www.raisecom.com

RAX711-L (A)
Configuration Guide
(Rel_04)

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

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied.

Preface

Objectives

This document describes features and related configurations supported by the RAX711-L, including basic principles and configuration procedures of Ethernet, clock synchronization, network reliability, DHCP Client, OAM, security, QoS, and system management and maintenance. In addition, this document provides related configuration examples. The appendix lists terms, acronyms, and abbreviations involved in this document.

This document helps you master principles and configurations of the RAX711-L systematically, as well as networking with the RAX711-L.

Versions

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

Product name	Product version	Hardware version
RAX711-L-4GC4E1-S	P200R001	A.00 or later
RAX711-L-4GC4E1-BL-S	P200R001	A.00 or later
RAX711-L-4GC	P200R001	A.00 or later
RAX711-L-4GE	P200R001	A.00 or later

Conventions

Symbol conventions

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

Symbol	Description
	Indicate a hazard with a medium or low level of risk which, if not avoided, could result in minor or moderate injury.

Symbol	Description
Caution	Indicate a potentially hazardous situation that, if not avoided, could cause equipment damage, data loss, and performance degradation, or unexpected results.
Note	Provide additional information to emphasize or supplement important points of the main text.
Tip	Indicate a tip that may help you solve a problem or save time.

General conventions

Convention	Description
Times New Roman	Normal paragraphs are in Times New Roman.
Arial	Paragraphs in Warning, Caution, Notes, and Tip are in Arial.
Boldface	Buttons and navigation path are in **Boldface**.
Italic	Book titles are in *italics*.
`Lucida Console`	Terminal display is in `Lucida Console`.
Book Antiqua	Heading 1, Heading 2, Heading 3, and Block are in Book Antiqua.

Command conventions

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

Change history

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

Issue 04 (2016-02-29)

Fourth commercial release

- Supported creating the SLA TWAMP test operation.
- Supported the PTP clock.
- Supported viewing PW configurations in the form of VLAN list.
- Supported viewing operating information about the interface.

Issue 03 (2015-07-31)

Third commercial release

- Supported IPv6 address.
- Supported configuring the restart time of the RAX711-L.
- Supported the Web network management.
- Supported NDP.
- Supported STP.
- Supported global loopback detection by default.
- Supported fault source as MC-LAG and ELPS of the failover.
- Supported configuring PHY interface management and support MAC address drifting.
- Supported ALS.
- Supported multicast.
- Supported configuring ARP detection times and displaying dynamic ARP.
- Supported uploading and downloading configuration files through SFTP.
- Supported adding configuration files.
- Supported enabling/disabling failover.
- Supported configuring MEP priority.
- Added enhanced capacity of the Loopback.
- Added enhanced capacity of the QoS.
- Added enhanced capacity of the Y.1564.

Issue 02 (2015-02-16)

Second commercial release

- Added the ACL classification rules configured based on Layer 2 and Layer 3.
- Added the feature of querying the MAC address of the peer through EFM OAM in passive mode.
- Fixed known bugs.

Issue 01 (2014-07-31)

Initial commercial release

Contents

Figures

1 Basic configurations

This chapter describes basic information and configuration procedures of the RAX711-L, as well as related configuration examples, including following sections:

- CLI
- Accessing device
- Web network management
- Zero-configuration on the remote devices
- Configuring IP address of device
- Configuring time management
- Configuring static route
- NDP
- Configuring Ethernet interface
- Configuring SNMP
- Configuring Banner
- Configuration examples

1.1 CLI

1.1.1 Overview

The Command Line Interface (CLI) is a medium for you communicating with the RAX711-L. You can configure, monitor, and manage the RAX711-L through the CLI.

You can log in to the RAX711-L through the terminal device or through a computer that runs the terminal emulation program. Enter commands at the system prompt.

The CLI supports following features:

- Configure the RAX711-L locally through the Console interface.
- Configure the RAX711-L 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 RAX711-L.
- Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.
- The RAX711-L supports multiple intelligent analysis methods, such as fuzzy match and context association.

1.1.2 Levels

The RAX711-L classifies CLI into 15 levels in a descending order:

- 1–4: checking level. You can execute basic commands, such as **ping**, **clear**, and **history**, to perform network diagnostic function, clear system information and show command history.
- 5–10: monitoring level. You can execute these commands, such as **show**, for system maintenance.
- 11–14: configuration level. You can execute these commands for configuring services, such as Virtual Local Area Network (VLAN) and Internet Protocol (IP) route.
- 15: management level. You can execute these commands for running systems.

1.1.3 Modes

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 RAX711-L, enter the user name and password to enter the user EXEC mode, where the following command is displayed:

```
Raisecom>
```

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

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

Command modes supported by the RAX711-L are listed in the following table.

Mode	Access mode	Prompt
User EXEC	Log in to the RAX711-L, and then enter the correct user name and password.	`Raisecom>`
Privileged EXEC	In user EXEC mode, enter the **enable** command and correct password.	`Raisecom#`
Global configuration	In privileged EXEC mode, enter the **config** command.	`Raisecom(config)#`
Physical layer interface configuration	In global configuration mode, enter the **interface** *interface-type interface-number* command.	`Raisecom(config-port)#`
TDM interface configuration	In global configuration mode, enter the **interface tdm** *interface-number* command.	`Raisecom(config-tdm-port)#`
PW configuration	In global configuration mode, enter the **cespw** *pw-name* command.	`Raisecom(config-cespw)#`
Layer 3 interface configuration	In global configuration mode, enter the **interface ip** *if-number* command.	`Raisecom(config-ip)#`
VLAN configuration	In global configuration mode, enter the **vlan** *vlan-id* command.	`Raisecom(config-vlan)#`
Service instance configuration	In global configuration mode, enter the **service** *cis-id* **level** *ma-level* command.	`Raisecom(config-service)#`
Traffic classification configuration	In global configuration mode, enter the **class-map** *class-map-name* command.	`Raisecom(config-cmap)#`
Traffic policy configuration	In global configuration mode, enter the **policy-map** *policy-map-name* command.	`Raisecom(config-pmap)#`

