raisecom(config-pool)#**option 43** [**sub-option** *option-id*] { **hex** | **ascii** } *string*	Configure the information carried by Option43.
9	Raisecom(config-pool)#**tftp-server** *ip-address*	Configure the TFTP server of the IPv4 address pool.
10	Raisecom(config-pool)#**trap server-ip** *ip-address*	Configure the Trap server of the IPv4 address pool.

7.8.3 Configuring DHCP v4 Server on interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
	Raisecom(config-port)#**no portswitch**	Switch the interface to Layer 3 router mode.
3	Raisecom(config-port)#**ip dhcp server**	Enable DHCP v4 Server.

7.8.4 Checking configurations

No.	Command	Description
1	Raisecom(config)#**show ip dhcp server**	Show DHCP server configurations.

No.	Command	Description
2	Raisecom(config)#**show ip dhcp server lease**	Show assigned IPv4 addresses and client information.
3	Raisecom(config)#**show ip dhcp server statistics**	Show packet statistics of the DHCP v4 server.
4	Raisecom(config)#**show ip dhcp static-bind**	Show DHCP v4 static lease information.
5	Raisecom(config)#**show ip server pool** [*pool-name*]	Show configurations of the DHCPv4 address pool.

7.9 Configuring DHCPv6 server

7.9.1 Enabling global DHCPv6 Server

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 dhcp server**	Enable global DHCPv6 Server.

7.9.2 Creating and configuring IPv6 address pool

To assign IPv6 addresses and network parameters to clients through DHCPv6 Server, an address pool must be created on the DHCPv6 Server.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 dhcp server pool** *pool-name*	Create an address pool for assigning addresses and enter address pool mode.
3	Raisecom(dhcp-pool)#**address prefix** *ipv6-address/prefix-length*	Configure the prefix of the address pool.
4	Raisecom(dhcp-pool)#**lifetime preferred-lifetime** { *preferred-minute* | **infinite** } **valid-lifetime** { *valid-minute* | **infinite** }	(Optional) configure the lease time of the address pool, including the preferred time and effective time.
5	Raisecom(dhcp-pool)#**dns-server** *ipv6-address*	(Optional) configure the DNS server address of the address pool.

7.9.3 Creating and configuring IPv6 prefix pool

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 dhcp server prefix-pool** *pool-name*	Create an address pool for assigning addresses and enter prefix address pool.
3	Raisecom(dhcp-prefix-pool)#**prefix-delegation** *ipv6-address/prefix-length*	Specify the address prefix of the IPv6 prefix pool.

7.9.4 Configuring DHCPv6 Server on interface

Only when DHCPv6 Server is enabled globally and on the interface, and the address pool is bound to the interface, can the interface receive and process the client's DHCPv6 request packets.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 dhcp server**	Enable global DHCPv6 Server.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical interface configuration mode or sub-interface configuration mode. By default, the interface is in router mode.
4	Raisecom(config-port)#**ipv6 dhcp server**	Enable DHCPv6 Server on the interface.
5	Raisecom(config-port)#**ipv6 dhcp server rapid-commit**	(Optional) enable rapid interaction on the interface.
6	Raisecom(config-port)#**ipv6 dhcp server pool** *pool-name*	Bind the address pool to the interface.
7	Raisecom(config-port)#**ipv6 dhcp server prefix-pool** *pool-name*	Bind the prefix pool to the interface.

7.9.5 Checking configurations

No.	Command	Description
1	Raisecom#**show ipv6 dhcp server**	Show DHCPv6 Server configurations.
2	Raisecom#**show ipv6 dhcp server pool** [*pool-name*]	Show configurations of the DHCPv6 Server address pool.
3	Raisecom#**show ipv6 dhcp server prefix-pool** [*pool-name*]	Show configurations of the DHCPv6 Server prefix pool.
4	Raisecom#**show ipv6 dhcp server binding**	Show information about the assigned IPv6 address and its clients.

No.	Command	Description
5	Raisecom#**show ipv6 dhcp pd server binding**	Show binding information about the DHCPv6 prefix entrusting server.

7.10 Configuring DHCPv4 Client

7.10.1 Preparing for configurations

Scenario

When working as the DHCPv4 client, the RAX721-A can obtain an IP address from the DHCPv4 server. You can use the IP address to manage the RAX721-A.

When IP addresses are assigned in a dynamic mode, the IP address assigned to the DHCPv4 client has a lease period. When the lease period expires, the DHCPv4 server will withdraw the IP address. If the DHCPv4 client wishes to continue to use the IP address, it needs to renew the IP address. If the lease period does not expire and the DHCPv4 client does not need to use the IP address, it can release the IP address.

Prerequisite

The RAX721-A is not enabled with DHCPv4 Server and works in common DHCP Client mode.

7.10.2 (Optional) configuring DHCPv4 client information

Note

Before enabling the DHCPv4 client on the Layer 3 interface to apply for the IP address, configure DHCPv4 client information.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 3 interface configuration mode.
3	Raisecom(config-port)#**ip dhcp client** { **class-id** *class-id* | **client-id** *client-id* | **hostname** *hostname* }	Configure DHCPv4 Option 60 client, including the type identifier, client identifier, and host name. This command only takes effect on the Layer 3 interface.

7.10.3 Configuring DHCPv4 Client on Layer 3 interface

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter Layer 3 interface configuration mode.
3	`Raisecom(config-port)#ip address dhcp [ server-ip` *ip-address* `]`	Configure DHCPv4 Client and specify the IP address of the DHCPv4 server. It means enabling the DHCPv4 client to apply for the IP address. The command is valid on the Layer 3 interface only.

7.10.4 Renewing or releasing IPv4 address

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter Layer 3 physical interface configuration mode.
3	`Raisecom(config-port)#ip dhcp client renew`	Renew the IPv4 address. This command takes effect only on Layer 3 interface.
4	`Raisecom(config-port)#no ip address dhcp`	Release the IPv4 address. This command takes effect only on Layer 3 interface.

7.10.5 Checking configurations

No.	Command	Description
1	`Raisecom#show ip dhcp client`	Show configurations of the DHCPv4 client.

7.11 Configuring DHCPv6 client

7.11.1 Configuring DHCPv6 client

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter Layer 3 physical interface configuration mode.

Step	Command	Description
3	Raisecom(config-port)#**ipv6 address dhcp** [**server-ip** *ipv6-address*]	Apply the IPv6 address through DHCPv6.
4	Raisecom(config-port)# **ipv6 dhcp client pd**	Configure the prefix address pool of the DHCPv6 client.
5	Raisecom(config-port)#**ipv6 dhcp client renew**	(Optional) renew the IP address. If the IP interface of the device has obtained an IP address through DHCP, the IP address will automatically renew when its lease time expires.
6	Raisecom(config-port)#**ipv6 dhcp client rapid-commit**	(Optional) enable the DHCPv6 Client to apply for fast interaction mode.
7	Raisecom(config-port)#**ipv6 dhcp client information-request**	(Optional) configure applying DNS, domain name, and other configurations through DHCPv6.

7.11.2 Checking configurations

No.	Command	Description
1	Raisecom#**show ipv6 dhcp client**	Show DHCPv6 Client configurations.

7.12 Configuring DHCPv4 Relay

7.12.1 Preparing for configurations

Scenario

When the RAX721-A works as the DHCPv4 relay, the DHCPv4 clients can communicate with DHCPv4 servers in other network segments through the DHCPv4 relay to obtain IP addresses. Therefore, DHCPv4 clients in different network segments can apply for IP addresses from the same DHCPv4 server. This facilitates saving costs and managing all devices together.

Prerequisite

The RAX721-A is not enabled with DHCPv4 Client or DHCPv4 Server.

7.12.2 Configuring global DHCPv4 Relay

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp relay**	Enable global DHCPv4 relay.

7.12.3 Configuring DHCPv4 relay on interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip dhcp relay**	Enable DHCPv4 Relay on the interface.
4	Raisecom(config-port)#**ip dhcp relay target-ip** *ip-address*	Configure the destination IP address for forwarding the packets.
5	Raisecom(config-port)#**ip dhcp relay relay-ip** *ip-address*	Configure the relay IP address and interface relay.

7.12.4 Configuring DHCPv4 relay Option 82

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp relay information option**	Configure DHCPv4 relay Option 82.
3	Raisecom(config)#**ip dhcp relay information policy** { **drop** | **keep** | **replace** }	Configure the processing policy for the DHCPv4 relay to process DHCP packet containing Option 82.
4	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
5	Raisecom(config-port)#**ip dhcp relay information trusted**	Configure DHCPv4 relay trusted interface.

7.12.5 Checking configurations

No.	Command	Description
1	Raisecom#**show ip dhcp relay**	Show configurations of DHCPv4 relay.
2	Raisecom#**show ip dhcp relay information**	Show DHCPv4 relay Option 82.
3	Raisecom#**show ip dhcp relay binding**	Show binding information about DHCPv4 relay.
4	Raisecom#**show ip dhcp relay statistics**	Show statistics about DHCPv4 relay.

7.13 Configuring DHCPv6 relay

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 dhcp relay**	Enable global DHCPv6 relay.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode. By default, the interface is in router mode.
4	Raisecom(config-port)#**ipv6 dhcp relay**	Enable interface DHCPv6 relay.
4	Raisecom(config-port)#**ipv6 dhcp relay target-ip** *ipv6-address*	Configure the destination IPv6 address for forwarding packets.

7.14 Configuring DHCPv4 Snooping

7.14.1 Preparing for configurations

Scenario

As a security feature of DHCP, DHCP Snooping is used to ensure that the DHCP client obtains an IP address from a legitimate DHCP server and records the correspondence between the DHCP client IP address and MAC address.

The Option field in the DHCP packet records the location of the DHCP client. Administrators can use this option to locate the DHCP client to control the client's security and billing. A switch configured with DHCP Snooping Option can process the packets according to whether the packet contains the Option field.

Prerequisite

N/A

7.14.2 Configuring DHCPv4 Snooping

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp snooping**	Enable global DHCPv4 Snooping.
3	Raisecom(config)#**ip dhcp snooping binding max-learning-num** *number*	Configure the maximum number of DHCPv4 Snooping binding tables.
4	Raisecom(config)#**ip dhcp snooping option client-id**	(Optional) configure DHCPv4 Snooping Option61.
5	Raisecom(config)#**ip dhcp snooping option** *optiong-code*	Configure DHCPv4 Snooping Option.

Step	Command	Description
6	Raisecom(config)#**ip dhcp snooping autosave enable**	(Optional) enable automatic saving of the DHCPv4 Snooping binding table.
7	Raisecom(config)#**ip dhcp snooping autosave write-interval** *time*	(Optional) configure the interval for automatically saving the DHCPv4 Snooping binding table.
8	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
9	Raisecom(config-port)#**ip dhcp snooping trust**	Configure the interface to a DHCP Snooping trusted interface.
10	Raisecom(config-port)#**ip dhcp snooping vlan** *vlan-id*	Enable DHCP Snooping on a specified interface and a specified VLAN.

7.14.3 Configuring DHCPv4 Snooping Option 82

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp snooping information option**	Enable global DHCP Snooping Option 82.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
4	Raisecom(config-port)#**ip dhcp snooping information option vlan-list** *vlan-list*	Configure the VLAN list of interface DHCP Snooping Option 82 VLAN.

7.14.4 Checking configurations

No.	Command	Description
1	Raisecom#**show ip dhcp snooping**	Show configurations of DHCPv4 Snooping.
2	Raisecom#**show ip dhcp snooping autosave**	Show the automatic saving status of the DHCPv4 Snooping binding table.
3	Raisecom#**show ip dhcp snooping binding** [**max-learning-num**]	Show the DHCPv4 Snooping binding table.

7.15 Configuring DHCPv6 Snooping

7.15.1 Configuring DHCPv6 Snooping

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 dhcp snooping**	Enable global DHCPv6 Snooping.
3	Raisecom(config)#**ipv6 dhcp snooping binding max-learning-num** *number*	Configure the maximum number of DHCPv6 Snooping binding tables.
4	Raisecom(config)#**ipv6 dhcp snooping option** *optiong-code*	Configure DHCPv6 Snooping Option.
5	Raisecom(config)#**ipv6 dhcp snooping option remote-id**	Configure DHCPv6 Snooping Option37.
6	Raisecom(config)#**ipv6 dhcp snooping option interface-id**	Configure DHCPv6 Snooping Option18.
7	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
8	Raisecom(config-port)#**ipv6 dhcp snooping trust**	Configure the interface to a DHCPv6 Snooping trusted interface.
9	Raisecom(config-port)#**ipv6 dhcp snooping vlan** *vlan-id*	Enable DHCPv6 Snooping on a specified interface and a specified VLAN.

7.15.2 Checking configurations

No.	Command	Description
1	Raisecom#**show ipv6 dhcp snooping**	Show DHCPv6 Snooping configurations.
2	Raisecom#**show ipv6 dhcp snooping binding** [**max-learning-num**]	Show information about the DHCPv6 Snooping binding table.

7.16 Configuring DHCPv4/DHCPv6 Option

7.16.1 Preparing for configurations

Scenario

The 61 and 82 fields in the DHCP Option are options for the relay agent information in the DHCP message. When the DHCP client sends a request message to the DHCP server, if the request packet needs to go through DHCP Snooping or DHCP relay, the DHCP Snooping or DHCP relay adds the Option field to the request message.

The DHCP Option 61 and 82 fields are used to record DHCP client information based on IPv4. Based on this type of information, the DHCP server can be used in conjunction with other software to implement functions such as IP address allocation restrictions and accounting.

Option 18 refers to the interface ID option. After receiving the request message sent by the DHCPv6 client to the DHCPv6 server, the DHCPv6 Snooping device adds the Option 18 option to the message and forwards it to the DHCPv6 server. The DHCPv6 server selects an appropriate address pool according to the client information carried in Option 18 and allocates an IPv6 addresses for the DHCPv6 client.

Option 37 refers to the remote ID option. After receiving the request message sent by the DHCPv6 client to the DHCPv6 server, the DHCPv6 Snooping device adds the Option 37 option to the message and forwards it to the DHCPv6 server. The DHCPv6 server can use the information in Option 37 to locate the DHCPv6 client, thus allocating IPv6 addresses.

Prerequisite

DHCP Option needs to be used on the DHCP Snooping device. To validate DHCP Option, you need to enable DHCP Snooping on the device.

7.16.2 Configuring IPv4 DHCP Option 82

Option 82 should be used on the device with DHCP Snooping enabled.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp information option attach-string** *attach-string*	Configure additional information for the Option 82 field.
3	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**ip dhcp information option circuit-id** *circuit-id*	Configure the circuit ID sub-option of the Option 82 field under the interface.
4	Raisecom(config-port)#**exit** Raisecom(config)#**ip dhcp information option remote-id** { **client-mac** | **client-mac-string** | **hostname** | **switch-mac** | **switch-mac-string** | **string** *string* }	Configure the remote ID sub-option in the Option 82 field.

7.16.3 Configuring IPv4 DHCP Option 61

Option 61 should be used on the device with DHCP Snooping enabled.

The follow steps can be in any sequence.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv4 dhcp option client-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }	Configure Option 61.

Step	Command	Description
3	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**ipv4 dhcp option client-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }	Configure Option 61 on the interface.

7.16.4 Configuring IPv4 self-defined DHCP Option

Self-defined Option should be used on the device with DHCP Snooping enabled.

The follow steps can be in any sequence.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv4 dhcp option** *option-id* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }	(Optional) create a self-defined Option field based on IPv4.
3	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**ipv4 dhcp option** *option-id* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }	(Optional) create a self-defined Option field based on IPv4 on the interface.

7.16.5 Configuring IPv6 DHCP Option 18

Option 18 should be used on the device with DHCP Snooping enabled.

The follow steps can be in any sequence.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 dhcp snooping option interface-id**	Configure the Option device to support Option 18.
3	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**ipv6 dhcp option interface-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ipv6-address** *ip-address* }	(Optional) configure Option 18 on the interface.
4	Raisecom(config)#**ipv6 dhcp option interface-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ipv6-address** *ip-address* }	(Optional) create IPv6-based Option 18.
5	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**ipv6 dhcp option interface-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ipv6-address** *ip-address* }	(Optional) create IPv6-based Option 18 on the interface.

7.16.6 Configuring IPv6 DHCP Option 37

Option 37 should be used on the device with DHCP Snooping enabled.

The follow steps can be in any sequence.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 dhcp option remote-id** { **ascii** *ascii-string* | **hex** *hex-string* | **mac-format** *mac-string* }	Configure Option 37.

7.16.7 Configuring IPv6 DHCP Option 38

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 dhcp client option38 enable**	Enable Option 38 选项功能。.

7.16.8 Configuring IPv6 self-defined DHCP Option

Self-defined Option should be used on the device with DHCP Snooping enabled.

The follow steps can be in any sequence.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 dhcp option** { *option-id* | **interface-id** } { **ascii** *ascii-string* | **hex** *hex-string* | **ipv6-address** *ip-address* }	(Optional) create a self-defined Option field based on IPv6.
3	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**ipv6 dhcp option** *option-id* { **ascii** *ascii-string* | **hex** *hex-string* | **ipv6-address** *ip-address* }	(Optional) create a self-defined Option field based on IPv6 on the interface.

7.16.9 Checking configurations

No.	Command	Description
1	Raisecom#**show ipv6 dhcp snooping**	Show DHCPv6 Snooping configurations.
2	Raisecom#**show ipv6 dhcp snooping binding** [**max-learning-num**]	Show binding information about DHCPv6 Snooping.
3	Raisecom#**show ip dhcp information option**	Show configurations of DHCP Option.

8 IP routing

This chapter describes principles and configuration procedures of IP routing, including following sections:

- Configuring routing management
- Configuring static route
- Configuring routing policy
- Configuring OSPFv2
- Configuring OSPFv3
- Configuring ISIS
- Configuring ISISv6
- Configuring BGP
- Configuring BGP4+
- Configuring RIP
- Configuring RIPng

8.1 Configuring routing management

8.1.1 Configuring routing management

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router id** *router-id*	Configure the Router ID. By default, the Router ID is 192.168.1.1.

8.1.2 Configuring IP FRR

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

Step	Command	Description
2	Raisecom(config)#**ip frr route-map** *map-name* [**wtr-timer** *timer*]	Configure IP FRR.

8.1.3 Checking configurations

No.	Command	Description
1	Raisecom#**show router id**	Show the Router ID.
2	Raisecom#**show fib** [**vrf** *vrf-name*] [*ip-address* | *ipv6-address/m*]	Show the route forwarding table.
3	Raisecom#**show fib** [**vrf** *vrf-name*] [**domain** { **ipv4** | **ipv6** }]	Show the domain of the route forwarding table.
4	Raisecom#**show fib summary [all | vrf vrf-name]**	Show statistics of the route forwarding table.

8.2 Configuring static route

8.2.1 Preparing for configurations

Scenario

The static route has the following advantages:

- Consume less time for the CPU to process them.
- Facilitate the administrator to learn the route.
- Be configured easily.

However, when configuring the static route, you need to consider the whole network. If the network structure is changed, you need to modify the routing table manually. Once the network scale is enlarged, it will consume lots of time to configure and maintain the network. In addition, it may cause more errors.

The default route is a specific static route. It will be used when no matched route is found in the routing table.

Prerequisite

N/A

8.2.2 IPv4 static route

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

Step	Command	Description
2	Raisecom(config)#**ip route** [**vrf** *vrf-name*] { *ip-address mask-address* | *ip-address/m* } [**vrf** *vrf-name*] *next-hop* [*interface-type interface-number* | **port-channel** *channel-number* | **vlan** *vlan-id*] [**distance** *distance-value*] [**description** *words*] [**tag** *tag-value*]	Configure IPv4 static routes.
3	Raisecom(config)#**ip route** [**vrf** *vrf-name*] *ip-address mask-address* **NULL 0** [**distance** *distance-value*] [**description** *words*] [**tag** *tag-value*]	(Optional) configure the IPv4 static route of the NULL interface.
4	Raisecom(config)#**ip route static distance** *distance*	(Optional) configure the default administrative distance of the IPv4 static route. The default administrative distance is 1.

8.2.3 IPv6 static route

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 route** [**vrf** *vrf-name*] { *ipv6-address/0* | *ipv6-address/m* } [**vrf** *vrf-name*] *ipv6-next-hop* [*interface-type interface-number* | **port-channel** *channel-number*] [**distance** *distance-value*] [**description** *words*] [**tag** *tag-value*]	Configure the IPv6 static route.
3	Raisecom(config)#**ipv6 route** [**vrf** *vrf-name*] { *ipv6-address/0* | *ipv6-address/m* } **NULL 0** [**distance** *distance-value*] [**description** *words*] [**tag** *tag-value*]	(Optional) configure the IPv6 static route of the NULL interface.
4	Raisecom(config)#**ipv6 route static distance** *distance*	(Optional) configure the default administrative distance of the IPv6 static route. The default administrative distance is 1.

8.2.4 Configuring BFD for static routes

BFD for IPv4 static route

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

Step	Command	Description
2	Raisecom(config)#**ip route** [**vrf** *vrf-name*] { *ip-address mask-address* | *ip-address/m* } [**vrf** *vrf-name*] *next-hop* [*interface-type interface-number* | **port-channel** *channel-number* | **vlan** *vlan-id*] **track bfd-session** *bfd-session-id*	Bind static routes with BFD sessions. BFD can achieve fast response to faults and route switching.
	Raisecom(config)#**ip route** [**vrf** *vrf-name*] *ip-address mask-address* **NULL 0 track bfd-session** *bfd-session-id*	

BFD for IPv6 static route

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 route** [**vrf** *vrf-name*] { *ipv6-address/0* | *ipv6-address/m* } [**vrf** *vrf-name*] *ipv6-next-hop* [*interface-type interface-number* | **port-channel** *channel-number*] **track bfd-session** *bfd-session-id*	Bind static routes with BFD sessions. BFD can achieve fast response to faults and route switching.
	Raisecom(config)#**ipv6 route** [**vrf** *vrf-name*] { *ipv6-address/0* | *ipv6-address/m* } **NULL 0 track bfd-session** *bfd-session-id*	

8.2.5 Checking configurations

No.	Command	Description
1	Raisecom#**show ip route** [**all** | **vrf** *vrf-name*] [**protocol** { **static** | **connected** | **bgp** | **ospf** | **isis** | **rip** }] [**detail**]	Show information about the IPv4 routing table.
2	Raisecom#**show ip route** [**vrf** *vrf-name*] *ip-address* [*mask-address*] [**longer-prefixes**] [**detail**]	Show the route to a destination IPv4 address.
3	Raisecom#**show ip route** [**vrf** *vrf-name*] *ip-address1* [*mask-address1*] *ip-address2* [*mask-address2*] [**detail**]	Show routing information between two IPv4 addresses.
4	Raisecom#**show ipv6 route** [**all** | **vrf** *vrf-name*] [**protocol** { **static** | **connected** | **bgp** | **ospf** | **isis** | **rip** }] [**detail**]	Show the IPv6 routing table.
5	Raisecom#**show ip route** [**vrf** *vrf-name*] **summary**	Show the IPv4 route summary.
6	Raisecom#**show ipv6 route** [**vrf** *vrf-name*] **summary**	Show the IPv6 route summary.
7	Raisecom#**show ipv6 route** [**vrf** *vrf-name*] { *start-ipv6-address/***0** | *start-ipv6-address/m* } { *end-ipv6-address/***0** | *end-ipv6-address/m* } [**detail**]	Show routing information between two IPv6 addresses.

No.	Command	Description
8	Raisecom#**show ipv6 route** [**vrf** *vrf-name*] *ipv6-address* [*prefix-length*] [**longer-prefixes**] [**detail**]	Show the route to a destination IPv6 address.

8.3 Configuring routing policy

8.3.1 Configuring IPv4 routing policy

IPv4 prefix list

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip prefix-list** *prefix-name* [**seq** *seq-number*] { **deny** | **permit** } { *ip-address/mask* | **any** }	Create an IPv4 prefix-list or add a node to the IP prefix-list. If no prefix-list ID (*seq-number*) is configured, the system will generate a prefix-list ID automatically. The generated pre-fix list ID has 5 digits.
	Raisecom(config)#**ip prefix-list** *prefix-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-address/mask* { **ge** *min-length* | **ge** *min-length* **le** *max-length* }	
	Raisecom(config)#**ip prefix-list** *prefix-name* [**seq** *seq-number*] { **deny** | **permit** } *ip-address/mask*{ **le** *max-length* | **le** *max-length* **ge** *min-length* }	
3	Raisecom(config)#**ip prefix-list** *prefix-name* **description** *string*	Configure descriptions of the IPv4 prefix-list. If the length of descriptions exceeds 80 characters, the first 80 characters are available.

Note

- If one record is in permit type, all mismatched routes are in deny type by default. Only matched routes can pass filtering of the IP prefix-list.
- If one record is in deny type, all mismatched routes are in deny type by default. Even matched routes cannot pass filtering of the IP prefix-list. Therefore, you need to add a permit record after multiple deny records to allow other routes to pass.
- If there are multiple records in the IP prefix-list, there must be a record in permit type.

Configuring BGP filter

BGP routing policy filters include: AS path filter, community attribute filter, extended community attribute filter, and RD filter.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip as-path access-list** *access-list-number* { **permit** | **deny** } *regexp*	(Optional) configure the filter that is based on AS path of the BGP route.
3	Raisecom(config)#**ip community-list** { *standard-list-number* | **standard** *standard-list-name* }{ **permit** | **deny** } *community-number* [**internet**] [**local-as**] [**no-advertise**] [**no-export**]	(Optional) configure the filter that is based on standard or advanced community properties of the BGP route.
	Raisecom(config)#**ip community-list** { *expanded-list-number* | **expanded** *expanded-list-name* } { **permit** | **deny** } *regexp*	
4	Raisecom(config)#**ip extcommunity-list** { *standard-list-number* | **standard** *standard-list-name* }{ **permit** | **deny** } **rt** *rout-target-number*	(Optional) configure the filter that is based on standard community properties of the BGP route.
5	Raisecom(config)#**ip rd-filter** *rd-filter-number* { **permit** | **deny** } **rd** *rd -number*	(Optional) configure the filter that is based on RD property of the BGP route.

IPv4 routing table

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**route-map** *map-name* { **permit** | **deny** } *number*	Create the route mapping table and enter route mapping configuration mode.
3	Raisecom(config-route-map)#**description** *string*	Configure descriptions of the route mapping table. If there is any space in descriptions, descriptions should be within quotes.
4	Raisecom(config-route-map)#**on-match next**	Configure the on-match clause to continuing to match at the next node. By default, the process is finished after matching.
5	Raisecom(config-route-map)#**on-match goto** *number*	Configure the on-match clause to continuing to match at some node. By default, the process is finished after matching.
6	Raisecom(config-route-map)#**call** *map-name*	Continue to match routes by scheduling other routing table after matching the route. By default, the process is finished after matching.
7	Raisecom(config-route-map)#**match ip next-hop** *acl-number*	Configure the match clause to matching the next hop based on extended IP ACL.

8	Raisecom(config-route-map)#**match ip next-hop prefix-list** *prefix-name*	Configure the match clause to matching the next hop based on IP prefix-list.
9	Raisecom(config-route-map)#**match ip address** *acl-number*	Configure the match clause to matching the IP address based on extended IP ACL.
10	Raisecom(config-route-map)#**match ip address prefix-list** *prefix-name*	Configure the match clause to matching the IP address based on IP prefix-list.
11	Raisecom(config-route-map)#**match interface** *name*	Configure the match clause to matching the interface name.
12	Raisecom(config-route-map)#**match metric** *metric*	Configure the match clause to the matching rule that is based on route metric value.
13	Raisecom(config-route-map)#**match tag** *tag*	Configure the match clause to the matching rule that is based on Tag field of the route tagging.
14	Raisecom(config-route-map)#**match as-path** *path-list-number*	Configure the match clause to the BGP routing information matching rule that is based on AS-Path filter.
15	Raisecom(config-route-map)#**match community** { *community-list-number* | *community-list-name* } [**exact-match**]	Configure the match clause to the BGP routing information matching rule that is based on community filter.
16	Raisecom(config-route-map)#**extcommunity** { *extcommunity-list-number* | *extcommunity-list-name* }	Configure the match clause to the BGP routing information matching rule that is based on extcommunity filter.
17	Raisecom(config-route-map)#**match ip route-source prefix-list** *prefix-name*	Configure the match clause to the BGP routing information matching rule that is based on prefix-list matching with source address of the route.
18	Raisecom(config-route-map)# **match rd-filter** *rd-filter-number*	Configure the match clause to the BGP routing information matching rule that is based on RD property filter.
19	Raisecom(config-route-map)#**set metric** [**+** | **-**] *metric*	Configure the set clause to modifying the route metric value after matching.
20	Raisecom(config-route-map)#**set metric-type** { **type-1** | **type-2** }	Configure the set clause to modifying the route metric type after matching.
21	Raisecom(config-route-map)#**set src** *ip-address*	Configure the set clause to modifying the source IP address after matching.
22	Raisecom(config-route-map)#**set ip next-hop** *ip-address*	Configure the set clause to modifying the next-hop IP address of the route after matching.
23	Raisecom(config-route-map)#**set tag** *tag*	Configure the set clause to modifying the routing information tag after matching.
24	Raisecom(config-route-map)#**set origin** { **egp** *as-number* | **igp** | **incomplete** }	Configure the set clause to modifying the route source of the BGP routing information that matches with the routing policy.

25	Raisecom(config-route-map)#**set as-path prepend** *as-number*	Configure the set clause to modifying the as-path property of the BGP routing information that matches with the routing policy.
26	Raisecom(config-route-map)#**set local-preference** *preference*	Configure the set clause to modifying the local priority of the BGP routing information that matches with the routing policy.
27	Raisecom(config-route-map)#**set community** { *community-number* | **internet** | **local-as** | **no-advertise** | **no-export** } * [**additive**] Raisecom(config-route-map)# **set community none**	Configure the set clause to setting or deleting the community property of the BGP routing information that matches with the routing policy.
28	Raisecom(config-route-map)#**set comm-list** { *community-list-number* | *community-list-name* } **delete**	Configure the set clause to deleting the community property of the BGP routing information that matches with the routing policy.
29	Raisecom(config-route-map)#**set extcommunity rt** *route-target-number* [**additive**]	Configure the set clause to adding or modifying the community property of the BGP routing information that matches with the routing policy.
30	Raisecom(config-route-map)#**set ip backup-interface** *interface-type interface-number*	Configure the set clause to modifying the backup egress interface after matching the policy.
31	Raisecom(config-route-map)#**set ip backup-nexthop** *nexthop-address*	Configure the set clause to modifying the backup next-hop address after matching the policy.

8.3.2 Configuring IPv6 routing policy

IPv6 prefix list

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 prefix-list** *prefix-name* [**seq** *seq-number*] { **deny** | **permit** } { *ipv6-address/m* | **any** }	Create an IPv6 prefix list, or add a node to it. If you do not configure the prefix list *seq-number*, the sequence number be automatically generated by the system with a step of 5.
	Raisecom(config)#**ipv6 prefix-list** *prefix-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv6-address/m* { **ge** *min-length* | **ge** *min-length* **le** *max-length* }	
	Raisecom(config)#**ipv6 prefix-list** *prefix-name* [**seq** *seq-number*] { **deny** | **permit** } *ipv6-address/m*{ **le** *max-length* | **le** *max-length* **ge** *min-length* }	

Step	Command	Description
3	Raisecom(config)#**ipv6 prefix-list** *prefix-name* **description** *string*	Configure description of the IPv6 prefix list. If the input description exceeds 80 characters, the first 80 characters will be applied.

IPv6 routing table

Step	Command	Description
1	Raisecom(config)#**route-map** *map-name* { **permit** | **deny** } *number*	Create a routing table and enter routing table configuration mode.
2	Raisecom(config-route-map)#**match ipv6 address** *acl-number*	Configure a match clause to matching the IP address based on extended IP ACL. The corresponding ACL list ranges from 7000 to 7999.
3	Raisecom(config-route-map)#**match ipv6 address prefix-list** *prefix-name*	Configure a match clause to matching the IP address based on IP prefix list.
4	Raisecom(config-route-map)#**match ipv6 next-hop** *acl-number*	Configure a match clause to matching the next hop based on extended IP ACL. The corresponding ACL list ranges from 7000 to 7999.
5	Raisecom(config-route-map)#**match ipv6 next-hop prefix-list** *prefix-name*	Configure a match clause to matching the next hop based on IP prefix list.
6	Raisecom(config-route-map)#**match ipv6 route-source prefix-list** *prefix-name*	Configure a match clause to matching routing source address based on prefix list for the BGP routing matching rules.
7	Raisecom(config-route-map)#**set ipv6 next-hop** { *ipv6-address* | *peer-address* }	Configure the set clause to modifying the next-hop IP address after matching.
8	Raisecom(config-route-map)#**set ipv6 backup-interface** *interface-type interface-number*	Configure the set clause to modifying the egress interface after matching.
9	Raisecom(config-route-map)#**set ipv6 backup-nexthop** *ipv6-address*	Configure the set clause to modifying the next-hop address after matching.

8.3.3 Checking configurations

No.	Command	Description
1	Raisecom#**show ip as-path access-list** *access-list-number*	Show filtering information about the AS-path list.
2	Raisecom#**show ip prefix-list** [*prefix-name*] [**seq** *seq-number*]	Show information about the IP prefix list.

No.	Command	Description
3	Raisecom#**show ip prefix-list** *prefix-name ip-address/m* { **longer** | **first-match** }	
4	Raisecom#**show ip prefix-list summary** [*prefix-name*]	Show summary of the IP prefix list.
5	Raisecom#**show ip prefix-list detail** [*prefix-name*]	Show statistics on the IP prefix list.
6	Raisecom#**show ipv6 prefix-list** [*prefix-name*] [**seq** *seq-number*]	Show information about the IPv6 prefix list.
7	Raisecom#**show ipv6 prefix-list** *prefix-name ipv6-address/m* { **longer** | **first-match** }	
8	Raisecom#**show ipv6 prefix-list summary** [*prefix-name*]	Show summary of the IPv6 prefix list.
9	Raisecom#**show ipv6 prefix-list detail** [*prefix-name*]	Show statistics on the IPv6 prefix list.
10	Raisecom#**show route-map** *map-name*	Show information about the routing table.
11	Raisecom#**show ip rd-filter**	Show detailed configurations of the RD attribute filter.
12	Raisecom#**show ip community-list** [*community-list-number*] [*community-list-name*]	Show information about the group attribute list.
13	Raisecom#**show ip extcommunity-list** [*community-list-number*] [*community-list-name*]	Show information about the extended group attribute list.

8.4 Configuring OSPFv2

The device supports OSPFv2 and OSPFv3.

- In terms of working mechanism, OSPFv2 is basically the same as OSPFv3.
- In terms of network suitability,
  - OSPFv2 is mainly applicable to IPv4 networks.
  - OSPFv3 is mainly applicable to IPv6 networks.

Note

OSPF runs on L3 interfaces. By default, the interface is in routed mode. If the current interface is configured to the switch mode, you have to use the **no portswitch** command to return the interface to the routed mode.

8.4.1 Configuring OSPF basic functions

Starting OSPF network process

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

Step	Command	Description
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Enable an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**network** *ip-address wild-card-mask* **area** *area-id*	Configure network segments included in the OSPF area.

- If you manually configure the *router-id* parameter through the optional parameters in the router ospf *process-id* [router-id *router-id*] command, the OSPF process will select the *router-id* parameter first. Otherwise, the parameter is selected automatically.
- If the OSPF process is configured or selects the *router-id* parameter, after being modified, the *router-id* parameter takes effect after the OSPF process is rebooted.

(Optional) configuring OSPF DCN process

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Enable an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**capability opaque**	Enable OSPF opaque LSA. By default, opaque LSA is disabled.
4	Raisecom(config-router-ospf)#**capability dcn**	Enable OSPF network management self-connection. By default, OSPF network management self-connection is enabled.

8.4.2 Configuring OSPF route properties

Configuring OSPF cost value of interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 3 interface configuration mode.
3	Raisecom(config-port)#**ip ospf cost** *cost*	Configure the OSPF cost of the IP interface.

Configuring bandwidth reference value

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router ospf` *process-id* `[ router-id` *router-id* `]`	Enable an OSPF process and enter OSPF configuration mode.
3	`Raisecom(config-router-ospf)#reference-bandwidth` *bandwidth*	Configure the bandwidth reference value of the link. By default, the bandwidth reference value is 100 Mbit/s.

Note

- After the routing cost is manually configured through the ip ospf cost command, the manually-configured routing cost takes effect.
- If the routing cost is not configured manually but the link bandwidth reference value is configured, the routing cost is automatically configured based on link bandwidth reference value. The formula is: cost = link bandwidth reference value (bit/s) / link bandwidth. If the cost value is greater than 65535, it is configured to 65535. If no link bandwidth reference value is configured, it is configured to 100 Mbit/s by default.

Configuring OSPF administrative distance

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router ospf` *process-id* `[ router-id` *router-id* `]`	Enable an OSPF process and enter OSPF configuration mode.
3	`Raisecom(config-router-ospf)#distance` *administrative-distance*	Configure the OSPF administrative distance. By default, it is 110.
4	`Raisecom(config-router-ospf)#distance ospf { intra-area | inter-area | external }` *distance*	Configure the administrative distance of OSPF specified route. By default, it is 0. However, it takes 110 as the standard.

8.4.3 Configuring OSPF network type

Configuring OSPF network

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

Step	Command	Description
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip ospf network** { **broadcast** | **non-broadcast** | **ptmp** | **ptp** }	Configuring the network type of the interface. By default, it is the broadcast network.

Configuring DR election priority

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip ospf priority** *priority*	Configure the DR election priority on the IP interface. By default, it is 1.

Configuring OSPF NBMA network neighbor

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip ospf network non-broadcast** Raisecom(config-port)#**exit**	Configure the interface network mode to NBMA and exit interface configuration mode.
4	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Enable an OSPF process and enter OSPF configuration mode.
5	Raisecom(config-router-ospf)#**neighbor** *ip-address* [**priority** *priority*]	Configure the NBMA neighbor and its priority. By default, no NBMA neighbor is configured and the priority is 0 when you configure the NBMA neighbor.