Mode	Access mode	Prompt
Traffic policy bound with traffic classification configuration	In traffic policy configuration mode, enter the **class-map** *class-map-name* command.	`Raisecom(config-pmap-c)#`
CoS-to-Pri configuration	In global configuration mode, enter the **mls qos mapping cos-to-local-priority** *profile-id* command.	`Raisecom(cos-to-pri)#`
DSCP-to-Pri configuration	In global configuration mode, enter the **mls qos mapping dscp-to-local-priority** *profile-id* command.	`Raisecom(dscp-to-pri)#`
ACL configuration	In global configuration mode, enter the **access-list-map** *acl-number* { **deny** | **permit** } command.	`Raisecom(config-aclmap)#`
Aggregation group configuration	In global configuration mode, enter the **interface port-channel** *port-channel-number* command.	`Raisecom(config-aggregator)#`
Clock configuration	In global configuration mode, enter the **clock-mgmt slot** *slot-number* command.	`Raisecom(config-clock)#`
MST domin configuration	In global configuration mode, enter the **spanning-tree region-configuration** command**.**	`Raisecom(config-region)#`
RSOM configuration	In privileged EXEC mode, enter the **mefservice** command.	`Raisecom(mefservice)#`
RSOM bandwidth profiles group configuration	In RSOM configuration mode, enter **bandwidth-profile** *bandwidth-profile-id* command.	`Raisecom(mefservice-bwpprofile)#`
RSOM UNI configuration	In RSOM UNI configuration mode, enter the **interface** *interface-type interface-number* command.	`Raisecom(mefservice-interface)#`
RSOM EVC configuration	In RSOM EVC configuration mode, enter the **service** *service-id* command.	`Raisecom(mefservice-evc)`
RSOM EVC-UNI configuration	In RSOM EVC-UNI configuration mode, enter the **sap** *interface-type interface-number* command.	`Raisecom(mefservice-evcuni)#`

Mode	Access mode	Prompt
RSOM bandwidth profile configuration	In RSOM bandwidth profile group configuration mode, enter the **bandwidth-item** *bandwidth-item-id* command.	`Raisecom(mefservice-bwpitem)#`
RSOM CoS profile configuration	In RSOM configuration mode, enter the **cos-profile** *cos-profile-id* command.	`Raisecom(mefservice-cosprofile)#`
RSOM threshold profile configuration	In RSOM configuration mode, enter the **performance-tier** *performance-tier-id* command.	`Raisecom(mefservice-thresholdprofile)#`
RSOM L2CP profiles group configuration	In RSOM L2CP profiles group configuration mode, enter the **l2cp-profile** *l2cp-profile-id* command.	`Raisecom(mefservice-l2cpprofile)#`
RSOM L2CP bandwidth profile configuration	In RSOM L2CP bandwidth profile configuration mode, enter the **l2cp-item** *l2cp-item-id* command.	`Raisecom(mefservice-l2cpitem)#`
RSOM traffic profile configuration	In RSOM configuration mode, enter the **flow profile** *flow-profile-id* command.	`Raisecom(mefservice-flowprofile)#`

1.1.4 Shortcut keys

The RAX711-L supports following shortcut keys.

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

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

1.1.5 Flitering commands

The RAX711-L provides a series of commands which begin with "**list**" to show configuration, running status, or diagnostic message of the device. You can add filtering rules to remove unwanted information.

The **list** command supports 3 filtering modes:

- | **begin** *string*: show all commands which start from matched specific character string.
- | **exclude** *string*: show all commands which do not match specific character string.
- | **include** *string*: show all commands which only match specific character string.

1.1.6 Viewing command history

The RAX711-L support viewing or executing a historical command through the **history** command in any command mode. By default, the last 20 historical commands are saved.

The RAX711-L can save a maximum of 20 historical commands through the **terminal history** command in user EXEC mode.

1.1.7 Acquiring help

Complete help

You can acquire complete help under following three conditions:

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

```
Raisecom>?
```

The output is displayed as follows:

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

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

```
Raisecom(config)#ntp?
```

The output is displayed as follows:

```
peer            Configure NTP peer
refclock-master Set local clock as reference clock
server          Configure NTP server
```

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

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

The output is displayed as follows:

```
{1-4}  Port number list
<1-4>  Port 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 follows:

```
cespw            cespw
cfm              Connectivity fault management protocol
class-map        Set class map
clear            Clear screen
clock-mgmt       Clock management
command-log      Log the command to the file
cpu              Configure cpu parameters
create           Create static VLAN
```

- 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 follows:

```
link-aggregation   Link aggregation
link-fault         link-fault
```

- 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.

Error message

The following table lists some error messages that you might encounter while using the CLI to configure the RAX711-L.

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

1.2 Accessing device

Note

When you first enable the RAX711-L, you need to access the device through the Console interface and then configure its IP address. You cannot access the RAX711-L through Telnet/SSHv2 unless you enable Telnet/SSHv2 service.

You can configure the RAX711-L through the CLI after accessing it through the following 3 modes:

- Accessing the RAX711-L through the Console Interface
- Accessing the RAX711-L through Telnet
- Accessing the RAX711-L through SSHv2

1.2.1 Accessing device through Console interface

Note

The Console interface of the RAX711-L is a Universal Serial Bus (USB) A female interface, which is translated into a Universal Asynchronous Receiver/Transmitter (UART) in the device.

The Console interface is used as an interface for the RAX711-L being connected to a PC that runs the terminal emulation program. You can configure and manage the RAX711-L through this interface. This management method does not involve network communication.

You must log in to the RAX711-L through the Console interface under the following 2 conditions:

- The RAX711-L is powered on for the first time.
- You cannot login through Telnet.

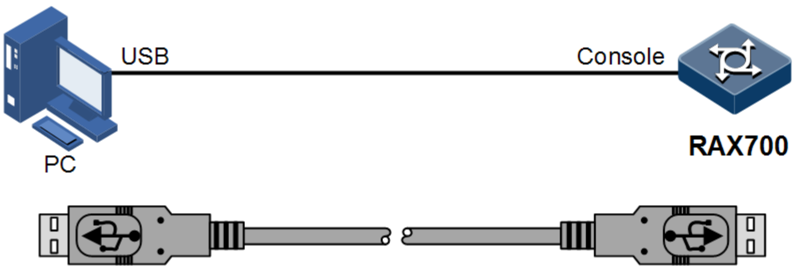
To log in to the RAX711-L through the Console interface, follow these steps:

Step 1 Download the USB_Console_Driver.zip file from http://www.raisecom.com/Drive/USB_Console_Driver.zip and then install it to the PC.

Step 2 Right-click My Computer and then choose **Manage** from the right-click menu. Choose **System Tools** > **Device Manager** > **Ports** to view whether the USB driver program is installed successfully. Then record the COM interface to be used, such as RAISECOM Gazelle USB to UART Bridge (COM1).

Step 3 Connect the Console interface of the RAX711-L to the USB interface of the PC through a dual USM male interface cable, as shown in Figure 1-1.

Figure 1-1 Logging in to the device through the Console interface

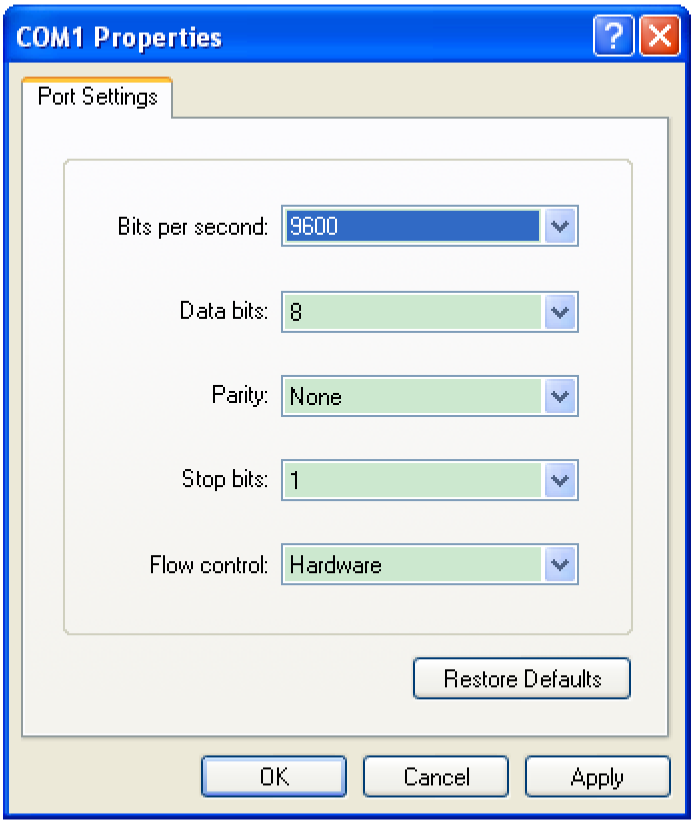


Step 4 Run the terminal emulation program on the PC, such as Hyper Terminal on Microsoft Windows XP. Enter the connection name at the Connection Description dialog box and then click **OK**.

Step 5 Select COM 1 at the Connect To dialog box and then click **OK**.

Step 6 Configure parameters are shown in Figure 1-2 and then click **OK**.

Figure 1-2 Configuring parameters for Hyper Terminal



Step 7 Enter the configuration interface and then enter the user name and password to log in to the RAX711-L. By default, both the user name and password are set to raisecom.

Note

Hyper Terminal is not available on Windows Vista or later Windows Operating Systems (OSs). For these OSs, download Hyper Terminal package and install it. This program is free for personal application.

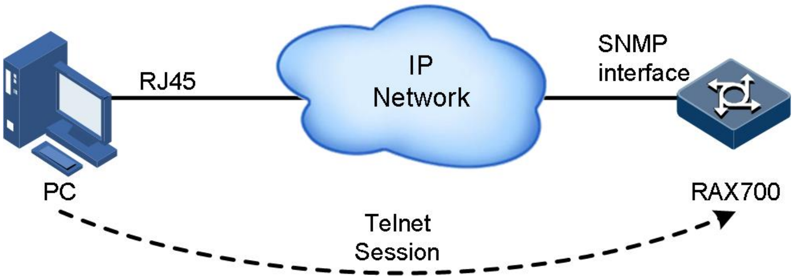
1.2.2 Accessing device through Telnet

Through Telnet, you can remotely log in to the RAX711-L through a PC. In this way, it is not necessary to prepare a PC for each RAX711-L.

The RAX711-L supports the following two Telnet services:

- Telnet Server: as shown in Figure 1-3, connect the PC and the RAX711-L and ensure that the route between them is reachable. You can log in to and configure the RAX711-L by running Telnet program on a PC. Now the RAX711-L provides Telnet server service.

Figure 1-3 The device working as the Telnet Server



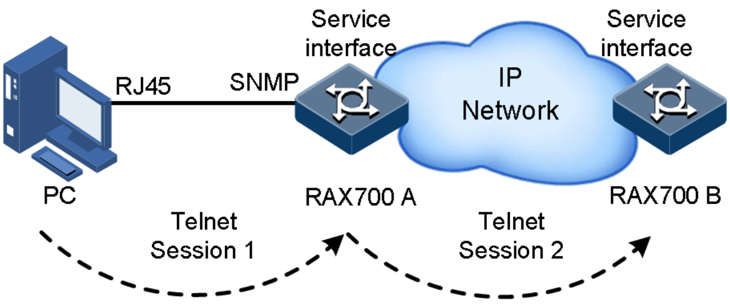
Note

Before logging in to the RAX711-L through Telnet, you must log in to the RAX711-L through the Console interface, configure the IP address of the SNMP interface, and enable Telnet service.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`management-port ip address`** *`ip-address`* `[` *`ip-mask`* `]`	Configure the IP address of the SNMP interface.