Caution

Priorities configured by the **neighbour** and **ip ospf priority** *priority* commands are different:

- The priority configured by the neighbor command indicates that whether the neighbor has the right to vote. If you set the priority to 0 when configuring the neighbor, the local router believes that the neighbor has no right to vote and will not sent Hello packets to the neighbor. This method helps reduce the number of Hello packets transmitted through the network during DR and BDR election

processes. However, if the local router is a DR or BDR, it will send the Hello packet to the neighbor, whose priority is configured to 0, to establish the neighboring relationship.

- The priority configured by the ip ospf priority *priority* command is used for actual DR election.

8.4.4 Configuring OSPF area

Configuring OSPF NSSA area

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter the OSPF configuration mode.
3	Raisecom(config-router-ospf)#**area** *area-id* **nssa** [**no-summary**]	Configure the area to be NSSA area. Only non-backbone area can be NSSA area. By default, the non-backbone areas are all common areas.

Configuring Stub area

For the non-backbone area at the edge of Autonomous System (AS), you can configure the **stub** command on all routers in the area to configure the area to a Stub area. In this case, Type5 LSA, which is used to describe external routes of the AS, cannot be flooded in the Stub area. This facilitates reducing the routing table size.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Enable an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**area** *area-id* **stub** [**no-summary**]	Configure the area to a Stub area. The **no-summary** parameter is used to disable the ABR to send Summary LSA to the Stub area. It means that it is a Totally Stub area and the ABR is available for the Stub only. By default, no area is the Stub area.
4	Raisecom(config-router-ospf)#**area** *area-id* **default-cost** *cost*	Configure the default route cost of the Stub area. This command is available for the ABR in the Stub area only. By default, it is 1.

Caution

- All routers in the Stub area must be configured with the Stub property through the **area** *area-id* **stub** command.

- To set an area to a Totally Stub area, all routers in the area must be configured by the **area** *area-id* **stub** command. In addition, all ABRs in the area must be configured by the **area** *area-id* **stub** no-summary command.
- The backbone area cannot be set to the Stub area.
- ASBR should not be in the Stub area. It means that routers besides the AS cannot be transmitted in the Stub area.

8.4.5 Configuring load balancing

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**maximum load-balancing** *number*	Configure the maximum number of paths of IP ECMP.

8.4.6 Maximizing LSA metric

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**max-metric router-lsa** [**include-stub**] [**on-startup** *time*]	Configure maximum metric of the OSPF LSA packets. The metric of LSA packets in the corresponding area will be automatically configured to 0xFFFF. By default, it is disabled.

8.4.7 Optimizing OSPF network

Configuring OSPF packet timer

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip ospf dead-interval** *seconds*	Configure the OSPF neighbor dead interval. By default, it is 4 times of Hello packet delivery interval. If no Hello packet delivery interval is configured, it is 40s for P2P and Broadcast interfaces and 120s for P2MP and NBMA interfaces by default.

Step	Command	Description
4	Raisecom(config-port)#**ip ospf hello-interval** *seconds*	Configure the ODPF Hello packet delivery interval. By default, it is 10s for P2P and Broadcast interfaces and 30s for P2MP and NBMA interfaces
5	Raisecom(config-port)#**ip ospf poll-interval** *seconds*	Configure the OSPF Poll timer interval. By default, it is 120s.
6	Raisecom(config-port)#**ip ospf retransmit-interval** *seconds*	Configure the LAS retransmission interval on the IP interface. By default, it is 5s.
7	Raisecom(config-port)#**ip ospf transmit-delay** *seconds*	Configure the LSA retransmission delay on the IP interface. By default, it is 1s.

Caution

- When the dead-interval is not manually configured, after hello-interval is configured, dead-interval and poll-interval is changed to 4 times of hello-interval.
- When the dead-interval is manually configured, after hello-interval is configured, no effect is brought to the dead-interval and poll-interval. No matter whether you configure the poll interval or not, the poll-interval changes with the dead-interval.

Therefore, we recommend configure these 3 values in the following order: hello-interval, dead-interval, and poll-interval.

Configuring SPF calculation interval

When the OSPF Link State Database (LSDB) changes, it needs to re-calculate the shortest path. If the network changes frequently and it needs to calculate the shortest path immediately, it will occupy a great amount of system resources and affect efficiency of the router. By adjusting the SPF calculation interval, you can prevent some effects brought by frequent network changes.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Enable an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**timers spf** { *delay-time hold-time* | **millisecond** *delay-milliseconds hold-milliseconds* }	Configure the calculation delay and interval of the OSPF route. By default, the calculation delay is 2s and the calculation interval is 3s.

Configuring OSPF passive interface

To make some OSPF routing information not obtained by some router on the network, you can configure the interface to an OSFP passive interface to disable the interface to send OSPF packets.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip ospf passive-interface enable**	Enable passive interface on the OSPF interface. By default, it is disabled.

Configuring MTU ignorance

By default, the value of MTU domain in the DD packet is the MTU value of the interface, which sends the packet. Default MTU values may vary on devices. In addition, if the MTU value of the DD packet is greater than the one of the interface, the packet will be discarded. To ensure receiving the packet properly, enable MTU ignorance to set the MTU value to 0. Therefore, all devices can receive the packet.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip ospf mtu-ignore enable**	Enable MTU ignorance on the IP interface. By default, MTU ignorance is disabled on the IP interface to check MTU of the OSPF Hello packet.

Preventing Hello packet attacks

To prevent Hello packet attacks, configure the interval for sending Hello packets, that is, the interval at which the router periodically sends Hello packets to neighbor routers.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Start an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**hello-reverse-attack suppression** *interval*	Configure the sending interval of Hello packets. By default, the sending interval of Hello packets is 10s.

8.4.8 Configuring OSPF authentication policy

Configuring OSPF area authentication policy

All routers in an area need to be configured with the identical area authentication policy (non-authentication, simple authentication, or MD5 authentication). The OSPF area has no authentication password but adopts the interface authentication password. If no interface authentication password is configured, the empty password will be used for authentication.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router ospf` *process-id* `[ router-id` *router-id* `]`	Enable an OSPF process and enter OSPF configuration mode.
3	`Raisecom(config-router-ospf)#area` *area-id* `authentication { md5 | simple }`	Configure the area authentication mode. By default, it is non-authentication.

Configuring OSPF interface authentication policy

Packet authentication prioritizes selecting the interface authentication mode. If the interface authentication mode is configured to non-authentication mode, the area authentication mode will be selected. OSPF interfaces cannot establish the neighbor relationship unless the authentication mode and authentication password are identical.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter interface configuration mode.
3	`Raisecom(config-port)#ip ospf authentication { md5 | simple }`	Configure the authentication mode of the IP interface. By default, it is non-authentication. It means adopting the area authentication mode.
4	`Raisecom(config-port)#ip ospf authentication-key { simple [ 0 | 7 ]` *password* `| md5 { [` *key-id* `[ 0 | 7 ]` *password* `] | keychain` *keychain-name* `} }`	Configure the authentication password of the IP interface.

8.4.9 Controlling OSPF redistributed routes

Configuring OSPF redistributed routes

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

Step	Command	Description
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Enable an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**redistribute** { **static** | **connected** | **isis** | **bgp** } [metric *metric*] [**metric-type** { **1** | **2** }] [**tag** *tag-value*] [**route-map** *map-name*] Raisecom(config-router-ospf)#**redistribute ospf** [*process-id*] [**metric** *metric*] [**metric-type** { **1** | **2**] [**tag** *tag-value*] [**route-map** *map-name*]	Configure OSPF route redistribution polity. By default, no external route is redistributed. When an external route is redistributed: • When the directly-connected and static route is redistributed, the metric is 1 by default. When other routes are redistributed, take the original metric of the external route as the metric of the LSA. • If no Metric-type is specified, the Metric-type is Type2 by default. • If no Tag is specified, take the original Tag of the external route as the Tag of the LSA.
4	Raisecom(config-router-ospf)#**redistribute limit** *limit-number*	Configure the threshold of redistributed OSPF external routes. By default, no threshold is configured.

Configuring inter-area route aggregation

If there are sequent network segments in the area, you can configure route aggregation on the ABR to aggregate these network segments to a network segment. When sending routing information, the ABR generates Type3 LSA by taking the network segment as the unit.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Enable an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**area** *area-id* **range** *ip-address ip-mask* [**not-advertise**]	Configure the inter-area route aggregation. By default, no inter-area route aggregation is configured. When you configure the aggregated route, the cost is the maximum Metric of the LSA by default. In addition, the aggregated route is redistributed.

Aggregating redistributed external routes

After the external route is redistributed, configure route aggregation on the ASBR. The RAX721-A just puts the aggregated route on the ASE LSA. This helps reduces the number of LSAs in the LSDB.

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

Step	Command	Description
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Enable an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**summary-address** *ip-address ip-mask* [**not-advertise**] [**metric** *metric*]	Aggregate external routes. By default, external routes are not aggregated. When external aggregates are aggregated, the Metric is the maximum Metric of the LSA by default.

Advertising default route

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Enable an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**default-information originate** [**always**] [**metric** *metric*] [**type** { **1** | **2** }]	Advertise the default route. By default, no default route is generated. When the default LSA is generated, if the **always** key word is specified, the default Metric is 1. If the **always** key word is not specified, the Metric is 10.

8.4.10 Configuring OSPF routing policy

Configuring OSPF receiving policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip prefix-list** *list-name* { **permit** | **deny** } *ip-address mask-length* [**ge** *ge-length*] [**le** *le-length*]	Configure the IP prefix-list.
3	Raisecom(config)#**access-list** *acl-number*	Create an ACL and enter ACL configuration mode. Enter basic IP ACL configuration mode when the *acl-number* ranges from 1000 to 1999.
	Raisecom(config-ipv4-std)#**rule** [*rule-id*] { **deny** | **permit** } { *source-ip-address source-ip-mask* | **any** }	Configure basic IP ACL rules.
4	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Enable an OSPF process and enter OSPF configuration mode.

Step	Command	Description
5	Raisecom(config-router-ospf)#**distribute-list** { **ip-access-list** *acl-number* | **prefix-list** *list-name* } **in**	Configure the OSPF filtering policy for receiving the OSPF inter-area routes, intra-area routes, and AS external routes.

- Before configuring OSPF receiving policy, ensure that the IP ACL used by the OSPF receiving policy has been created.
- When the RAX721-A performs filtering based on IP ACL, if the ACL mode is configured to permit, all routes, which match with the ACL, can pass. Others are filtered.
- You cannot modify the IP ACL unless it is not used by any routing policy.
- Different from IP ACL, the IP prefix-list can be modified even it is being used.
- If the configured IP prefix-list does not exist, do not filter received routes.

Configuring OSPF releasing policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip prefix-list** *list-name* { **permit** | **deny** } *ip-address mask-length* [**ge** *ge-length*] [**le** *le-length*]	Configure the IP prefix-list. You can use the **no ip prefix-list** *list-name* command to delete the configuration.
3	Raisecom(config)#**access-list** *acl-number*	Create an ACL and enter ACL configuration mode. Enter basic IP ACL configuration mode when the *acl-number* ranges from 1000 to 1999.
	Raisecom(config-acl-ip-std)#**rule** [*rule-id*] { **deny** | **permit** } { *source-ip-address source-ip-mask* | **any** }	Configure the basic IP ACL rule.
4	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Enable an OSPF process and enter OSPF configuration mode.
5	Raisecom(config-router-ospf)#**distribute-list** { **ip-access-list** *acl-number* | **prefix-list** *list-name* } **out**	Configure the filtering policy that the OSPF releases 5 types of LSAs to the AS.
6	Raisecom(config-router-ospf)#**distribute-list** { **ip-access-list** *acl-number* | **prefix-list** *list-name* } **out** [**static** | **connected** | **bgp** | **rip**]	Configure the OSPF releasing policy.
	Raisecom(config-router-ospf)#**distribute-list** { **ip-access-list** *acl-number* | **prefix-list** *list-name* } **out ospf** *process-id*	

- Before configuring OSPF global releasing policy, ensure that the IP ACL used by the OSPF global releasing policy has been created.
- You cannot modify the IP ACL unless it is not used by any routing policy.
- Different from IP ACL, the IP prefix-list can be modified even it is being used.
- After global releasing policy is configured, routes cannot be redistributed to the local LSDB unless it passes the global releasing policy. After protocol releasing policy is configured, the route can be redistributed through the protocol releasing policy.
- After protocol releasing policy is configured, the redistributed protocol route can be redistributed to the local LSDB through the protocol releasing policy. If global releasing policy is also configured, the route must be redistributed through the global releasing policy.

Configuring Type3 LSA filtering policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip prefix-list** *list-name* { **permit** | **deny** } *ip-address mask-length* [**ge** *ge-length*] [**le** *le-length*]	Configure the IP prefix-list. You can use the **no ip prefix-list** *list-name* command to delete the configuration.
3	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Enable an OSPF process and enter OSPF configuration mode.
4	Raisecom(config-router-ospf)#**area** *area-id* **filter prefix-list** *list-name* { **in** | **out** }	Configure Type3 LSA filtering policy in the area.

If the configured filtering policy does not exist, it believes that the command fails to configure the filtering policy and no filtering operation is performed on received routes.

8.4.11 Configuring BFD for OSPF

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Enter OSPF configuration mode.
3	Raisecom((config-router-ospf))#**bfd all-interfaces**	Enable global BFD. By default, it is disabled.
4	Raisecom(config-router-ospf)#**exit**	Enter global configuration mode.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.

Step	Command	Description
6	Raisecom(config-port)#**ip ospf bfd**	Enable BFD on the interface. By default, it is disabled.

Note

- If global BFD is enabled through the bfd all-interfaces command, no matter what BFD configurations are set on the interface, BFD is enabled.
- If global BFD is disabled, BFD configurations on the interface take effect.

8.4.12 Configuring OSPF for MPLS-TE

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ospf** *process-id* [**router-id** *router-id*]	Enable an OSPF process and enter OSPF configuration mode.
3	Raisecom(config-router-ospf)#**capability opaque**	Enable OSPF opaque LSA. By default, it is disabled.
4	Raisecom(config-router-ospf)#**mpls traffic-eng area** *area-id*	Enable TE in the OSPF area. By default, it is disabled.
5	Raisecom(config-router-ospf)#**mpls traffic-eng router-id** *router-id*	Configure the Router ID of the MPLS-TE router.

8.4.13 Checking configurations

No.	Command	Description
1	Raisecom#**show ip ospf** [*process-id*]	Show OSPF basic information.
2	Raisecom#**show ip ospf** [*process-id*] **route**	Show OSPF routing information.
3	Raisecom#**show ip ospf** [*process-id*] **interface** [*interface-type interface-number*]	Show OSPF interface information.
4	Raisecom#**show ip ospf** [*process-id*] **neighbor** [*interface-type interface-number*] [*ip-address*]	Show OSPF neighbor information.
5	Raisecom#**show ip ospf** [*process-id*] **neighbor statistics**	Show OSPF neighbor statistics.
6	Raisecom#**show ip ospf** [*process-id*] **database** [**max-age** | **self-originate**]	Show information about OSPF link status database.

No.	Command	Description
7	Raisecom#**show ip ospf** [*process-id*] **database** { **asbr-summary** | **external** | **network** | **router** | **summary** | **nssa-external** | **opaque-link** | **opaque-area** | **opaque-as** } [*ip-address*] [**adv-router** *ip-address* | **self-originate**]	Show details about the OSPF link status database.
8	Raisecom#**show ip ospf** [*process-id*] **database statistics**	Show information about area border router and ASBR.
9	Raisecom#**show ip ospf** [*process-id*] **border-routers**	Show external statistics about OSPF ASBR.
10	Raisecom#**show ip ospf** [*process-id*] **summay-address**	Show summary about the OSPF ASBR external route.

8.4.14 Maintenance

Command	Description
Rasiecom#**clear ip ospf** [*process-id*] **process** [**graceful**]	Restart the OSPF process.
Raisecom(config-router-ospf)#**capability restart** { **graceful** | **signaling** }	Configure OSPF GR which can ensure that routers running OSPF forward services normally when the active/standby switchover starts or OSPF restarts.

8.5 Configuring OSPFv3

8.5.1 Starting OSPFv3 process

Starting OSPFv3 process

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	Start an OSPFv3 process and enter OSPFv3 configuration mode. **Note** The device supports at most one OSPFv3 process, and one process can contain multiple OSPFv3 instances.
3	Raisecom(config-ospf6)#**router-id** *router-id*	Configure the Router-ID of the OSPF process.

Configuring process IPsec authentication policy

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ipv6 router ospf process-id [ vrf vrf-name ]`	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	`Raisecom(config-ospf6)#ipsec policy policy-name`	Configure the IPsec authentication policy of the OSPF process. The various parameters of the authentication policy must be valid so that the policy can be applied. By default, the process is not authenticated.

8.5.2 Configuring OSPFv3 network type

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface interface-type interface-number`	Enter interface configuration mode.
3	`Raisecom(config-port)#ipv6 ospf network { broadcast | nbma | ptmp | ptp } [ instance-id instance-id ]`	Configure the network type of the OSPFv3 area interface. By default, the network type of the OSPFv3 area is broadcast.

8.5.3 Configuring OSPFv3 area

Configuring Stub area

For non-backbone areas at the edge of the AS, you can configure the stub command on all routing devices in the area to configure the area as a stub area. In this way, Type5 LSAs describing external routes of the autonomous system will not flood in the stub area, reducing the size of the routing table.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ipv6 router ospf process-id [ vrf vrf-name ]`	Start an OSPFv3 process and enter OSPFv3 configuration mode. **Note** The device supports at most one OSPFv3 process, and one process can contain multiple OSPFv3 instances.

Step	Command	Description
3	Raisecom(config-ospf6)#**area** { *area-id* | *ip-format-area-id* } **stub** [**no-summary**]	Configure the area to a Stub area. The no-summary parameter is used to prevent the ABR from sending a Summary LSA to the Stub area, that is, the Totally Stub area, which is only used for the ABR of the Stub area.

Caution

- All routing devices in the stub area must be configured with the stub attribute using the **area** *area-id* **stub** command.
- If you want to configure an area as a totally stub area, all routers in the area must be configured with the **area** *area-id* **stub** command, and the ABR routing device in the area must be configured with the **area** *area-id* **stub no-summary** command.
- Only non-backbone areas can be configured as stub areas.
- ASBR cannot exist in the stub area, that is, routes outside the autonomous system cannot be propagated in the area.

Configuring area virtual link

OSPF uses a regional design, and conventional areas can only exchange LSAs with backbone areas. However, in actual networking, some conventional areas cannot be directly connected to the backbone area but can only be directly connected to other conventional areas. In this scenario, OSPF virtual links are used to virtualize the adjacent conventional areas as the backbone area, so that those conventional areas that cannot be directly connected to the backbone area can also obtain routes from other OSPF areas.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	Raisecom(config-ospf6)#**area** *area-id* **virtual-link** *router-id* [**dead-interval** *dead-interval* | **hello-interval** *hello-interval*] [**retransmit-interval** *retransmit-interval*] [**transmit-delay** *transmit-delay*] [**instance-id** *instance-id*]	Configure the virtual link.

8.5.4 Configuring OSPFv3 interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.

Step	Command	Description
3	Raisecom(config-port)#**ipv6 ospf** *process-id* **area** *area-id* [**instance-id** *instance-id*]	Configure the local area of the interface.
4	Raisecom(config-port)#**ipv6 ospf mtu-ignore** [**instance-id** *instance-id*]	Configure the OSPFv3 area interface to ignore MTU check when checking packets. By default, the OSPFv3 area interface checks the MTU.
5	Raisecom(config-port)#**ipv6 ospf passive-interface** [**instance-id** *instance-id*]	(Optional) configure the interface to a passive interface. By default, the interface is a passive interface.
6	Raisecom(config-port)#**ipv6 ospf neighbor router-id** *router-id ipv6-address* [**priority** *priority*] [**poll-interval** *poll-interval*] [**instance-id** *instance-id*]Raisecom(config-ospf6)#**exit**	Configure the NBMA neighbor, its priority, and sending interval.
7	Raisecom(config-port)#**ipv6 ospf poll-interval** *interval* [**instance-id** *instance-id*]	Configure the Poll-Interval timer in the NBMA network. By default, the Poll-Interval timer is 60s.

8.5.5 Controlling OSPFv3 redistributed routes

Configuring OSPFv3 redistributed routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode. **Note** The device supports up to one OSPFv3 process, and one process can contain multiple OSPFv3 instances.

Step	Command	Description
3	Raisecom(config-ospf6)#**redistribute** { **static** | **connected** | **isisv6** *process-id* | **bgp4+** | **ripng** | **ospfv3** *process-id* } [**metric** *metric*] [**metric-type** { **1** | **2** }] [**tag** *tag-value*] [**route-map** *map-name*]	Configure OSPFv3 route redistributing policies. By default, no external route is redistributed. When redistributing the external routes: • When direct routes and static routes are imported, the metric is 1 by default. When other types of routes are imported, the original metric of the external route is used as the LSA metric. • If Metric-type is not specified, the default Metric-type is Type2. • If no tag is specified, the original tag of the external route is used as the LSA tag.

Configuring inter-domain route aggregation

If there are some continuous network segments in an area, you can configure route aggregation on the ABR to aggregate these continuous network segments into one network segment. When ABR sends routing information to other areas, it generates Type3 LSAs in units of network segments.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode. **Note** The device supports up to one OSPFv3 process, and one process can contain multiple OSPFv3 instances.
3	Raisecom(config-ospf6)#**area** *area-id* **range** *ipv6-address/mask* [**not-advertise**]	Configure inter-domain route aggregation.

Aggregating redistributed external routes

After ASBR imports external routes, if you configure route aggregation, the device only puts the aggregated routes in ASE LSA for announcement, reducing the number of LSAs in LSDB.

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

Step	Command	Description
2	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	Raisecom(config-ospf6)#**summary-address** *ipv6-address/mask* [**not-advertise**]	Configure external route aggregation. By default, external routes are not aggregated.

Advertising default route

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	Raisecom(config-ospf6)#**default-information originate** [**always**] [**metric** *metric*] [**type** { **1** | **2** }]	Advertise the default route. By default, no default route is generated. When the system generates the default LSA, if the **always** keyword is specified, the default metric is 1, otherwise the metric is 10.

8.5.6 Configuring timer of OSPFv3 packets

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ipv6 ospf hello-interval** *seconds* [**instance-id** *instance-id*]	Configure the interval for sending Hello packets on the OSPFv3 area interface. By default, the interval is 10s.
4	Raisecom(config-port)#**ipv6 ospf dead-interval** *seconds* [**instance-id** *instance-id*]	Configure the neighbor dead time on the OSPFv3 area interface. By default, the neighbor dead time is 4 times the interval for sending Hello packets; if the interval for sending Hello packets is not configured, then it is 40s by default.
5	Raisecom(config-port)#**ipv6 ospf transmit-delay** *seconds* [**instance-id** *instance-id*]	Configure the transmission delay time of LSA on the OSPFv3 area interface. By default, it is 1s.

Step	Command	Description
6	Raisecom(config-port)#**ipv6 ospf retransmit-interval** *seconds* [**instance-id** *instance-id*]	Configure the interval for retransmitting the lost LSA packets on the OSPFv3 area interface. By default, it is 5s.

8.5.7 Configuring OSPFv3 route management

Configuring route attributes on OSPFv3 interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ipv6 ospf cost** *value* [**instance-id** *instance-id*]	Configure the routing cost on the OSPFv3 area interface. By default, the routing cost of an OSPFv3 interface = 10^8 (bit / s)/interface bandwidth (bit / s). If the calculated cost is greater than 65535, the maximum value is 65535.
4	Raisecom(config-port)#**ipv6 ospf priority** *value* [**instance-id** *instance-id*]	Configure the routing priority on the OSPFv3 area interface. By default, the routing priority on the OSPFv3 area interface is 1.

Configuring OSPFv3 administrative distance

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode. **Note** The device supports up to one OSPFv3 process, and one process can contain multiple OSPFv3 instances.
3	Raisecom(config-ospf6)#**distance** *administrative-distance*	Configure OSPFv3 administrative distance. By default, it is 110.

Configuring bandwidth reference value

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ipv6 router ospf process-id`	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	`Raisecom(config-ospf6)#reference-bandwidth bandwidth`	Configure the bandwidth reference value of the link. By default, the bandwidth reference value is 100 Mbit/s.

Configuring SPF calculation interval

When the OSPF Link State Database (LSDB) changes, the shortest path needs to be recalculated. If the network changes frequently, and the shortest path is calculated immediately for each change, it will occupy a lot of system resources and affect the efficiency of the routing device. By adjusting the SPF calculation interval, you can suppress the impact of frequent network changes.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ipv6 router ospf process-id`	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	`Raisecom(config-ospf6)#timers spf delay-time hold-time`	Configure the delay time and interval of OSPFv3 route calculation. By default, the delay is 2s and the interval is 3s.

Configuring load balancing

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ipv6 router ospf process-id`	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	`Raisecom(config-ospf6)#maximum load-balancing number`	Configure the maximum number of IP ECMP paths supported by OSPFv3.

8.5.8 Configuring OSPFv3 routing policy

Configuring OSPFv3 receiving policy

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ipv6 prefix-list` *prefix-name* `seq` *seq-number* { `deny` | `permit` } *ip-address/mask* [`ge` *min-length*] [`le` *max-length*]	(Optional) configure the address prefix list.
3	`Raisecom(config)#access-list` *acl-number*	(Optional) create an ACL and enter ACL configuration mode. When the *acl-number* ranges from 7000 to 7999, the system will enter extended IPv6 ACL configuration mode.
	`Raisecom(config-acl-ipv6-advanced)#rule` [*rule-id*] { `deny` | `permit` } { *protocol-id* | `ipv6` } { *source-ip-address/prefix-length* | `any` } { *destination-ip-address/prefix-length* | `any` } [`dscp` *dscp-value*]	(Optional) configure extended IPv6 ACL rules.
4	`Raisecom(config)#ipv6 router ospf` *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.
5	`Raisecom(config-ospf6)#distribute-list` { `ipv6-access-list` *acl-number* | `ipv6-prefix-list` *list-name* } `in`	Configure the filtering policy for OSPFv3 to receive OSPF intra-area, inter-area, and AS external routes.

Note

- Before configuring OSPFv3 acceptance filtering policy, you need to ensure that the IPv6 ACL referenced by the policy has been created.
- When filtering is based on IPv6 ACL, if the ACL mode is permit, the route matching the ACL will pass, otherwise the routes will be denied.
- The IPv6 ACL can only be modified if and only if it is not referenced by any routing policy.
- Unlike IPv6 ACL, the address prefix list can be modified when it is referenced.
- If the configured prefix list does not exist, the received routes are not filtered.

Configuring OSPFv3 advertisement policy

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ipv6 prefix-list` *prefix-name* `seq` *seq-number* { `deny` | `permit` } *ip-address/mask* [`ge` *min-length*] [`le` *max-length*]	(Optional) configure the address prefix list.

Step	Command	Description
3	Raisecom(config)#**access-list** *acl-number*	(Optional) create an ACL and enter ACL configuration mode. When the *acl-number* ranges from 7000 to 7999, the system will enter extended IPv6 ACL configuration mode.
	Raisecom(config-acl-ipv6-advanced)#**rule** [*rule-id*] { **deny** | **permit** } { *protocol-id* | **ipv6** } { *source-ip-address/prefix-length* | **any** } { *destination-ip-address/prefix-length* | **any** } [**dscp** *dscp-value*]	(Optional) configure extended IPv6 ACL rules.
4	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.
5	Raisecom(config-ospf6)#**distribute-list** { **ipv6-access-list** *acl-number* | **ipv6-prefix-list** *list-name* } **out** [**static** | **connected** | **bgp4+** | **ripng** | **isisv6** *process-id*]	Configure a filtering policy that OSPFv3 advertises the imported routing information to the autonomous system in form of Type 5 LSA.

Note

- Before configuring the OSPF global advertisement policy, you need to ensure that the IP ACL referenced by the policy has been created.
- The IP ACL can only be modified if and only if it is not referenced by any routing policy.
- Unlike IP ACL, the address prefix list can be modified when it is referenced.
- After the global advertisement policy is configured, only imported routes can be imported into the local LSDB after matching the global advertisement policy. After the protocol advertisement policy is configured, the routes need to match the protocol advertising policy to be imported.
- After the protocol advertisement policy is configured, the imported protocol routes can be imported into the local LSDB only when they match the protocol advertisement policy. If the global advertisement policy is configured at the same time, the routes need to match the global advertisement policy to be imported.

Configuring Type3 LSA filtering policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 prefix-list** *prefix-name* **seq** *seq-number* { **deny** | **permit** } *ip-address/mask* [**ge** *min-length*] [**le** *max-length*]	(Optional) configure the address prefix list.
3	Raisecom(config)#**ipv6 router ospf** *process-id*	Start an OSPFv3 process and enter OSPFv3 configuration mode.

Step	Command	Description
4	Raisecom(config-ospf6)#**area** { *area-id* | *ip-format-area-id* } **filter ipv6-prefix-list** *list-name* { **in** | **out** }	Configure the filtering rule in the egress/ingress direction of the area. Configure the rules for filtering the Summary-LSA in the ingress or egress directions of the area on the ABR.

8.5.9 Configuring OSPFv3 authentication policy

Configuring interface authentication policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ipv6 ospf ipsec policy** *policy-name* [**instance-id** *instance-id*]	Configure IPsec authentication policy on the OSPF interface. The priority of the interface authentication policy is higher than that of the process and area authentication policies. By default, the interface is not authenticated.

Configuring area IPsec authentication policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id* [**vrf** *vrf-name*]	Start an OSPFv3 process and enter OSPFv3 configuration mode.
3	Raisecom(config-ospf6)#**area** { *area-id* | *ip-format-area-id* } **ipsec policy** *policy-name*	Configure the IPsec authentication policy for OSPF areas. The parameters of the authentication policy must be valid so that the policy can be applied. The priority of the area authentication policy is higher than that of the process authentication policies. By default, the area is not authenticated.

8.5.10 Configuring BFD for OSPFv3

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 router ospf** *process-id* [**router-id** *router-id*]	Enter OSPF configuration mode.
3	Raisecom((config-router-ospf))#**bfd all-interfaces**	Enable global BFD. By default, global BFD is not enabled.
4	Raisecom(config-router-ospf)#**exit**	Enter global configuration mode.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
6	Raisecom(config-port)#**ipv6 ospf bfd** [**instance-id** *instance-id*]	Enable interface BFD. By default, interface BFD is not enabled.

8.5.11 Checking configurations

Step	Command	Description
1	Raisecom#**show ipv6 ospf** [*process-id*] [**vrf** *vrf-name*]	Show basic information about OSPFv3.
2	Raisecom#**show ipv6 ospf** [*process-id*] **interface** [*interface-type interface-number*]	Show information about the OSPFv3 interface.
3	Raisecom#**show ipv6 ospf** [*process-id*] **neighbor** [*neighbor-id*]	Show information about OSPFv3 neighbors.
4	Raisecom#**show ipv6 ospf** [*process-id*] **route**	Show OSPFv3 routs.
5	Raisecom#**show ipv6 ospf database** { **router | network | inter-area-prefix | inter-area-router | external | nssa-external | link | intra-area-prefix** }	Show information about OSPFv3 link status database.
6	Raisecom#**show ipv6 ospf asbr**	Show basic information about ASBR.
7	Raisecom#**show ipv6 ospf** [*process-id*] **topology**	Show information about the OSPFv3 topology.
8	Raisecom#**show ipv6 ospf** [*process-id*] **vlink**	Show information about OSPFv3 virtual links.

8.5.12 Maintenance

Command	Description
Rasiecom#**clear ipv6 ospf** [*process-id*] **process** [**graceful**]	Restart the OSPFv3 process.
Raisecom(config-ospf6)#**ospf restart grace-period** *seconds*	Configure the graceful restart period of OSPFv3.
Raisecom(config-ospf6)#**capability restart** { **graceful** | **signaling** }	Configure OSPFv3 GR. OSPFv3 GR can ensure that routers running OSPFv3 forward the service normally when the master/slave switchover starts or OSPFv3 restarts.
Raisecom(config-ospf6)#**ospf restart helper** { **never** | **planned-only** }	Configure rules to enter help mode in OSPFv3 graceful restart mode.
Raisecom(config-ospf6)#**ospf restart helper** [**planned-only**] **max-grace-period** *seconds*	Configure the maximum restart period in OSPFv3 graceful restart help mode.

8.6 Configuring ISIS

8.6.1 Configuring ISIS basic function

To run ISIS normally, two steps need to be done: start ISIS process and configure the name of network entity.

- Use the **router isis** command to start ISIS process.
- Use the **ip router isis** command to start ISIS process on the interface.

step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*] [**vrf** *vrf-name*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config)#**interface** interface-type interface-number	(Optional) enter interface configuration mode.
4	Raisecom(config-port)#**ip router isis** [*area tag*] Raisecom(config-port)#**exit**	(Optional) start an ISIS process on the interface.
5	Raisecom(config)#**router isis** [*area-tag*]	Enter ISIS configuration mode.
6	Raisecom(config-router-isis)#**net** *network-entity*	Configure the network identifier entity of ISIS routing process.

8.6.2 Configuring ISIS routing

Configuring router type

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**is-type** { **level-1** | **level-1-2** | **level-2-only** }	Configure the router type. By default, it is level-1-2.
4	Raisecom(config-router-isis)#**hostname dynamic**	(Optional) enable the switching mechanism of dynamic hostname. By default, it is disabled.

Configuring overhead

The ISIS overhead can be configured automatically or manually. After the automatic calculation of the overhead on the interface is enabled, the ISIS will automatically calculate the overhead on the interface according to the following rules:

- When the type of overhead is configured to wide, ISIS will automatically calculate the value according to the interface rate, the formula is: overhead on the interface = reference rate/interface rate ×10, and the max value obtained is 16777214.
- When the type of overhead is configured to narrow, the interface overhead is:
  - 60 for interface rate between 1 and 10 Mbit/s
  - 50 for interface rate between 1 and 100 Mbit/s
  - 40 for interface rate between 101 and 155 Mbit/s
  - 30 for interface rate between 156 and 622 Mbit/s
  - 20 for interface rate between 623 and 2500 Mbit/s
  - 10 for other conditions

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**metric-style** { **narrow** | **transition** | **wide** } Raisecom(config-router-isis)#**exit**	Configure the type of ISIS overhead. By default, it is narrow.
4	Raisecom(config-router-isis)#**auto-metric** { **enable** | **disable** }	Enable automatic calculation of overhead on the interface. By default, it is disabled.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.

Step	Command	Description
6	Raisecom(config-port)#**isis metric** *metric* [**level-1** | **level-2**]	Configure the overload value on the interface. By default, it is 10.

Configuring reference bandwidth

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**reference-bandwidth** *bandwidth*	Configure reference rate referred to while calculating technical link overhead. By default, it is 100 Mbit/s.

Configuring ISIS administrative distance

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**distance** *distance* [*ip-address mask-address*]	Configure the management distance of ISIS routing. By default, it is 115.

8.6.3 Configuring ISIS network

Configuring type of ISIS network

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**isis network point-to-point**	Configure the type of interface network to P2P. By default, it is broadcast.

Adjacencies

This configuration is only applied to Level-1-2 routers.

- If the host is Level-1-2 router, it needs to establish association with peer router in certain area (Level-1 or Level-2). Configuring an area for establishing adjacency can restrain the interface from receiving and sending the Hello packet only from that certain area.
- In the point-to-point link, the interface can only receive and send one type of Hello packet. Configuring an area for establishing adjacency can reduce the processing time between routers and save bandwidth.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**isis circuit-type** { **level-1** | **level-1-2** | **level-2-only** }	Configure an area for establishing interface adjacency. By default, it is Level-1-2.

Configuring DIS priority

The Designated Intermedia System (DIS) election of the ISIS is preemptive and predictable. There is not backup DIS in the ISIS. Therefore, when one DIS does not work, another DIS will be elected. The rules for electing the DIS are as below:

- The router with highest DIS election priority will be elected. If all routers have the same priority, the router with biggest MAC address will be elected.
- The DIS in Level-1 and Level-2 are elected respectively but the result may be not the same IS.
- The interval between sending Hello packet by DIS is 1/3 times of that by common routers, which can ensure that the invalid DIS be detected in no time.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**isis priority** *priority* [**level-1** | **level-2**]	Configure the DIS priority on the interface in different areas. By default, it is 64.

8.6.4 Optimizing ISIS network

Configuring ISIS packet timer

The invalid number of Hello packet is decided by the Holddown time. If the router cannot receive Hello packet sent by the peer router within the Holddown time, the peer router can be considered invalid. The Holddown time is configured based on interface and different router in the same area can set different the Holddown time.

By changing the time interval for sending Hello packet of ISIS or the invalid number of Hello packet, you can adjust the Holddown time.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** interface-type interface-number	Enter interface configuration mode.
3	Raisecom(config-port)#**isis hello-interval** *seconds* [**level-1 | level-2**]	Configure the interval between sending Hello packets on the interface of different areas. By default, it is 10s.
4	Raisecom(config-port)#**isis hello-multiplier** *number* [**level-1 | level-2**]	Configure the number of invalid ISIS neighbor Hello packets on the interface of different areas.
5	Raisecom(config-port)#**isis csnp-interval** *seconds* [**level-1 | level-2**]	Configure the interval between sending CSNP packets on the interface of different areas in the broadcast network. By default, it is 10s.

Configuring LSP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** interface-type interface-number	Enter interface configuration mode.
3	Raisecom(config-port)#**isis lsp-interval** *milliseconds*	Configure the interval between sending LSP packets. By default, it is 33ms.
4	Raisecom(config-port)#**isis retransmit-interval** *seconds* Raisecom(config-port)#**exit**	Configure retransmission interval between sending LSP packets on the point-to-point link. By default, it is 5s.
5	Raisecom(config)#**router isis** [*area-tag*] Raisecom(config-router-isis)#**lsp-gen-interval** *seconds* [**level-1** | **level-2**]	Configure the interval between generating LSP. By default, it is 5s.
6	Raisecom(config-router-isis)#**max-lsp-lifetime** *seconds* [**level-1** | **level-2**]	Configure the longest TTL of the LSP generated. By default, it is 1200s.
7	Raisecom(config-router-isis)#**lsp-refresh-interval** *seconds* [**level-1** | **level-2**]	Configure the refresh time of LSP. By default, it is 900s.
8	Raisecom(config-router-isis)#**ignore-lsp-errors**	Enable ignoring the checkout for LSP. By default, it is disabled.