3	`Raisecom(config)#`**`telnet-server accept`** *`interface-type interface-list`*	(Optional) configure the interface that supports Telnet.
4	`Raisecom(config)#`**`telnet-server close terminal-telnet`** *`session-number`*	(Optional) close the specified Telnet session.
5	`Raisecom(config)#`**`telnet-server max-session`** *`session-number`*	(Optional) configure the maximum number of Telnet sessions supported by the RAX711-L. By default, up to 10 Telnet sessions are available.

- Telnet Client: after connecting the RAX711-L through the terminal emulation program or Telnet, you can log in to, manage, and configure another RAX711-L through Telnet. As shown in Figure 1-4. The RAX711-L provides both Telnet server and Telnet client services.

Figure 1-4 The device working as the Telnet Client



Step	Command	Description
1	`Raisecom#`**`telnet`** `{` *`ip-address`* `|` *`ipv6-address`* `}` `[` **`port`** *`port-number`*`]`	Log in to other devices through Telnet.

1.2.3 Accessing device through SSHv2

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

SSHv2 builds up a secure channel over TCP. Besides, SSHv2 is in support of other service ports as well as standard port 22, thus to avoid illegal attack from network.

Before accessing the RAX711-L via SSHv2, you must log in to the RAX711-L through the Console interface and enables 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. By default, the length of the local SSHv2 key pair is set to 512 bits.
3	Raisecom(config)#**ssh2 server**	Start SSHv2 server. By default, the RAX711-L does not start the SSHv2 server.
4	Raisecom(config)#**ssh2 server authentication { password | rsa-key }**	(Optional) configure SSHv2 authentication method. By default, the RAX711-L adopts the **password** authentication mode.
5	Raisecom(config)#**ssh2 server authentication public-key**	(Optional) when the **rsa-key** authentication method is adopted, type the public key of clients to the RAX711-L.
6	Raisecom(config)#**ssh2 server authentication-timeout** *period*	(Optional) configure SSHv2 authentication timeout. The RAX711-L refuses to authenticate and open the connection when client authentication time exceeds the upper threshold. By default, the SSHv2 authentication timeout is set to 600s.
7	Raisecom(config)#**ssh2 server authentication-retries** *times*	(Optional) configure the allowable times for SSHv2 authentication failure. The RAX711-L refuses to authenticate and open the connection when client authentication failure times exceed the upper threshold. By default, the allowable times for SSHv2 authentication failure are set to 20.
8	Raisecom(config)#**ssh2 server port** *port-number*	(Optional) configure the SSHv2 listening port ID. By default, the SSHv2 listening port ID is set to 22. **Note** When configuring the SSHv2 listening port ID, the input parameter cannot take effect immediately without reboot the SSHv2 service.
9	Raisecom(config)#**ssh2 server session** *session-list* **enable**	(Optional) enable SSHv2 session. By default SSHv2 session is enabled.

1.2.4 Managing users

When you start the RAX711-L 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 RAX711-L.

Note

By default, both the user name and password are raisecom

If there is not any privilege restriction, any remote can log in to the RAX711-L via 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 RAX711-L and network. Creating the user name and setting the password and privilege help manage the login users and ensure network and device security.

Step	Command	Description
1	Raisecom#**user name** *user-name* **password** *password*	Create or modify the user name and password.
2	Raisecom#**user name** *user-name* **privilege** *privilege-level*	Configure the level and privilege of the user.
3	Raisecom#**user** *user-name* { **allow-exec** | **disallow-exec** } *first-keyword* [*second-keyword*]	Configure the priority rule for the user to perform the command line. The **allow-exec** parameter will allow the user to perform commands higher than the current priority. The **disallow-exec** parameter disallows the user to perform commands that match the keyword.