Configure ISIS passive interface

If you do not wish the ISIS routing information to be obtained by the router in a network, you can configure the interface to ISIS passive interface to prevent it from sending ISIS packets.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**isis passive**	Enable the passive function on ISIS interface. By default, it is disabled.

Configure Hello packet padding

Hello packet padding refers to padding Hello packet with MTU field, thus notifying peer and local interface of the MTU.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**hello padding**	Enable Hello Packet padding. By default, all types of interface are padded with standard Hello packet.

8.6.5 Configure ISIS authentication

Configuring ISIS interface authentication

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**isis password** { **clear** *password* | **md5** *password* } [**level-1** | **level-2**]	Configure the ISIS authentication mode and password of the interface.

Configuring ISIS area authentication

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

Step	Command	Description
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**area-password** { **clear** *password* | **md5** *password* } [**authenticate snp** { **send-only** | **validate** }]	Configure Level-1 area authentication.
4	Raisecom(config-router-isis)#**domain-password** { **clear** *password* | **md5** *password* } [**authenticate snp** { **send-only** | **validate** }]	Configure Level-2 area authentication.

8.6.6 Controlling ISIS routing information

Configuring ISIS redistributed routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**redistribute** { **connected** | **static** | **rip** | **ospf** *process-id* | **isis** *area-tag* | **bgp** } [**route-map** *map-name*] [**level-1** | **level-2** | **level-1-2**] [**metric** *metric*] [**metric-type** { **external** | **internal** }]	Configure protocol route redistributed policy. By default, ISIS does not redistribute other protocol routes. If you do not specify the area when it redistributes routes, it will redistribute routes to Level-2 by default.
4	Raisecom(config-router-isis)#**redistribute isis ip level-2 into level-1**	Configure ISIS route redistributed policy among areas. By default, the routing information in level-2 will not be distributed to Level-1.

Configuring advertising default route

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**default-information originate**	Configure advertising Level-2 default route.

Configuring ISIS route aggregation

Route aggregation can not only reduce the scale of routing table but also shrink the size of LSP packet generated by the local router and reduce the scale of LSDB.

- The aggregated route can be the route found by the ISIS and the route redistributed externally.
- The overload of aggregated route takes the minimum overload among all the routes aggregated.
- The router only aggregates the route generated in the local LSP.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**summary-address** *ip-address mask-address* [**level-1** | **level-2** | **level-2-only**]	Configure route aggregation among areas. By default, there is no route aggregation. The overload while configuring route aggregation is the maximum Metric in the LSA. And the route aggregation will be advertised.

Configuring ISIS equal-cost multi-path load balancing

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**maximum load-balancing** *number*	Configure the maximum number of ISIS equal-cost multi-path load balancing paths.

Configuring ISIS route filtering

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*] [**vrf** *vrf-name*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**distribute-list** { **ip access-list** *acl-number* | **prefix-list** *list-name* | **route-map** *map-name* } **out** [**connected** | **static** | **rip** | **ospf** *process-id* | **isis** *area-tag* | **bgp**]	Configure route filtering rules and filter the routes which are to be advertised. By default, route filtering is disabled.

Step	Command	Description
4	Raisecom(config-router-isis)#**distribute-list** { **ip access-list** *acl-number* | **prefix-list** *list-name* | **route-map** *map-name* } **in**	Configure the route filtering rules to filter the receiving rules. By default, route filtering is disabled.

8.6.7 Configuring ISIS BFD

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**isis bfd enable**	Enable interface ISIS BFD. By default, it is disabled.
4	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
5	Raisecom(config-router-isis)#**bfd all-interfaces**	Enable ISIS BFD on all interfaces. By default, it is disabled.

8.6.8 Configuring ISIS GR

Configure ISIS graceful restart, that is, the switchover ensures no service interruption while the RAX721-A is rebooted.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**graceful-restart**	Enable ISIS graceful restart. By default, it is disabled.
4	Raisecom(config-router-isis)#**graceful-restart interval** *seconds*	Enable the interval of ISIS graceful restart. By default, it is 300s.
5	Raisecom(config-router-isis)#**graceful-restart sa enable**	Enable ISIS graceful restart to restrain the neighbor device from advertising routes. By default, it is enabled.

8.6.9 Configuring ISIS TE

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**mpls traffic-eng** { **level-1** | **level-2** }	Enable MPLS-TE and configure MPLS-TE level. By default, it is disabled.
4	Raisecom(config-router-isis)#**mpls traffic-eng router-id** *router-id*	Configure the Router ID of MPLS-TE router. By default, the ISIS Router ID is used.

8.6.10 Checking configurations

Step	Command	Description
1	Raisecom#**show isis interface** [**detail**]	Show ISIS interface.
2	Raisecom#**show isis neighbor** [*system-id* | **detail**]	Show ISIS neighbors.
3	Raisecom#**show isis hostname**	Show the mapping between host name and system ID.
4	Raisecom#**show isis route**	Show ISIS IPv4 route.
5	Raisecom#**show isis topology** [**level-1** | **level-2**]	Show ISIS topology.
6	Raisecom#**show isis database** [*lsp-id* | **detail**]	Show database about ISIS link status.
7	Raisecom#**show isis summary**	Show basic configurations about ISIS.
8	Raisecom#**show isis mpls traffic-eng advertisements**	Show interface advertised by the router.

8.6.11 Maintenance

No.	Command	Description
1	Rasiecom#**clear isis process** *process-id* [**graceful-restart**]	Clear ISIS.
2	Rasiecom#**clear isis neighbor** [*system-id*]	Clear ISIS neighbors.

8.7 Configuring ISISv6

8.7.1 Configuring ISISv6 basic functions

The normal operation of ISIS requires two steps: starting the ISIS process and configuring the network entity name.

- Use the **router isis** command to start the ISIS process.
- Use the **ipv6 router isis** command to start the ISIS process on the interface.

Starting ISIS process

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router isis [ area-tag ] [ vrf vrf-name ]`	Start an ISIS process and enter ISIS configuration mode.
3	`Raisecom(config)#interface interface-type interface-number`	Enter interface configuration mode.
4	`Raisecom(config-port)#ipv6 router isis [ area tag ]` `Raisecom(config-port)#exit`	Enable ISISv6 capabilities on the interface. Establish ISIS neighbor relationship through the interface.
5	`Raisecom(config)#router isis [ area-tag ]`	Enter ISIS configuration mode.
6	`Raisecom(config-router-isis)#net network-entity`	Configure the network ID entity of the ISIS routing process.

Configuring Level

The device establishes neighbor relationship according to the level and maintains the link status database.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router isis [ area-tag ] [ vrf vrf-name ]`	Start an ISIS process and enter ISIS configuration mode.
3	`Raisecom(config-router-isis)#is-type { level-1 | level-1-2 | level-2-only }`	Configure the type of the ISIS router. By default, the type of the ISIS router is level-1-2.

Enabling IPv6 multi-topology

If IPv6 multi-topology is enabled, the system will maintain two independent routing tables, namely IPv4 routing table and IPv6 routing table. If the network is a mixed topology of IPv4

and IPv6, two topology trees of IPv4 and IPv6 will be generated and the IPv4 and IPv6 routes will be calculated respectively.

If IPv6 multi-topology is disabled, the system will recalculate the topology tree and routes. You can view the topology information through the **show isis topology** command and you can view the calculated routing information through the **show isis route** command.

Please perform the following configuration on the device.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router isis [ area-tag ] [ vrf vrf-name ]`	Start an ISIS process and enter ISIS configuration mode.
3	`Raisecom(config-router-isis)#ipv6 multi-topology`	Enable IPv6 route multi-topology. By default, it is disabled.

8.7.2 Configuring ISISv6 authentication

Configuring interface authentication

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface interface-type interface-number`	Enter interface configuration mode.
3	`Raisecom(config-port)#isis password { clear password | md5 password } [ level-1 | level-2 ]`	Configure the ISIS authentication mode and password of the interface.

Configuring area authentication

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router isis [ area-tag ]`	Start an ISIS process and enter ISIS configuration mode.
3	`Raisecom(config-router-isis)#area-password { clear password | md5 password } [ authenticate snp { send-only | validate } ]`	Configure Level-1 area authentication.
4	`Raisecom(config-router-isis)#domain-password { clear password | md5 password } [ authenticate snp { send-only | validate } ]`	Configure Level-2 area authentication.

8.7.3 Configuring ISISv6 route selection parameters

Configuring cost value

The ISIS cost can be calculated automatically or manually configured. After automatic cost calculation is enabled on the interface, the interface cost is calculated automatically according to the following rules:

When the cost type is wide, ISIS will automatically calculate the cost based on the bandwidth of the interface. The formula: interface cost = bandwidth reference value/interface bandwidth *10, the maximum value of the calculated cost is 16777214.

When the cost value type is narrow,

- if the interface bandwidth is 1 Mbit/s–10 Mbit/s, the interface cost is 60.
- if the interface bandwidth is 11 Mbit/s–100 Mbit/s, the interface cost is 50.
- if the interface bandwidth is 101 Mbit/s–155 Mbit/s, the interface cost is 40.
- if the interface bandwidth is 156 Mbit/s–622 Mbit/s, the interface cost is 30.
- if the interface bandwidth is 623 Mbit/s–2500 Mbit/s, the interface cost is 20.
- In other cases, the interface cost is 10.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**metric-style** { **narrow** | **transition** | **wide** } Raisecom(config-router-isis)#**exit**	Configure the type of ISIS cost. By default, the cost type is narrow.
4	Raisecom(config-router-isis)#**auto-metric** { **enable** | **disable** }	Enable automatic calculation of interface cost. By default, it is not enabled.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
6	Raisecom(config-port)#**ipv6 isis metric** *metric-value* [**level-1** | **level-2**]	Configure the link cost of the ISISv6 interface. By default, the cost of the ISIS interface is 10.

Configuring administrative distance

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.

Step	Command	Description
3	Raisecom(config-router-isis)#**ipv6 distance** *distance* [*ip-address mask-address*]	Configure the administrative distance of ISIS routes. By default, the administrative distance of ISIS routes is 115.

8.7.4 Controlling ISISv6 routing information

Advertising default routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**ipv6 default-information originate**	Advertise Level-2 default routes.

Redistributing routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**ipv6 redistribute** { **connected** | **static** | **ripng** | **ospfv3** *process-id* | **isisv6** *area-tag* | **bgp4+** } [**level-1** | **level-2** | **level-1-2**] [**metric** *metric-value*] [**metric-type** { **external** | **internal** }] [**route-map** *map-name*]	Redistribute the routing information about other IPv6 routing protocols and notify related areas. By default, ISIS does not redistribute other protocol routes. If no area is specified during redistribution, the routes will be redistributed to Level-2 by default. Metric-type is internal by default. If no metric is specified when redistributing a route, the metric value of the original route will be inherited.

Step	Command	Description
4	Raisecom(config-router-isis)#**ipv6 redistribute limit** *max-number* [**level-1** | **level-1-2** | **level-2**]	Configure the limit on the number of IPv6 routes redistributed from other routing protocols. By default, the number of external routes is not limited. When this number limit is configured, the default value of Level is level-2. **Note** If level-1 is configured first, and then the same number of level-2 is configured, the **show running-config** command displays level-1-2.
5	Raisecom(config-router-isis)#**redistribute isis ipv6 level-2 into level-1**	Configure routes in Level-2 area to be redistributed into Level-1 area. By default, the routing information in Level-2 area is not advertised to the Level-1 area.

Configuring ISISv6 route aggregation

Route aggregation can not only reduce the size of routing tables, but also reduce the size of LSP packets and the size of LSDB generated by this router.

The route being aggregated may be a route discovered by ISIS or a redistributed external route.

The cost of the aggregated route takes the minimum value of the cost of all aggregated routes.

The router only aggregates the routes in the locally generated LSP.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**ipv6 summary-prefix** *ipv6-address/m* [**level-1** | **level-2** | **level-2-only**]	Configure IPv6 route aggregation. By default, there is no summary route. If you configure an aggregate route without specifying a domain, only Level-2 routes are aggregated.

Configuring ISISv6 route filtering

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*] [**vrf** *vrf-name*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**ipv6 distribute-list** { **ipv6-access-list** *acl-number* | **ipv6-prefix-list** *list-name* | **route-map** *map-name* } **out** [**connected** | **static** | **ripng** | **ospfv3** *process-id* | **isisv6** *area-tag* | **bgp4+**]	Configure IPv6 route filtering rules to filter the IPv6 routes to be advertised. By default, it is not filtered.
4	Raisecom(config-router-isis)#**ipv6 distribute-list** { **ipv6-access-list** *acl-number* | **ipv6-prefix-list** *list-name* | **route-map** *map-name* } **in**	Configure IPv6 route filtering rules to filter the received IPv6 routes. By default, it is not filtered.

8.7.5 Configuring ISISv6 load balancing

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**ipv6 maximum load-balancing** *number*	Configure the maximum number of ISIS ECMPs.

8.7.6 Configuring ISISv6 BFD

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router isis** [*area-tag*]	Start an ISIS process and enter ISIS configuration mode.
3	Raisecom(config-router-isis)#**isis ipv6 bfd enable**	Enable global ISISv6 BFD. By default, it is disabled.
4	Raisecom(config-router-isis)#**ipv6 bfd all-interfaces**	Enable ISIS BFD on all interfaces. By default, it is disabled.

8.7.7 Checking configurations

Step	Command	Description
1	Raisecom#**show isis interface** [**detail**] [*interface-number*] [**vrf** *vrf-name*]	Show information about the ISIS interface.
2	Raisecom#**show isis neighbor** [*system-id* | **detail**] [**vrf** *vrf-name*]	Show ISIS neighbor information.
3	Raisecom#**show isis hostname**	Show the mapping table between the host name and the system ID.
4	Raisecom#**show isis topology** [**level-1** | **level-2**] [**vrf** *vrf-name*]	Show information about the ISIS topology.
5	Raisecom#**show isis database** [**local**] [**level-1** | **level-2**] [*lsp-id*] [**detail**] [**vrf** *vrf-name*]	Show ISIS link status database.
6	Raisecom#**show isis summary**	Show ISIS basic configurations.

8.7.8 Maintenance

Command	Description
Rasiecom#**clear isis process** *process-id* [**graceful-restart**] [**vrf** *vrf-name*]	Clear ISISv6 information.
Rasiecom#**clear isis neighbor** [*system-id*] [**vrf** *vrf-name*]	Clear ISISv6 neighbor information.

8.8 Configuring BGP

8.8.1 Configuring BGP basic functions

Enabling BGP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enable BGP and create a BGP instance. Enter BGP configuration mode.
3	Raisecom(config-router)#**bgp router-id** *router-id*	(Optional) Configure the BGP Router ID. By default, the BGP Router ID is the same as the global Router ID of the router.

Configuring BGP peer

BGP uses the TCP connection. Therefore, when configuring BGP, you need to configure the IP address of the BGP neighbor. The BGP neighbor can be non-adjacent routers. You can establish a BGP neighborship. To enhance stability of the BGP connection, we recommend using the loopback interface address to establish the connection.

Specified IP addresses of BGP neighbors are divided into 2 types:

- Interface IP address of the directly-connected BGP neighbor
- Loopback interface address of the BGP neighbor, where the route can reach. In this mode, you need to configure the route update source to ensure that the BGP neighbor is established properly.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**neighbor** *ip-address* **remote-as** *as-id*	Create a BGP neighbor and specify the AS ID of the BGP neighbor. • IBGP peer: configure the peer AS ID to be the same as the local AS ID. • EBGP peer: configure the peer AS ID to be different from the local AS ID. By default, there is no BGP neighbor.
4	Raisecom(config-router)#**neighbor** *ip-address* **activate**	Enable the BGP neighbor to exchange the specified address family route. By default, enable the BGP neighbor to exchange the IPv4 unicast address family route only.
5	Raisecom(config-router)#**neighbor** *ip-address1* **update-source** *ip-address2* Raisecom(config-router)#**neighbor** *ip-address* **update-source** *interface-type interface-number*	Configure using the specified source IP address or local source interface when establishing a BGP connection. Local source interfaces include physical layer interfaces, VLAN interfaces, loopback interfaces, and sub-interfaces. If one of the two ends of the connection is configured with the correct update source, the BGP connection can be successfully established, but there may be a problem that the connection establishment time is too long. To ensure the stability of the connection establishment at both ends, it is recommended that both ends of the peer be configured to update the source address at the same time.
6	Raisecom(config-router)#**neighbor** *ip-address* **weight** *weight*	(Optional) configure the weight of the routes learned from the BGP peer. By default, it is 0.
7	Raisecom(config-router)#**neighbor** *ip-address* **default-originate** [**route-map** *route-map-name*]	(Optional) Enable the feature of sending the default route to the BGP neighbor. By default, do not send the default route to the BGP neighbor.

Step	Command	Description
8	Raisecom(config-router)#**neighbor** *ip-address* **description** *string*	(Optional) Configure descriptions of the BGP neighbor. By default, there is no description of the BGP neighbor.
9	Raisecom(config-router)#**neighbor** *ip-address* **next-hop-self**	(Optional) Configure the router to modify the next-hop address of the route to the IP address of the Tx end, when the router releases the route to the BGP neighbor. By default, when the router releases the route to the BGP neighbor, the next-hop address of the route is identical to the next-hop IP address of the route in the local BGP routing table.
10	Raisecom(config-router)#**bgp log-neighbor-changes**	(Optional) Enable the log which is used to inform the BGP neighbor of state change. By default, it is enabled.
11	Raisecom(config-router)#**neighbor** *ip-address* **shutdown**	(Optional) disallow the RAX721-A to establish the BGP connection with the specified BGP neighbor. By default, establishing the BGP connection with the BGP neighbor is allowed.
12	Raisecom(config-router)#**neighbor** *ip-address* **ebgp-multihop** [*ttl*]	(Optional) allow the RAX721-A to establish the EBGP connection with BGP neighbors in the indirectly-connected network. In addition, specify the maximum hops allowable for the specified EBGP connection. By default, only physically directly-connected BGP neighbors can establish the EBGP connection.
13	Raisecom(config-router)#**bgp redistribute-internal**	(Optional) allow the device to redistribute the routing information, learned from the IBGP neighbor, to the IGP. By default, redistributing the IBGP route to the IGP is disabled.
14	Raisecom(config-router)#**bgp enforce-first-as**	Enforce the first AS number in the AS path received from an EBGP peer to be the AS where the EBGP peer is located.

Configuring BGP peer (IPv4 based on VPN instance)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enable BGP and create a BGP instance, and enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter the IPv4 address family configuration mode of the BGP VPN instance.
4	Raisecom(config-router-af)#**neighbor** *ip-address* **remote-as** *as-id*	Create the MP-BGP peer and specify the peer AS ID.

Step	Command	Description
5	Raisecom(config-router-af)#**neighbor** *ip-address* **activate**	Enable the exchange of routing information of the specified IPv6 address family between BGP peers.
6	Raisecom(config-router-af)#**neighbor** *ip-address1* **update-source** *ipv6-address2* Raisecom(config-router-af)#**neighbor** *ip-address* **update-source** *interface-type interface-number*	Use the specified source IP address or local source interface when establishing a BGP connection. Local source interfaces include physical layer interfaces, VLAN interfaces, loopback interfaces, and sub-interfaces. If one of the two ends of the connection is configured with the correct update source, the BGP connection can be successfully established, but there may be a problem that the connection establishment takes too long. To ensure the stability of the connection establishment at both ends, we recommend configuring both ends of the peer with the update source address.
7	Raisecom(config-router-af)#**neighbor** *ip-address* **weight** *weight*	(Optional) configure the weight of routes learned from BGP peers. By default, the weight of routes learned from BGP peers is 0.
8	Raisecom(config-router-af)#**neighbor** *ip-address* **default-originate** [**route-map** *route-map-name*]	(Optional) enable the function of sending the default route to the peer. By default, no default route is sent to the peer.
9	Raisecom(config-router-af)#**neighbor** *ip-address* **next-hop-self**	(Optional) configure the router to modify the next hop address of the route to its own IP address when advertising the route to the peer. By default, when the router advertises routes to IBGP peers, the next-hop IP address of the route is the same as the next-hop IP address of the route in the local BGP routing table.
10	Raisecom(config-router-af)#**neighbor** *ip-address* **ebgp-multihop** [*ttl*]	(Optional) configure the peers on the non-directly connected network to establish EBGP connections, and specify the maximum number of hops allowed for EBGP connections. By default, only physically directly-connected peers are allowed to establish EBGP connections.
11	Raisecom(config-router-af)#**bgp log-neighbor-changes**	(Optional) enable logging for prompting the status change of BGP peers. By default, it is enabled.

Step	Command	Description
12	Raisecom(config-router-af)#**bgp redistribute-internal**	(Optional) re-advertise the routing information learned from IBGP peers to the IGP. By default, it is prohibited to redistribute IBGP routes to IGP.
13	Raisecom(config-router-af)#**neighbor** *ip-address* **shutdown**	(Optional) prohibit the establishment of BGP connection with the specified peer. By default, BGP connections with BGP peers are allowed.
14	Raisecom(config-router-af)#**neighbor** *ip-address* **description** *string*	(Optional) configure description of the BGP peer. By default, there is no description for the BGP peer.

Configuring BGP peer (VPNv4)

The configuration is applicable to the MPLS L3VPN.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enable BGP and create a BGP instance, and enter BGP configuration mode.
3	Raisecom(config-router)#**neighbor** *ip-address* **remote-as** *as-id*	Create an MP-BGP peer and specify the AS number of the peer.
4	Raisecom(config-router)#**address-family vpnv4**	Enter BGP VPNv4 address family configuration mode.
5	Raisecom(config-router-af)#**neighbor** *ip-address* **activate**	Enable the function of exchanging routing information of the specified VPNv4 address family between BGP peers.

8.8.2 Configuring BGP redistributed routes

BGP redistributed routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.

Step	Command	Description
3	Raisecom(config-router)#**network** *ip-address* [*mask-address*] [**route-map** *route-map-name*]	Inject static routes into the BGP routing table and advertise them to other ASs or local AS peers.

BGP redistributed routes(VPN-based IPv4)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter the IPv4 address family configuration mode of the BGP VPN instance.
4	Raisecom(config-router-af)#**network** *ip-address* [*mask-address*] [**route-map** *route-map-name*]	Inject static routes into the BGP routing table and advertise them to other ASs or local AS peers.

8.8.3 Configuring BGP to redistribute routes

Redistributing default route

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**default-information originate**	Configure the BGP to redistribute the default route.

Redistributing default route (IPv4 based on VPN instance)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter the IPv4 address family configuration mode of the BGP VPN instance.
4	Raisecom(config-router-af)#**default-information originate**	Configure the BGP to redistribute the default route.

Configuring BGP to redistribute IGP routes

BGP cannot discover routes by itself, so it is necessary to redistribute routes of other protocols (such as IGP or static routes) into the BGP routing table and advertise these routes to other ASs or local AS peers.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router bgp as-id`	Enter BGP configuration mode.
3	`Raisecom(config-router)#redistribute { connected | static | rip | ospf process-id | isis process-id } [ metric metric ] [ route-map map ]`	Configure BGP to redistribute routes of other protocols into the BGP routing table through re-advertising.

Configuring BGP to redistribute IGP routes (IPv4 based on VPN instance)

BGP cannot discover routes by itself, so it is necessary to redistribute routes of other protocols (such as IGP or static routes) into the BGP routing table and advertise these routes to other ASs or local AS peers.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router bgp as-id`	Enter BGP configuration mode.
3	`Raisecom(config-router)#address-family ipv4 vrf vrf-name`	Enter the IPv4 address family configuration mode of the BGP VPN instance.
4	`Raisecom(config-router)#redistribute { connected | static | rip | ospf process-id | isis process-id } [ metric metric ] [ route-map map ]`	Configure BGP to redistribute routes of other protocols through re-advertising.

8.8.4 Configuring BGP routing

BGP routing attributes are a set of parameters advertised together with routing information. The route attribute is information that further describes a specific route, so that the route receiver can filter and select the route based on the route attribute value.

Configuring BGP administrative distance

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router bgp as-id`	Enter BGP configuration mode.

Step	Command	Description
3	Raisecom(config-router)#**distance bgp ebgp** *distance1* **ibgp** *distance2* **local** *distance3*	Configure the administrative distance of the BGP route. • The administrative distance of external routes (routes learned through the EBGP) is 20 by default. • The administrative distance of internal routes (routes learned through the IBGP) is 200 by default. • The administrative distance of local routes (BGP routes redistributed through the aggregation command) is 200 by default.

Configuring BGP administrative distance (IPv4 based on VPN instance)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter the IPv4 address family configuration mode of the BGP VPN instance.
4	Raisecom(config-router-af)#**distance bgp ebgp** *distance1* **ibgp** *distance2* **local** *distance3*	Configure the administrative distance of BGP routes. By default: • The administrative distance of external routes (routes learned through EBGP) is 20. • The administrative distance of internal routes (routes learned through IBGP) is 200. • The administrative distance of local routes (routes redistributed into BGP through aggregation commands) is 200.

Configuring BGP path selection policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**bgp deterministic-med**	(Optional) configure the BGP not to consider the receiving sequence when selecting the route. By default, the BGP considers the receiving sequence when selecting the route.
4	Raisecom(config-router)#**bgp always-compare-med**	Configure the BGP to compare the MED for all paths.
5	Raisecom(config-router)#**bgp bestpath compare-routerid**	Configure BGP to compare the EBGP Router-ID for selecting the best path. By default, BGP prefers the earliest received EBGP route, without comparing the EBGP Router-ID.

Step	Command	Description
6	Raisecom(config-router)#**bgp bestpath as-path ignore**	Configure the BGP to ignore the AS-PATH property when selecting the optimum path.

Configuring BGP path selection policy (IPv4 based on VPN instance)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter the IPv4 address family configuration mode of the BGP VPN instance.
3	Raisecom(config-router-af)#**bgp deterministic-med**	(Optional) configure BGP route preference without considering the route receiving order. By default, BGP route preference considers the route receiving order.
4	Raisecom(config-router-af)#**bgp always-compare-med**	Configure BGP to compare MED for all paths.
5	Raisecom(config-router-af)#**bgp bestpath compare-routerid**	Configure BGP to compare the EBGP Router-ID for selecting the best path. By default, BGP prefers the earliest received EBGP route, without comparing the EBGP Router-ID.
6	Raisecom(config-router-af)#**bgp bestpath as-path ignore**	Configure the BGP to ignore the AS-PATH attribute when selecting the optimal path.

Configuring default MED of BGP default route

The Multi Exit Discriminator (MED) attribute is equivalent to the metric used by IGP. It is used to determine the best route for traffic to enter the AS. When a BGP router obtains multiple routes through different EBGP peers, the destination addresses of these routes are the same, but the next-hop addresses are different. Under the same conditions, the router will choose the route with the smaller MED as the best route.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**default-metric** *metric-value*	Configure the default MED of the local BGP router. This configuration only takes effect on redistributed routes and aggregated routes.

Configuring BGP and IGP route synchronization

After BGP synchronization is enabled,

- The BGP route can participate into selection if it meets the following requirements. Then, if it is selected, the RM is applied to the routing table.
  - In the RM, the BGP route learned through IBGP can exactly match the route learned through IGP.
  - The administrative distance of the IGP route is shorter than the administrative distance of the BGP route.
- The BGP route status will flap and it may participate into selection or not, if it meets the following requirements:
  - The BGP route learned through IBGP can exactly match the route learned through IGP.
  - The administrative distance of the IGP route is greater than the administrative distance of the BGP route.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**synchronization**	Enable BGP and IGP route synchronization. By default, it is disabled.

Configuring route dampening

Route flapping is one route instability form. Route flapping refers that a route appears and then disappears alternatively. Route dampening can be used to overcome route flapping.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**bgp dampening** *half-life reuse suppress max-suppress-time*	Enable BGP route dampening or modify the BGP route dampening parameter. By default, BGP route dampening is disabled. After BGP dampening is enabled, the default values of all parameters are shown as below. • Half-life: 15min • Reuse value: 750 • Dampening threshold: 2000 • Maximum suppress time: 60min

Configuring BGP community attribute

The community attribute is an optional delivery attribute of BGP routes and can be added to the prefix of each route. If a route contains a community attribute, it indicates that the route is a member of a routing community with routes of one or more the same characteristics. According to these features, the configuration of the routing policy can be greatly simplified, and the capability of the routing policy is also enhanced.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** [*as-id*]	Enter BGP configuration mode.
3	Raisecom(config-router)#**neighbor** *ip-address* **send-community standard**	Enable the BGP-enabled device to send standard community attribute to the peer.

Configuring BGP community attribute(IPv4 based on VPN instance)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** [*as-id*]	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter the IPv4 address family configuration mode of the BGP VPN instance.
4	Raisecom(config-router-af)#**neighbor** *ip-address* **send-community standard**	Enable BGP to send standard group attributes to the peer.

8.8.5 Configuring BGP network

Configuring RR

Prefix notification rules of the Router Reflector (RR) are shown as below:

- Rule 1: the RR just notifies or reflects the optimum path to which it returns.
- Rule 2: the RR always notifies the prefix to the BGP neighbor.
- Rule 3: when notifying the prefix, the RR client follows the common IBGP loopback prevention rule.
- Rule 4: to notify the IBGP neighbor, client, or non-client of the prefix, follow rules 5, 6, and 7.
- Rule 5: the RR will notify all its clients and non-clients of the prefix, which is learned from the external BGP neighbor.
- Rule 6: the RR will notify all its clients of the prefix, which reaches the RR through a non-client IBGP neighbor.

- Rule 7: the RR will notify other clients and non-clients of the route, if the prefix reaches the RR through a client.

In some networks, clients of the RR have established a full-connection. They can exchange routing information directly without using route reflection. In this case, you can use the **no bgp client-to-client reflection** command to disable route reflection among clients of the RR.
To enhance network reliability and prevent faults from occurring at a node, you need to configure one or more RR in a cluster. You can configure the identical cluster ID for all RRs in the cluster to identify the cluster. This helps avoid the loopback.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**neighbor** *ip-address* **route-reflector-client**	Configure the device to the RR and set the specified neighbor as the client of the RR. By default, route reflection is disabled.
4	Raisecom(config-router)#**bgp client-to-client reflection**	Enable route reflection among clients of the RR. By default, route reflection among clients of the RR is enabled.
5	Raisecom(config-router)#**bgp cluster-id** *cluster-id*	Configure the cluster ID of the RR. By default, it is the Router ID.

Configuring route reflector (VPNv4)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family vpnv4**	Enter BGP VPNv4 address family configuration mode.
4	Raisecom(config-router-af)#**neighbor** *ip-address* **route-reflector-client**	Configure the local device as the route reflector and configure the specified peer as the client of the route reflector. By default, route reflector is disabled.

Configuring BGP default local priority

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.

Step	Command	Description
3	Raisecom(config-router)#**bgp default local-preference** *priority*	Configure BGP default local priority. By default, it is 100.

Configuring BGP timer

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**bgp scan-time** *time*	Configure the interval for scanning the BGP routing table. By default, it is 60s.
4	Raisecom(config-router)#**timers bgp** *keep-alive-time hold-time*	Configure the live and hold time of the global BGP connection. By default, the live and hold time of the global BGP connection are configured to 60s and 180s respectively.
5	Raisecom(config-router)#**neighbor** *ip-address* **timers** *keep-alive-time hold-time*	Configure the live and hold time of the neighbor. By default, the live and hold time of the neighbor are identical to the ones of the global BGP connection.

Configuring BGP route aggregation

- At present, the RAX721-A supports BGP manual aggregation. Manual aggregation is only valid for existing routes in the BGP local routing table. If there is no route, whose mask size is greater than 16 bytes, in the BGP routing table, the BGP will not release the aggregated route even you use the aggregate 10.1.1.1 255.255.0.0 command to aggregate the route.
- The aggregated route cannot be set to the default route (0.0.0.0/0).

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**aggregate-address** *ip-address mask-address*	Configure BGP route aggregation and release the aggregated route and detail route.
4	Raisecom(config-router)#**aggregate-address** *ip-address mask-address* **summary-only**	Configure BGP route aggregation, release the aggregated route only and dampens the detail route.
5	Raisecom(config-router)#**aggregate-address** *ip-address mask-address* **as-set**	Configure BGP route aggregation and set the AS_SET option. The generated aggregated route includes all AS IDs in the AS_PATH and takes them as an AS_SET to prevent the route loop.

Configuring BGP route aggregation (IPv4 based on VPN instance)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter IPv4 address family configuration mode of the BGP VPN instance.
4	Raisecom(config-router-af)#**aggregate-address** *ip-address mask-address*	Configure BGP route aggregation and advertise aggregated routes and detailed routes.
5	Raisecom(config-router-af)#**aggregate-address** *ip-address mask-address* **summary-only**	Configure BGP route aggregation. Advertise aggregated routes but suppress detailed routes.
6	Raisecom(config-router-af)#**aggregate-address** *ip-address mask-address* **as-set**	Configure BGP route aggregation and configure the AS_SET option. The generated aggregated route includes all AS numbers in the AS_PATH and will be considered as an AS_SET to prevent loops.

Configuring BGP route filtering

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip as-path access-list** *access-list-number* { **permit** | **deny** } *regexp*	Configure the filter of the AS_PATH list.
3	Raisecom(config)#**router bgp** [*as-id*]	Enter BGP configuration mode.
4	Raisecom(config-router)#**neighbor** *ip-address* **filter-list** *access-list-number* { **in** | **out** }	Configure the BGP route filtering policy based on AS_PATH list. By default, it is disabled. It receives all route updates from the peer.
5	Raisecom(config-router)#**neighbor** *ip-address* **route-map** *map-name* { **in** | **out** }	Apply the routing policy to the specified neighbor to filter or release the route.
6	Raisecom(config-router)#**neighbor** *ip-address* **prefix-list** *prefix-list-name* { **in** | **out** }	Configure the specified neighbor to filter received or released routes based on IP prefix-list.

Configuring BGP route filtering (IPv4 based on VPN instance)

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

Step	Command	Description
2	Raisecom(config)#**ip as-path access-list** *access-list-number* { **permint** | **deny** } *regexp*	Configure the filter of AS path list.
3	Raisecom(config)#**router bgp** [*as-id*]	Enter BGP configuration mode.
4	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter IPv4 address family configuration mode of the BGP VPN instance.
5	Raisecom(config-router-af)#**neighbor** *ip-address* **filter-list** *access-list-number* { **in** | **out** }	Configure the BGP route filtering policy based on AS path list.
6	Raisecom(config-router-af)#**neighbor** *ip-address* **route-map** *map-name* { **in** | **out** }	Apply the routing policy to a specified peer to filter the received or advertised routes.
7	Raisecom(config-router-af)#**neighbor** *ip-address* **prefix-list** *prefix-list-name* { **in** | **out** }	Configure a specified peer to filter the received or advertised routes based on IP prefix list.

Configuring BGP route filtering (VPNv4)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip as-path access-list** *access-list-number* { **permint** | **deny** } *regexp*	Configure the filter of AS path list.
3	Raisecom(config)#**router bgp** [*as-id*]	Enter BGP configuration mode.
4	Raisecom(config-router)#**address-family vpnv4**	Enter BGP VPNv4 address family configuration mode.
5	Raisecom(config-router-af)#**neighbor** *ip-address* **filter-list** *access-list-number* { **in** | **out** }	Configure the BGP route filtering policy based on AS path list.
6	Raisecom(config-router-af)#**neighbor** *ip-address* **route-map** *map-name* { **in** | **out** }	Apply the routing policy to a specified peer to filter the received or advertised routes.
7	Raisecom(config-router-af)#**neighbor** *ip-address* **prefix-list** *prefix-list-name* { **in** | **out** }	Configure a specified peer to filter the received or advertised routes based on IP prefix list.

8.8.6 Configuring BFD for BGP

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

Step	Command	Description
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**neighbor** *ip-address* **fall-over bfd**	Enable BFD for BGP. By default, it is disabled.

IPv4 mode based on VPN instance

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter IPv4 address family configuration mode of the BGP VPN instance.
4	Raisecom(config-router-af)#**neighbor** *ip-address* **fall-over bfd**	Enable BFD for peer BGP connections. By default, it is disabled.

8.8.7 Configuring BGP authentication

Configuring BGP authentication

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**neighbor** *ip-address* **password** *password*	Enable to perform MD5 authentication on the BGP message when the BGP neighbor establishes the TCP connection. By default, it is disabled.

Configuring BGP authentication (IPv4 based on VPN instance)

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv4 vrf** *vrf-name*	Enter IPv4 address family configuration mode of the BGP VPN instance.

Step	Command	Description
4	Raisecom(config-router-af)#**neighbor** *ip-address* **password** *password*	Enable MD5 authentication on BGP messages when the BGP peer establishes TCP connections. By default, it is disabled.

8.8.8 Checking configurations

No.	Command	Description
1	Raisecom#**show ip bgp**	Show contents of the local BGP routing table.
2	Raisecom#**show ip bgp** *ip-address* [*ip-mask*]	Show information about the specified network in the local BGP routing table.
3	Raisecom#**show ip bgp dampening dampened-paths**	Show information about the dampened routes.
4	Raisecom#**show ip bgp dampening parameters**	Show route dampening parameters.
5	Raisecom#**show ip bgp dampening flap-statistics**	Show route flapping statistics.
6	Raisecom#**show ip bgp summary**	Show summary of the BGP peer.
7	Raisecom#**show ip bgp neighbors** [*ip-address*]	Show detailed status of the BGP peer.
8	Raisecom#**show ip bgp vpnv4** { **all** | **rd** *rd* | **vrf** *vrf-name* }	Show routing information about all or the specified BGP VPNv4.
9	Raisecom#**show ip bgp vpnv4** { **all** | **vrf** *vrf-name* } *ip-address* [*mask-address*]	Show routing information in the specified network segment of the BGP VPNv4 address family.
10	Raisecom#**show ip bgp vpnv4** { **all** | **vrf** *vrf-name* } **summary**	Show summary routing information about the BGP VPNv4 address family.
11	Raisecom#**show ip bgp vpnv4** { **all** | **vrf** *vrf-name* } **neighbors** *router-id* [**routes**]	Show routing information about the specified BGP VPNv4 peer.
12	Raisecom#**show ip bgp vpnv4 all labels**	Show label information about the BGP VPNv4 route prefix.