4	Raisecom#**user login** { **local-user** | **radius-user** | **local-radius** | **radius-local** [**server-no-response**] }	(Optional) configure the authentication mode for logging in to the RAX711-L when the RADIUS service is adopted.
5	Raisecom#**enable login** { **local-user** | **radius-user** | **local-radius** | **radius-local** [**server-no-response**] }	(Optional) configure the authentication mode for entering privileged EXEC mode when the RADIUS service is adopted.
6	Raisecom#**user login** { **local-user** | **tacacs-user** | **local-tacacs** | **tacacs-local** [**server-no-response**] }	(Optional) configure the authentication mode for logging in to the RAX711-L when the TACACS+ service is adopted.
7	Raisecom#**enable login** { **local-user** | **tacacs-user** | **local-tacacs** | **tacacs-local** [**server-no-response**] }	(Optional) configure the authentication mode for entering privileged EXEC mode when the TACACS+ service is adopted.
8	Raisecom#**enable auth** { **bypass** | **default** | **user** }	(Optional) configure the authentication mode of the privileged user.

1.2.5 Checking configurations

No.	Command	Description
1	`Raisecom#show user [ detail ]`	Show the user information.

1.3 Web network management

1.3.1 Logging in to Web configuration interface

Scenario

To better configure and maintain the RAX711-L, you can log in to Web management interface.

If you wish to manage the RAX711-L through Web configuration interface, you should use a PC to internetwork with the RAX711-L.

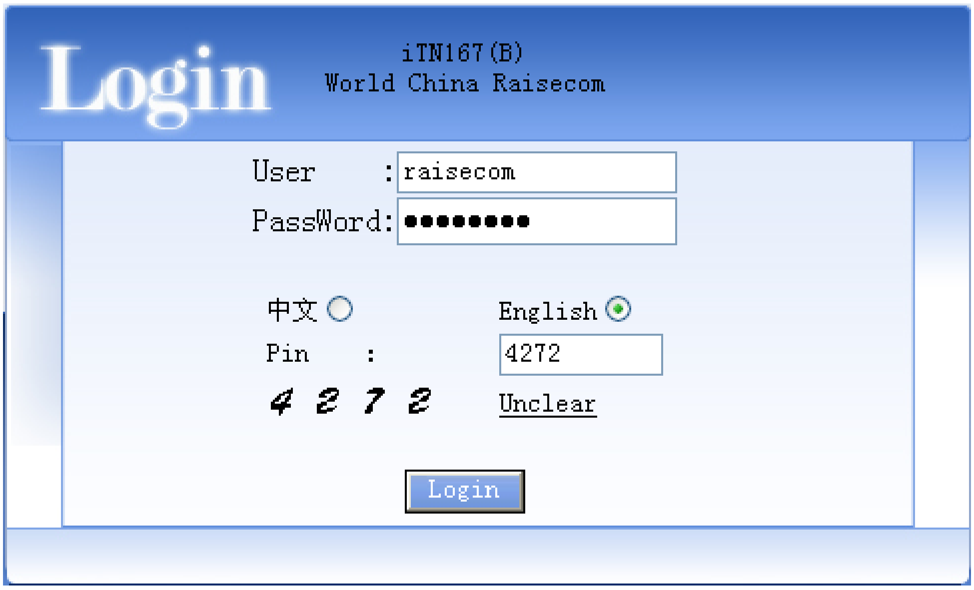
Configuration steps

Log in Web configuration interface as below.

Step 1 Open the IE browser on the PC.

Step 2 Enter the IP address of the RAX711-L in the address bar, for example, enter "http://192.168.18.111" and press **Enter**, and then the Web login interface appears, as shown in Figure 1-5.

Figure 1-5 Login interface



Step 3 Enter user name and password on the login interface.

Step 4 Choose English on the interface, and input random authentication code. If the current authentication code is illegible, you can click **Unclear** to update it.

Step 5 Click **Login**, and enter the Web management interface.

Note

Before logging in the Web management interface, you should use the **ip http server enable** command to enable the Web network management server.
If you log in the Web management interface for the first time, you can use the default user name and password raisecom.

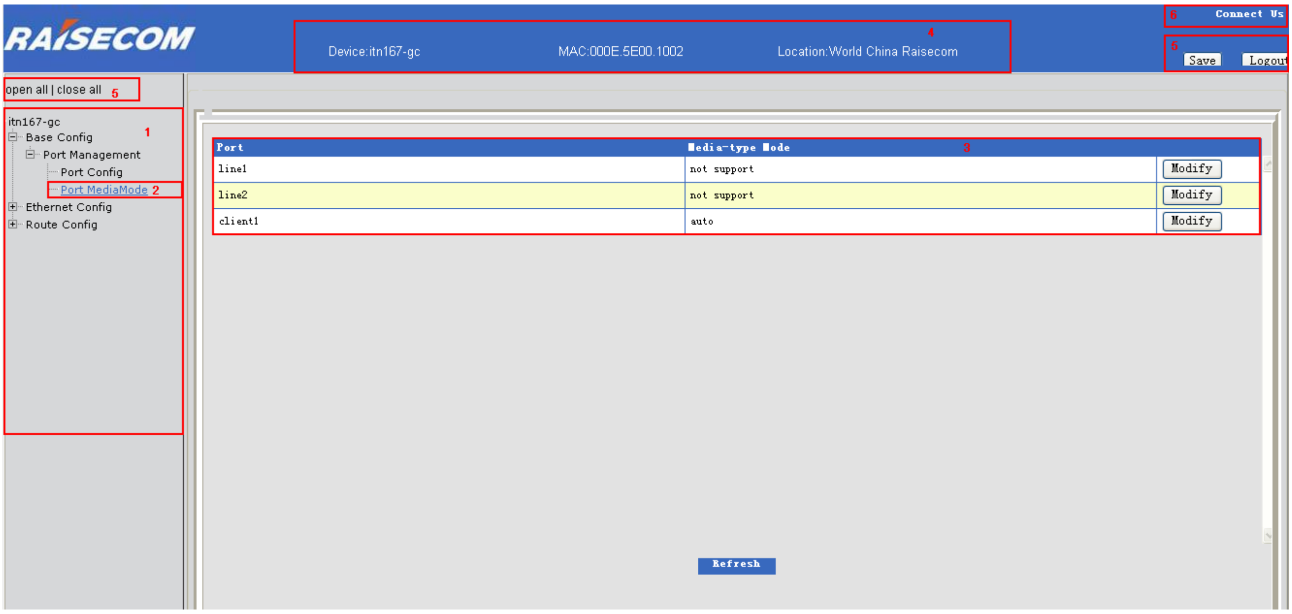
1.3.2 Introduction to Web configuration interface

Interface structure

The Web configuration interface of Client is unified and is easy to operate. Learning Web configuration interface can help you find entrances to functions to promote operations efficiency.

Figure 1-6 shows the typical Web configuration page.

Figure 1-6 Typical Web configuration page



1	Navigation bar	2	Current location
3	Current configuration page	4	Device information
5	Common buttons	6	Contact information

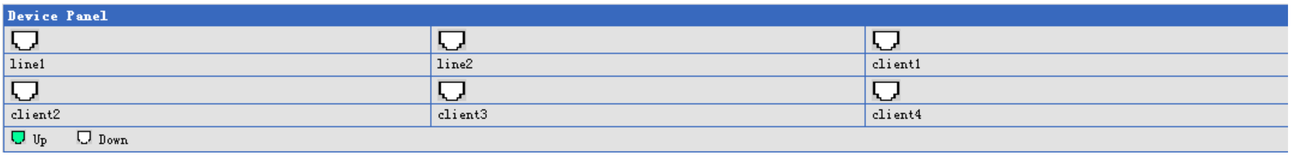
Device overview

When you log in the Web configuration interface through the Web system, The Device overview page is displayed by default. The device overview page displays device panel, device information, and system state, etc.

When you wish to return from present page to Device overview page, you can click the device name RAX 700 (A) in the left navigation bar.

- Device panel
  - According to the connected device type, the device panel page directly displays information about interface. It will display device interface IDs and interface working state (if the interface LED is green, it displays that the interface is in the connected status), as shown in Figure 1-7.

Figure 1-7 Device panel



Tip

Move the cursor on the interface, numbering information about the interface will be displayed.

- Equipment information