8.8.9 Maintenance

Command	Description
Rasiecom#**clear ip bgp dampening** [*network-address* [*network-mask*]]	Clear information about routing attenuation.

Command	Description
Rasiecom#**clear ip bgp external** [**ipv4 unicast** | **ipv6 unicast** | **vpnv4 unicast** | **vrf** *vrf-name*]	Hard reset all or specified EBGP connections and the connection is interrupted.
Rasiecom#**clear ip bgp external** [**ipv4 unicast** | **ipv6 unicast** | **vpnv4 unicast** | **vrf** *vrf-name*] { **in** | **out** | **soft** }	Soft reset all or specified EBGP connections. The connection is not interrupted and only the route is refreshed.
Rasiecom#**clear ip bgp internal** [**ipv4 unicast** | **ipv6 unicast** | **vpnv4 unicast**]	Hard reset all or specified IBGP connections, and the connection is interrupted.
Rasiecom#**clear ip bgp internal** [**ipv4 unicast** | **ipv6 unicast** | **vpnv4 unicast**] { **in** | **out** | **soft** }	Soft reset all or specified IBGP connections. The connection is not interrupted and only the route is refreshed.
Rasiecom#**clear ip bgp** [**ipv4 unicast** | **ipv6 unicast** | **vpnv4 unicast** | **vrf** *vrf-name*] *as-id*	Hard reset the BGP connection of the specified AS, or hard reset the BGP connection of the specified address family under the specified AS, and the connection is interrupted.
Rasiecom#**clear ip bgp** [**ipv4 unicast** | **ipv6 unicast** | **vpnv4 unicast** | **vrf** *vrf-name*] *as-id* { **in** | **out** | **soft** }	Soft reset the BGP connection of the specified AS, or soft reset the BGP connection of the specified address family under the specified AS. The connection is not interrupted and only the route is refreshed.
Rasiecom#**clear ip bgp all** [**ipv4 unicast** | **ipv6 unicast** | **vpnv4 unicast** | **vrf** *vrf-name*]	Hard reset all BGP connections, or reset all BGP connections of the specified address family, and the connection is interrupted.
Rasiecom#**clear ip bgp all** [**ipv4 unicast** | **ipv6 unicast** | **pnv4 unicast** | **vrf** *vrf-name*] { **in** | **out** | **soft** }	Soft reset all BGP connections, or reset all BGP connections of the specified address family. The connection is not interrupted and only the route is refreshed.
Rasiecom#**clear ip bgp** *ip-address* [**ipv4 unicast** | **vpnv4 unicast** | **vrf** *vrf-name*]	Hard reset the BGP connection with the specified IP address, and the connection is interrupted.
Rasiecom#**clear ip bgp** *ip-address* [**ipv4 unicast** | **vpnv4 unicast** | **vrf** *vrf-name*] { **in** | **out** | **soft** }	Soft reset the BGP connection of the specified IP address. The connection is not interrupted and only the route is refreshed.
Rasiecom#**clear ip bgp ipv6 unicast** *ipv6-address*	Hard reset the BGP connection with the specified IPv6 address, and the connection is interrupted.

Command	Description
Rasiecom#**clear ip bgp ipv6 unicast** *ipv6-address* { **in** | **out** | **soft** }	Soft reset the BGP connection of the specified IPv6 address. The connection is not interrupted and only the route is refreshed.

8.9 Configuring BGP4+

8.9.1 Configuring BGP4+ basic functions

Enabling BGP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enable BGP and create a BGP instance. Enter BGP configuration mode.
3	Raisecom(config-router)#**bgp router-id** *router-id*	(Optional) configure BGP Router ID. By default, the BGP Router ID is the same as the global Router ID of the router.

Configuring BGP+ peer

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enable BGP and create a BGP instance. Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**neighbor** *ipv6-address* **remote-as** *as-id*	Create a BGP peer and specify the AS ID of the peer.
5	Raisecom(config-router-af)#**neighbor** *ipv6-address1* **update-source** *ipv6-address2*	Use the specified source IPv6 address or local source interface when establishing a BGP

Step	Command	Description
	Raisecom(config-router-af)#**neighbor** *ipv6-address* **update-source** *interface-type interface-number*	connection. Local source interfaces include physical layer interfaces, VLAN interfaces, loopback interfaces, and sub-interfaces. If one of the two ends of the connection is configured with the correct update source, the BGP connection can be successfully established, but there may be a problem that the connection establishment takes too long. To ensure the stability of the connection establishment at both ends, we recommend configuring both ends of the peer with the update source address.
6	Raisecom(config-router-af)#**neighbor** *ipv6-address* **weight** *weight*	(Optional) configure the weight of routes learned from BGP peers. By default, the weight of routes learned from BGP peers is 0.
7	Raisecom(config-router-af)#**neighbor** *ipv6-address* **default-originate** [**route-map** *route-map-name*]	(Optional) enable the function of sending the default route to the peer. By default, no default route is sent to the peer.
8	Raisecom(config-router-af)#**neighbor** *ipv6-address* **next-hop-self**	(Optional) configure the router to modify the next hop address of the route to its own IP address when advertising the route to the peer. By default, when the router advertises routes to IBGP peers, the next-hop IP address of the route is the same as the next-hop IP address of the route in the local BGP routing table.
9	Raisecom(config-router-af)#**neighbor** *ipv6-address* **ebgp-multihop** [*ttl*]	(Optional) configure the peers on the non-directly connected network to establish EBGP connections, and specify the maximum number of hops allowed for EBGP connections. By default, only physically directly-connected peers are allowed to establish EBGP connections.
10	Raisecom(config-router-af)#**neighbor** *ipv6-address* **route-update-interval** *second*	(Optional) configure the interval for sending packets with the same route prefix to the peer.

8.9.2 Configuring BGP4+ advertised routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.

Step	Command	Description
4	Raisecom(config-router-af)#**network** *ipv6-address* [**route-map** *route-map-name*]	Inject static routes into the BGP routing table and advertise them to other ASs or local AS peers.

8.9.3 Configuring BGP4+ redistributed routes

Redistributing default route

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**default-information originate**	Configure the BGP to redistribute the default route.

Redistributing IGP routes

BGP cannot discover routes by itself, so it is necessary to redistribute routes of other protocols (such as IGP or static routes) into the BGP routing table and advertise these routes to other ASs or local AS peers.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**redistribute** { **connected** | **static** | **ripng** | **ospfv3 1** | **isisv6** *process-id* } [**metric** *metric*] [**route-map** *map*]	Configure BGP to redistribute routes of other protocols into the BGP routing table through re-advertising.

8.9.4 Configuring BGP4+ route attributes

Configuring BGP4+ administrative distance

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.

Step	Command	Description
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**distance bgp ebgp** *distance1* **ibgp** *distance2* **local** *distance3*	Configure the administrative distance of the BGP route. • The administrative distance of external routes (routes learned through the EBGP) is 20 by default. • The administrative distance of internal routes (routes learned through the IBGP) is 200 by default. • The administrative distance of local routes (BGP routes redistributed through the aggregation command) is 200 by default.

Configuring default MED of BGP4+ route

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**default-metric** *metric-value*	Configure the default MED of the local BGP router. This configuration only takes effect on imported routes and aggregated routes.

Synchronizing BGP4+ with IGP route

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**synchronization**	Enable BGP and IGP route synchronization. By default, the synchronization between BGP and IGP routes is disabled.

Configuring BGP4+ group attribute

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** [*as-id*]	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**neighbor** *ipv6-address* **send-community standard**	Enable BGP to send standard community attributes to peers. By default, this feature is disabled.
5	Raisecom(config-router-af)#**neighbor** *ipv6-address* **send-community extended**	Enable BGP to send extended community attributes to peers. By default, this feature is disabled.

8.9.5 Configuring BGP4+ network

Configuring BGP4+ route aggregation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**aggregate-address** *ipv6-address/prefix-length*	Configure BGP route aggregation, and advertise aggregated routes and detailed routes.
5	Raisecom(config-router-af)#**aggregate-address** *ipv6-address/prefix-length* **summary-only**	Configure BGP route aggregation and only advertise aggregated routes to suppress detailed routes.
6	Raisecom(config-router-af)#**aggregate-address** *ipv6-address/prefix-length* **as-set**	Configure BGP route aggregation and set the AS_SET option so that the aggregated route includes AS path information of its detailed routes, effectively preventing routing loops.

Configuring BGP4+ route reflector

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.

Step	Command	Description
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**neighbor** *ipv6-address* **route-reflector-client**	Configure the host as a route reflector and use the specified peer as a client of the route reflector. By default, the route reflector is disabled.
5	Raisecom(config-router-af)#**bgp client-to-client reflection**	Enable route reflection between route reflector clients. By default, route reflection between route reflector clients is enabled.

Configuring BGP4+ default local priority

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**bgp default local-preference** *priority*	Configure the default local priority of BGP. By default, the default local priority of BGP is 100.

Configuring BGP4+ route filtering

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip as-path access-list** *access-list-number* { **permint** | **deny** } *regexp*	Configure the filter of the AS path list.
3	Raisecom(config)#**router bgp** [*as-id*]	Enter BGP configuration mode.
4	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
5	Raisecom(config-router-af)#**neighbor** *ipv6-address* **filter-list** *access-list-number* { **in** | **out** }	Configure the BGP route filtering policy based on the AS path list. By default, it is not based on AS path filtering and receives all routing updates from this peer.
6	Raisecom(config-router-af)#**neighbor** *ipv6-address* **route-map** *map-name* { **in** | **out** }	Apply routing policies to the specified peers to filter received or advertised routes.

Step	Command	Description
7	Raisecom(config-router-af)#**neighbor** *ipv6-address* **prefix-list** *prefix-list-name* { **in** | **out** }	Configure the specified peer to filter the received or advertised routes based on IP prefix list.

8.9.6 Configuring BGP4+ authentication

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router bgp** *as-id*	Enter BGP configuration mode.
3	Raisecom(config-router)#**address-family ipv6**	Enter BGP IPv6 address family configuration mode.
4	Raisecom(config-router-af)#**neighbor** *ipv6-address* **password** *password*	Enable BGP peers to establish MD connections and perform MD5 authentication on BGP packets. By default, this feature is disabled.

8.9.7 Checking configurations

Step	Command	Description
1	Raisecom#**show ip bgp ipv6 unicast summary**	Show summary information about IPv6 BGP peers.
23	Raisecom#**show ip bgp ipv6 unicast neighbors** [*ipv6-address*]	Show the status information about IPv6 BGP peers.
3	Raisecom#**show ip bgp ipv6 unicast dampening dampened-paths**	Show suppressed routing information in the IPv6 unicast routing table.
4	Raisecom#**show ip bgp ipv6 unicast dampening flap-statistics**	Show the statistics of route flapping in the IPv6 unicast routing table.
5	Raisecom#**show ip bgp ipv6 unicast** [*ipv6-address* | *ipv6-address/prefix-length*]	Show information about the specified network in the BGP routing table.

8.9.8 Maintenance

For BGP4+ maintenance commands, refer to section 8.9.8 Maintenance.

8.10 Configuring RIP

8.10.1 Configuring basic RIP functions

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router rip**	Enable RIP, and enter RIP configuration mode.
3	Raisecom(config-rip)#**network** *ip-address*	Configure a directly-connected and effective network based on RIP.
4	Raisecom(config-rip)#**offset-list** access-list-name { **in** | **out** } offset-value [*interface-type interface-number*]	Configure the additional metrics when the interface receives or sends RIP routes. By default, it is 0.
5	Raisecom(config-rip)#**passive-interface** { *interface-type interface-number* | **default** }	(Optional) configure the interface to be a passive interface. By default, it is a non-passive interface.

8.10.2 Configuring RIP version

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router rip**	Enable RIP, and enter RIP configuration mode.
3	Raisecom(config-rip)#**version** *version-id* Raisecom(config-rip)#**exit**	Configure global RIP version ID. By default, global RIP version is not configured. In this case, interfaces which are configured with RIP but not configured with the RIP version in the Tx direction will send V1 packets. Interfaces which are enabled with RIP but not configured with the RIP version in the Rx direction will receive packets of any version.
4	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
5	Raisecom(config-port)#**ip rip receive version** { **1** | **2** }*	Configure the receiving RIP version. By default, the receiving RIP version is subjected to the global RIP version.
6	Raisecom(config-port)#**ip rip send version** { **1** | **2** } *	Configure the sending RIP version. By default, the sending RIP version is subjected to the global RIP version.
7	Raisecom(config-port)#**ip rip v2-broadcast**	Configure the interface which runs RIPv2 to send broadcast updates. By default, it sends multicast updates.

You can configure RIP version globally and on the interface of the RAX721-A. If the interface is configured with RIP version, then this RIP version prevails.

8.10.3 Redistributing external routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router rip**	Enable RIP, and enter RIP configuration mode.
3	Raisecom(config-rip)#**host-route**	Enable the function of receiving host routes. By default, it is enabled.
4	Raisecom(config-rip)#**default-information originate**	Enable broadcasting the default route. By default, it is disabled.
5	Raisecom(config-rip)#**redistribute** { **static** | **connected** | **isis** *area-tag* | **bgp** | **ospf** *process-id* } [**metric** *metric*] [**route-map** *map-name*] [**tag** *tag-value*]	Configure the policy for redistributing RIP routes.
6	Raisecom(config-rip)#**default-metric** *metric*	Configure the default metrics of redistributing external routes. By default, it is 1.
7	Raisecom(config-rip)#**auto-summary**	Enable automatic aggregation (support RIPv2 only). By default, it is enabled.
8	Raisecom(config-rip)#**validate-update-source**	Enabled the function of checking the source IP address of the received RIP packets. By default, it is enabled.

8.10.4 Configuring timer

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router rip**	Enable RIP, and enter RIP configuration mode.
3	Raisecom(config-rip)#**timers basic** update-time invalid-time holddown-time flush-time	Configure RIP timer. By default, the update interval is 30s. The invalid interval is 180s. The suppression interval is 120s. The refreshing interval is 120s.

8.10.5 Configuring loop suppression

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip rip split-horizon**	Enable split horizon on the interface, that is, the route learned from one interface will not be broadcasted back to the interface again. Be default, it is enabled.
4	Raisecom(config-port)#**ip rip poisoned-reverse**	Enable poison reverse on the interface, that is, the route learned from one interface can be advertised to other interfaces through this interface. However, the metrics of those routes is configured to 16, namely, unreachable. By default, it is disabled.

Note

If poison reverse and split horizon are enabled together, split horizon will be invalid.

8.10.6 Configuring RIP authentication

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ip rip authentication mode** { **text** | **md5** }	Configure the packet authentication mode on the interface. By default, the authentication mode of RIP packets on the interface is no authentication.
4	Raisecom(config-port)#**ip rip authentication string** *password-string*	Configure the interface-associated password.
5	Raisecom(config-port)#**ip rip authentication key-chain** *key-chain-name*	Configure the interface-associated authentication secret string.

8.10.7 Configuring routing policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router rip**	Enable RIP, and enter RIP configuration mode.

Step	Command	Description
3	Raisecom(config-rip)#**distribute-list** { **ip-access-list** *acl-number* | **prefix-list** *list-name* | **route-map** *rmap-name* } **in** [*interface-type interface-number*]	Configure RIP ingress routing policy.
4	Raisecom(config-rip)#**distribute-list** { **ip-access-list** *acl-number* | **prefix-list** *list-name* | **route-map** *rmap-name* } **out** [*interface-type interface-number*]	Configure RIP egress routing policy.
5	Raisecom(config-rip)#**distribute-list gateway** *list-name* **in** [*interface-type interface-number*]	Execute routing policies on the source address of the received packets through RIP.

8.10.8 Configuring route calculation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router rip**	Enable RIP, and enter RIP configuration mode.
3	Raisecom(config-rip)#**distance** *distance-value* [*ip-address wild-card-mask*]	Configure the administrative distance of RIP, namely, the protocol priority. The shorter the administrative distance is, the higher the priority will be. By default, the administrative distance is 120.
4	Raisecom(config-rip)#**maximum load-balancing** *number*	Configure the maximum number of IP equal-cost multi-path load balancing paths.

8.10.9 Checking configurations

No.	Command	Description
1	Raisecom#**show ip rip**	Show basic information about RIP.
2	Raisecom#**show ip rip database**	Show information about RIP routing database.
3	Raisecom#**show ip rip interface** [*interface-type interface-number*]	Show configurations and status of the interface which runs RIP.

8.11 Configuring RIPng

8.11.1 Configuring RIPng basic functions

Starting RIPng process

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ripng**	Start the RIPng process and enter RIPng configuration mode.
3	Raisecom(config-ripng)#**network** *interface-type interface-number*	Configure the network where RIPng direct connection is valid.
4	Raisecom(config-ripng)#**ipv6 ripng offset-list** *ipv6-access-list-name* { **in** | **out** } *offset-value* Raisecom(config-ripng)#**exit**	Configure additional metrics when the interface receives or sends RIPng routes. By default, the additional metric value when an interface receives or sends a RIPng route is 0.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
6	Raisecom(config-port)#**ipv6 ripng enable**	Enable RIPng capacity on the interface.

Configuring RIPng passive interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ipv6 ripng passive-interface enable**	Configure the interface as a RIPng passive interface. By default, no interface is passive interface.

8.11.2 Controlling routing information

Redistributing routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ripng**	Start the RIPng process and enter RIPng configuration mode.

Step	Command	Description
3	Raisecom(config-ripng)#**redistribute** { **static** | **connected** | **isisv6** *area-tag* | **bgp4+** | **ospfv3** *process-id* } [**metric** *metric*] [**route-map** *map-name*] [**tag** *tag-value*]	Configure the RIPng route redistributing policy.
4	Raisecom(config-ripng)#**default-metric** *metric*	Configure the default metric for the redistributed external routes. By default, the metric of the redistributed external routes is 1.

Configuring broadcast default route

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ripng**	Start the RIPng process and enter RIPng configuration mode.
3	Raisecom(config-ripng)#**default-information originate** Raisecom(config-ripng)#**exit**	Enable broadcast default route. By default, it is disabled.

Advertising aggregated routes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
4	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
5	Raisecom(config-port)#**ipv6 ripng summary-address** *ipv6-address/m*	Advertise the aggregated IPv6 prefix information on the interface.

8.11.3 Configuring timer

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ripng**	Start the RIPng process and enter RIPng configuration mode.
3	Raisecom(config-ripng)#**timers basic** *update-time invalid-time holddown-time flush-time*	Configure the RIPng timer. By default, the update interval is 30s, the failure interval is 180s, the suppression interval is 120s, and the refresh interval is 120s.

8.11.4 Configuring loop suppression

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ipv6 ripng split-horizon**	Enable split horizon, that is, the routes learned from an interface will not be broadcast back to the interface. By default, split horizon is enabled.
4	Raisecom(config-port)#**ipv6 ripng poisoned-reverse**	Enable poison reverse, that is, the routes learned from an interface can also be advertised out from this interface, but the metric of these routes has been set to 16, which is unreachable. By default, poison reverse is disabled.

Note

If poison reverse and split horizon are enabled at the same time, split horizon will be invalid.

8.11.5 Configuring RIPng authentication

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ipv6 ripng ipsec policy** *policy-name* Raisecom(config-port)#**exit**	Configuring IPsec authentication on the interface.
4	Raisecom(config)#**router ripng**	Start the RIPng process and enter RIPng configuration mode.
5	Raisecom(config-ripng)#**ipsec policy** *policy-name*	Configure process IPsec authentication.

8.11.6 Configuring routing policy

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ripng**	Start an RIPng process and enter RIP configuration mode.

Step	Command	Description
3	Raisecom(config-ripng)#**distribute-list** { **ipv6-access-list** *acl-number* | **prefix-list** *list-name* | **route-map** *rmap-name* } **in** [*interface-type interface-number*]	Configure the routing policy of RIPng in the ingress direction.
4	Raisecom(config-ripng)#**distribute-list** { **ipv6-access-list** *acl-number* | **prefix-list** *list-name* | **route-map** *rmap-name* } **out** [*interface-type interface-number*]	Configure the routing policy of RIPng in the egress direction.

8.11.7 Configuring route calculation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ripng**	Start an RIPng process and enter RIP configuration mode.
3	Raisecom(config-ripng)#**distance** *distance-value*	Configure the RIPng administrative distance, namely, the routing priority. The smaller the administrative distance is, the higher the priority will be. By default, the RIPng administrative distance is 120.

8.11.8 Checking configurations

No.	Command	Description
1	Raisecom#**show ipv6 ripng protocol**	Show RIPng basic information.
2	Raisecom#**show ipv6 ripng database** [**statistics**]	Show information about the RIPng routing database.
3	Raisecom#**show ipv6 ripng interface** [*interface-type interface-number*]	Show configurations and status of the interface running RIPng.

9 QoS

This chapter describes principles and configuration procedures of QoS, as well as related configuration examples, including following sections:

- Configuring ACL
- Configuring priority trust and priority mapping
- Configuring traffic classification and traffic policy
- Configuring congestion avoidance and queue shaping
- Configuring interface rate limiting
- Configuring hierarchical bandwidth rate limiting
- Configuring traffic statistics
- Maintenance

9.1 Configuring ACL

9.1.1 Preparing for configurations

Scenario

To filter data packets, the device needs to be configured with ACL to identify data packets to be filtered. Devices allow/disallow related data packets to pass based on pre-configured policies unless they identify specified data packets.

Prerequisite

N/A

9.1.2 Configuring ACL

Select Steps 3–7 as required.

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

Step	Command	Description
2	Raisecom(config)#**access-list** *acl-number*	Create an ACL, select an ACL value, and enter the corresponding ACL configuration mode. The value of *acl-number* parameter defines the type of ACL configuration mode. • Values 1000–0999: basic IP ACL • Values 2000–2999: extended IP ACL • Values 3000–3999: MAC ACL • Values 4000–4999: MPLS ACL • Values 5000–5999: user-defined ACL • Values 6000–6999: basic IPv6 ACL • Vaules 7000–7999: extended IPv6 ACL • Values 8000–8999: advanced ACL
3	Raisecom(config-acl-ip-std)#**rule** [*rule-id*] { **deny** | **permit** } { *source-ip-address source-ip-mask* | **any** } [**time-range** *time-range-name*]	Configure the basic IP ACL rule in basic IP ACL configuration mode.
4	Raisecom(config-acl-ip-ext)#**rule** [*rule-id*] { **deny** | **permit** } { *protocol-id* | **icmp** | **ip** } { *source-ip-address source-ip-mask* | **any** } { *destination-ip-address destination-ip-mask* | **any** } [**dscp** *dscp-value* | **precedence** *precedence-value* | **tos** *tos-value*] [**ttl** *ttl-value*] [**vrf** *vrf-name*] [**vni** *vni-value*] [**fragment**] [**time-range** *time-range-name*]	(Optional) configure the extended IP ACL rule in IP ACL configuration mode.
	Raisecom(config-acl-ip-ext)#**rule** [*rule-id*] { **deny** | **permit** } **udp** { *source-ip-address source-ip-mask* | **any** } [*source-port*]{ *destination-ip-address destination-ip-mask* | **any** } [*destination-port*] [**dscp** *dscp-value* | **precedence** *precedence-value* | **tos** *tos-value*] [**ttl** *ttl-value*] [**vrf** *vrf-name*] [**vni** *vni-value*] [**fragment**] [**time-range** *time-range-name*]	
	Raisecom(config-acl-ip-ext)#**rule** [*rule-id*] { **deny** | **permit** } **tcp** { *source-ip-address source-ip-mask* | **any** } [*source-port*]{ *destination-ip-address destination-ip-mask* | **any** } [*destination-port*] [**tcpflag** *flag-value* **tcpflagmask** *mask-value*] [**dscp** *dscp-value* | **precedence** *precedence-value* | **tos** *tos-value*] [**ttl** *ttl-value*] [**vrf** *vrf-name*] [**vni** *vni-value*] [**url-group** *group-value*] [**fragment**] [**time-range** *time-range-name*]	

Step	Command	Description
	Raisecom(config-acl-ip-ext)#**rule** [*rule-id*] { **deny** | **permit** } **icmp** { *source-ip-address source-ip-mask* | **any** } { *destination-ip-address destination-ip-mask* | **any** } **icmp-type** *type-value* [*type-value*] [**dscp** *dscp-value* | **precedence** *precedence-value* | **tos** *tos-value*] [**ttl** *ttl-value*] [**vrf** *vrf-name*] [**vni** *vni-value*] [**fragment**] [**time-range** *time-range-name*]	
5	Raisecom(config-acl-mac)#**rule** [*rule-id*] { **deny** | **permit** } { *source-mac-address source-mac-mask* | **any** } { *destination-mac-address destination-mac-mask* | **any** } [**ethertype** { *ethertype* [*ethertype-mask*] | **ip** | **arp** }] [**svlan** *svlanid*] [**cvlan** *cvlanid*] [**svlan-cos** *svlan-cos*] [**cvlan-cos** *cvlan-cos*] [**time-range** *time-range-name*]	(Optional) configure the MAC ACL rules in MAC ACL configuration mode.
6	Raisecom(config-acl-mpls)#**rule** [*rule-id*] { **deny** | **permit** } **label** { *label-value* | **any** } [**exp** *exp-value*] [**ttl** *ttl-value*] [**second-label** { *label-value* | **any** } [**second-exp** *exp-value*] [**second-ttl** *ttl-value*]] [**third-label** { *label-value* | **any** } [**third -exp** *exp-value*] [**third -ttl** *ttl-value*]] [**time-range** *time-range-name*]	Configure the MPLS ACL rules in MPLS ACL configuration mode.
7	Raisecom(config-acl-udf)#**rule** [*rule-id*] { **deny** | **permit** } [**ethertype** { *ethertype* [*ethertype-mask*] | **ip** | **arp** }] **layer2** *rule-string rule-mask offset* [**second** rule-string rule-mask offset] [**third** { *rule-string rule-mask offset*] [**time-range** *time-range-name*]	Configure user-defined ACL rules in user-defined ACL configuration mode.
8	Raisecom(config-acl-ipv6-std)#**rule** [*rule-id*] { **deny** | **permit** } { *source-ip-address/prefix-length* | **any** } [**time-range** *time-range-name*]	Configure IPv6 ACL rules in IPv6 ACL configuration mode.
9	Raisecom(config-acl-ipv6-ext)#**rule** [*rule-id*] { **deny** | **permit** } **tcp** { *source-ip-address/prefix-length* | **any** } [*source-port*] { *destination-ip-address/prefix-length* | **any** } [*destination-port*] [**tcpflag** *flag-value* **tcpflagmask** *mask-value*] [**dscp** *dscp-value*] [**flow-label** *label-value*] [**fragment**] [**time-range** *time-range-name*]	(Optional) configure the extended IPv6 ACL rules in extended IPv6 ACL configuration mode.

Step	Command	Description
	Raisecom(config-acl-ipv6-ext)#**rule** [*rule-id*] { **deny** | **permit** } **udp** { *source-ip-address/prefix-length* | **any** } [*source-port*] { *destination-ip-address destination-ip-mask* | **any** } [*destination-port*] [**dscp** *dscp-value*] [**flow-label** *label-value*] [**fragment**] [**time-range** *time-range-name*]	
	Raisecom(config-acl-ipv6-ext)#**rule** [*rule-id*] { **deny** | **permit** } **icmpv6** { *source-ip-address/prefix-length* | **any** } { *destination-ip-address destination-ip-mask* | **any** } [**icmpv6-type** *icmpv6-value* [*icmpv6-code*]] [**dscp** *dscp-value*] [**flow-label** *label-value*] [**fragment**] [**time-range** *time-range-name*]	
10	Raisecom(config-acl-advanced)#**rule** [*rule-id*] { **deny** | **permit** } { *source-mac-address source-mac-mask* | **any** } { *destination-mac-address destination-mac-mask* | **any** } [**svlan** *svlanid*] [**cvlan** *cvlanid*] [**cos** *cos-value*] [**inner-cos** *inner-cos-value*] { *source-ip-address source-ip-mask* | **any** } { *destination-ip-address destination-ip-mask* | **any** } [**dscp** *dscp-value* | **precedence** *precedence-value* | **tos** *tos-value*] [**ttl** *ttl-value*] [**fragment**] [**time-range** *time-range-name*]	Configure Advanced ACL rules.
11	Raisecom(config)#**access-list copy** *dest-acl-number source-acl-number*	Copy to generate the same ACL rule.

9.1.3 Creating time period

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**time-range** *time-range-name start-time* **to** *end-time* { *weekday-list* | **mon** | **tue** | **wed** | **thu** | **fri** | **sta** | **sun** | **off-day** | **working-day** | **daily** } [**from** *time date* [**to** *time date*] | **to** *time date*]	Create the time period, which can be referred to by the ACL rule.
	Raisecom(config)#**time-range** *time-range-nam* { **from** *time date* [**to** *time date*] | to *time date* }	

9.1.4 Configuring filter

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**filter** { **ingress** | **egress** } **access-list** { *acl-number* | **name** *acl-name* } [**statistics**] Raisecom(config-port)#**exit**	Apply the ACL rule to the ingress and egress interfaces. The ACL rule cannot be modified once it is applied to the interface and the number of ACL rules must be greater than 0.
4	Raisecom(config)#**clear filter statistics interface** *interface-type interface-number* { **ingress** | **egress** } [**access-list** { *acl-number* | **name** *acl-name* }]	(Optional) clear filter statistics.

9.1.5 Checking configurations

No.	Command	Description
1	Raisecom#**show access-list** [*acl-number* | **name** *acl-name*]	Show ACL information.
2	Raisecom#**show filter interface**	Show filter information.
	Raisecom#**show filter interface** *interface-type interface-number* [**ingress** | **egress**]	
	Raisecom#**show filter statistics interface** *interface-type interface-number* { **ingress** | **egress** } **access-list** *acl-number* { *acl-number* | **name** *acl-name* }	
3	Raisecom#**show time-range** [*time-range-name*]	Show configurations of the time period.

9.2 Configuring priority trust and priority mapping

9.2.1 Preparing for configurations

Scenario

For packets from upstream devices, you can select to trust the priorities taken by these packets. For packets whose priorities are not trusted, you can process them with traffic classification and traffic policy. In addition, you can modify DSCP priorities by configure interface-based DSCP priority remarking. After configuring priority trust, the RAX721-A can perform different operations on packets with different priorities, providing related services.

Before performing queue scheduling, you need to assign a local priority for a packet. For packets from the upstream device, you can map the outer priorities of these packets to various local priorities. In addition, you can directly configure local priorities for these packets based on interfaces. And then device will perform queue scheduling on these packets basing on local priorities.

In general, for IP packets, you need to configure the mapping between DHCP priority and local priority, and mapping between IP Precedence (IPP) and local priority. For VLAN packets, you need to configure the mapping between CoS priority and local priority. For MPLS packets, you need to configure the mapping between the Exp field and the local priority.

Prerequisite

N/A

9.2.2 Configuring priority trust

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter interface configuration mode.
3	`Raisecom(config-port)#mls qos trust { cos | dscp }`	Configure the priority trusted by an interface. By default, the Layer 2 interface trusts the CoS priority and the Layer 3 interface trusts the DHCP priority.
4	`Raisecom(config-port)#mls qos trust ipp`	Configure the interface to trust IPP.
5	`Raisecom(config-port)#mls qos trust port-priority`	Configure the interface to trust interface priority.
6	`Raisecom(config-port)#mls qos priority` *priority*	Configure the interface priority. By default, it is 5.

9.2.3 Configuring mapping between DSCP priority and local priority based on interface

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#mls qos mapping dscp-to-local-priority` *profile-id*	Create the DSCP-to-local priority (color) mapping profile and enter dscp-to-pri configuration mode.
3	`Raisecom(dscp-to-pri)#dscp` *dscp-value* `to local-priority` *localpri-value* `[ color { green | red | yellow } ]`	Configure mapping between the DSCP priority and local priority (color).
4	`Raisecom(dscp-to-pri)#exit` `Raisecom(config)#interface` *interface-type interface-number*	Exit dscp-to-pri configuration mode. Enter interface configuration mode.

Step	Command	Description
5	Raisecom(config-port)#**mls qos dscp-to-local-priority** *profile-id*	Apply the DSCP-to-local priority (color) mapping profile to an interface.

9.2.4 Configuring mapping between CoS priority and local priority based on interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos mapping cos-to-local-priority** *profile-id*	Create the CoS-to-local priority (color) mapping profile and enter cos-to-pri configuration mode.
3	Raisecom(dscp-to-pri)#**cos** *cos-value* **to local-priority** *localpri-value* [**color** { **green** | **red** | **yellow** }]	Configure mapping between the CoS priority and local priority (color).
4	Raisecom(dscp-to-pri)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Exit cos-to-pri configuration mode. Enter interface configuration mode.
5	Raisecom(config-port)#**mls qos cos-to-local-priority** *profile-id* [**dei enable**]	Apply the CoS-to-local priority (color) mapping profile to an interface or enable color marking for outgoing packets on the interface.

9.2.5 Configuring DSCP priority remarking

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos mapping dscp-mutation** *profile-id*	Create the DSCP remarking profile and enter dscp-mutation configuration mode.
3	Raisecom(dscp-mutation)#**dscp** *dscp-value* **to new-dscp** *dscp-value*	Remark the DSCP priority of specified packets.
4	Raisecom(dscp-mutation)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Exit dscp-mutation configuration mode. Enter interface configuration mode.
5	Raisecom(config-port)#**mls qos dscp-mutation** *profile-id*	Apply the DSCP remarking profile to an interface.

9.2.6 Configuring CoS priority remarking

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos mapping cos-remark** *profile-id*	Create the CoS remarking profile and enter dscp-remark configuration mode.
3	Raisecom(cos-remark)#**local-priority** *localpri-value* **to cos** *cos-value*	Configure the mapping between the local priority and CoS priority.
4	Raisecom(cos-remark)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Exit cos-remark configuration mode. Enter interface configuration mode.
5	Raisecom(config-port)# **mls qos cos-remark-mapping enable** [**dei enable**]	Enable local priority-to-CoS mapping or enable color marking for outgoing packets on the interface.
6	Raisecom(config-port)#**mls qos cos-remark** *profile-id*	Apply the CoS remarking profile to an interface.

9.2.7 Checking configurations

No.	Command	Description
1	Raisecom#**show mls qos mapping dscp-to-local-priority** [**default** | *profile-id*]	Show information about the DSCP-to-local priority (color) mapping profile.
2	Raisecom#**show mls qos mapping cos-to-local-priority** [**default** | *profile-id*]	Show information about the CoS-to-local priority (color) mapping profile.
3	Raisecom#**show mls qos mapping dscp-mutation** [**default** | *profile-id*]	Show information about the DSCP remarking profile.
4	Raisecom#**show mls qos mapping cos-remark** [**default** | *profile-id*]	Show information about the CoS remarking profile.
5	Raisecom#**show mls qos mapping local-priority-to-exp** [**default** | *profile-id*]	Show information about the local-to-Exp priority mapping profile.
6	Raisecom#**show mls qos interface** [*interface-type interface-number*]	Show QoS information on the interface.

9.3 Configuring traffic classification and traffic policy

9.3.1 Preparing for configurations

Scenario

Traffic classification is the basis of QoS. For packets from upstream devices, you can classify them according to ACL rules. After traffic classification, the device can provide related operations for different packets, providing differentiated services.

After configurations, the traffic classification cannot take effect until being bound to traffic policy. The selection of traffic policy depends on the packet status and current network load status. In general, when a packet is sent to the network, you need to limit the speed according to Committed Information Rate (CIR) and remark the packet according to the service feature.

Prerequisite

N/A

9.3.2 Creating and configuring traffic classification

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**class-map** *class-map-name* [**match all** | **match any**]	Create traffic classification and enter CMAP configuration mode.
3	Raisecom(config-cmap)#**match access-list** { *acl-number* | **name** *acl-name* }	Define the ACL matched with the traffic classification. ACL rules cannot be modified once they are applied to the interface. The number of ACL rules must be greater than 0.
	Raisecom(config-cmap)#**match** { **dscp** *dscp-list* | **cos** *cos-list* | **inner-cos** *cos-list* | **inner-vlan** *inner-vlan-list* | **ip precedence** *ipp-list* | **ip tos** *tos-list* | **ipv6 dscp** *dscp-list* | **label** *lable-list* | **second-label** *lable-list* | **vlan** *vlan-list* }	Configure the rule lists of various types that match the traffic classification rule. • **dscp** *dscp-list*: match the DSCP value. • **cos** *cos-list*: match the CoS. • **inner-cos** *cos-list*: match the inner CoS. • **inner-vlan** *inner-vlan-list*: match the inner VLAN list. • **ip precedence** *ipp-list*: match the IP priority. • **ip tos** *tos-list*: match the ToS. • **ipv6 dscp** *dscp-list*: match the IPv6 DSCP value. • **label** *lable-list*: match the label value. • **second-label** *lable-list*: match the second-label value. • **vlan** *vlan-list*: match the VLAN list.

9.3.3 Creating and configuring traffic policing profile

To perform traffic policing on packets, you need to configure traffic policing profile and then quote this profile under the traffic classification, which is bound to traffic policy.

On the traffic policing profile, you can configure traffic policing rules or perform relate operations on specified packets based on color.

The single bucket does not support the color-sensitive mode or commands with the yellow key word.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos policer-profile** *policer-name* [**single**]	Create the traffic policing profile and enter traffic policing profile configuration mode.
3	Raisecom(traffic-policer)#**drop-color** { **red** | **yellow** } *	(Optional) discard packets with specified color.
4	Raisecom(traffic-policer)#**set-cos** { **green** *green-value* [**red** *red-value*] [**yellow** *yellow-value*] | **red** *red-value* }	(Optional) configure the mapping between packet color and CoS priority.
5	Raisecom(traffic-policer)#**set-dscp** { **green** *green-value* [**red** *red-value*] [**yellow** *yellow-value*] | **red** *red-value* }	(Optional) configure the mapping between packet color and DHCP priority.
6	Raisecom(traffic-policer)#**recolor** { **green-recolor** { **red** | **yellow** } | **red-recolor** { **green** | **yellow** } | **yellow-recolor** { **green** | **red** } } *	(Optional) re-color the packet. QoS use the CAR to classify and color the packet. The downstream network can accept the color result of the upstream network or re-color the packet based on its classification standard.
7	Raisecom(traffic-policer)#**cir** *cir* **cbs** *cbs* [**ebs** *ebs*]	(Optional) configure rate limiting parameters.
	Raisecom(traffic-policer)#**cir** *cir* **cbs** *cbs* **eir** *eir* **ebs** *ebs* [**coupling**]	
	Raisecom(traffic-policer)#**cir** *cir* **cbs** *cbs* **pir** *pir* **pbs** *pbs*	

9.3.4 Creating and configuring traffic policy

Steps 5–10 are coordinate. You can select one as required.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**policy-map** *policy-map-name*	Create a traffic policy and enter PMAP configuration mode.

Step	Command	Description
3	Raisecom(config-pmap)#**class-map** *class-map-name*	Add the traffic classification to the traffic policy and enter CMAP configuration mode. **Note** The traffic classification, bound with the traffic policy, must be based on at least one rule. Otherwise, the binding operation fails. When the traffic policy is applied to an interface, you cannot delete the bound traffic classification or modify its configuration. One traffic classification can be applied to multiple traffic policies.
4	Raisecom(config-pmap-c)#**policer** *policer-name*	Import a traffic policing profile (policer) into the traffic policy.
5	Raisecom(config-pmap-c)#**set** { **cos** *cos-value* | **local-priority** *value* } Raisecom(config-pmap-c)#**set** { **inner-vlan** *inner-vlan-id* | **vlan** *vlan-id* }	(Optional) configure packet remarking.
6	Raisecom(config-pmap-c)#**add outer-vlan** *vlan-id*	(Optional) configure the VLAN ID of the added outer VLAN Tag.
7	Raisecom(config-pmap-c)#**redirect-to** *interface-type interface-number*	(Optional) configure the redirection rule to forward matched packets through the specified interface.
8	Raisecom(config-pmap-c)#**copy-to-mirror mirror-group** *group-id*	(Optional) copy the traffic to the mirroring monitoring interface.
9	Raisecom(config-pmap-c)#**forward-to-cpu**	(Optional) forward traffic to the CPU.
10	Raisecom(config-pmap-c)#**statistics enable**	(Optional) enable traffic statistics.
11	Raisecom(config-pmap-c)#**exit** Raisecom(config-pmap)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Exit CMAP configuration mode. Exit PMAP configuration mode. Enter interface configuration mode.
12	Raisecom(config-port)#**service-policy** { **ingress** | **egress** } *policy-map-name*	Apply the traffic policy to an interface.

9.3.5 Checking configurations

No.	Command	Description
1	Raisecom#**show class-map** [*class-map-name*]	Show traffic classification information.
2	Raisecom#**show mls qos policer** [*policer-name*]	Show traffic policing rules.
3	Raisecom#**show policy-map** [*policy-map-name*] [**class-map** *class-map-name*]	Show traffic policy information.

No.	Command	Description
4	Raisecom#**show service-policy interface**	Show information about applied policies.
	Raisecom#**show service-policy interface** *interface-type interface-number* [**egress** | **ingress**]	
5	Raisecom#**show service-policy statistics interface** *interface-type interface-number* { **egress** | **ingress** } **policy-map** *policy-map-name* [**class-map** *class-map-name*]	Show statistics about applied traffic policies.

9.4 Configuring congestion avoidance and queue shaping

9.4.1 Preparing for configurations

Scenario

To prevent network congestion from occurring and to resolve TCP global synchronization, you can configure congestion avoidance to adjust the network traffic and resolve network overload. The RAX721-A supports WRED-based congestion avoidance.

When the interface speed of downstream devices is smaller than the one of upstream devices, congestion avoidance may occur on interfaces of downstream devices. At this time, you can configure queue and traffic shaping on the egress interface of upstream devices to shape upstream traffic.

Prerequisite

N/A

9.4.2 Configuring WRED profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos wred profile** *profile-id*	Create the WRED profile and enter WRED profile configuration mode.
3	Raisecom(wred)#**wred** [**color** { **green** | **red** | **yellow** }] **start-drop-threshold** *start-drop* **end-drop-threshold** *end-drop* **max-drop-probability** *max-drop*	Configure WRED profile information. For non-TCP packets, it does not distinguish the color. You need to configure the **wred start-drop-threshold**/**wred color green** parameter.
4	Raisecom(wred)#**wred start-drop-threshold** *start-value* **end-drop-threshold** *end-value* **max-drop-probability** *max-value*	Configure the drop threshold of the WRED profile.

9.4.3 Configuring flow queue profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos flow-queue profile** *flow-profile-id*	Create a flow profile and enter flow profile configuration mode.
3	Raisecom(flow-queue)#**scheduler wrr**	Configure the queue scheduling policy. By default, it is SP.
4	Raisecom(flow-queue)#**queue** *queue-id* [**weight** *weight-value*] [**shaping cir** *cir-value* [**cbs** *cbs-value*] **pir** *pir-value* [**pbs** *pbs-value*]] [**wred profile** *profile-id*]	Configure the queue, weight, shaping, and WRED information of the flow profile. If no weight is configured, SP scheduling mode is adopted.
5	Raisecom(flow-queue)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Exit flow profile configuration mode. Enter interface configuration mode.
6	Raisecom(config-port)# **mls qos flow-queue** *profile-id*	Apply the flow profile to an interface.

9.4.4 Configuring queue shaping

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**mls qos shaping egress pir** *pir-value* [**pbs** *pbs-value*]	Configure queue shaping for queues of the interface.

9.4.5 Checking configurations

No.	Command	Description
1	Raisecom#**show mls qos wred profile** [*profile-list*]	Show WRED profile configurations.
2	Raisecom#**show mls qos flow-queue profile** *flow-profile-list*	Show flow profile configurations.
3	Raisecom#**show mls qos shaping interface** [*interface-type interface-number* **egress**]	Show queue shaping information.
4	Raisecom#**show mls qos queue statistics interface** *interface-type interface-number*	Show queue statistics of the interface.

9.5 Configuring interface rate limiting

9.5.1 Preparing for configurations

Scenario

To avoid/remit network congestion, you can configure interface-based rate limiting. Rate limiting is used to make packets transmitted at a relative average speed by controlling the burst traffic on an interface.

Prerequisite

N/A

9.5.2 Configuring interface-based rate limiting

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**rate-limit ingress cir** *cir-value* **cbs** *cbs-value* **pir** *pir-value* **pbs** *pbs-value* Raisecom(config-port)#**exit**	Configure rate limiting in the ingress direction and egress direction of the interface. Rate limiting can be based on the following interfaces: • Layer 3 physical interface • VLAN Layer 2 physical interface • Sub-interface • Link aggregation interface
4	Raisecom(config)#**rate-limit mode** { **l1** | **l2** }	(Optional) configure the rate limiting mode. • l1: physical layer mode • l2: data link layer mode

9.5.3 Checking configurations

No.	Command	Description
1	Raisecom#**show rate-limit interface**	Show interface-based rate limiting.
	Raisecom#**show rate-limit interface** *interface-type interface-number* [**ingress** | **egress**]	

9.6 Configuring hierarchical bandwidth rate limiting

9.6.1 Preparing for configurations

Scenario

In order to ensure that special services can still be transmitted as required when the network is congested, you can configure hierarchical bandwidth rate limiting. Configure a bandwidth guarantee profile and a hierarchical bandwidth guarantee profile to match the packets received on the interface with the profile to ensure the normal transmission of special services.

Prerequisite

N/A

9.6.2 Configuring bandwidth guarantee

Creating bandwidth guarantee template

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#bandwidth-profile bwp-profile-id cir cir cbs cbs [ pir pir-value pbs pbs-value ] [ color-aware ]`	Create a bandwidth guarantee template.
	`Raisecom(config)#bandwidth-profile bwp-profile-id cir cir cbs cbs eir eir ebs ebs [ color-aware [ coupling ] ]`	
3	`Raisecom(config)#bandwidth-profile bwp-profile-id description word`	Configure the description of the bandwidth guarantee template.

Note

If the bandwidth guarantee template is quoted by other hierarchical templates or is applied, you will fail to delete it.

9.6.3 Configuring hierarchical bandwidth gaurantee

Configuring hierarchical VLAN bandwidth guarantee

No.	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#bandwidth-profile profile-id cir cir cbs cbs [ eir eir ebs ebs ] [ color-aware ]`	Create a bandwidth guarantee template.

No.	Command	Description
3	Raisecom(config)#**hierarchy-vlan bandwidth-profile** *hc-profile-id*	Create a hierarchical VLAN template and enter hierarchical VLAN configuration mode.
4	Raisecom(config-hvlan)#**bandwidth vlanlist** *vlan-list bwp-profile-id* Raisecom(config-hcos)#**exit**	Configure a hierarchical VLAN template.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
6	Raisecom(config-port)#**bandwidth** { **ingress** | **egress** } **vlan** *vlan-id bwp-profile-id*	Apply the VLAN bandwidth rate-limiting template to the interface.
7	Raisecom(config-port)#**bandwidth ingress vlan** *vlan-id* **coslist** *cos-value bwp-profile-id*	Apply the VLAN+CoS bandwidth rate-limiting template to the interface.

Configuring hierarchical CoS bandwidth guarantee

No.	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#**bandwidth-profile** *profile-id* **cir** *cir* **cbs** *cbs* [**eir** *eir* **ebs** *ebs*] [**color-aware**]	Create a bandwidth guarantee template.
3	Raisecom(config)#**hierarchy-cos bandwidth-profile** *hc-profile-id*	Create a hierarchical CoS template and enter HCoS configuration mode.
4	Raisecom(config-hcos)#**bandwidth coslist** *cos-list bwp-profile-id* Raisecom(config-hcos)#**exit**	Configure a hierarchical CoS template.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
6	Raisecom(config-port)#**bandwidth** { **ingress** | **egress** } **vlan** *vlan-id* **coslist** *cos-value bwp-profile-id*	Apply the VLAN+CoS bandwidth rate-limiting template to the interface.
7	Raisecom(config-port)#**bandwidth ingress vlan** *vlan-id bwp-profile-id* **hierarchy-cos** *hcos-profile-id*	Apply the VLAN+CoS hierarchical bandwidth rate-limiting template to the interface.

9.6.4 Checking configurations

No.	Command	Description
1	Raisecom#**show bandwidth-profile** [*bwp-profile-id*]	Show information about the bandwidth guarantee template.
2	Raisecom#**show bandwidth interface** *interface-type interface-number*	Show bandwidth guarantee configurations on the interface.
3	Raisecom#**show hierarchy-cos-bandwidth profile** [*hc-profile-id*]	Show information about the hierarchical CoS bandwidth guarantee template.
4	Raisecom#**show hierarchy-vlan-bandwidth profile** [*hd-profile-id*]	Show information about hierarchical VLAN bandwidth guarantee template.

9.7 Configuring traffic statistics

9.7.1 Configuring performance statistics

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode. By default, it is routing mode.
3	Raisecom(config-port)#**portswitch**	Configure the interface to switch mode.
4	Raisecom(config-port)#**performance statistics enable**	Enable performance statistics on the interface.
5	Raisecom(config-port)#**performance statistics vlan** *vlan-list* [**cos** *cos-value*] **enable** Raisecom(config-port)#**exit**	Enable interface+VLAN or interface+VLAN+CoS performance statistics.
6	Raisecom(config)#**performance statistics interval buckets** *buckets-value*	Configure the interval buckets of performance statistics.

9.7.2 Checking configurations

No.	Command	Description
1	Raisecom#**show performance statistics interval buckets**	Show global performance statistics.

No.	Command	Description
2	Raisecom#**show performance statistics interface** *interface-type interface-number* [**vlan** *vlan-list* [**cos** *cos-value*]] { **current** | **history** }	Show current or history performance statistics on the interface, interface + VLAN, or interface + VLAN + CoS.

9.8 Maintenance

Command	Description
Raisecom(config)#**clear service-policy statistics interface** *interface-type interface-number* { **egress** | **ingress** }	Clearing traffic policy statistics.
Raisecom(config)#**clear service-policy statistics interface** *interface-type interface-number* { **egress** | **ingress** } **policy-map** *policy-map-name* [**class-map** *class-map-name*]	
Raisecom(config)#**clear mls qos queue statistics interface** *interface-type interface-number* [**queueid** *queue-id*]	Clear queue statistics of interfaces.
Raisecom(config)#**clear filter statistics interface** *interface-type interface-number* { **ingress** | **egress** } [**access-list** *acl-number*]	Clear ACL statistics.
Raisecom(config)#**clear performance statistics histroy**	Clear performance statistics on all history groups.

10 Multicast

This chapter describes basic principles and configuration procedures for multicast, and provides related configuration examples, including the following sections:

- Configuring IGMP multicast basic functions
- Configuring IGMP Snooping
- Configuring IGMP Querier
- Configuring IGMP MVR
- Configuring IGMP filtering
- Configuirng multicast VLAN copy
- Configuring PIM
- Configuring MLD L2 multicast
- Configuring MLD L3 multicast

10.1 Configuring IGMP multicast basic functions

10.1.1 Configuring basic functions of L2 multicast

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#igmp mrouter vlan` *`vlan-id interface-type interface-number`*	(Optional) configure the multicast routing interface.
3	`Raisecom(config)#igmp member-timeout { seconds | infinite }`	(Optional) configure the aging time of IGMP members.
4	`Raisecom(config)#igmp ring` *`interface-type interface-number`*	(Optional) enable IGMP ring network forwarding on the interface.
5	`Raisecom(config)#igmp report-suppression`	(Optional) enable Report suppression. Packet suppression and Proxy conflict with each other.
6	`Raisecom(config)#igmp version { 2 | 3 }`	(Optional) configure the IGMP version.

7	Raisecom(config)#**igmp mrouter vlan** *vlan-list* **priority** *priority-number*	(Optional) configure the CoS priority of the IGMP routing VLAN.
8	Raisecom(config-port)#**igmp immediate-leave vlan** *vlan-list*	Configure immediate leave. If the downstream interface is not enabled with immediate leave, the routing interface will calculate the aging time according to the robust coefficient when receiving the leave packet. The group timeout timer is configured to GMI (Group Membership Interval), GMI = (robust-value * lastmember-queryinterval).

10.1.2 Checking configurations

No.	Command	Description
1	Raisecom#**show igmp configuration**	Show IGMP basic configurations.
2	Raisecom#**show igmp mrouter**	Show configurations of the multicast routing interface.
3	Raisecom#**show igmp immediate-leave** [*interface-type interface-number*]	Show configurations of L2 multicast immediate leave.
4	Raisecom#**show igmp statistics** [*interface-type interface-number*]	Show L2 multicast statistics.
5	Raisecom#**show igmp mrouter vlan-priority**	Show the CoS priority of the IGMP routing VLAN.
6	Raisecom#**show igmp ring**	Show information about the IGMP ring network interface.

10.1.3 Maintenance

Command	Description
Raisecom(config)#**clear igmp statistics** [*interface-type interface-number*]	Clear statistics on L2 multicast IGMP.
Raisecom(config)#**no igmp member** *interface-type interface-number*	Delete the specified multicast forwarding entry.

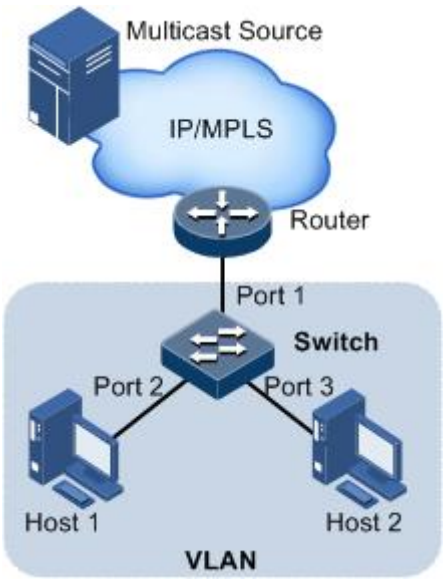
10.2 Configuring IGMP Snooping

10.2.1 Preparing for configurations

Scenario

As shown in Figure 10-1, multiple hosts receive data from the multicast source, and multiple hosts belong to the same VLAN. You can run IGMP Snooping on the switch between the multicast router and the host. You can establish and maintain a multicast forwarding table by monitoring IGMP packets between the multicast router and the host to implement Layer 2 multicast.

Figure 10-1 IGMP Snooping scenario



Prerequisite

Before configuring IGMP Snooping, complete the following tasks:

- Disable multicast VLAN copy on the device.
- Create a VLAN and add the corresponding interface to the VLAN.

10.2.2 Configuring IGMP Snooping

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#igmp snooping`	Enable global IGMP Snooping.
3	`Raisecom(config)#igmp member-timeout { seconds | infinite }`	(Optional) configure the aging time of IGMP members.
4	`Raisecom(config)#igmp snooping vlan vlan-list`	(Optional) enable IGMP Snooping in global VLAN.

Step	Command	Description
5	Raisecom(config)#**vlan** *vlan-id* Raisecom(config-vlan)#**igmp snooping static** *ip-address* [*interface-type interface-number*]	(Optional) configure the static members of IGMP Snooping in VLAN mode.

Note

- IGMP snooping and IGMP MVR cannot be enabled at the same time in the same multicast VLAN, otherwise the configuration fails.
- IGMP Snooping and multicast VLAN copy cannot be enabled at the same time in the same multicast VLAN, otherwise the configuration fails.

10.2.3 Checking configurations

No.	Command	Description
1	Raisecom#**show igmp snooping** [**vlan** *vlan-id* | **member vlan** *vlan-list* | **mrouter vlan-priority**]	Show IGMP Snooping configurations.
2	Raisecom#**show igmp snooping member** [*interface-type interface-number* | **vlan** *vlan-id*]	Show multicast members of IGMP Snooping.
3	Raisecom#**show igmp snooping member count** [*interface-type interface-number* | **vlan** *vlan-id*]	Show the number of IGMP Snooping multicast group members.
4	Raisecom#**show igmp snooping vlan** *vlan-id*	Show configurations of IGMP Snooping in the specified VLAN.

10.3 Configuring IGMP Querier

10.3.1 Preparing for configurations

Scenario

In a network with multicast routing protocols widely applied, there are multiple hosts or client subnets that receive multicast information. You can configure IGMP Querier on the switch connected to the multicast router and the host to intercept the IGMP packets between the host and the router, thus reducing the network burden.

Configuring IGMP Querier can reduce the configuration and management of the client subnet by the multicast router, and at the same time realize the multicast connection of the client subnet.

IGMP Querier is generally used in conjunction with IGMP Snooping or IGMP MVR.

Prerequisite

Before configuring IGMP Querier, perform the following tasks:

- Create a VLAN.
- Add the corresponding interface to the VLAN.

10.3.2 Configuring IGMP Querier

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**igmp querier**	Enable IGMP querier.
3	Raisecom(config)#**igmp source-ip** *ip-address*	(Optional) configure the source IP address for IGMP queriers to send Query packets.
4	Raisecom(config)#**igmp query-interval** *period*	(Optional) configure the IGMP query interval.
5	Raisecom(config)#**igmp query-max-response-time** *period*	(Optional) configure the maximum response time of Query packets.
6	Raisecom(config)#**igmp last-member-query-interval** *period*	(Optional) configure the interval for the last group member to send Query packets.
7	Raisecom(config)#**igmp proxy**	Configure IGMP proxy.

Note

- If IGMP Querier is not enabled, you can configure IGMP Querier, including configuring the source IP address, query interval, maximum response time for sending Query packets, and the interval for the last member to send Query packets. When IGMP Querier is enabled, these configurations take effect immediately.
- IGMP Querier can be activated when IGMP Snooping or IGMP MVR is enabled.
- IGMP Proxy conflicts with IGMP Querier. IGMP Proxy conflicts with IGMP Report-Suppression.

10.3.3 Checking configurations

No.	Item	Description
1	Raisecom#**show igmp querier**	Show configurations of IGMP querier.

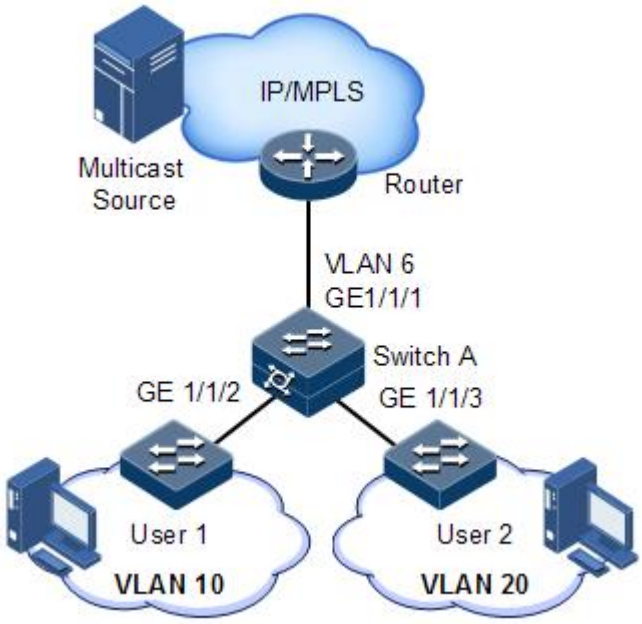
10.4 Configuring IGMP MVR

10.4.1 Preparing for configurations

Scenario

As shown in Figure 10-2, multiple users receive data from the multicast source, and multiple users and multicast routers belong to different VLANs. You can run IGMP MVR on Switch A and configure multicast VLANs to enable users in different VLANs to share the same multicast VLAN to receive the same multicast data, while also reducing bandwidth waste.

Figure 10-2 IGMP MVR application



Prerequisite

Before configuring IGMP MVR, complete the following tasks:

- Disable multicast VLAN copy on the device.
- Create a VLAN and add the corresponding interface to the VLAN.

10.4.2 Configuring IGMP MVR

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#igmp mvr`	Enable IGMP MVR.

Step	Command	Description
3	Raisecom(config)#**igmp mvr mcast-vlan** *vlan-id* **group** { *start-ip-address* [*end-ip-address*] | **any** }	Configure the group address set of multicast VLAN. **Note** After IGMP MVR is enabled on the device, you need to configure the multicast VLAN and the bound group address set. If the received IGMP Report packet does not belong to any VLAN group address set, the report packet is not processed and the user cannot subscribe to multicast flow.
4	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
5	Raisecom(config-gigaethernet1/1/port)#**igmp mvr mcast-vlan** *vlan-id* **static** *ip-address* **user-vlan** *vlan-id*	(Optional) configure the MVR static multicast member.
6	Raisecom(config-gigaethernet1/1/port)#**igmp mvr user-vlan** *vlan-id*	(Optional) configure the effective range of multicast cross VLAN copy.
7	Raisecom(config-gigaethernet1/1/port)#**igmp mvr mcast-vlan** *vlan-id* **static** *ip-address*	(Optional) configure the static multicast members of MVR.

Note

- IGMP MVR and IGMP snooping cannot be enabled at the same time in the same multicast VLAN, otherwise the configuration fails.
- IGMP MVR and multicast VLAN copy cannot be enabled simultaneously in the same multicast VLAN and multicast group, otherwise the configuration fails.

10.4.3 Checking configurations

Step	Command	Description
1	Raisecom# **show igmp mvr** { **interface** | *interface-type interface-number* }	Show configurations of the IGMP MVR of the specified interface.
2	Raisecom#**show igmp mvr member** [*interface-type interface-number* | **user-vlan** *vlan-id*]	Show information about IGMP MVR multicast group members.
3	Raisecom#**show igmp mvr member count** { *interface-type interface-number* | **user-vlan** *vlan-id* }	Show the number of members in the IGMP MVR multicast group.
4	Raisecom#**show igmp mvr vlan-group** [**mcast-vlan** *vlan-id*]	Show the multicast VLAN and its group address set.

10.5 Configuring IGMP filtering

10.5.1 Preparing for configurations

Scenario

Different users in the same multicast have different requirements or permissions to receive multicast packets. It is allowed to configure the filtering rules on the switch connected to the multicast router and the host to restrict the multicast users.

You can also configure the maximum number of multicast groups that users are allowed to join.

IGMP filtering is generally used in conjunction with IGMP Snooping or IGMP MVR.

Prerequisite

Before configuring IGMP, complete the following tasks:

- Create a VLAN.
- Add the corresponding interface to the VLAN.

10.5.2 Enabling IGMP filtering globally

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#igmp filter`	Enable IGMP filtering globally.

Note

When configuring the IGMP filtering templates or the maximum number of groups, you need to execute the **igmp filter** command to enable IGMP filtering globally.

10.5.3 Configuring IGMP filtering template

The IGMP filtering template can be used under the interface, and can also be applied on "interface + VLAN".

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#igmp filter profile` *`profile-number`*	Create an IGMP profile and enter profile configuration mode.
3	`Raisecom(config-igmp-profile)#{ permit | deny }`	Configure IGMP profile actions.
4	`Raisecom(config-igmp-profile)#range` *`range-id start-ip-address [ end-ip-address ]`*	Configure the IP multicast address or range of control access.

Step	Command	Description
5	Raisecom(config-igmp-profile)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode or aggregation group configuration mode.
6	Raisecom(config-port)#**igmp filter profile** *profile-number* [**vlan** *vlan-list*] Raisecom(config-port)#**exit**	Apply the IGMP profile filtering template to the physical layer interface or "interface+VLAN".
	Raisecom(config-port-channel1)#**igmp filter profile** *profile-number* [**vlan** *vlan-list*] Raisecom(config-port-channel1)#**exit**	Apply the IGMP profile filtering template to the aggregation group interface or "interface+VLAN".

Note

By executing the **igmp filter profile** *profile-number* command in interface configuration mode, you can apply the created IGMP profile to the specified interface. An IGMP profile can be applied to multiple interfaces, but each interface can only have one IGMP profile.

10.5.4 Configuring maximum number of groups

The maximum number of groups that a user can join can be applied to the interface or "interface + VLAN".

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter the physical layer interface configuration mode or aggregation group configuration mode.
3	Raisecom(config-port)#**igmp filter max-groups** *group-number* [**vlan** *vlan-list*]	Configure the maximum number of groups allowed on the physical layer interface or "interface + VLAN".
	Raisecom(config-portchannel1)#**igmp filter max-groups** *group-number* [**vlan** *vlan-list*]	Configure the maximum number of groups allowed to be added to an aggregation group interface or "interface + VLAN".
4	Raisecom(config-port)#**igmp filter max-groups action** { **drop** | **replace** } [**vlan** *vlan-list*]	(Optional) configure actions to be taken when the number of physical layer interfaces or "interface + VLAN" groups exceeds the maximum number of groups.
	Raisecom(config-portchannel1)#**igmp filter max-groups action** { **drop** | **replace** } [**vlan** *vlan-list*]	(Optional) configure actions to be taken when the number of groups added to an aggregation group interface or "interface + VLAN" exceeds the maximum number.

10.5.5 Checking configurations

No.	Command	Description
1	Raisecom#**show igmp filter** [**interface**	*interface-type interface-number* [**vlan** *vlan-id*]]	Show configurations of IGMP filtering.
2	Raisecom#**show igmp filter profile** [*profile-number*]	Show information about the IGMP Profile.

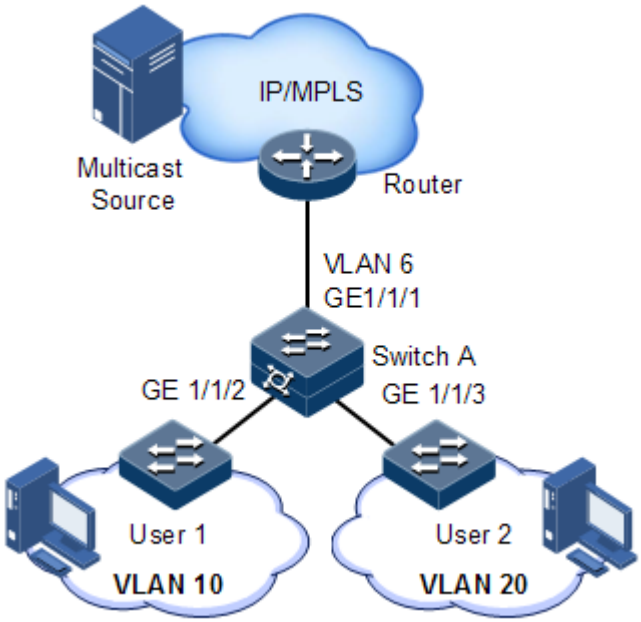
10.6 Configuirng multicast VLAN copy

10.6.1 Preparing for configurations

Scenario

As shown in Figure 10-1, multiple hosts receive data from the multicast source, and multiple hosts belong to different VLANs. You can run multicast VLAN copy on Switch A, configure the multicast VLAN, and copy the multicast data to the user VLAN on the receiving interface, so that users in different VLANs share the same multicast VLAN to receive the same multicast data, and can also reduce bandwidth waste.

Figure 10-3 Multicast VLAN copy scenario



Prerequisite

Before configuring multicast VLAN copy, perform the following task:

- Create a VLAN and add the corresponding interface to the VLAN.

- When N: 1 VLAN conversion and VLAN copy are configured at the same time, you need to configure VLAN copy first, and then configure N: 1 VLAN mapping.
- When N: 1 VLAN conversion and PIM are configured at the same time, you need to configure PIM first, and then configure N: 1 VLAN mapping.

10.6.2 Configuring multicast VLAN copy

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#igmp vlan-copy`	Enable global multicast VLAN copy.
3	`Raisecom(config)#igmp vlan-copy mcast-vlan` *vlan-id* `group` { *start-ip* [*end-ip*] | `any` }	Configure the group address set of the multicast VLAN. Note After multicast VLAN copy is enabled on the device, you need to configure the multicast VLAN and the bound group address set. If the received IGMP Report packet does not belong to any VLAN group address set, the report message will not be processed and the user cannot receive multicast streaming.

10.6.3 Configuring static multicast members of VLAN-Copy

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter physical interface configuration mode.
3	`Raisecom(config-port)#igmp vlan-copy mcast-vlan` *vlan-id* `static` *ip-address* `user-vlan` *vlan-id*	Configure static multicast members of VLAN-Copy.

- Multicast VLAN copy and IGMP MVR cannot be enabled at the same time in the same multicast VLAN, otherwise the configuration fails.
- Multicast VLAN copy and IGMP Snooping cannot be enabled simultaneously in the same multicast VLAN, otherwise the configuration fails.

10.6.4 Configuring VLAN-Copy user VLAN

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical interface configuration mode.
3	Raisecom(config-port)#**igmp vlan-copy user-vlan** *vlan-id*	Configure the user VLAN of multicast VLAN copy.

10.6.5 Checking configurations

No.	Command	Description
1	Raisecom#**show igmp vlan-copy**	Show related configurations of multicast VLAN copy.
2	Raisecom#**show igmp vlan-copy** *interface-type interface-number*	Show configurations of multicast VLAN copy on a specified interface.
3	Raisecom#**show igmp vlan-copy member**	Show multicast group members of multicast VLAN copy.
4	Raisecom#**show igmp vlan-copy member** *interface-type interface-number*	Show multicast group members of multicast VLAN copy on a specified interface.
5	Raisecom#**show igmp vlan-copy member user-vlan** *vlan-id*	Show multicast group members of multicast VLAN copy of the specified user VLAN.
6	Raisecom#**show igmp vlan-copy vlan-group** [**mcast-vlan** *vlan-id*]	Show the multicast VLAN and the bound address set of multicast VLAN copy.

10.7 Configuring PIM

10.7.1 Preparing for configurations

Scenario

Compared with unicast and broadcast, the biggest advantage of multicast is that it implements single-point transmission and multipoint reception with minimal network overhead. Configure the PIM to build a multicast distribution tree, so that the multicast source only needs to send a piece of information, and the transmitted information is copied and distributed only at the network node (RP) as far as possible from the multicast source.

Prerequisite

N/A

10.7.2 Enabling PIM

Enabling IPv4 PIM

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter interface configuration mode.
3	`Raisecom(config-port)#ip pim sparse-mode`	Enable IPv4 PIM-SM on the interface. By default, PIM-SM is disabled on the interface.

Enabling IPv6 PIM

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter interface configuration mode.
3	`Raisecom(config-port)#ipv6 pim sparse-mode`	Enable IPv6 PIM-SM on the interface. By default, PIM-SM is disabled.

10.7.3 Configuring PIM domain DR election

Configuring IPv4 PIM domain DR

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter interface configuration mode.
3	`Raisecom(config-port)#ip pim dr-priority` *priority-value*	In the IPv4-based PIM domain, configure the priority of interfaces participating in DR elections. By default, the DR priority on the interface is 1.

Configuring IPv6 PIM domain DR

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

Step	Command	Description
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ipv6 pim dr-priority** *priority-value*	In the IPv6-based PIM domain, configure the priority of interfaces participating in DR elections. By default, the DR priority on the interface is 1.

10.7.4 Configuring PIM domain RP election

Configuring IPv4-based PIM domain RP election

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router pim**	Enter IPv4 PIM configuration mode.
3	Raisecom(config-router-pim6)#**bsr-candidate** *interface-type interface-number* [*hash-mask-length* [*priority*]]	Configure the candidate election router of the PIM domain.
4	Raisecom(config-router-pim6)#**rp-candidate** *interface-type interface-number* [**group-policy** *acl-number*]	Configure the candidate RP parameter of the PIM domain.

Configuring IPv6-based PIM domain RP election

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ipv6 pim**	Enter IPv6-based PIM configuration mode.
3	Raisecom(config-router-pim6)#**bsr-candidate** *ipv6-address* [*hash-mask-length* [*priority*]]	Configure the candidate election router of the PIM domain.
4	Raisecom(config-router-pim6)#**rp-candidate** *ipv6-address* [**group-policy** *acl-number*]	Configure the candidate RP parameter of the PIM domain.

10.7.5 Configuring PIM multicast source

Configuring IPv4 multicast source

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router pim`	Enter IPv4 PIM configuration mode.
3	`Raisecom(config-router-pim)#source-lifetime` *interval*	Configure the multicast source survival time. By default, the lifetime of a multicast source is 210s.
4	`Raisecom(config-router-pim)#ssm-poliy` *acl-number*	Configure the SSM source address range. This configuration needs to be used in conjunction with IP ACL.

Configuring IPv6 multicast source

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router ipv6 pim`	Enter IPv6 PIM configuration mode.
3	`Raisecom(config-router-pim6)#source-lifetime` *interval*	Configure the multicast source survival time. By default, the lifetime of a multicast source is 210s.
4	`Raisecom(config-router-pim6)#ssm-poliy` *acl-number*	Configure the SSM source address range. This configuration needs to be used in conjunction with IP ACL.

10.7.6 Switching from RPT to SPT

The PIM-SM multicast router initially forwards multicast data via RPT, but if the rate at which multicast data passes exceeds a certain threshold, the receiver-side DR will initiate the RPT-to-SPT switch.

IPv4-based switching

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#router pim`	Enter IPv4 PIM configuration mode.

Step	Command	Description
3	Raisecom(config-router-pim)#**spt-threshold** { *traffic-rate* | **infinity** } [**group-policy** *acl-number*]	Configure the control parameters for multicast members to switch from RPT to SPT. By default, SPT is switched immediately after receiving the first multicast data packet from RPT.
4	Raisecom(config-router-pim)#**timer spt-switch** *interval*	Configure the interval to check whether the multicast data rate reaches the threshold before switching from RPT to SPT. By default, the interval to check whether the multicast data rate reaches the threshold before RPT-to-SPT switching is 15s.

Configuring IPv6-based switching

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**router ipv6 pim**	Enter IPv6 PIM configuration mode.
3	Raisecom(config-router-pim6)#**spt-threshold** { *traffic-rate* | **infinity** } [**group-policy** *acl-number*]	Configure the control parameters for multicast members to switch from RPT to SPT. By default, SPT switching is performed immediately after the first multicast data packet is received from RPT.
4	Raisecom(config-router-pim6)#**timer spt-switch** *interval*	Configure the interval to check whether the multicast data rate reaches the threshold before RPT-to-SPT switching is performed. By default, the interval to check whether the multicast data rate reaches the threshold before RPT-to-SPT switching is 15s.

10.7.7 Checking configurations

No.	Command	Description
1	Raisecom#**show** { **ip** | **ipv6** } **pim bsr-router**	Show election router of the PIM domain.
2	Raisecom#**show** { **ip** | **ipv6** } **pim interface**	Show information about the PIM interface.
3	Raisecom#**show** { **ip** | **ipv6** } **pim routing-table**	Show information about the PIM routing table.
4	Raisecom#**show** { **ip** | **ipv6** } **pim rp**	Show RP information about the PIM.

No.	Command	Description
5	Raisecom#**show { ip | ipv6 } pim rp-candidate**	Show candidate RP information about the PIM.
6	Raisecom#**show { ip | ipv6 } pim neighbor**	Show PIM neighbor information.

10.7.8 Maintenance

Command	Description
Rasiecom#**clear { ip | ipv6 } pim process**	Reconfigure IPv4/IPv6 PIM multicast and clear PIM configurations on the current device.

10.8 Configuring MLD L2 multicast

10.8.1 Preparing for configurations

Scenario

The multicast technology that appeared in the IPv4 era effectively solved the problems of single-point transmission and multi-point reception, and realized efficient data transmission from point to multipoint in the network, which can greatly save network bandwidth and reduce network load. In IPv6 networks, the application of multicast technology has been further enriched and strengthened. The device establishes a forwarding table of multicast packets by listening to MLD packets, thereby managing and controlling the forwarding of multicast data packets, and forwarding the multicast data packets to the host that needs to receive the data.

Prerequisite

N/A

10.8.2 Configuring MLD basic function

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mld mrouter vlan** *vlan-id interface-type interface-number*	Create a multicast router interface in the specified VLAN.
3	Raisecom(config)#**mld ring** *interface-type interface-number*	Enable MLD ring network forwarding on the interface.

Step	Command	Description
4	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**prtswtich** Raisecom(config-port)#**mld immediate-leave** [**vlan** *vlan-list*] Raisecom(config-port)#**exit**	Enable MLD immediate leave on the interface or "interface + VLAN". If immediate leave is not enabled on the downstream interface, the routing interface will calculate the aging time according to the robust coefficient when it receives leave packets. The group timeout timer is set to GMI (Group Membership Interval), GMI = (robust-value * lastmember-queryinterval).
5	Raisecom(config)#**mld report-suppression**	(Optional) enable Report suppression. The device receives multiple report packets of the same group within a certain period of time, and only forwards one report packet to the routing port. Other packets will be suppressed.
6	Raisecom(config)#**mld member-timeout** { *second* | **infinite** }	(Optional) configure the aging time of MLD members.
7	Raisecom(config)#**mld version** { **1** | **2** }	Configure the MLD version.