This area can display product model of the device, software version, and hardware version, etc., as shown in Figure 1-8.

Figure 1-8 Device information

Device Information	
Product name	iTN167(B)
RITP Version	5.3
Product Version	iTN167(B)_2.0--
Boot Version	BOOTROM_1.0.7
FPGA Version	fpga:1.5 fpga-ces:2.6
Hardware Version	2.0
System MacAddress	000E.5E01.0001
Serial number	123456789098765432123456
Memory	DRAM:128 MB / Flash:32 MB
System uptime	4 days, 6 hours, 29 minutes
Current system time	2059-12-04,14:30:36
Timezone offset	+08:00-CCT

- System status

  This area shows the CPU utilization, memory utilization, chassis temperature, and power status of the present device, as shown in Figure 1-9.

Figure 1-9 System status

System Status	
CPU utilization	In Second: 6% / In Minute: 8%
Memory utilization	48.20%
Case Temperature(Reference Range:-10℃~75℃)	50℃
Power Status	power1: off / power2: on
Current Voltage(reference:3300mv)	3334mv

Common buttons

The buttons with the same name have the same functions. Table 1-1 lists common buttons on the Web configuration interface.

Table 1-1 Lists common buttons on the Web configuration interface

Button	Description
open all	Unfold each level of navigation bar.
close all	Close each navigation bar to primary navigation.
Add	Add an item in the current page.
Cancel	Cancel current configurations.
Modify	Modify a selected item in the current page.
Delete	Delete a selected item in the current page.
Refresh	Refresh information in the current page.
Apply	Finish configurations and apply the current configurations to the system software.
Logout	Log out from the current page.
Save	Save the current configurations.

1.3.3 Saving configurations

Note

- After configurations are complete in the current page, click **Apply**. Configurations that are saved in the memory are not saved in the configuration file. If the RAX711-L encounters power failure or is rebooted at this time, configurations will be lost.
- After all the present configurations are finished, click Save. If the RAX711-L encounters power is power failure or is rebooted, configurations that are saved in the configured file are not lost.

The Web interface offers two methods for saving configurations.

- Click **Apply** in the present Web configuration interface, and save the present interface configurations in the memory.
- Click **Save** at top right corner in any interface, and save current configurations in the configured file.

1.3.4 Exit Web configuration interface

When configurations are complete, you need to exit the Web configuration interface to ensure system security.

Caution

Before exiting the Web configuration interface, you need to save the present information to avoid losing configurations.

There are two methods for exiting the Web configuration interface.

- Click on the IE browser, close IE browser, and exit the Web configuration interface.
- Click **Logout** at top right corner on the Web configuration interface, and exit the Web configuration interface.

1.3.5 Configuring interfaces

The Web configuration interface supports configuring parameters of device interface status and duplex, operation rate and flow control.

The device supports Ethernet electrical interface and Ethernet optical interface. You can choose configuration interface according to the fact.

Configuring interface basic properties

Step 1 Choose **Base Config** > **Port Management** > **Port Config**, and the Port Configuration page appears.

Step 2 In the Port Config page, check configurations of each interface. Click **Modify** corresponding to the specified interface, the Port Information Configuration page appears, where you can configure interface properties, as shown in Table 1-2.

Step 3 After configurations, click **Apply**.

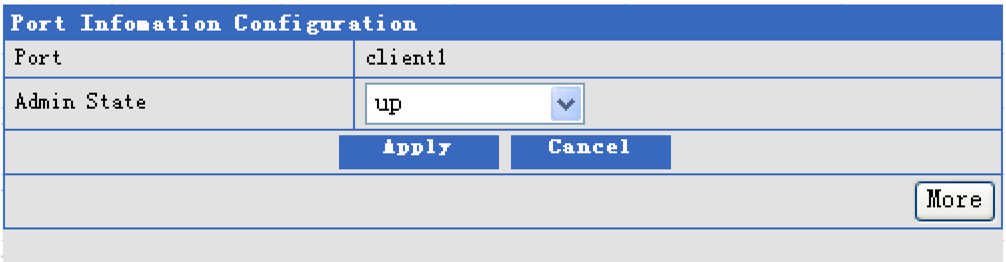


Table 1-2 Basic configuration items on the Port Information Configuration page

Configuration item	Description
Port	Interface name and interface ID.
Administration State	Modify the current configuration state of the configuration interface through the following drop-down box. • Up • Down