10.8.3 Configuring MLD Snooping

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mld snooping**	Enable MLD Snooping.
3	Raisecom(config)#**mld snooping vlan** *vlan-list*	(Optional) enable MLD Snooping in global VLAN.
4	Raisecom(config)#**vlan** *vlan-id* Raisecom(config-vlan)#**mld snooping static** *ip-address* [*interface-type interface-number*]	(Optional) configure the static members of MLD Snooping in VLAN mode.

10.8.4 Adjusting MLD performance

Configuring MLD Querier

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mld querier**	Enable MLD querier.

Step	Command	Description
3	Raisecom(config)#**mld source-ip** *ip-address*	(Optional) configure the source IP address for MLD queriers to send Query packets.
4	Raisecom(config)#**mld query-interval** *period*	(Optional) configure the MLD query interval.
5	Raisecom(config)#**mld query-max-response-time** *period*	(Optional) configure the maximum response time of Query packets.
6	Raisecom(config)#**mld last-member-query-interval** *period*	(Optional) configure the interval for the last group member to send Query packets.
7	Raisecom(config)#**mld robust-count** *value*	Configure the MLD robust coefficient.
8	Raisecom(config)#**mld proxy**	Enable MLD Proxy.

Note

- If MLD Querier is not enabled, you can configure MLD Querier, including the source IP address, query of the interval, and the maximum response time for the sent Query packets, and the interval for the last member to send Query packets. When MLD Querier is enabled, these configurations take effect immediately.
- MLD proxy conflicts with MLD querier. MLD proxy conflicts with MLD report-suppression.

Configuring interface MLD robust coefficient

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode. By default, the interface is in Layer 3 router mode.
3	Raisecom(config-port)#**ipv6 mld robustness-variable** *value*	Configure the MLD robust coefficient on the interface. By default, the MLD robust coefficient is 2.

Configuring interface MLD query and response

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode. By default, the interface is in Layer 3 router mode.

Step	Command	Description
3	Raisecom(config-port)#**ipv6 mld query-max-response-time** *seconds*	Configure the maximum MLD query response time on the interface. By default, the maximum query response time is 12s.
4	Raisecom(config-port)#**ipv6 mld query-interval** *seconds*	Configure the general MLD query interval of the interface. By default, the general MLD query interval is 125s.
5	Raisecom(config-port)#**ipv6 mld last-member-query-interval** *seconds*	Configure the last member query interval of MLD on the interface. By default, the last member query interval is 1s.

Configuring immediate leave of multicast members

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode. By default, the interface is in Layer 3 router mode.
3	Raisecom(config-port)#**ipv6 mld immediate-leave**	Enable immediate leave of MLD members. By default, it is disabled.

10.8.5 Configuring MLD filtering

Enabling MLD filtering globally

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mld filter**	Enable global MLD filtering.

Note

When configuring the application of the MLD filter template or the maximum number of groups, you need to execute the **mld filter** command to enable MLD filtering globally.

Configuring MLD filtering template

The MLD filtering template can be applied to the interface or interface + VLAN.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mld filter profile** *profile-number*	Create a MLD profile and enter profile configuration mode.
3	Raisecom(config-mld-profile)#{ **permit** | **deny** }	Configure the action of the MLD profile.
4	Raisecom(config-mld-profile)#**range** *range-id start-ip-address* [*end-ip-address*]	Configure the IPv6 multicast address or range of access control.
5	Raisecom(config-mld-profile)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode or aggregation group configuration mode.
6	Raisecom(config-port)#**mld filter profile** *profile-number* [**vlan** *vlan-list*]	Apply the MLD filtering profile to the physical layer interface or interface + VLAN.
	Raisecom(config-portchannel1)#**mld filter profile** *profile-number* [**vlan** *vlan-list*] Raisecom(config-portchannel1)#**exit**	Apply the MLD filtering profile to the aggregation group interface or interface + VLAN.

Note

By executing the **mld filter profile** *profile-number* command in interface configuration mode, you can apply the created MLD Profile to the specified interface. An MLD Profile can be applied to multiple interfaces, but each interface can only have one MLD Profile.

Configuring maximum number of groups

You can configure the maximum number of groups that can be joined by users. You can apply it to the interface or interface + VLAN.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode or aggregation group configuration mode.
3	Raisecom(config-port)#**mld filter max-groups** *group-number* [**vlan** *vlan-list*]	Configure the maximum number of groups allowed on the physical layer interface, aggregation group interface, or "interface + VLAN".
4	Raisecom(config-port)#**mld filter max-groups action** { **drop** | **replace** } [**vlan** *vlan-list*]	(Optional) configure actions to be taken when the number of physical layer interfaces, aggregation group interfaces, or "interface + VLAN" groups exceeds the maximum number of groups.

10.8.6 Checking configurations

Step	Command	Description
1	Raisecom#**show mld immediate-leave** [*interface-type interface-number* | **port-channel** *port-channel-id*]	Show configurations of MLD immediate leave.
2	Raisecom#**show mld mrouter**	Show information about MLD multicast router interface.
3	Raisecom#**show mld snooping** [**vlan** *vlan-id*]	Show configurations of MLD Snooping.
4	Raisecom#**show mld snooping member** [*interface-type interface-number* | **vlan** *vlan-id*]	Show multicast group members of MLD Snooping.
5	Raisecom#**show mld snooping member count** [*interface-type interface-number* | **vlan** *vlan-id*]	Show the number of multicast group members of MLD Snooping.
6	Raisecom#**show mld statistics** [*interface-type interface-number*]	Show MLD packet statistics.
7	Raisecom# **show mld filter** [**interface** | **gigaehternet** *interface-number* [**vlan** *vlan-id*]]	Show configurations of MLD filtering.
8	Raisecom# **show mld filter profile** [*profile-number*]	Show configurations of the MLD filtering profile.
9	Raisecom#**show mld configuration**	Show MLD basic configurations.

10.8.7 Maintenance

Command	Description
Rasiecom#**clear mld statistics** [*interface-type interface-number*]	Clear MLD statistics.
Rasiecom#**no mld member** *interface-type interface-number*	Delete the multicast forwarding entries of a specified interface.

10.9 Configuring MLD L3 multicast

10.9.1 Configuring MLD basic functions on interface

Enabling MLD

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter interface configuration mode. By default, the interface is in L3 router mode.
3	`Raisecom(config-port)#ipv6 mld enable`	Enable interface MLD. By default, interface MLD is disabled.

Configuring MLD version

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter interface configuration mode. By default, the interface is in L3 router mode.
3	`Raisecom(config-port)#ipv6 mld version { 1 | 2 }`	Configure the MLD version on the interface. By default, the MLD version is version 2.

Statically joining multicast group

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter interface configuration mode. By default, the interface is in L3 router mode.
3	`Raisecom(config-port)#ipv6 mld static group` *ipv6-address*	Configure the static multicast group members on the interface.

Configuring access control for multicast group and multicast source

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

Step	Command	Description
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)# **ipv6 mld group-policy** *acl-number*	Configure the range of multicast groups for interfaces to join.
4	Raisecom(config-port)#**ipv6 mld source-ip-policy** *acl-number*	Configure the source address range of the VOD of the interface.
5	Raisecom(config-port)#**ipv6 mld limit** *limit-number*	Configure the maximum number of multicast groups that an interface can join.

10.9.2 Adjusting MLD performance

Configuring MLD robustness coefficient

Step	Command	Description
1	Raisecom#config	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ipv6 mld robustness-variable** *value*	Configure the MLD robustness coefficient on the interface.

Configuring MLD query and response

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**ipv6 mld query-max-response-time** *value*	Configure the maximum MLD query response time on the interface.
4	Raisecom(config-port)#**ipv6 mld query-interval** *value*	Configure the general MLD query interval on the interface.
5	Raisecom(config-port)#**ipv6 mld last-member-query-interval** *value*	Configure the MLD last member query interval on the interface.

Configure immediate leave of multicast group members

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

Step	Command	Description
2	Raisecom(config)#interface interface-type interface-number	Enter interface configuration mode.
3	Raisecom(config-port)#**ipv6 mld immediate-leave**	Enable immediate leave of MLD members.

10.9.3 Checking configurations

No.	Command	Description
1	Raisecom#**show ipv6 mld group** [*ipv6-address* | *interface-type interface-number*]	Show MLD group member relationship.
2	Raisecom#**show ipv6 mld interface** [*interface-type interface-number*]	Show MLD configurations on the interface.
3	Raisecom#**show ipv6 mld statistics** [*interface-type interface-number*]	Show MLD packet statistics on the interface.
4	Raisecom#**show ipv6 mld mroute**	Show the IPv6 multicast routing table.
5	Rasiecom#**show ipv6 mld ssm-mapping group**	Show mapping relationship.

10.9.4 Maintenance

Command	Description
Rasiecom#**clear ipv6 mld group** [*ipv6-address* | *interface-type interface-number*]	Clear the MLD dynamic forwarding table.
Rasiecom#**clear ipv6 mld statistics** [*interface-type interface-number*]	Clear MLD statistics.
Rasiecom#**clear ipv6 mfib statistics**	Clear statistics of the IPv6 multicast forwarding table.

11 OAM

This chapter describes principles and configuration procedures of OAM, as well as related configuration examples, including following sections:

- Configuring EFM
- Configuring CFM
- Configuring BFD
- Configuring SLA
- Configuring SLA test alarm
- Configuring interface loopback
- Configuring SLA test alarm
- Configuring interface loopback
- Configuring ULDP
- Maintenance

11.1 Configuring EFM

11.1.1 Preparing for configurations

Scenario

Deploying EFM between directly-connected devices can effectively improve the management and maintenance capability of Ethernet links and ensure network running smoothly.

Prerequisite

Connect interfaces and configure physical parameters of interfaces. Make the physical layer Up.

11.1.2 Configuring EFM basic functions

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

Step	Command	Description
2	Raisecom(config)#**oam send-period** *period-ms* **timeout** *seconds*	(Optional) configure the OAM PDU delivery period and timeout. By default, the OAM PDU delivery time is 1s (the parameter is 10, 10 × 100ms = 1s) and the timeout is 5s.
3	Raisecom(config)#**interface gigaethernet** *interface-number*	Enter Layer 2 or 3 physical interface configuration mode.
4	Raisecom(config-port)#oam { **active** | **passive** }	Configure the working mode of EFM. By default, it is passive.
5	Raisecom(config-port)#**oam enable**	Enable EFM OAM of the link. By default, it is enabled.

11.1.3 Configuring EFM active functions

Note

EFM active functions can be configured when the RAX721-A is in active mode.

(Optional) configuring RAX721-A to initiate EFM remote loopback

Note

- You can discover network faults in time by periodically detecting loopbacks. By detecting loopbacks in segments, you can locate exact areas where faults occur and you can troubleshoot these faults.
- When a link is in the loopback status, the RAX721-A returns all packets but OAM packets received by the link to the peer. At this time, the user data packet cannot be forwarded properly. Therefore, disable this function immediately when detection is not required.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gigaethernet** *interface-number*	Enter GE interface configuration mode.
3	Raisecom(config-port)#**oam remote-loopback**	Enable the interface to initiate remote loopback.
4	Raisecom(config-port)#**oam loopback timeout** *time*	(Optional) configure the timeout for the interface to initiate remote loopback. By default, it is 3s.
5	Raisecom(config-port)#**oam loopback retry** *times*	(Optional) configure the retry times for the interface to initiate remote loopback. By default, it is 2 times.

(Optional) viewing current variable values of peer device

By getting the current variable values of the peer, you can get current link status. IEEE 802.3 Clause 30 defines and explains supported variables and their denotation gotten by OAM in details. The variable takes Object as the maximum unit. Each object contains Package and Attribute. A package contains several attributes. Attribute is the minimum unit of a variable. When an OAM variable is obtained, object, package, branch, and leaf description of attributes are defined by Clause 30 to describe requesting object, and the branch and leaf are followed by variable to denote object responds variable request. The RAX721-A supports getting OAM information and interface statistics.
Peer variable cannot be obtained unless EFM connection is established.

Step	Command	Description
1	Raisecom#**show oam peer oam-info** [**gigaethernet** *interface-number*] Raisecom#**show oam peer** [**gigaethernet** *interface-number*]	Show OAM basic information about the peer device.

11.1.4 Configuring EFM passive functions

The passive functions of EFM can be configured regardless of the RAX721-A is in active or passive mode.

(Optional) configuring RAX721-A to respond to EFM remote loopback

The peer EFM remote loopback will not take effect until the remote loopback response is configured on the local device.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gigaethernet** *interface-number*	Enter GE interface configuration mode.
3	Raisecom(config)#**oam loopback** { **ignore** | **process** }	Configure the interface to ignore/respond to EFM remote loopback sent by the peer device. By default, the Layer 2 physical interface ignores EFM remote loopback.

11.1.5 Configuring link monitoring and fault indication

(Optional) configuring OAM link monitoring

OAM link monitoring is used to detect and report link errors in different conditions. When detecting a fault on a link, the RAX721-A provides the peer with the generated time, window, and threshold, etc. by OAM event notification packets. The peer receives event notification and reports it to the NView NNM system through SNMP Trap. Besides, the local device can directly report events to the NView NNM system through SNMP Trap.
By default, the system sets default value for error generated time, window, and threshold.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gigaethernet** *interface-number*	Enter GE interface configuration mode.
3	Raisecom(config-port)#**oam errored-frame window** *framewindow* **threshold** *framethreshold*	Configure the monitor window and threshold for an error frame event. By default, the monitor window is 1s and the threshold is 1 error frame.
4	Raisecom(config-port)#**oam errored-frame-period window** *frameperiodwindow* **threshold** *frameperiodthreshold*	Configure the monitor window and threshold for an error frame period event. By default, the monitor window is 1000ms and the threshold is 1 error frame.
5	Raisecom(config-port)#**oam errored-frame-seconds window** *framesecswindow* **threshold** *framesecsthreshold*	Configure the monitor window and threshold for an error frame seconds event. By default, the monitor window is 60s and the threshold is 1s.
6	Raisecom(config-port)#**oam errored-symbol-period window** *symperiodwindow* **threshold** *symperiodthreshold*	Configure the monitor window and threshold for an error symbol event. By default, the monitor window is 1s and the threshold is 1 error frame.

(Optional) configuring OAM fault indication

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gigaethernet** *interface-number*	Enter GE interface configuration mode.

Step	Command	Description
3	Raisecom(config-port)#**oam notify** { **critical-event** | **dying-gasp** | **errored-frame** | **errored-frame-period** | **errored-frame-seconds** | **errored-symbol-period** } **enable**	Enable OAM notification of fault information and OAM link events. By default, OAM notification of all links is enabled.
4	Raisecom(config-port)#**oam event trap enable**	Enable OAM Trap of local OAM link events. By default, it is disabled.
5	Raisecom(config-port)#**oam peer event trap** { **enable** | **disable** }	Enable OAM Trap of peer OAM link events. By default, it is disabled.

11.1.6 Configuring extended OAM

Both Layer 2 and Layer 3 interfaces on the RAX721-A support extended OAM. Configuring OAM on Layer 3 interface does not affect configurations of its sub-interfaces.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical interface configuration mode.
3	Raisecom(config-port)#**oam enable**	Enable OAM on the interface.
4	Raisecom(config-port)#**oam** { **active** | **passive** }	Configure the working mode of OAM. By default, it is passive.
5	Raisecom(config-port)#**remote-device**	Enter remote configuration mode.
6	Raisecom(config-remote)#**hostname** *hostname*	Configure the host name of the remote device.
7	Raisecom(config-remote)#**ip address** *ip-address* [*ip-mask*] [*vlan-id*]	Configure the IP address of the remote device. **Note** • We recommend that you not use this command together with zero-configuration, because it may cause the remote device out of control. • When the remote device is an IP RAN device, its IP address should be configured on interface Loopback 1. If you configure the management VLAN ID, the sub-interface (the parent interface is enabled with OAM) will use the IP address of interface Loopback 1, otherwise, it will not. • When the remote device is a PTN device, you should configure its IP address on IP interface 0. If you configure the management VLAN ID, the VLAN will be associated with IP interface 0.

After entering remote configuration mode, you can show the command list supported by the remote device by using the **list** command. Then you can manage the remote device by using those commands. For example:

- Use the snmp-server community command to configure the network management for the remote device.
- Use the switch-mode dot1q-vlan native-vlan command to configure VLAN for the remote device.
- Use the reboot command to reboot the remote device.
- Use the erase command to delete configuration files from the remote device.

There are multiple commands available for you to monitor and manage the remote device through extended OAM. They are not listed here one by one, and you can use them as required. Using some commands remotely on the remote device has the same effect as using these commands locally on the remote device.

11.1.7 Checking configurations

No.	Command	Description
1	Raisecom#**show oam** [*interface-type interface-number*]	Show configurations of OAM basic functions.
2	Raisecom#**show oam event** [*interface-type interface-number*] [**critical**]	Show local OAM link events.
3	Raisecom#**show oam loopback** [*interface-type interface-number*]	Show OAM remote loopback configurations.
4	Raisecom#**show oam notify** [*interface-type interface-number*]	Show OAM notification configurations.
5	Raisecom#**show oam peer event** [*interface-type interface-number*] [**critical**]	Show information about OAM peer events.
6	Raisecom#**show oam peer link-statistic** [*interface-type interface-number*]	Show peer OAM link statistics.
7	Raisecom#**show oam statistics** [*interface-type interface-number*]	Show OAM statistics.
8	Raisecom#**show oam trap** [*interface-type interface-number*]	Show OAM Trap information.

11.2 Configuring CFM

11.2.1 Preparing for configurations

Scenario

To expand application of Ethernet technologies at a carrier-grade network, the Ethernet must ensure the same QoS as the Telecom-grade transport network. CFM solves this problem by providing overall OAM tools for the Telecom-grade Ethernet.

CFM can provide following OAM functions:

- Fault detection (Continuity Check, CC)
- Fault acknowledgement (LoopBack, LB)
- Fault location (LinkTrace, LT)
- Alarm Indication Signal (AIS)
- Ethernet lock signal (Lock, LCK)
- Client Signal Fail (CSF)

Prerequisite

- Connect interfaces and configure physical parameters of the interfaces. Make the physical layer Up.
- Create a VLAN.
- Add interfaces to the VLAN.

11.2.2 Enabling CFM

- CFM fault detection and CFM fault location functions cannot take effect until the CFM is enabled.
- To enable CFM on an interface, you need to enable global CFM in global configuration mode and then enable CFM on the interface.
- When global CFM is disabled, it does not affect enabling/disabling EFM on the interface.
- Ethernet LM cannot take effect unless CFM is enabled on the ingress interface of the service packet and MEP-related interfaces.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ethernet cfm enable`	Enable global CFM. By default, it is disabled.
3	`Raisecom(config)#interface gigaethernet` *`interface-number`*	Enter GE interface configuration mode.
	`Raisecom(config-port)#portswitch`	Switch the interface to L2 switching mode.
4	`Raisecom(config-port)#ethernet cfm enable`	Enable CFM on the interface. By default, it is disabled.

11.2.3 Configuring CFM basic functions

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

Step	Command	Description
2	Raisecom(config)#**ethernet cfm domain** [**md-name** *domain-name*] **level** *md-level*	Create a MD. • If a MD name is assigned by the **md-name** parameter, it indicates that the MD is in 802.1ag style. And all MAs and CCMs in the MD are in 802.1ag style. • If a MD name is not assigned, the MD is in Y.1731 style and all MAs and CCMs in the MD are in Y.1731 style. • Do not support configuring Y.1731 and 802.1ag CFM concurrently. • If the MD name is specified, it must be globally unique. • Levels of different MDs must be different.
3	Raisecom(config)#**service** *instance-name* **level** *md-level*	Create a service instance and enter service instance configuration mode.
4	Raisecom(config-service)#**service vlan-list** *vlan-list* [**primary** *vlan-id*]	Configure the VLAN related to the MA.
5	Raisecom(config-service)#**service mep** [**up** | **down**] **mpid** *mep-id* [*interface-type interface-number*] [**priority** *value*]	Configure the MEP based on service instance. Before configuring MEP, relating the service instance to the VLAN.
6	Raisecom(config-service)#**service remote-mep** *mep-list interface-type interface-number*	Add static remote MEP of the service instance manually. **Note** 802.1ag down MEP needs to manually add the remote MEP and specify the interface. It fails to find the remote MEP automatically.
7	Raisecom(config-service)#**service suppress-alarms enable mep** { *mep-list* | **all** }	Enable alarm inhibition. By default, it is enabled.

11.2.4 Configuring fault detection

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet cfm errors archive-hold-time** *minutes*	(Optional) configure the archive-hold time of error CCMs. By default, it is 100min.
3	Raisecom(config)#**service** *instance-nameinstance-name* **level** *md-level*	Enter service instance configuration mode.

Step	Command	Description
4	Raisecom(config-service)#**service cc interval** { **3ms** | **10ms** | **100ms** | **1** | **10** | **60** | **600** }	(Optional) configure the delivery period of CCMs.
5	Raisecom(config-service)#**service cc enable mep** { *mep-list* | **all** }	Enable MEP to send CCMs.
6	Raisecom(config-service)#**service cvlan** *vlan-id*	(Optional) configure the CVLAN of the MA.
7	Raisecom(config-service)#**service priority** *priority*	(Optional) configure the priority of CFM OAM packets. By default, it is 7.

11.2.5 Configuring fault acknowledgement

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**service** *instance-name* **level** *md-level*	Enter service instance configuration mode.
3	Raisecom(config-service)#**ping** *mac-address* [**count** *count-number*] [**size** *size*] [**source** *mep-id*] [**timeout** *time*] [**padding** { **null** | **null-crc** | **prbs** | **prbs-crc** }] Raisecom(config-service)#**ping mep** *mep-id* [**ttl** *ttl*] [**count** *count-number*] [**size** *size*] [**source** *mep-id*] [**timeout** *time*] [**padding** { **null** | **null-crc** | **prbs** | **prbs-crc** }]	Perform Layer 2 Ping for acknowledging faults. By default, 3 LBMs are sent. The TLV length of a packet is 64. The RAX721-A automatically looks for an available source MEP. **Note** To perform Ping MEP operation, 802.1ag down MEP needs to be configured with the static remote MAC address.
4	Raisecom(config-service)#**ping ethernet multicast** [**size** *size*] [**timeout** *time*] [**padding** { **null** | **null-crc** | **prbs** | **prbs-crc** }]	Perform Layer 2 multicast Ping for acknowledging faults.

Note

- Before executing this command, ensure that global CFM is enabled. Otherwise, the Ping operation fails.
- If there is no MEP in a service instance, Ping operation will fail because of failing to find source MEP.
- Ping operation will fail if the specified source MEP is invalid. For example, the specified source MEP does not exist or CFM is disabled on the interface where the specified source MEP is.

- Ping operation will fail if the Ping operation is performed based on specified destination MEP ID and the MAC address of destination is not found based on MEP ID.
- Ping operation will fail if other users are using the specified source MEP to perform Ping operation.
- If the service instance associates with the emulated Ethernet PW, when LB is performed, you need to enable global CFM and Ethernet CFM on the AC-side interface.

11.2.6 Configuring fault location

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#service` *instance-name* `level` *md-level*	Enter service instance configuration mode.
3	`Raisecom(config-service)#traceroute` *mac-address* `[ ttl` *ttl* `] [ source` *mep-id* `]` `Raisecom(config-service)#traceroute mep` *mep-id* `[ ttl` *ttl* `] [ source` *mep-id* `] [ interface-mode ] [ timeout` *time* `size` *size-value* `]`	Perform Layer 2 Traceroute for locating faults. By default, the TLV length of a packet is 64. The RAX721-A automatically looks for an available source MEP. **Note** To perform Traceroute MEP operation, 802.1ag down MEP needs to be configured with the static remote MAC address.
4	`Raisecom(config)#ethernet cfm traceroute cache enable`	(Optional) enable LinkTrace cache. When LinkTrace cache is enabled, you can use the **show ethernet cfm traceroute cache** command to learn the routes discovered through the cache storage protocol. When LinkTrace cache is disabled, the result will be automatically erased by the **traceroute** command. By default, LinkTrace cache is disabled.
5	`Raisecom(config)#ethernet cfm traceroute cache { hold-time` *minute* `| size` *size* `}`	(Optional) configure the hold time of data in the LinkTrace cache and LinkTrace cache size. By default, the hold time is 100min and the LinkTrace cache size is 100.

Note

- Before executing this command, ensure that global CFM is enabled. Otherwise, the Traceroute operation fails.
- If there is no MEP in a service instance, Traceroute operation will fail because of failing to find source MEP.
- Traceroute operation will fail if the specified source MEP is invalid. For example, the specified source MEP does not exist or CFM is disabled on the interface where the specified source MEP is.
- Traceroute operation will fail if the Ping operation is performed based on specified destination MEP ID and the MAC address of destination is not found based on MEP ID.

- If the CC feature is invalid, you can ensure Layer 2 Traceroute operation works normally by configuring static RMEP and specifying MAC address.
- Traceroute operation will fail if other users are using the specified source MEP to perform Traceroute operation.

11.2.7 Configuring AIS

- Configure AIS on server devices.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ethernet cfm domain [ md-name domain-name ] level md-level`	Create a MD.
3	`Raisecom(config)#service instance-name level md-level`	Enter service instance configuration mode.
4	`Raisecom(config-service)#service ais level md-level`	Configure the level of the MD to which AIS is sent. **Note** The MD level must be higher than the service instance level.
5	`Raisecom(config-service)#service ais period { 1 | 60 }`	(Optional) configure the AIS delivery period. By default, the AIS delivery period is 1s.
6	`Raisecom(config-service)#service ais enable`	Enable AIS delivery. By default, AIS delivery is disabled.

- Configure AIS on client devices.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ethernet cfm domain [ md-name domain-name ] level md-level`	Create a MD.
3	`Raisecom(config)#service instance-name level md-level`	Enter service instance configuration mode.
4	`Raisecom(config-service)#service suppress-alarms enable mep { mep-list | all }`	Enable alarm inhibition. By default, alarm inhibition is enabled.

11.2.8 Configuring LCK

Configuring LCK on server-layer devices

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet cfm domain** [**md-name** *domain-name*] **level** *md-level*	Create a MD.
3	Raisecom(config)#**service** *instance-name* **level** *md-level*	Enter service instance configuration mode.
4	Raisecom(config-service)#**service lck level** *md-level* [**vlan** *vlan-id*]	Configure the level for sending the LCK packet. The level must be higher than the service instance level. By default, the level of the MIP is used, which is higher than the MEP level, to send the LCK packet.
5	Raisecom(config-service)#s **service lck period** { **1** | **60** }	(Optional) configure the LCK packet delivery period. By default, it is 1s.
6	Raisecom(config-service)#**service lck start mep** { *mep-list* | **all** }	Configure the MEP to send the LCK packet. By default, the MEP does not send the LCK packet.

Configuring LCK on client-layer devices

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet cfm domain** [**md-name** *domain-name*] **level** *md-level*	Create a MD.
3	Raisecom(config)#**service** *instance-name* **level** *md-level*	Enter service instance configuration mode.
4	Raisecom(config-service)#**service suppress-alarms enable mep** { *mep-list* | **all** }	Enable alarm inhibition. By default, alarm inhibition is enabled.

11.2.9 Configuring CSF

- Configure LCK on server devices.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet cfm domain** [**md-name** *domain-name*] **level** *md-level*	Create a MD.

Step	Command	Description
3	Raisecom(config)#**service** *instance-name* **level** *md-level*	Enter service instance configuration mode.
4	Raisecom(config-service)#**service csf period** { **1** | **60** }	(Optional) configure the CSF packet delivery period. By default, the CSF packet delivery period is 1s.
5	Raisecom(config-service)#**service csf enable mpid** *mep-id*	Enable the MEP to send the LCK packet.
6	Raisecom(config-service)#**service csf trap enable**	(Optional) enable CSF Trap.

11.2.10 Checking configurations

No.	Command	Description
1	Raisecom#**show cfm csf**	Show CSF information.
2	Raisecom#**show ethernet cfm**	Show CFM global configurations.
3	Raisecom#**show ethernet cfm ais** [**level** *md-level*] [*source*]	Show AIS information. **Note** 802.1ag MDs do not support AIS.
4	Raisecom#**show ethernet cfm domain** [**level** *md-level*]	Show MD configurations.
5	Raisecom#**show ethernet cfm errors** [**level** *md-level*]	Show error CCM information.
6	Raisecom#**show ethernet cfm lck** [**level** *md-level*] [**source**]	Show LCK information. **Note** The 802.1ag MDs do not support LCK.
7	Raisecom#**show ethernet cfm local-mp** [**interface** *interface-type interface-number*] Raisecom#**show ethernet cfm local-mp** [**level** *md-level*]	Show local MEP configurations.
8	Raisecom#**show ethernet cfm remote-mep** [**level** *md-level* [**service** *instance-nameinstance-name* [**mpid** *mep-id*]]]	Show remote MEP configurations.
9	Raisecom#**show ethernet cfm remote-mep static** [**level** *md-level*]	Show remote static MEP configurations.
10	Raisecom#**show ethernet cfm traceroute-cache**	Show information about routes in the LinkTrace cache.

11.3 Configuring BFD

11.3.1 Preparing for configurations

Scenario

To reduce effect of faults on the device and improve network availability, the RAX721-A needs to detect communication faults with adjacent devices. Therefore, it can take actions immediately to ensure service being transmitted properly.

BFD is a one-way detection. Therefore, both the local device and the peer device should be enabled with BFD. Otherwise, detection will fail.

Prerequisite

The DUT is configured with an IP address and routes between all devices are available.

11.3.2 Configuring BFD for IP

Creating BFD for IP sessions

When you create the BFD binding:

- It indicates detecting multi-hop routes if you only specify the peer IP address.
- It indicates detecting the single-hop route if you specify both the local interface and the peer IP address, which refers to detecting the fixed route with the local interface as the egress interface and the peer IP address as the next-hop address.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**bfd** *session-id* **bind peer-ip** *ip-address* [**source-ip** *ip-address*]	Create multi-hop routes of BFD session detection and enter BFD session mode. You must configure the source IP address when creating a multi-hop session.
3	Raisecom(config)#**bfd** *session-id* **bind peer-ip** *ip-address* **interface** *interface-type interface-number*	Create a single-hop route of static BFD session detection, bind Layer 3 physical interface, sub-interface, VLAN interface or Layer 3 LAG interface, and enter BFD session mode.

Configuring BFD session parameters

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

Step	Command	Description
2	Raisecom(config)#**bfd** *session-id*	Enter BFD session mode. **Note** You cannot use this command to enter BFD session mode unless you create the BFD and bind the related path.
3	Raisecom(config-bfd-session)#**description** *description*	Configure descriptions of the BFD session.
4	Raisecom(config-bfd-session)#**local discriminator** *value*	(Optional) configure the local identifier of the BFD session. By default, the local identifier is displayed as 0, which indicates that no local identifier is configured. **Note** You need to configure this parameter for static BFD only. It is automatically generated by the system if not configured.
5	Raisecom(config-bfd-session)#**min send-interval** *interval*	Configure the minimum delivery interval of the BFD session. By default, it is 10ms.
6	Raisecom(config-bfd-session)#**min receive-interval** *interval*	Configure the minimum receiving interval of the BFD session. By default, it is 10ms.
7	Raisecom(config-bfd-session)#**detect-multiplier** *multiplier*	Configure the local detection times of the BFD session. By default, it is 3 times.
8	Raisecom(config-bfd-session)#**remote discriminator** *value*	(Optional) configure the remote identifier of the BFD session. By default, the remote identifier is displayed as 0, which indicates that no remote identifier is configured. **Note** You need to configure this parameter for static BFD only. It is automatically generated by the system if not configured.
9	Raisecom(config-bfd-session)#**session enable**	Enable BFD session. By default, it is disabled.
10	Raisecom(config-bfd-session)#**vid** *vlan-id*	Configure the VLAN ID of Default-IP session packets.

11.3.3 Configuring BFD for link aggregation group interface

Creating BFD for link aggregation group interface sessions

It is used for detecting the Up/Down status of the member interfaces in the aggregation group.

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

Step	Command	Description
2	Raisecom(config)#**bfd** *session-id* **bind link-bundle peer-ip** *ip-address* **interface port-channel 1** [**source-ip** *ip-address*]	Create a BFD session to detect the status of member interfaces in the link aggregation group based on IPv4.
3	Raisecom(config)#**bfd** *session-id* **bind link-bundle peer-ipv6** *ipv6-address* **interface port-channel 1** [**source-ip** *ipv6-address*]	Create a BFD session to detect the status of member interfaces in the link aggregation group based on IPv6.

Configuring BFD session parameters

See section Configuring BFD session parameters in 11.3.2 Configuring BFD for IP.

11.3.4 Configuring BFD for VRF

Creating BFD for VRF

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**bfd** *session-id* **bind peer-ip** *ip-address* **vrf-name** *vrf-name* **interface** *interface-type interface-number* **source-ip** *ip-address*	Create single-hop BFD for IPv4 VRF and enter BFD session mode.
3	Raisecom(config)# **bfd** *session-id* **bind peer-ip** *ip-address* **vrf-name** *vrf-name* [**source-ip** *ip-address*]	Create multi-hop BFD for IPv4 VRF and enter BFD session mode.

Configuring BFD session parameters

See section Configuring BFD session parameters in 11.3.2 Configuring BFD for IP.

11.3.5 Configuring BFD Trap

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**bfd trap enable**	Enable BFD Trap. By default, BFD Trap is enabled.

11.3.6 Checking configurations

No.	Command	Description
1	Raisecom#**show bfd**	Show BFD global configurations.

No.	Command	Description
2	Raisecom#**show bfd** [*session-id*] [**config**]	Show configurations about the specified BFD session.
3	Raisecom#**show bfd** *session-id* **state**	Show status about the specified BFD session.
4	Raisecom#**show bfd** *session-id* **statistics**	Show statistics about the specified BFD session.
	Raisecom#**show bfd** [*sessionid*] **diagnostic-code**	Show the diagnostic code of BFD session.

11.4 Configuring SLA

11.4.1 Preparing for configurations

Scenario

To provide users with qualified network services, the carrier signs a SLA with users. To carry out SLA effectively, the ISP needs to deploy SLA feature on devices to measure the network performance, taking the measured results as an evidence for ensuring the network performance.

By selecting two detection points (source and destination RAX700 devices), SLA configures and schedules SLA operations on a detection point. Therefore, network performance between these 2 detection points can be detected.

SLA takes statistics on round-trip packet loss ratio, round-trip/unidirectional (SD/DS) delay, jitter, throughput, and LM packet loss ratio test. In addition, it reports these data to the upper monitoring software (such as the NView NNM system) to help analyze network performance for obtaining an expected result.

Note

When configuring SLA on the RAX721-A, note the following matters:

- Up to 16 operations can be configured and scheduled concurrently.
- Before scheduling a SLA operation, establish the CFM environment.
- Do not modify the scheduling information or re-schedule the SLA operation if the current scheduling does not stop.
- Up to 20 detections are available for one test and up to 5 pieces of statistics records are shown.

Prerequisite

- When you configure Layer 2 tests, deploy CFM between local and remote devices that need to be detected. Layer 2 Ping operation succeeds between local and remote devices.
- When you configure Layer 3 tests (icmp-echo and icmp-jitter), Layer 3 Ping operation succeeds between local and remote devices.

11.4.2 Configuring Y.1731-based SLA

When conducting delay test based on Ethernet, LSP, and PW, you can conduct delay compensation according to the interface rate and packet length, obtaining a delay/jitter value close to the actual value. This function can be user-defined.

Configuring SLA delay test

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla** *oper-num* **y1731 latency remote-mep** *mep-id* **level** *level* **svlan** *vlan-id* [**cvlan** *cvlan-id*] [**cos** *cos-value*] [**interval** *interval-num*]	Configure the Y1731-echo delay test based on destination MEP ID.
	Raisecom(config)#**sla** *oper-num* **y1731 latency remote-mep** *mep-id* **level** *level* **svlan** *vlan-id* [**cvlan** *cvlan-id*] [**cos** *cos-value*] [**interval** *interval-num*] [**size** *size-value*] **dm**	
3	Raisecom(config)#**sla** *oper-num* **y1731 latency remote-mac** *mac-address* **level** *level* **svlan** *vlan-id* [**cvlan** *cvlan-id*] [**cos** *cos-value*] [**interval** *interval-num*]	Configure the Y1731-delay test based on destination MAC address.
	Raisecom(config)#**sla** *oper-num* **y1731 latency remote-mac** *mac-address* **level** *level* **svlan** *vlan-id* [**cvlan** *cvlan-id*] [**cos** *cos-value*] [**interval** *interval-num*] [**size** *size-value*] **dm**	

Configuring SLA packet loss test

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla** *oper-num* **y1731 pkt-loss remote-mep** *mep-id* **level** *level* **svlan** *vlan-id* [**cvlan** *cvlan-id*] [**cos** *cos-value*] [**interval** *interval-num*] **[size size-value] slm**	Configure the Y1731 packet loss test operation according to the destination MEP ID. **Note** When testing the packet loss rate according to the MEP ID, it is recommended that the user specify the MAC address when using the **service remote-mep** command to configure the remote MEP.
3	Raisecom(config)#**sla** *oper-num* **y1731 pkt-loss remote-mac** *mac-address* **level** *level* **svlan** *vlan-id* [**cvlan** *cvlan-id*] [**cos** *cos-value*] [**interval** *interval-num*] [**size** *size*-value] **slm**	Configure the Y1731 packet loss test operation according to the destination MAC address.

- After configuring one operation (differed by operation ID), you cannot modify or configure it again. You need to delete the operation in advance if you need to configure it again.
- SLA supports scheduling up to 16 operations at a time. Before you stop scheduling the same operation, you cannot modify scheduling information or re-schedule the operation. If you need to reschedule the operation, you need to finish the scheduling (reach scheduling life time or stop scheduling) before performing the next scheduling.
- When configuring LSP-based SLA operation, note the name of lsp-ingress (LSP Ingress node) is the one of the LSP Ingress node for creating the LSP and the name of the LSP Egress node is the one of the LSP Egress node for creating the LSP.

Enabling SLA packets to encapsulate TLV

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla private-tlv enable**	Enable SLA test packets to encapsulate private TLV.

11.4.3 Configuring SLA operation scheduling

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla schedule** { *oper-num* | **all** } [**life** { **forever** | *life-time* }] [**period** *second*]	Configure SLA scheduling information, including the lifetime period and executive interval, and enable SLA operation scheduling. By default, SLA operation scheduling is disabled.

- The operation lifetime should not be shorter than the interval for scheduling the SLA operation.
- The interval for scheduling the SLA operation should not be shorter than 20s.

11.4.4 Checking configurations

No.	Command	Description
1	Raisecom#**show sla**	Show SLA global information.
2	Raisecom#**show sla** { **all** | *oper-num* | } **configuration**	Show information about SLA operation.

No.	Command	Description
3	Raisecom#**show sla** { **all** | *oper-num* | } **result** { **current-interval** | **current-period** | **history-period** | **latest-period** | **tests** }	Show test information about the operation.
4	Raisecom#**show sla** { **all** | *oper-num* } **threshold**	Show threshold alarms of operation scheduling.

11.5 Configuring SLA test alarm

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla** *oper-num* **loss-rate-threshold** { **current** | **average** } [**ds** | **sd** | **twoway**] *threshold*	Configure the alarm threshold of packet loss rate. By default, it is 999999.
3	Raisecom(config)#**sla** *oper-num* **loss-pkt-trap** { **current** | **average** } **enable**	Enable the packet loss rate alarm. By default, the packet loss rate alarm is disabled.
4	Raisecom(config)#**sla** *oper-num* **delay-threshold** { **current** | **average** } [**ds** | **sd** | **two-way**] *threshold*	Configure the delay alarm threshold. By default, the delay alarm threshold is 5000000us.
5	Raisecom(config)#**sla** *oper-num* **delay-trap** { **current** | **average** } [**ds** | **sd** | **two-way**] **enable**	Enable delay alarm. By default, delay alarm is disabled.

11.6 Configuring interface loopback

11.6.1 Preparing for configurations

Scenario

The network maintenance personnel can detect and analyse interface and network faults through interface loopback. The device supports physical interface loopback and LAG interface loopback.

Prerequisite

The interface status is Up.

11.6.2 Configuring interface loopback

Steps 2 and 3 are optional. To perform interface loopback, execute step 2. To perform link aggregation group loopback, execute step 3.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode and enable interface loopback.
	Raisecom(config-port)#**loopback external** [**access-list** *acl-number* | **rc-sam**] **swap smac** *mac-address* **swap dmac-** *mac-address*	
3	Raisecom(config)#**interface port-channel** *channel-number*	Enter link aggregation configuration mode and enable loopback on the link aggregation group interface.
	Raisecom(config-port-channel*)#**loopback external** [**access-list** *acl-number* **rc-sam**] **swap smac** *mac-address* **swap dmac-** *mac-address*	

11.6.3 Configuring loopback duration

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode and configure the loopback duration.
	Raisecom(config-port)#**loopback timeout** *minutes*	

Note

- The first 3 bytes of the destination MAC address cannot be configured to 0x0180C2.
- The source MAC address cannot be a multicast or broadcast MAC address.

11.6.4 Checking configurations

No.	Command	Description
1	Raisecom#**show interface** *interface-type interface-number*	Show interface status.
2	Raisecom#**show loopback** *interface-type interface-number*	Show configurations of the loopback interface.

11.7 Configuring ULDP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**uldp enable**	Enable ULDP. By default, ULDP is disabled.
3	Raisecom(config)#**uldp recovery-time** *seconds*	Configure the ULDP recovery time. By default, the recovery time is 15s.
4	Raisecom(config)#**show uldp**	Show ULDP configurations.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
6	Raisecom(config-port)#**uldp enable**	Enable ULDP.

11.8 Maintenance

Command	Description
Raisecom(config)#**clear oam config**	Clear OAM configurations.
Raisecom(config-port)#**clear oam event**	Clear OAM event statistics.
Raisecom(config-port)#**clear oam statistics**	Clear OAM statistics.
Raisecom(config)#**clear ethernet cfm errors** [**level** *md-level*]	Clear error CCM records.
Raisecom(config)#**clear ethernet cfm remote-mep** [**level** *md-level*]	Clear information about discovered remote MEPs.
Raisecom(config)#**clear ethernet cfm suppress-alarm source**	Clear alarm inhibition information about MEPs.
Raisecom(config)#**clear ethernet cfm traceroute-cache**	Clear LinkTrace cache configurations.

Command	Description
Raisecom(config)#**clear bfd** *session-id* **statistics**	Clear statistics about specified BFD sessions.
Raisecom(config)#**clear cfm suppress-alarm source**	Clear alarm inhibition information about MPLS-TP MEPs.

12 Security

This chapter describes principles and configuration procedures of security, as well as related configuration examples, including following sections:

- Configuring storm control
- Configuring CPU protection
- Configuring CPU monitoring
- Configuring RADIUS
- Configuring TACACS+
- Configuring RADIUS/TACACS+ accounting management
- Configuring dot.1x
- Configuring interface isolation
- Configuring port mirroring
- Configuring PPPoE+
- Configuring dynamic ARP inspection

12.1 Configuring storm control

12.1.1 Preparing for configurations

Scenario

In the Layer 2 network, after storm control is configured, it can inhabit generation of broadcast storm, when unknown multicast, unknown unicast, and broadcast packets increase, to ensure forwarding normal packets.

Prerequisite

Configure physical parameters on an interface and make the physical layer Up.

12.1.2 Configuring storm control

Configuring storm control on physical interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**storm-control** { **broadcast** | **unknown-multicast** | **dlf** | **all** } **enable**	Enable storm control. By default, storm control of broadcast packets, unknown multicast packets, and unknown unicast packets is disabled.
4	Raisecom(config-port)#**storm-control mode** { **kbps** | **pps** | **ratio** }	Configure the storm control mode to kbps.
5	Raisecom(config-port)#**storm-control** { **broadcast** | **unknown-multicast** | **dlf** } { **kbps** *kbps-value* | **pps** *pps-value* | **ratio** *ratio-vaule* } [**brust** *brust-value*]	Configure the rate limiting threshold of storm control.

Note

When storm control is enabled, you can configure rate limiting. However, configurations cannot take effect. When storm control is disabled, rate limiting configurations take effect automatically.

12.1.3 Checking configurations

No.	Command	Description
1	Raisecom#**show storm-control interface** [*interface-type interface-number*]	Show storm control configurations.

12.2 Configuring CPU protection

12.2.1 Preparing for configurations

Scenario

When the device receives a great number of attack packets in a short period, the CPU will run with full load and the CPU utilization rate reaches to 100%. This will cause the normal functions of the device to fail. CPU CAR helps to efficiently limit the speed of packets, which enters the CPU.

Prerequisite

N/A

12.2.2 Configuring global CPU CAR

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**cpu-protect car type** { **arp** | **bpdu** | **dhcp** | **icmp** | **igmp** | **mld** | **ndp** | **oam** } **queue** *queue-id*	Configure the protocol binding queue of CPU protection.
3	Raisecom(config)#**cpu-protect car global kbps cir** *cir* **cbs** *cbs*	Configure the rate limiting mode of global CPU packet protection.
4	Raisecom(config)#**cpu-protect car queue** *queue-id* **kbps cir** *cir* **cbs** *cbs*	Configure the rate limiting mode of CPU protection queue.

12.2.3 Clear statistics

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**clear** cpu-protect car **global statistics**	Clear statistics about global statistics on CPU protection.
3	Raisecom(config)#**clear** cpu-protect car **queue** *queue-id* **statistics**	Clear statistics on the specified queue of CPU protection.

12.2.4 Checking configurations

No.	Command	Description
1	Raisecom#**show cpu-protect car statistics**	Show CPU CAR statistics.

12.3 Configuring CPU monitoring

12.3.1 Preparing for configurations

Scenario

CPU monitoring is used to monitor task status, CPU utilization rate, and stack usage in real time. It provides CPU utilization threshold alarm to facilitate discovering and eliminating a hidden danger, helping the administrator locate the fault quickly.

Prerequisite

To output CPU monitoring alarms in a Trap form. You need to configure the IP address of Trap target host on the RAX721-A, that is, the IP address of the NView NNM system.

12.3.2 Configuring CPU monitoring alarm

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)# **cpu threshold recovering** *recovering-threshold-value* **rising** *rising-threshold-value*	Configure the CPU alarm rising threshold and recovery threshold.
3	Raisecom(config)#**cpu interval** *interval-value*	(Optional) configure the CPU alarm sampling interval. By default, the sampling interval of CPU alarm is 60s.
4	Raisecom#**show cpu-utilization** [**dynamic**]	Show the CPU utilization rate.
5	Raisecom#**show cpu-utilization history** { **10min** | **1min** | **2hour** | **5sec** }	
6	Raisecom#**show process** [**dead** | **sorted** { **priority** | **name** } | *taskname*]	Show status of each task.
7	Raisecom#**show process cpu** [**sorted** [**10min** | **1min** | **5sec** | **invoked**]]	

12.4 Configuring RADIUS

12.4.1 Preparing for configurations

Scenario

To control users accessing devices and network, you can deploy the RADIUS server at the network to authenticate and account users. The RAX721-A can be used as a Proxy of the RADIUS server to authenticate users based on results returned by the RADIUS server.

Prerequisite

N/A

12.4.2 Configuring IPv4 RADIUS authentication

Step	Command	Description
1	Raisecom#**radius** [**backup**] *ip-address* [**auth-port** *port-id*]	Specify the IP address and port ID of the RADIUS authentication server. The **backup** parameter is used to specify a backup RADIUS authentication server.
2	Raisecom#**radius-key** *string*	Configure the shared key of the RADIUS authentication server.
3	Raisecom#**radius-encrypt-key** *string*	Configure the shared ciphertext key of the RADIUS authentication server.
4	Raisecom#**radius backup key** *string*	Configure the shared key of the backup RADIUS authentication server.
5	Raisecom#**radius backup encrypt-key** *string*	Configure the ciphertext shared key of the backup RADIUS authentication server.
6	Raisecom#**radius response-timeout** *seconds*	(Optional) configure the response timeout time of the RADIUS server.
7	Raisecom#**radius authentication fail trap enable**	Enable authentication failure alarm reporting.

12.4.3 Configuring IPv6 RADIUS authentication

Step	Command	Description
1	Raisecom#**radius** [**backup**] *ipv6-address* [**auth-port** *port-id*]	Specify the IPv6 address and authentication interface ID of the RADIUS authentication server. Configure the **backup** parameter to specify the backup RADIUS authentication server.
3	Raisecom#**radius-key** *string*	Configure the shared key of the RADIUS authentication server.
4	Raisecom#**radius-encrypt-key** *string*	Configure the ciphertext shared secret key of the RADIUS authentication server.
5	Raisecom#**radius backup key** *string*	Configure the shared key of the backup RADIUS authentication server.
6	Raisecom#**radius backup encrypt-key** *string*	Configure the ciphertext shared secret key of the backup RADIUS authentication server.
7	Raisecom#**radius response-timeout** *seconds*	(Optional) configure the response timeout time of the RADIUS server.
8	Raisecom#**radius authentication fail trap enable**	Enable alarm reporting for authentication failure.

Step	Command	Description
1	Raisecom#**radius** [**backup**] *ipv6-address* [**auth-port** *port-id*]	Specify the IPv6 address and authentication interface ID of the RADIUS authentication server. Configure the **backup** parameter to specify the backup RADIUS authentication server.

12.4.4 Configuring IPv4 RADIUS accounting

Step	Command	Description
1	Raisecom#**radius** [**backup**] **accounting-server** *ip-address* [**acct-port** *port-id*]	Specify the IP address and accounting interface ID of the RADIUS accounting server. By default, the interface ID is 1813. Configure the **backup** parameter to specify the backup RADIUS accounting server.
2	Raisecom#**radius accounting-server key** *string*	Configure the shared key to communicate with the RADIUS accounting server.
3	Raisecom#**radius accounting-server encrypt-key** *string*	Configure the encrypted shared key to communicate with the RADIUS accounting server.
4	Raisecom#**radius authorization no-privilege** { **offline** | *priority-value* }	Configure the processing policy for accounting authorization failure. • **offline**: force offline. If the authorization fails, the user is forced to go offline. • *priority-value*: user priority. If authorization fails, the user uses the specified priority.

12.4.5 Configuring IPv6 RADIUS accounting

Step	Command	Description
1	Raisecom#**radius** [**backup**] **accounting-server** *ipv6-address* [**acct-port** *port-id*]	Specify the IPv6 address and accounting interface ID of the RADIUS accounting server. By default, the interface ID is 1813. Configure the **backup** parameter to specify the backup RADIUS accounting server.
2	Raisecom#**radius accounting-server key** *string*	Configure the shared key to communicate with the RADIUS accounting server.
3	Raisecom#**radius accounting-server encrypt-key** *string*	Configure the encrypted shared key to communicate with the RADIUS accounting server.
4	Raisecom#**radius authorization no-privilege** { **offline** | *priority-value* }	Configure the processing policy for accounting authorization failure. • **offline**: force offline. If the authorization fails, the user is forced to go offline. • *priority-value*: user priority. If authorization fails, the user uses the specified priority.

12.4.6 Checking configurations

No.	Command	Description
1	Raisecom#**show radius-server**	Show configurations of the RADIUS server.

12.5 Configuring TACACS+

12.5.1 Preparing for configurations

Scenario

To control users accessing devices and network, you can deploy the RADIUS server on the network to authenticate and account users. Compared with RADIUS, TACACS+ is more secure and reliable. The RAX721-A can be used as a Proxy of the TACACS+ server to authenticate users based on results returned by the TACACS+ server.

Prerequisite

N/A

12.5.2 Configuring IPv4 TACACS+ authentication

Step	Command	Description
1	Raisecom#**tacacs-server** [**backup**] *ip-address* [**auth-port** *port-id*]	Specify the IP address and port ID of the TACACS+ authentication server. The **backup** parameter is used to specify a backup TACACS+ authentication server.
2	Raisecom#**tacacs-server** [**backup**] **key** *string*	Configure the shared key of TACACS+ authentication. The **backup** parameter refers to the backup server.
3	Raisecom#**tacacs-server** [**backup**] **encrypt-key** *string*	Configure the ciphertext shared key of the TACACS+ authentication server. The **backup** parameter refers to the backup server.

12.5.3 Configuring IPv6 TACACS+ authentication

Step	Command	Description
1	Raisecom#**tacacs-server** [**backup**] *ipv6-address* [**auth-port** *port-id*]	Specify the IPv6 address of the TACACS+ authentication server. Configure the **backup** parameter to specify the backup TACACS+ authentication server.

Step	Command	Description
2	Raisecom#**tacacs-server key** *string*	Configure the shared key of TACACS+ authentication.
3	Raisecom#**tacacs-server** [**backup**] **key** *string*	Configure the shared key of TACACS+ authentication. The **backup** parameter refers to the backup server.
4	Raisecom#**tacacs-server** [**backup**] **encrypt-key** *string*	Configure the ciphertext shared key of the TACACS+ authentication server. The **backup** parameter refers to the backup server.

12.5.4 Configuring IPv4 TACACS+ accounting

Step	Command	Description
1	Raisecom#**tacacs** [**backup**] **accounting-server** *ip-address*	Configure the IPv4 address of the TACACS+ accounting server. Select the **backup** parameter to configure the IP address of the backup server.
2	Raisecom#**tacacs accounting-server key** *string*	Configure the shared key for communicating with the TACACS+ accounting server.
4	Raisecom#**tacacs accounting-server encrypt-key** *string*	Configure the encrypted shared key for communicating with the TACACS+ accounting server.

12.5.5 Configuring IPv6 TACACS+ accounting

Step	Command	Description
1	Raisecom#**tacacs** [**backup**] **accounting-server** *ipv6-address*	Configure the IPv6 address of the TACACS+ accounting server. Select the **backup** parameter to configure the IP address of the backup server.
2	Raisecom#**tacacs accounting-server key** *string*	Configure the shared key for communicating with the TACACS+ accounting server.
4	Raisecom#**tacacs accounting-server encrypt-key** *string*	Configure the encrypted shared key for communicating with the TACACS+ accounting server.

12.5.6 Checking configurations

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

12.6 Configuring RADIUS/TACACS+ accounting management

12.6.1 Configuring accounting policy

Step	Command	Description
1	Raisecom#**aaa**	Enter the charging configuration mode.
2	Raisecom(aaa)#**domain** { **default** | **default_admin** | *domain-name* }	Configure the accounting domain.
3	Raisecom(aaa)#**aaa accounting login enable**	Enable accounting. By default, the system is not enabled with accounting.
4	Raisecom(aaa)#**aaa command authorize enable**	Enable authentication of accounting command line.
5	Raisecom(aaa)#**login-trap enable**	Enable accounting login Trap.
6	Raisecom(aaa)#**aaa accounting fail** { **online** | **offline** }	Configure the processing policy for accounting failure. By default, it is online, that is, login is allowed after accounting fails.
7	Raisecom(aaa)#**aaa accounting update** *period*	Configure the sending interval for accounting update packets. If it is configured to 0, no accounting update packet is sent. By default, the sending interval is 0. **Note** The RADIUS accounting server can record each user's access time and operation by receiving the accounting start packet, accounting update packet, and accounting end packet.

12.6.2 Configuring user management

Step	Command	Description
1	Raisecom#**aaa**	Enter accounting configuration mode.
2	Raisecom(aaa)#**user name** *user-name* **password** [**plain**] [**cipher**] *password*	Configure the user name and password.
3	Raisecom(aaa)#**user name** *user-name* **privilege** *priority-value*	Configure the user priority.
4	Raisecom(aaa)#**user name** *user-name* **state** { **active** | **inactive** }	Configure the user status.
5	Raisecom(aaa)#**user** *user-name* **bind-ip** *ip-address*	(Optional) bind the user with an IPv4 address.
	Raisecom(aaa)#**user** *user-name* **bind-ipv6** *ipv6-address*	(Optional) bind the user with an IPv6 address.
6	Raisecom(aaa)#**user_group** *group-id*	Create a user group.
7	Raisecom(aaa)#**user** *user-name* **user_group** *group-id*	Configure the members of the user group.
8	Raisecom(aaa)#**user** *user-name* { **allow-exec** | **disallow-exec** } *first-keyword* [*second-keyword*]	Configure the user naming conventions.
9	Raisecom(aaa)#**user** *user-name* **service-scheme** *scheme-name*	Configure the user service plan.

12.6.3 Checking configurations

No.	Command	Description
1	Raisecom#**show aaa**	Show AAA configurations.

12.7 Configuring dot.1x

12.7.1 Preparing for configurations

Scenario

The network space of the Wi-Fi LAN features openness and mobility of terminals. It is not like the wired LAN in which you can determine whether the terminals belong to the network through physical network space. Therefore, how to prevent illegal access through interface authentication challenges the Wi-Fi network. However, IEEE 802.1X can solve this problem.

12.7.2 Configuring basic dot.1x

- Dot.1X and STP are mutually exclusive on the interface and cannot be used at the same time.
- An interface can only handle one user authentication request at a time.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#dot1x enable`	Enable global Dot.1X.
3	`Raisecom(config)#dot1x authentication-method { chap | pap | eap }`	Configure the global authentication method.
4	`Raisecom(config)#dot1x auth-mode { radius | local | tacacs+ }`	Configure the authentication mode for Dot.1X authentication.
5	`Raisecom(config)#dot1x free-ip` *ip-address* `[` *ip-mask* `|` *mask-lenth* `]`	Configure an IP address segment that can be accessed by Dot.1X terminal users who fail authentication or exit authorization.
6	`Raisecom(config)#interface` *interface-type interface-number*	Enter physical layer interface configuration mode.
7	`Raisecom(config-port)#dot1x enable`	Enable Dot.1X on the interface.
8	`Raisecom(config-port)#dot1x auth-control { auto | authorized-force | unauthorized-force }`	Configure the interface access control mode.
9	`Raisecom(config-port)#dot1x auth-method { portbased | macbased }`	Configure the interface access control mode.
10	`Raisecom(config-port)#dot1x keepalive { enable | disable }`	Enable/Disable Dot.1X handshake on the interface.
11	`Raisecom(config-port)#dot1x max-user` *user-number*	Configure the maximum number of users allowed for Dot.1X port authentication.

If Dot.1X is not enabled in global or interface mode, the interface control mode of Dot.1X is the mandatory authorization.

12.7.3 Configuring Dot.1X re-authentication

Re-authentication is initiated for authorized users, so before enabling re-authentication, you should ensure that global and interface Dot.1X are enabled. The interface in authorized state

still maintains the authorized state during the re-authentication process. If re-authentication fails, it enters the unauthorized state.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**dot1x reauthentication enable**	Enable Dot.1X re-authentication.

12.7.4 Configuring Dot.1X timer

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**dot1x timer reauth-period** *reauth-period*	Configure the re-authentication timer.
4	Raisecom(config-port)#**dot1x timer quiet-period** *second*	Configure the silent timer.
5	Raisecom(config-port)#**dot1x timer supp-timeout** *supp-timeout*	Configure the authentication timeout timer for applicants.
6	Raisecom(config-port)#**dot1x timer server-timeout** *server-timeout*	Configure the authentication server timeout timer.
7	Raisecom(config-port)#**dot1x timer keepalive-period** *second*	Configure the interval for Dot.1X to retransmit Keepalive packets on the interface.
8	Raisecom(config-port)#**dot1x timer tx-period** *second*	Configure the Request/Identity request packet timeout timer.

12.7.5 Checking configurations

No.	Command	Description
1	Raisecom#**show dot1x** *interface-type interface-list*	Show Dot.1X configurations on the interface.
2	Raisecom#**show dot1x** *interface-type interface-list* **statistics**	Show Dot.1X statistics on the interface.
3	Raisecom#**show dot1x** *interface-type interface-list* **user**	Show user information for Dot.1X authentication on the interface.

No.	Command	Description
4	Raisecom#**show dot1x free-ip**	Show the IP address segments that can be accessed by Dot.1X terminal users who fail authentication or exit authorization.

12.7.6 Maintenance

Command	Description
Raisecom(config)#**clear dot1x** *interface-type interface-list* **statistics**	Clear Dot.1X statistics on the interface.

12.8 Configuring interface isolation

12.8.1 Preparing for configurations

Scenario

To isolate Layer 2 data of interfaces in a VLAN and provide physical isolation between interfaces, you need to configure interface isolation.

By adding interfaces that need to be controlled to a VLAN protection group, you can enhance network security and provide flexible networking scheme for users.

Interface isolation helps isolate interfaces in a VLAN, enhance network security, and provide flexible networking schemes.

Prerequisite

N/A

12.8.2 Configuring interface isolation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**portswitch**	Enter Layer 2 physical interface configuration mode.
3	Raisecom(config-port)#**switchport protect**	Enable interface isolation.

12.8.3 Configuring VLAN isolation

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#protect-group` *group-id* `vlan` *vlan-id interface-type interface-number*	Create an isolation group and configure the isolation VLAN and isolation interface list associated with the isolation group.

12.8.4 Checking configurations

No.	Command	Description
1	`Raisecom#show switchport protect`	Show configurations of interface isolation.
2	`Raisecom#show protect-group { all |` *group-id* `}`	Show configurations of interface isolation.

12.9 Configuring port mirroring

12.9.1 Preparing for configurations

Scenario

Port mirroring refers to mirroring packets of the specified mirroring port to the destination port or aggregation group without affecting packet forwarding. With port mirroring, users can monitor transmitting and receiving status of one or more interfaces for analyzing network status.

Prerequisite

N/A

12.9.2 Configuring port mirroring

The same interface/link aggregation group cannot be a monitoring interface and a mirroring source interface concurrently. Therefore, the interface/link aggregation group in step 3 and step 4 cannot be the same one.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#mirror-group` *group-id*	Create a port mirroring group.
3	`Raisecom(config)#mirror-group` *group-id* `remote-vlan` *vlan-id*	Configure the remote mirroring VLAN of the mirroring group.

Step	Command	Description
4	Raisecom(config)#**mirror-group** *group-id* **reflector-port** *interface-type interface-number*	Configure the reflector interface of the mirroring group.
5	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**mirror-group** *group-id* **monitor-port** Raisecom(config-port)#**exit**	(Optional) enter interface configuration mode. Configure the interface as a monitoring interface.
	Raisecom(config)#**interface port-channel** *channel-number* Raisecom(config-port-channel*)#**mirror-group** *group-id* **monitor-port** Raisecom(config-port-channel*)#**exit**	(Optional) enter link aggregation configuration mode. Configure the link aggregation group as the monitoring interface.
6	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**mirror-group** *group-id* **source-port** [**ingress** | **egress**]	(Optional) enter interface configuration mode. Configure the interface as a mirroring source interface and configure mirroring rules to mirror the packets in the ingress direction, egress direction, or both directions of the source interface.
	Raisecom(config)#**interface port-channel** *channel-number* Raisecom(config-port-channel*)#**mirror-group** *group-id* **source-port** [**ingress** | **egress**]	(Optional) enter link aggregation configuration mode. Configure the link aggregation group as a mirroring source interface and configure mirroring rules to mirror the packets in the ingress direction, egress direction, or both directions of the source interface.
7	Raisecom(config-port)#**exit** Raisecom(config)#**mirror-group** *group-id* **source-cpu** [**ingress** | **egress**]	Configure the CPU as the source of the mirror group.

12.9.3 Checking configurations

No.	Command	Description
1	Raisecom#**show mirror-group** [*group-id*]	Show basic information about port mirroring.

12.10 Configuring PPPoE+

12.10.1 Preparing for configurations

Scenario

To prevent illegal users from accessing during the PPPoE authentication process, you need to configure PPPoE + and add additional user identification information to the PPPoE packets.

Since the added user identification information is related to the specific switch and interface, the authentication server can bind the user to the switch and interface and other information. Therefore, the problems of account sharing and account theft can be effectively prevented, and users can be better positioned to ensure network security.

Prerequisite

N/A

12.10.2 Configuring PPPoE+ basic functions

PPPoE + is used to process PADI and PADR messages, and only targets at PPPoE clients. Generally, only the interface connected to the client is enabled with PPPoE +, and the trusted interface refers to the interface connecting the switch and the PPPoE server. The roles of these two interfaces are mutually exclusive, that is, an interface cannot be both a PPPoE+ enabled interface and a trusted interface.

Enabling PPPoE+

After PPPoE + is enabled globally and on the interface of the device, the PPPoE authentication packet sent to the interface will be added with user information and then sent to the trusted interface.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**pppoeagent enable**	Enable global PPPoE+.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#**portswitch**	Configure the interface mode to switch mode.
5	Raisecom(config-port)#**pppoeagent enable**	Enable PPPoE+ on the interface.

Configuring PPPoE+ trusted interface

The PPPoE + trusted interface is configured to prevent PPPoE server spoofing and security risks caused by PPPoE packets being forwarded to other non-service interfaces. Generally, the interface connected to the PPPoE server is configured as the trusted interface. PPPoE packets from the PPPoE client to the server will only be forwarded by the trusted interface, and only PPPoE packets received from the trusted interface will be forwarded to the PPPoE client.

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

Step	Command	Description
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**portswitch**	Configure the interface mode to switching mode.
4	Raisecom(config-port)#**pppoeagent trust**	Configure the PPPoE+ trusted interface.

Because PPPoE + is aimed at the PPPoE client instead of the server, the downstream interface of the device cannot receive PADO and PADS packets, which means that the PPPoE + enabled interface cannot receive PADO and PADS packets. If the interface receives these packets, it indicates that there are error packets and the interface should discard them. However, the interface can forward PADO and PADS packets from the trusted interface. At the same time, PADI and PADR packets should only be forwarded to the trusted interface.

12.10.3 Configuring PPPoE+ packet information

PPPoE + mainly processes a specific Tag in PPPoE packets. This Tag contains two fields: Circuit ID and Remote ID:

- Circuit ID is filled with the VLAN ID, interface number and host name of the interface that receives the client request packets.
- Remote ID is filled with the MAC address of the client or the MAC address of the switch.

Configuring Circuit ID

Circuit ID has two filling modes: switch mode and ONU mode. The default is Switch mode. In ONU mode, the format of Circuit ID is fixed, and there is no customized format. These commands are used to configure the padding content of the Circuit ID in Switch mode.

In Switch mode, Circuit ID has two filling formats:

- Default format: when no custom Circuit ID is configured, it is filled with VLAN ID /interface number/additional string (if no additional string is defined, the default is the hostname).
- Customized format: when a customized Circuit ID is configured, it is filled with the configured Circuit ID string.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**pppoeagent circuit-id mode** { **onu** | **switch** | **olt** }	Configure the padding mode of Circuit ID.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#**portswitch**	Configure the interface mode to switching mode.

Step	Command	Description
5	Raisecom(config-port)#**pppoeagent circuit-id** *string*	(Optional) configure the Circuit ID as a customized character string.

Circuit ID contains an additional string in the default format. The additional string is the hostname of the switch by default. You can configure it as a customized string.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**pppoeagent circuit-id attach-string** *string*	(Optional) configure the additional string of the Circuit ID. If the Circuit ID is the default format, the contents configured by this command will be added to the Circuit ID.

Configuring Remote ID

Remote ID is filled with a MAC address, you can choose to fill in the MAC address of the switch or the MAC address of the client, and you can choose to fill in the Remote ID in binary or ASCII form.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**portswitch**	Configure the interface mode to switching mode.
4	Raisecom(config-port)#**pppoeagent remote-id** { **client-mac** | **switch-mac** }	(Optional) fill in the Remote ID of the interface PPPoE+ with the MAC address.
5	Raisecom(config-port)#**pppoeagent remote-id format** { **ascii** | **binary** }	(Optional) configure the Remote ID padding mode of the interface PPPoE+.

Configuring Tag overwriting

For some reasons, such as the tag of some information fields may be forged by the client, the original Tag of the packet needs to be overwritten. After Tag overwriting is enabled, if PPPoE packets already carry the information field Tag, the tag will be overwritten. If not, a tag will be added.

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

Step	Command	Description
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**portswitch**	Configure the interface mode to switching.
4	Raisecom(config-port)#**pppoeagent vendor-specific-tag overwrite enable**	Enable Tag overwriting.

12.10.4 Checking configurations

No.	Command	Description
1	Raisecom#**show pppoeagent** [*interface-type interface-list*]	Show PPPoE+ configurations.
2	Raisecom#**show pppoeagent statistic** [*interface-type interface-list*]	Show PPPoE+ statistics.

12.10.5 Maintenance

Command	Description
Raisecom(config)#**clear pppoeagent statistic**	Clear PPPoE+ statistics.

12.11 Configuring dynamic ARP inspection

12.11.1 Preparing for configurations

Scenario

Dynamic ARP inspection is used to prevent common ARP spoofing attacks in the network, and to isolate ARP packets from unsafe sources. Whether to trust ARP packets is achieved through the trust status of the interface, and whether it meets the requirements is achieved through the binding table.

Prerequisite

Before configuring dynamic ARP inspection, if there are DHCP users, you need to enable DHCP snooping.

12.11.2 Configuring trusted interface of dynamic ARP inspection

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

Step	Command	Description
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**ip arp-inspection trust**	Configure the interface as a trusted interface. You can use the **no ip arp-inspection trust** command to configure the interface to a non-trusted interface, which means that the interface does not trust ARP packets.

12.11.3 Configuring static binding of dynamic ARP inspection

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip arp-inspection static-config**	Enable global static binding.
3	Raisecom(config)#**ip arp-inspection binding** *ip-address* [*mac-address*] [**vlan** *vlan-id*] **port** *port-id*	Configure static binding relationship.

12.11.4 Configuring dynamic binding of dynamic ARP inspection

Caution

To enable dynamic binding of dynamic ARP inspection, use the **ip dhcp snooping** command to enable DHCP snooping.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip arp-inspection dhcp-snooping**	Enable global dynamic binding.

12.11.5 Configuring protection VLAN of dynamic ARP inspection

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip arp-inspection dhcp-snooping**	Enable global dynamic binding.
3	Raisecom(config)#**ip arp-inspection vlan** *vlan-list*	Configure the protection VLAN of dynamic ARP inspection.

12.11.6 Checking configurations

Step	Command	Description
1	Raisecom#**show ip arp-inspection**	Show configurations of dynamic ARP.
2	Raisecom#**show ip arp-inspection binding** [**interface-type interface-number**]	Show configurations of the dynamic ARP binding table.

13 Reliability

This chapter describes principles and configuration procedures of network reliability, as well as related configuration examples, including following sections:

- Configuring link aggregation
- Configuring interface backup
- Configuring ELPS
- Configuring ERPS
- Configuring VRRP
- Configuring link-state tracking
- Maintenance

13.1 Configuring link aggregation

13.1.1 Preparing for configurations

Scenario

When greater bandwidth and high reliability are needed for network links, you can configure manual or static LACP link aggregation.

Link aggregation aggregates multiple physical Ethernet interfaces into a logical link to provide load sharing of uplink and downlink traffic among member interfaces. This helps increase the bandwidth. In addition, connection reliability is enhanced when member interfaces back up for each other dynamically.

mLACP link aggregation is used for the AC-side link in dual-homed PW protection to provide communication between the DHD and 2 destination modes, as well as selection of active interfaces. It is used to resolve the problem for selecting the path, prevent the loop, and enhance the network availability.

Prerequisite

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

13.1.2 Configuring manual link aggregation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port-channel** *channel-number*	Enter LAG configuration mode.
3	Raisecom(config-port-channel*)#**mode manual**	Configure the manual link aggregation mode.
4	Raisecom(config-port-channel*)#**load-sharing mode** { **dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac** }	Configuring the load-sharing mode of the link aggregation. By default, load sharing mode is **rc-dst-mac**, which means selecting the forwarding interface according to OR operation result of source MAC address and destination MAC address.
5	Raisecom(config-port-channel*)#**exit**	Return to global configuration mode.
6	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical interface configuration mode.
7	Raisecom(config-port)#**portswitch**	Configure the interface as a switching interface or a Layer 3 interface working in Layer 2 mode.
8	Raisecom(config-port)#**port-channel** *group-id*	Add member interfaces to the LAG.
9	Raisecom(config-port)#**exit**	Return to global configuration mode.

Note

Ensure not to configure services on interfaces, which are added to the LAG.
In a LAG, member interfaces that share loads must be identically configured. Otherwise, data cannot be forwarded properly. For example, packets may be lost. These configurations include STP, QoS, QinQ, VLAN, interface properties, and MAC address learning.

- STP status on the interface, properties (point-to-point/non point-to-point) of the link connected to the interface, path cost of the interface, STP priority, packet Tx speed limit, whether the interface is configured with loopback protection, root protection, and whether the interface is an edge interface.
- QoS: traffic policing, traffic shaping, congestion avoidance, rate limiting, SP queue, WRR queue scheduling, WFQ queue, interface priority, and interface trust mode.
- QinQ: QinQ status on the interface, added outer VLAN tag, policies for adding outer VLAN Tags for different inner VLAN IDs.
- VLAN: the allowed VLAN, default VLAN, and the link type (Trunk, Hybrid, and Access) on the interface, and whether VLAN packets carry Tag.
- Interface properties: speed, duplex mode, and link Up/Down status.
- MAC address learning: MAC address learning status, MAC address limit, and whether to forward and control data after the MAC address table is full.

13.1.3 Configuring static LACP link aggregation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**lacp system-priority** *priority*	(Optional) configure the system LACP priority. The smaller the value is, the higher the system LACP priority is. The end with a higher system LACP priority is the active end. LACP selects the active interface and standby interface based on configurations on the active end. If the system LACP priorities are identical, select the one with a smaller MAC address as the active end. By default, the system LACP priority is 32768.
3	Raisecom(config)#**lacp timeout** { **fast** | **slow** }	(Optional) configure the LACP timeout mode.
4	Raisecom(config)#**interface port-channel** *channel-number*	Enter LAG configuration mode.
5	Raisecom(config-port-channel*)#**mode lacp**	Configure the working mode of the LAG to static LACP link aggregation.
6	Raisecom(config-port-channel*)#{ **max-active** | **min-active** } **links** *threshold*	(Optional) configure the maximum/minimum number of active links of the LACP LAG.
7	Raisecom(config-port-channel1)#**lacp priority preempt enable**	(Optional) enable priority preemption of the link aggregation group.
8	Raisecom(config-port-channel*)#**load-sharing mode** { **dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac** }	(Optional) configure the load balancing mode of link aggregation. By default, the system uses the **src-dst-mac** mode, which selects the forwarding interface based on logical OR of the source and destination MAC addresses.
9	Raisecom(config-port-channel*)#**exit**	Return to global configuration mode.
10	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical interface configuration mode.
11	Raisecom(config-port)#**portswitch**	Configure the interface to switch mode.
12	Raisecom(config-port)#**port-channel** *channel-number*	Add the interface to the LAG.
13	Raisecom(config-port)#**lacp mode** { **active** | **passive** }	(Optional) configure the LACP mode of member interfaces. By default, the LACP mode is active. LACP connection fails if both ends of a link are in passive mode.

Step	Command	Description
14	Raisecom(config-port)#**lacp port-priority** *priority*	(Optional) configure the interface LACP priority. The interface LACP priority affects the selection of LACP default interface. The smaller the number is, the higher the priority is. By default, it is 32768.
15	Raisecom(config-port)#**exit**	Exit global configuration mode.

- In a static LACP LAG, a member interface can be an active/standby one. Both the active interface and standby interface can receive and send LACPDU. However, the standby interface cannot forward user packets.
- The system selects a default interface based on following conditions in order: whether the neighbor is discovered, maximum interface speed, the highest interface LACP priority, and the smallest interface ID. The default interface is in active status. Interfaces, which have the same speed, peer device, and operation key of the operation key with the default interface, are in active status. Other interfaces are in standby status.
- When the number of member interfaces in the static LAG reaches the maximum number of active interfaces, the later-added interfaces cannot become active interfaces even they meet all requirements on active interfaces. This helps make traffic of current member interfaces continuous.

13.1.4 Configuring manual backup link aggregation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port-channel** *channel-number*	Enter aggregation group configuration mode.
3	Raisecom(config-port-channel*)#**mode manual backup**	Configure the working mode of the LAG to manual backup link aggregation.
4	Raisecom(config-port-channel*)#**master-port** *interface-type interface-number*	Configure the master interface of link aggregation.
5	Raisecom(config-port-channel*)#**restore-mode** { **non-revertive** | **revertive** [**restore-delay** *second*] }	Configure the restoration mode and restoration delay of the LAG. By default, the restoration mode is non-revertive.
6	Raisecom(config-port-channel*)#**exit**	Return to global configuration mode.
7	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 2 physical interface configuration mode.
8	Raisecom(config-port)#**portswitch**	Configure the interface as a switching interface or a Layer 3 interface working in Layer 2 mode.
9	Raisecom(config-port)#**port-channel** *channel-number*	Add member interfaces to the LAG.