Step 4 (Optional) click **More**, and the Port Information Configuration advanced page appears, where you can configure related items, as shown in Table 1-3. Click **Apply.**

Table 1-3 Advanced configuration items on the Port Information Configuration page

Configuration item	Description
Port	Interface name and interface ID
Operate State	The interface operate state
Administration State	Configure the association status of the interface. • Up • Down
Speed	Configure the speed of the interface. • Auto-negotiate • 100M: 100 Mbit/s • 1000M: 1000 Mbit/s
Duplex	Configure duplex mode of the interface. • Auto-negotiate • Half duplex • Full duplex
FlowControl (Tx)	Configure flow control in the Tx direction of the interface. • On • Off By default, it is disabled.
FlowControl (Rx)	Configure flow control in the Rx direction of the interface. • On • Off By default, it is disabled.
MDI	MDI wiring is fixed to auto, namely, auto switching mode.

Configuring interface media modes

Step 1 Choose **Base Config** > **Port Management > Port MediaMode**, and the Port MediaMode page appears.

Step 2 Click **Modify** corresponding to interface to be configured, and Port Information Configuration dialog box appears, where you can configure items, as shown in Table 1-4.

Step 3 After configurations, click **Apply**.

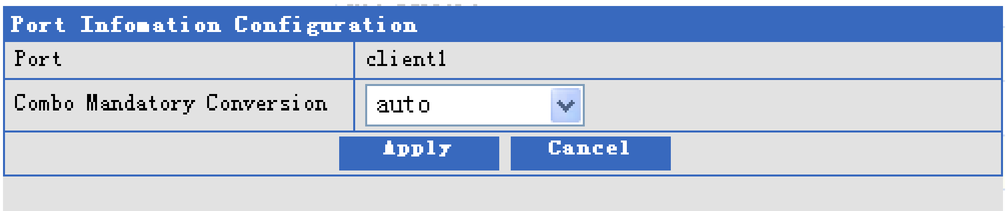


Table 1-4 Base configuration items on the Port Information Configuration

Configuration item	Description
Port	Interface type and ID
Combo Mandatory Conversion	Configure port media mode of the Combo. • auto: auto-negotiate according to accessed media mode. • fiber: it is fixed as optical interface. • Copper: it is fixed as the electrical interface.

1.3.6 Configuring base QinQ

To realize device interworking among different venders, the protocol type of outer VLAN Tag for QinQ on the interface should be configured as the protocol type that can be recognized by the device, which is connected with the interface,

You can add outer VLAN Tag and design their private network VLAN ID through base QinQ technology application. Thus data among the user devices on the both sides of the carrier can transparent transport, but it cannot conflict with VLAN ID provided by venders.

Step 1 Click **Ethernet Config** > **QinQ Config** > **Base Config** > **TPID Config**, and the Port TPID Configuration page appears.

Step 2 Click **Modify** in the Port TPID Configuration dialog box. A port TPID configuration page appears, where you can configure items, as shown in Table 1-5.

Step 3 After configurations, click **Apply**.

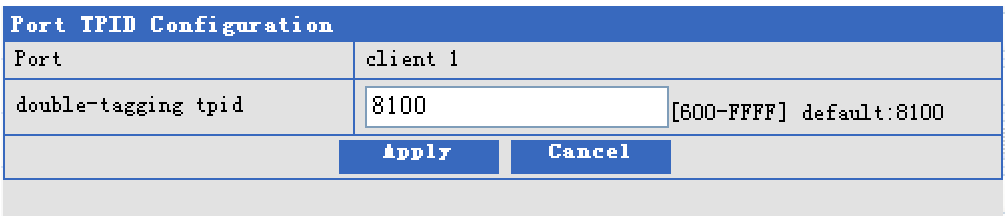


Table 1-5 Port TPID configuration item on the Port TPID Configuration page

Configuration item	Description
Double-tagging tpid	TPID of the outer VLAN Tag on the interface, hexadecimal notation, an integer, ranging from 600 to FFFF, and 8100 be default.

Step 4 Click **Ethernet Config** > **QinQ Config** > **Base Config** > **Status Config**, and the Port Status Configuration page appears.

Step 5 Click **Modify** corresponding to the specified interface, and Port Status Configuration page appears, where you can configure items, as shown in the Table 1-6.

Step 6 After configurations, click **Apply**.

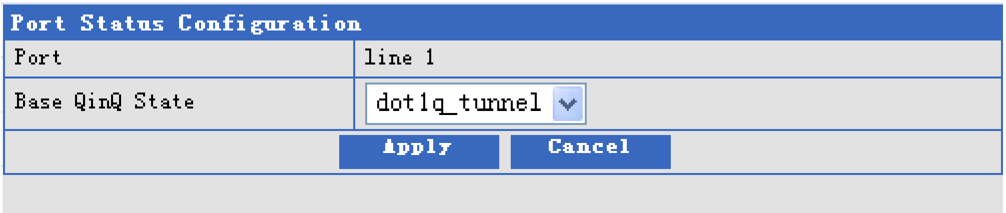


Table 1-6 Configuration item on the Port Status Configuration page

Configuration item	Description
Base QinQ State	Configure base QinQ. • None: disable base QinQ. • Dotlq-tunnel: enable base QinQ. By default, disable base QinQ for the RAX700.

1.3.7 Configuring selective QinQ

Different from basic QinQ, selective QinQ allows you to choose outer VLAN Tag according to different services. There are various services in the user network, and they are configured with different private VLAN IDs.

Step 1 Click **Ethernet Config** > **QinQ Config** > **Smart QinQ** > **VLAN Add** > **Base VLAN**, and the Add Outer-vlan Rule page appears.

Step 2 (Optional) check the current configuration rules for selective QinQ.