Step	Command	Description
10	Raisecom(config-port)#**exit**	Return to global configuration mode.

13.1.5 Configuring static LACP backup link aggregation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**lacp system-priority** *system-priority*	(Optional) configure the system LACP priority. The smaller the value is, the higher the system LACP priority is. The end with a higher system LACP priority is the active end. LACP selects the active interface and standby interface based on configurations on the active end. If the system LACP priorities are identical, select the one with a smaller MAC address as the active end. By default, it is configured to 32768.
3	Raisecom(config)#**lacp timeout** { **fast** | **slow** }	(Optional) configure the LACP timeout mode.
4	Raisecom(config)#**interface port-channel** *channel-number*	Enter aggregation group configuration mode.
5	Raisecom(config-port-channelif)#**mode lacp backup**	Configure the working mode of the LAG to static LACP backup link aggregation.
6	Raisecom(config-port-channelif)#**master-port** *interface-type interface-number*	Configure the master interface of link aggregation.
7	Raisecom(config-port-channelif)#**restore-mode** { **non-revertive** | **revertive** [**restore-delay** *second*] }	Configure the restoration mode and restoration delay of the LAG. By default, the restoration mode is non-revertive.
8	Raisecom(config-port-channelif)#**exit**	Return to global configuration mode.
9	Raisecom(config)#**interface** interface-type interface-number	Enter Layer 2 physical interface configuration mode.
10	Raisecom(config-port)#**portswitch**	Configure the interface as a switching interface or a Layer 3 interface working in Layer 2 mode.
11	Raisecom(config-port)#**port-channel** *channel-number*	Add Layer 2 physical interfaces to the LAG.
12	Raisecom(config-port)#**lacp mode** { **active** | **passive** }	(Optional) configure the LACP mode of member interfaces. By default, the LACP mode is active. LACP connection fails if both ends of a link are in passive mode.

Step	Command	Description
13	Raisecom(config-port)#**lacp port-priority** *port-priority*	(Optional) configure the interface LACP priority. The interface LACP priority affects the selection of the default LACP interface. The smaller the number is, the higher the priority is. By default, it is 32768.
14	Raisecom(config-port)#**exit**	Return to global configuration mode.

13.1.6 Configuring mLACP link aggregation

Configuring ICCP channel

In the application scenario of PW dual-homing protection, the user equipment accesses the network through two PE devices. An ICCP channel needs to be established between the two PE devices in order to carry DNI-PW (bypass PW).

Perform the following configurations on the MC-PW working node and protection node respectively.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**iccp local-ip** *ip-address*	Configure the local IP address of the ICCP channel. The IP address generally uses the IP address of the channel physical interface or channel aggregation interface.
3	Raisecom(config)#**iccp channel** *channel-id*	Create an ICCP channel and enter ICCP configuration mode.
4	Raisecom(config-iccp)#**member-ip** *ip-address*	Configure the IP address of the peer device of the ICCP channel.
5	Raisecom(config-iccp)#**iccp enable**	Enable the ICCP channel.

Configuring mLACP link aggregation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mlacp-group** *icg-id*	Create a chassis group and enter chassis group configuration mode.
3	Raisecom(config-ic-group)#**iccp-channel** *channel-id*	Bind an ICCP channel to the chassis group.
4	Raisecom(config-ic-group)#**mlacp** { **master** | **slave** }	Configure the mLACP role of the local device in the chassis group.

Step	Command	Description
5	Raisecom(config-ic-group)#**port-channel** *group-id*	Bind a LAG to the chassis group.
6	Raisecom(config-ic-group)#**restore-mode** { **non-revertive** | **revertive** [**restore-delay** *seconds*] }	Configure the fault restoration mode and delay of the LAG in the chassis group.
7	Raisecom(config-ic-group)#**mlacp system-priority** *system-priority*	Configure the mLACP system priority of the local device in the chassis group. By default, it is 32768.
8	Raisecom(config-ic-group)#**track pw** *pw-id* **peer** *ip-address*	Configure the PW to be monitored in the chassis group.

13.1.7 Checking configurations

No.	Command	Description
1	Raisecom#**show lacp internal**	Show local system LACP interface status, identifier, interface priority, management key, operation key, and interface status machine.
2	Raisecom#**show lacp neighbor** { **detail** }	Show neighbor LACP information, including the identifier, interface priority, device ID, Age, operation key ID, interface ID, and interface status machine.
3	Raisecom#**show lacp statistics**	Show interface LACP statistics, including the total number of received LACP packets, number of received and transmitted Marker packets, number of received and transmitted Marker Response packets, and number of error packets.
4	Raisecom#**show lacp sys-id**	Show global enabling status of local system LACP, device ID, LACP priority, and MAC address.
5	Raisecom#**show port-channel**	Show whether the current system is enabled with link aggregation, link aggregation load-sharing mode, member interfaces and currently-active member interfaces in all current LAGs. **Note** Currently active member interfaces refers to interfaces in UP status in the LAG.
6	Raisecom#**show mlacp-group** [*icg-list*]	Show configurations and running information about the MLACP group.
7	Raisecom#**show mlacp-group** [*icg-list*] **statistics**	Show packet receiving/sending statistics of the MLACP group.

13.2 Configuring interface backup

13.2.1 Preparing for configurations

Scenarios

In a dual-uplink networking scenario, you can realize redundancy backup of the primary/slave link and fast switching of services through interface backup, thus improving service reliability.

Prerequisite

N/A

13.2.2 Configuring interface backup group

The RAX721-A supports interface backup based on interface or interface+VLAN. Choose one from Step 3 and Step 4. By configuring optional parameters of the command, you can switch services of the specified VLAN or all services on the interface when faults occur based on interface backup.

No.	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-port)#**port backup** *interface-type interface-number* [**vlanlist** *vlanlist* **primaryvlan** *vlanid* [**md-level** *level-value*]] Raisecom(config-port)#**exit**	(Optional) create a backup interface based on interface for the primary interface. Interface-based interface backup supports switching or restoring services of the specified VLAN or all services on the interface.
4	Raisecom(config-port)#**port backup** *interface-type interface-number* **vlanlist** *vlanlist* **separate**	(Optional) create a backup interface based on interface+VLAN for the primary interface.
5	Raisecom(config-port)#**port backup restore-mode** { **non-revertive** | **revertive** [**restore-delay** *delay-time*] }	Configure the restoration mode and restoration delay of interface backup.
6	Raisecom(config-port)#**port backup fault-detect cfm**	Configure the fault detection mode of interface backup.
7	Raisecom(config-port)#**port backup** *interface-type interface-number* **force-switch** [**vlan** *vlan-id*]	(Optional) forcedly switch services to the backup link.

13.2.3 Checking configurations

No.	Item	Description
1	Raisecom#**show port backup**	Show basic information about interface backup.
2	Raisecom#**show port backup pb**	Show information about the interface backup group.

No.	Item	Description
3	Raisecom#**show port backup group**	Show interface status of the interface backup group.

13.3 Configuring ELPS

13.3.1 Preparing for configurations

Scenario

To make the Ethernet reliability up to Telecom-grade (network self-heal time less than 50ms), you can deploy ELPS at Ethernet. ELPS is used to protect the Ethernet connection. It is an end-to-end protection technology.

ELPS supports 1+1 and 1:1 protection switching modes. It is divided into unidirectional protection switching and bidirectional protection switching based on the fact that whether services of both ends are switched concurrently when the link fails. Unidirectional and bidirectional protection switching are available in 1+1 protection switching mode only. 1:1 protection switching mode supports bidirectional protection switching only.

ELPS provides 3 modes to detect a fault.

- Detect faults based on physical interface status: learning link fault quickly and switching services immediately, suitable for detecting the fault between neighbor devices.
- Detect faults based on CC: suitable for unidirectional detection or multi-device crossing detection.
- Detect faults based on physical interface status and CC.

Prerequisite

- Connect interfaces and configure physical parameters for them. Make the physical layer Up.
- Create a VLAN.
- Add the interface to the VLAN.
- Configure CFM detection and form a neighbor relationship (preparing for CC mode).

13.3.2 Creating protection pair

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

Step	Command	Description
2	Raisecom(config)#**ethernet line-protection** *line-number* **working** *interface-type interface-number vlan-list* **protection** *interface-type interface-number vlan-list* **one-to-one** [**non-revertive**] **protocol-vlan** *vlan-id*	Create the ELPS protection pair and configure the protection mode. The protection group is in non-revertive mode if you configure the **non-revertive** parameter. • In revertive mode, when the working line recovers from a fault, traffic is switched from the protection line to the working line. • In non-revertive mode, when the working line recovers from a fault, traffic is not switched from the protection line to the working line. By default, there is no ELPS protection pair.
3	Raisecom(config)#**ethernet line-protection** *line-number* **name** *string*	(Optional) configure a name for the ELPS protection pair. By default, there is no name for the ELPS protection pair.
4	Raisecom(config)#**ethernet line-protection** *line-number* **wtr-timer** *wtr-timer*	(Optional) configure the WTR timer. In revertive mode, when the working line recovers from a fault, traffic is not switched to the working line unless the WTR timer times out. By default the WTR timer value is 5min. **Note** We recommend that WTR timer configurations on both ends keep consistent. Otherwise, we cannot ensure 50ms quick switching.
5	Raisecom(config)#**ethernet line-protection** *line-number* **hold-off-timer** *hold-off-timer*	(Optional) configure the Holdoff timer. After the Holdoff timer is configured, when the working line fails, the system will delay to process the fault. It means that services will be delayed to be switched to the protection line. This can prevent frequent switching caused by flapping of the working line. By default, the Holdoff timer value is 0. **Note** If the Holdoff timer value is over great, it may influence 50ms switching performance. Therefore, we recommend configuring the Holdoff timer value to 0.

13.3.3 Configuring ELPS fault detection modes

Note

Fault detection modes of the working line and protection line can be different. However, we recommend that fault detection mode configurations of the working line and protection line keep consistent.

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

Step	Command	Description
2	Raisecom(config)#**ethernet line-protection** *line-number* { **working** | **protection** } **failure-detect physical-link**	Configure the fault detection mode of the working line/protection line to failure-detect physical-link. By default, the fault detection mode is failure-detect physical-link.
	Raisecom(config)#**ethernet line-protection** *line-number* { **working** | **protection** } **failure-detect cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	Configure the fault detection mode of the working line/protection line to failure-detect cc. This fault detection mode cannot take effect unless you finish related configurations on CFM.
	Raisecom(config)#**ethernet line-protection** *line-number* { **working** | **protection** } **failure-detect physical-link-or-cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	Configure the fault detection mode of the working line/protection line to failure-detect physical-link-or-cc. In this mode, it believes that the link fails when a fault is detected on the physical link/CC. This fault detection mode cannot take effect unless you finish related configurations on CFM.

13.3.4 (Optional) configuring ELPS switching control

Note

By default, traffic is automatically switched to the protection line when the working line fails. Therefore, you need to configure ELPS switching control in some special cases.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet line-protection** *line-number* **lockout**	Lock protection switching. After this configuration, the traffic is not switched to the protection line even the working line fails. By default, the traffic is automatically switched to the protection line when the working line fails.
3	Raisecom(config)#**ethernet line-protection** *line-number* **force-switch**	Switch the traffic from the working line to the protection line forcedly. By default, the traffic is automatically switched to the protection line when the working line fails.
4	Raisecom(config)#**ethernet line-protection** *line-number* **manual-switch**	Switch the traffic from the working line to the protection line manually. Its priority is lower than the one of forced switch and APS. By default, the traffic is automatically switched to the protection line when the working line fails.

Step	Command	Description
5	Raisecom(config)#**ethernet line-protection** *line-number* **manual-switch-to-work**	In non-revertive mode, switch the traffic from the protection line to the working line. **Note** After you execute a protection group command, if a fault/recovery event occurs or if other protection group commands, both ends of the protection group may select different lines. In this case, you should use the **clear ethernet line-protection end-to-end** command to delete the configured protection group command to make both ends of the protection group select the identical line.

13.3.5 Checking configurations

No.	Command	Description
1	Raisecom(config)#**show ethernet line-protection** [*line-number*]	Show configurations of the protection pair.
2	Raisecom(config)#**show ethernet line-protection** [*line-number*] **statistics**	Show statistics of the protection pair.
3	Raisecom(config)#**show ethernet line-protection** [*line-number*] **aps**	Show APS information about the protection pair.

13.4 Configuring ERPS

13.4.1 Preparing for configurations

Scenario

With development of Ethernet to Telecom-grade network, voice and video multicast services bring higher requirements on Ethernet redundant protection and fault-recovery time. The fault-recovery time of current STP system is in second level that cannot meet requirements.

By defining different roles for nodes on a ring, ERPS can block a loopback to avoid broadcast storm in normal condition. Therefore, the traffic can be quickly switched to the protection line when working lines or nodes on the ring fail. This helps eliminate the loopback, perform protection switching, and automatically recover from faults. In addition, the switching time is shorter than 50ms.

The RAX721-A supports the single ring, intersecting ring, and tangent ring.

ERPS provides 2 modes to detect a fault:

- Detect faults based on physical interface status: learning link fault quickly and switching services immediately, suitable for detecting the fault between neighbor devices.
- Detect faults based on CFM: suitable for unidirectional detection or multi-device crossing detection.

- Detect faults based on physical interface and CFM.

Prerequisite

- Connect interfaces and configure physical parameters for them. Make the physical layer Up.
- Create a VLAN.
- Add the interface to the VLAN.
- Create the management VLAN and VLANs of the working and protection interfaces.
- Configure CFM detection between devices and form a neighbor relationship (preparing for CFM detection mode).

13.4.2 Creating ERPS protection ring

Caution

- Only one device on the protection ring can be set to the Ring Protection Link (RPL) Owner and one device is configured to RPL Neighbor. Other devices are set to ring forwarding nodes.
- In actual, the tangent ring consists of 2 independent single rings. Configurations on the tangent ring are identical to the ones on the common single ring. The intersecting ring consists of a main ring and a tributary ring. Configurations on the main ring are identical to the ones on the common single ring.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ethernet ring-protection` *ring-number* `east` *interface-type interface-number* `west` *interface-type interface-number* `node-type rpl-owner rpl { east | west } [ not-revertive ] [ protocol-vlan` *vlan-id* `] [ block-vlanlist` *vlan-list* `]`	Create a protection ring and set the node to the RPL Owner. By default, the protocol VLAN is VLAN 1 and blocked VLANs are VLANs 1–4094. If you configure the not-revertive mode, the protection ring is in non-revertive mode. In revertive mode, the traffic is switched from the protection line back to the working line when the working line recovers from a fault. However, in non-revertive mode, the traffic is not switched. By default, the protection ring is in revertive mode. **Note** The east and west interfaces cannot be the same one.
	`Raisecom(config)#ethernet ring-protection` *ring-number* `east` *interface-type interface-number* `west` *interface-type interface-number* `node-type rpl-neighbour rpl { east | west } [ not-revertive ] [ protocol-vlan` *vlan-id* `] [ block-vlanlist` *vlan-list* `]`	Create a protection ring and set the node to the RPL Neighbour. By default, the protocol VLAN is VLAN 1 and blocked VLANs are VLANs 1–4094.

Step	Command	Description
	Raisecom(config)#**ethernet ring-protection** *ring-number* **east** *interface-type interface-number* **west** *interface-type interface-number* [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create a protection line and set the node to the RPL forwarding node. By default, the protocol VLAN is VLAN 1 and blocked VLANs are VLANs 1–4094.
3	Raisecom(config)#**ethernet ring-protection** *ring-number* **name** *string*	(Optional) configure a name for the protection ring.
4	Raisecom(config)#**ethernet ring-protection** *ring-number* **version** { **1** | **2** }	(Optional) configure the protocol version. Protocol versions of all nodes on a ring should be consistent. Version 1 distinguishes rings through the protocol VLAN. Therefore, you should configure different protocol VLANs for these rings. We recommend configuring different protocol VLANs for these rings, even you use version 2. By default, version 2 is used.
5	Raisecom(config)#**ethernet ring-protection** *ring-number* **guard-time** *guard-time*	(Optional) after the ring Guard timer is configured, the failed node does not process APS packets during a period. In a larger ring network, after the failed node is recovered, the node may be in down status again because it receives fault notifications sent by neighbor nodes. The ring Guard timer can resolve this problem. By default, the ring Guard timer is 200ms.
6	Raisecom(config)#**ethernet ring-protection** *ring-number* **wtr-time** *wtr-time*	(Optional) configure the ring WTR timer. In revertive mode, when the working line recovers from a fault, traffic is not switched to the working line unless the WTR timer times out. By default, the ring WTR time value is 5min.
7	Raisecom(config)#**ethernet ring-protection** *ring-number* **holdoff-time** *holdoff-time*	(Optional) configure the Holdoff timer. After the Holdoff timer is configured, when the working line fails, the system will delay to report the fault. It means that services will be delayed to be switched to the protection line. This can prevent frequent switching caused by flapping of the working line. By default, the Holdoff timer value is 100ms. **Note** If the Holdoff timer value is over great, it may influence 50ms switching performance. Therefore, we recommend configuring the Holdoff timer value to 0ms.

13.4.3 (Optional) creating ERPS protection tributary ring

Caution

- Only the intersecting ring consists of a main ring and a tributary ring. The main ring is a complete ring and all its nodes should be configured with double interfaces. The sub-interface is an incomplete ring and you must configure the single interface on the intersecting node.
- Configurations on the main ring are identical to the ones on the single ring/tangent ring.
- Configurations of non-intersecting nodes of the intersecting ring are identical to the ones on the single ring/tangent ring.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet ring-protection** *ring-number* **east** *interface-type interface-number* **west** *interface-type interface-number* **node-type rpl-owner rpl** { **east** | **west** } [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create the tributary ring on the intersecting node and set the intersecting node to the RPL Owner. If you configure the not-revertive mode, the protection ring is in non-revertive mode. In revertive mode, the traffic is switched from the protection line back to the working line when the working line recovers from a fault. However, in non-revertive mode, the traffic is not switched. By default, the protection ring is in revertive mode. **Note** The links between 2 intersecting nodes belong to the main ring. Therefore, when you configure the tributary ring on the intersecting node, you can only configure the west or east interface. By default, the protocol VLAN is VLAN 1 and blocked VLANs are VLANs 1–4094.
	Raisecom(config)#**ethernet ring-protection** *ring-number* **east** *interface-type interface-number* **west** *interface-type interface-number* **node-type rpl-neighbour rpl** { **east** | **west** } [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create the tributary ring on the intersecting node and set the intersecting node to the RPL Neighbour. By default, the protocol VLAN is VLAN 1 and blocked VLANs are VLANs 1–4094.
	Raisecom(config)#**ethernet ring-protection** *ring-number* **east** *interface-type interface-number* **west** *interface-type interface-number* [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create the tributary ring on the intersecting node and set the intersecting node to the RPL forwarding node. By default, the protocol VLAN is VLAN 1 and blocked VLANs are VLANs 1–4094.

Step	Command	Description
3	Raisecom(config)#**ethernet ring-protection** *ring-number* **raps-vc** { **with** | **without** }	(Optional) configure the tributary ring virtual channel mode on the intersecting node. Because the link between intersecting nodes belong to the main ring, the transmission mode of protocol packets of the tributary ring is different from the one of the main ring. It is divided into with and without modes. By default, the tributary ring virtual channel adopts the with mode. Transmission modes on 2 intersecting nodes must be identical.
4	Raisecom(config)#**ethernet ring-protection** *ring-number* **propagate enable**	Enable the ring Propagate switch on the intersecting node. Because data of the tributary ring need to be forwarded through the main ring, there is the MAC address table of the tributary ring on the main ring. When the topology of the tributary ring changes, the tributary ring should use the Propagate switch to inform the main ring to refresh the MAC address table to avoid traffic loss. By default, the ring Propagate switch is disabled. We recommend enabling ring Propagate switch.

13.4.4 Configuring ERPS fault detection modes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet ring-protection** *ring-number* { **east** | **west** } **failure-detect physical-link**	Configure the ERPS fault detection mode to failure-detect physical-link. By default, the ERPS fault detection mode is failure-detect physical-link.
	Raisecom(config)#**ethernet ring-protection** *ring-number* { **east** | **west** } **failure-detect cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	Configure the ERPS fault detection mode to failure-detect cc. This ERPL fault detection mode cannot take effect unless you finish related configurations on CFM. If you configure the MD, the MA should be below the configured md-level.
	Raisecom(config)#**ethernet ring-protection** *ring-number* { **east**| **west** } **failure-detect physical-link-or-cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	Configure the ERPS fault detection mode to failure-detect physical-link-or-cc. In this mode, it believes that the link fails when a fault is detected on the physical link/CC. This ERPL fault detection mode cannot take effect unless you finish related configurations on CFM. If you configure the MD, the MA should be below the configured md-level.

13.4.5 (Optional) configuring ERPS switching control

By default, traffic is automatically switched to the protection line when the working line fails. Therefore, you need to configure ERPS switching control in some special cases.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet ring-protection** *ring-number* **force-switch** { **east** | **west** }	Switch the traffic on the protection ring to the west/east interface forcedly.
3	Raisecom(config)#**ethernet ring-protection** *ring-number* **manual-switch** { **east** | **west** }	Switch the traffic on the protection ring to the west/east interface manually. Its priority is lower than the one of forced switch and APS.

13.4.6 Checking configurations

No.	Command	Description
1	Raisecom(config)#**show ethernet ring-protection**	Show ERPS protection ring configurations.
2	Raisecom(config)#**show ethernet ring-protection status**	Show ERPS protection ring status.
3	Raisecom(config)#**show ethernet ring-protection statistics**	Show ERPS protection ring statistics.

13.5 Configuring VRRP

13.5.1 Preparing for configurations

Scenario

In general, we configure a default route to the breakout gateway for all devices in a LAN. Therefore, these devices can communicate with the external network. If the gateway fails, devices in the LAN fail to communicate with the external network.

The VRRP technology combines multiple routers to form a backup group. By configuring a virtual IP address for the backup group, you can set the default gateway to the virtual IP address of the backup group to make devices in the LAN communicate with the external network.

VRRP helps improve network reliability. It facilitates avoiding network interruption caused by failure of s single link and prevents changing routing configurations because of link failure.

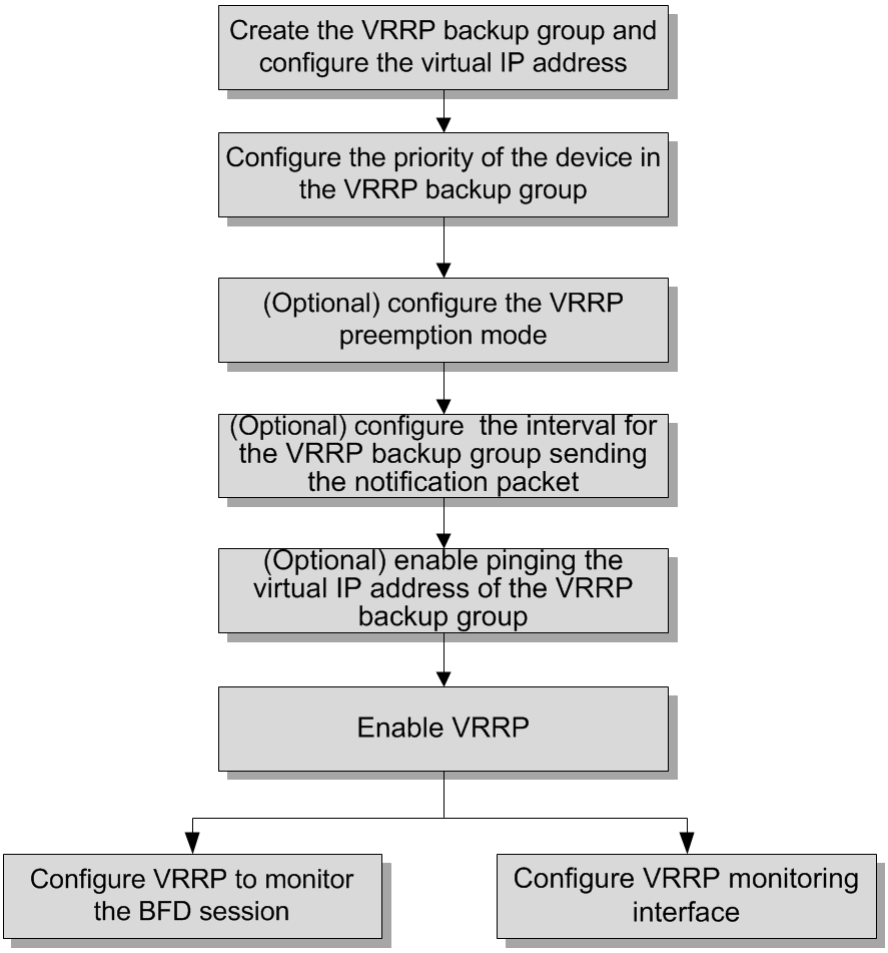
Prerequisite

The interface is in Layer 3 router mode and the IP address is configured.

13.5.2 Configuration procedure

Figure 13-1 shows the VRRP configuration procedure.

Figure 13-1 VRRP configuration procedure



13.5.3 Configuring VRRP backup group

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface` *interface-type interface-number*	Enter interface configuration mode.
3	`Raisecom(config-port)#vrrp` *group-id* `ip` *ip-address*	Create a VRRP backup group and configure a virtual IP address for the VRRP backup group. The virtual IP address must be at the same network segment with the interface IP address.
4	`Raisecom(config-port)#vrrp` *group-id* `description` *description*	(Optional) configure descriptions of the VRRP backup group.

Step	Command	Description
5	Raisecom(config-port)#**vrrp** *group-id* **preempt** [**delay-time** *second*]	(Optional) enable the preemption mode of the VRRP backup group. By default, the newly-created VRRP backup group is in preemption mode. The preemption delay is 0s.
6	Raisecom(config-port)#**vrrp** *group-id* **priority** *priority*	Configure the priority of the device in the VRRP backup group. By default, the priority of the newly-created VRRP backup group is 100.
7	Raisecom(config-port)#**vrrp** *group-id* **timers advertise-interval** *seconds*	(Optional) configure the interval for the VRRP backup group sending the notification packet. By default, it is 1s.
8	Raisecom(config-port)#**vrrp** *group-id* **enable**	Enable VRRP. By default, it is enabled.

13.5.4 Configuring VRRPv3 backup group

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**no portswitch**	Enter interface configuration mode.
3	Raisecom(config-port)#**vrrp6** *group-id* **ipv6** *ipv6-address*	Create a VRRPv3 backup group and configure the virtual IPv6 address for it. One VRRPv3 backup group can be configured with only 1 virtual IPv6 local link address and 15 virtual IPv6 global unicast address.
4	Raisecom(config-port)#**vrrp6** *group-id* **description** *description*	(Optional) configure the description of the VRRPv3 backup group.
5	Raisecom(config-port)#**vrrp6** *group-id* **preempt** [**delay-time** *second*]	(Optional) enable VRRPv3 backup group preemption mode. By default, the newly created VRRPv3 backup group is in preemption mode, and the preemption delay is 0s.
6	Raisecom(config-port)#**vrrp6** *group-id* **priority** *priority*	Configure the priority of the device in the VRRPv3 backup group. By default, the priority of a newly created VRRPv3 backup group is 100.
7	Raisecom(config-port)#**vrrp6** *group-id* **timers advertise-interval** *second*	(Optional) configure the interval for VRRPv3 backup groups to send advertisement packets. By default, the interval for sending advertisement packets is 1 second.

Step	Command	Description
8	Raisecom(config-port)#**vrrp6** *group-id* **enable**	Enable VRRPv3. By default, VRRPv3 of the newly created backup group is enabled.

13.5.5 (Optional) configuring ping function of VRRP virtual IP address

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**vrrp ping**	Ping the virtual IP address of the VRRP backup group. By default, pinging the virtual IP address of the newly-created VRRP backup group is enabled.

13.5.6 Configuring VRRP/VRRPv3 monitoring interface

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**no portswitch**	Enter interface configuration mode.
3	Raisecom(config-port)#**vrrp** *group-id* **track** *interface-type interface-number* [**reduce** *priority*]	Configure VRRP monitoring interface.
4	Raisecom(config-port)#**vrrp6** *group-id* **track** *interface-type interface-number* [**reduce** *priority*]	Configure the VRRPv3 monitor interface.

13.5.7 Configuring VRRP/VRRPv3 fast switching

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**no portswitch**	Enter interface configuration mode.
3	Raisecom(config-port)#**vrrp** *group-id* **track bfd-session** *session-id* [**increased** *priority* | **reduce** *priority*]	Configure the VRRP backup group to monitor the BFD session to realize fast switching.
4	Raisecom(config-port)#**vrrp6** *group-id* **track bfd-session** *session-id* [**increased** *priority* | **reduce** *priority*]	Configure the VRRPv3 backup group to monitor the BFD session to realize fast switching.

13.5.8 Checking configurations

No.	Command	Description
1	Raisecom#**show vrrp** *group-id*	Show VRRP backup group configurations.
2	Raisecom#**show vrrp interface** *interface-type interface-number* [*group-id*]	Show VRRP backup group configurations on the interface.
3	Raisecom#**show vrrp interface** *interface-type interface-number* [*group-id*] **statistics**	Show VRRP backup group statistics on the interface.
4	Raisecom#**show vrrp** [*group-id*] **track**	Show monitoring information about the VRRP backup group.

13.6 Configuring link-state tracking

13.6.1 Preparing for configurations

Scenario

When the uplink of the intermediate device fails, if the lower-layer device cannot be notified in time, the traffic cannot be switched to the backup path, resulting in traffic interruption.

The main function of link-state tracking is to perform pre-configured fault handling actions when the fault source fails, so that the fault of the upper layer device is quickly delivered to the lower layer devices, thereby triggering the active-standby switchover.

Prerequisite

Before configuring link-state tracking, you need to connect the interface and configure the physical parameters of the interface to make the interface Up.

13.6.2 Creating a link-state group

Creating interface-based link-state group

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**link-state-tracking group** *group-number*	Create a link-state group and configure link-state tracking.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.

Step	Command	Description
4	Raisecom(config-port)#**link-state-tracking group** *group-number* { **downstream** | **upstream** }	Configure the link-state group of the interface and the interface type. One interface only belongs to one link-state group and can only be configured to an uplink interface or a downlink interface.

- There can be multiple upstream interfaces in one link-state group. As long as one upstream interface is Up, no link-state tracking will occur. Link-state tracking will occur only when all upstream interfaces are Down.
- In global mode, when you use the **no link-state-tracking group** *group-number* command to disable link-state tracking, the link-state group will be deleted.
- In physical layer interface mode, you can use the **no link-state-tracking group** command to delete an interface from the link-state group. If you delete an interface and there are no other interfaces under the link-state group and the link-state group is not enabled, deleting the interface will also delete the link-state group.

Creating link-state group based on remote MEP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**link-state-tracking group** *group-number* **upstream ma-name** *name* **cfm-mepid** *mep-id* **level** *level-id*	Create a link-state group based on remote MEP and enable link-state tracking.

Creating link-state group based on ELPS

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**link-state-tracking group** *group-number* **upstream elps-8031-link** *value*	Create an ELPS-based link-state group and enable link-state tracking.

When creating an ELPS-based link-state group, if you configure the next action to shutting down interface list, you need to ensure that these interfaces are not the interfaces associated with ELPS protection.

Creating link-state group based on mLACP group

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**link-state-tracking group** *group-number* **upstream mlacp** *mlacp-id*	Create a link-state group based on link aggregation and enable link-state tracking.

13.6.3 Configuring fault processing action of link-state group

Interface fault processing mode

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**link-state-tracking group** *group-number* **action** { **blockvlanlist** *vlan-list* | **modify-pvid** *vlan-id* }	Configure the fault processing mode on the link-state interface.

Global fault processing mode

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**link-state-tracking group** *group-number* **action** { **delete-vlan** *vlan-id* | **flush-erps** *rind-id* }	Configure link-state tracking global fault processing mode.

13.6.4 Checking configurations

Step	Command	Description
1	Raisecom#**show link-state-tracking group** [*group-number*]	Show configurations and status of the link-state group.

13.7 Maintenance

Command	Description
Raisecom(config)#**clear lacp statistics** [*interface-type interface-number*]	Clear LACP statistics.
Raisecom(config)#**clear mlacp mlacp-group** [*icg-id*] **statistics**	Clear statistics of received and transmitted packets of the chassis group.
Raisecom(config)#**clear ethernet line-protection statistics**	Clear statistics of the protection group.
Raisecom(config)#**clear ethernet line-protection** *aps-id* **end-to-end command**	Clear end-to-end switching control commands.
Raisecom(config)#**clear ethernet ring-protection** *ring-number* **statistics**	Clear statistics of the protection ring, including the number of transmitted APS packets, the number of received APS packets, the last switching time, and the fault detection mode.
Raisecom(config)#**clear ethernet ring-protection** *ring-number* **command**	Clear switching control commands of the protection ring, including the **force-switch** and **manual-switch** commands.
Raisecom(config)#**clear iccp channel** [*channel-id*] **statistics**	Clear statistics of ICC received and transmitted packets.
Raisecom(config)#**clear vrrp statistics**	Clear packet statistics of all VRRP backup groups.

14 Appendix

This chapter lists terms, acronyms, and abbreviations involved in this document, including the following sections:

- Terms
- Acronyms and abbreviations

14.1 Terms

A

Access Control List (ACL)	A series of ordered rules composed of permit | deny sentences. These rules are based on source MAC address, destination MAC address, source IP address, destination IP address, interface ID, etc. The device decides to receive or refuse the packets based on these rules.

C

Connectivity Fault Management (CFM)	A standard defined by IEEE. It defines protocols and practices for OAM (Operations, Administration, and Maintenance) for paths through 802.1 bridges and local area networks (LANs). Used to diagnose fault for EVC (Ethernet Virtual Connection). Cost-effective by fault management function and improve Ethernet maintenance.

E

Encapsulation	A technology used by the layered protocol. When the lower protocol receives packets from the upper layer, it will map packets to the data of the lower protocol. The outer layer of the data is encapsulated with the lower layer overhead to form a lower protocol packet structure. For example, an IP packet from the IP protocol is mapped to the data of 802.1Q protocol. The outer layer is encapsulated by the 802.1Q frame header to form a VLAN frame structure.

A

Ethernet in the First Mile (EFM)	Complying with IEEE 802.3ah protocol, EFM is a link-level Ethernet OAM technology. It provides the link connectivity detection, link fault monitoring, and remote fault notification, etc. for a link between two directly-connected devices. EFM is mainly used for the Ethernet link on edges of the network accessed by users.

L

Link Aggregation	A computer networking term which describes using multiple network cables/ports in parallel to increase the link speed beyond the limits of any one single cable or port, and to increase the redundancy for higher availability.

P

Packet	In data communication field, packet is the data unit for switching and transmitting information. In transmission, it will be continuously encapsulated and decapsulated. The header is used to define the destination address and source address. The trailer contains information indicating the end of the packet. The payload data in between is the actual packet.
Packet switching	In packet switching network, data is partitioned into multiple data segments. The data segment is encapsulated by control information, such as, destination address, to form the switching packet. The switching packet is transmitted to the destination in the way of storage-forwarding on the network. Packet switching is developed based on storage-forwarding method and has merits of both circuit switching and packet switching.

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.

V

Virtual Local Area Network (VLAN)	VLAN is a protocol proposed to solve broadcast and security issues for Ethernet. It divides devices in a LAN into different segments logically rather than physically, thus implementing multiple virtual work groups which are based on Layer 2 isolation and do not affect each other.

A

VLAN mapping	VLAN mapping is mainly used to replace the private VLAN Tag of the Ethernet service packet with the ISP's VLAN Tag, making the packet transmitted according to ISP's VLAN forwarding rules. When the packet is sent to the peer private network from the ISP network, the VLAN Tag is restored to the original private VLAN Tag according to the same VLAN forwarding rules. Thus, the packet is sent to the destination correctly.

14.2 Acronyms and abbreviations

A

ACL	Access Control List
APS	Automatic Protection Switching

C

CE	Customer Edge
CFM	Connectivity Fault Management
CoS	Class of Service

D

DHD	Dual Home Device
DSCP	Differentiated Services Code Point

E

EFM	Ethernet in the First Mile

F

FTP	File Transfer Protocol

G

GPS	Global Positioning System
GSM	Global System for Mobile Communications

H

HA	High Availability

I

ICCP	Inter-Chassis Communication Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector

L

LACP	Link Aggregation Control Protocol
LBM	LoopBack Message
LBR	LoopBack Reply
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
LTM	LinkTrace Message
LTR	LinkTrace Reply

M

MA	Maintenance Association
MAC	Medium Access Control
MD	Maintenance Domain
MEG	Maintenance Entity Group
MEP	Maintenance associations End Point
MIB	Management Information Base
MIP	Maintenance association Intermediate Point
MTU	Maximum Transmission Unit

N

NTP	Network Time Protocol

O

OAM	Operation, Administration and Maintenance

P

PDU	Protocol Data Unit
PE	Provider Edge
PSN	Packet Switched Network
PTN	Packet Transport Network
PW	Pseudo Wire
PWE3	Pseudo Wire Emulation Edge-to-Edge

Q

QoS	Quality of Service

R

RMEP	Remote Maintenance association End Point
RMON	Remote Network Monitoring

S

SAToP	Structure-Agnostic TDM over Packet
SFP	Small Form-factor Pluggables
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict-Priority
SSH	Secure Shell

T

TCI	Tag Control Information
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLV	Type Length Value
ToS	Type of Service
TPID	Tag Protocol Identifier

V

VPN	Virtual Private Network
VLAN	Virtual Local Area Network

W

WRR	Weight Round Robin

瑞斯康达科技发展股份有限公司
RAISECOM TECHNOLOGY CO.,LTD.

Address: Raisecom Building, No. 11, East Area, No. 10 Block, East Xibeiwang Road, Haidian District, Beijing, P.R.China Postal code: 100094 Tel: +86-10-82883305
Fax: 8610-82883056 http://www.raisecom.com Email: export@raisecom.com