Step 3 In the configuration page, click **Add**, and the Add Outer-vlan Rule dialog box appears, where you can configure items, as shown in Table 1-7.

Step 4 After configurations, Click **Apply**.

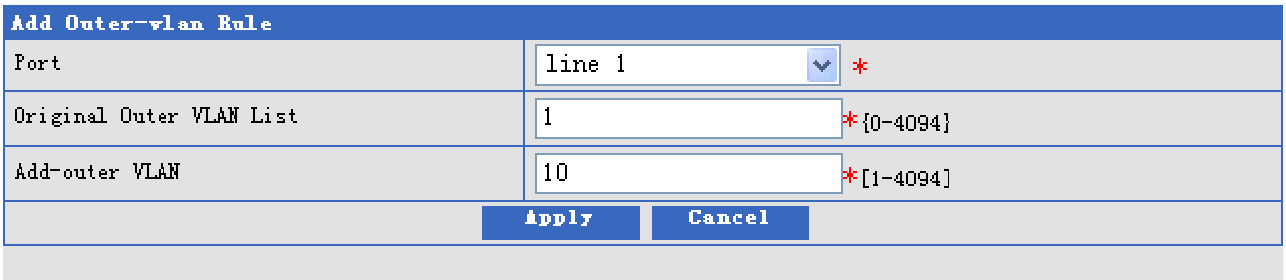


Table 1-7 Configurations items on the Add Outer-vlan Rule page

Configuration item	Description
Port	Interface of adding outer VLAN
Original Outer VLAN List	List of inner customer VLAN, an integer, ranging from 0 to 4094 Supporting multiple input of the VLAN mode, such as 1.2.3, supporting input of VLAN arrangement mode, such

	as 1-3 Packets without customer VLAN when it is 1
Add-outer VLAN	The ID of the adding outer VLAN Tag, an integer, ranging from 1 to 4094

1.3.8 Configuring VLAN mapping

Different from QinQ, VLAN mapping is to change VLAN label, not to encapsulate multilayer VLAN Tag. VLAN mapping only need to change VLAN Tag mark and transport according to VLAN transponding regular of the carrier network, but the frame length of the original packets cannot be increased.

VLAN mapping can be applied in the following scenarios.

- A kind of user service is converted as a VLAN ID of a carrier.
- Various user services are converted as a VLAN ID of a carrier.

Step 1 Click **Ethernet Config > QinQ Config > VLAN Translate> Base VLAN**, and the Add VLAN Translate Rule page appears.

Step 2 In the configuration page, you can check the current configuration rules for the VLAN translate. Click **Add**, and Add VLAN Translate Rule dialog box appears, as shown in Table 1-8.

Step 3 After configurations, click **Apply**.

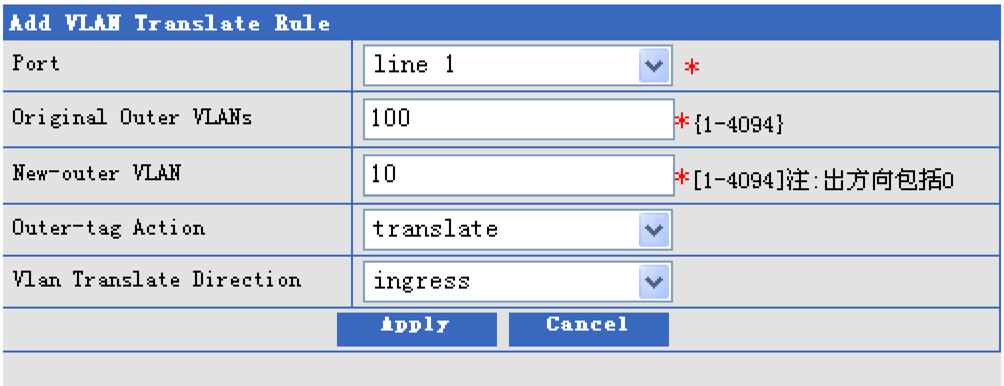


Table 1-8 Configurations items on the Add VLAN Translate Rule page

Configuration item	Description
Port	Interface of configuring VLAN translate
Original Outer VLANs	Original outer VLAN ID, an integer, ranging from 1 to 4094 It supports specific values, such as "1.2.3", It also supports range, such as "1-3".
New-outer VLAN	New outer VLAN ID, an integer, ranging from 1 to 4094

	The direction of VLAN mapping configured as egress, ranging from 0 to 4094
Outer-tag Action	Implementing rule of outer label
Vlan Translate Direction	Direction of VLAN mapping • ingress: in the ingress direction of the interface • egress: in the egress direction of the interface

1.3.9 Configuring 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. From functions, VLAN and LAN have the same features, but the major difference is that member in a same VLAN can have inter-access, not be restricted by the physical local.

Configuring VLAN base information

VLAN partitioning isolates hosts that need not to interwork with each other to increase network security, reduce broadcast traffic, and also reduce broadcast storm.

This page can be used to check, modify related information and create VLAN.

Step 1 Click **Ethernet Config > VLAN Config > Base Config**, and the VLAN Configuration Information page appears.

Step 2 In the configuration page, you can check configurations about each VLAN. Click **Config**, and VLAN Configuration Information dialog box appears, where you can configure items, as shown in Table 1-9.

Step 3 After configurations, click **Apply**.

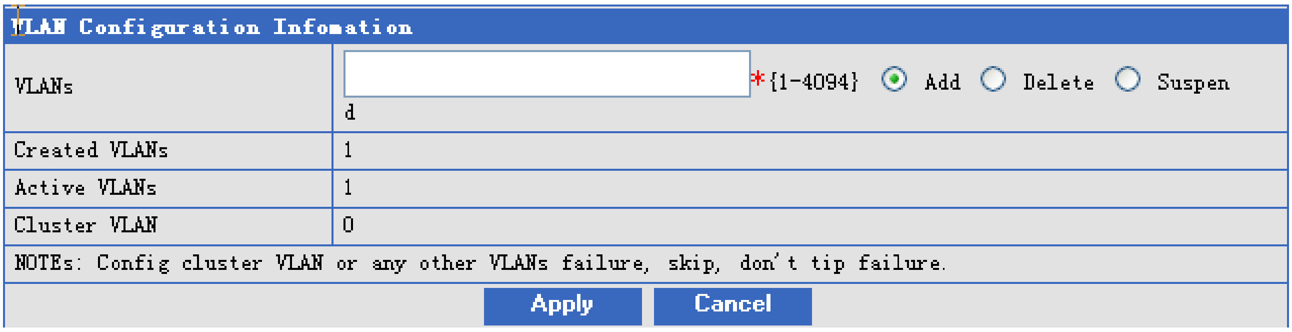


Table 1-9 Configuration item on the VLAN Configuration Information page

Configuration item	Description
VLAN	Enter VLANs. After entering, click a radio button to configure VLAN status. • Add: add the VLAN.

	• Delete: delete the VLAN. • Suspen: suspen the VLAN.

Configuring VLAN properties on the interface

Interface models are divided into Access and Trunk. You can check or modify VLAN configurations on the present interface on this page.

Step 1 Click **Ethernet Config** > **VLAN Config** > **VLAN Port Config**, the Port VLAN Configuration page appears.

Step 2 In the configuration page, you can check VLAN configurations. Click **Modify** in the corresponding row, and Port VLAN Configuration page appears, where you can configure items, as shown in Table 1-10.

Step 3 After configurations, click **Apply**.

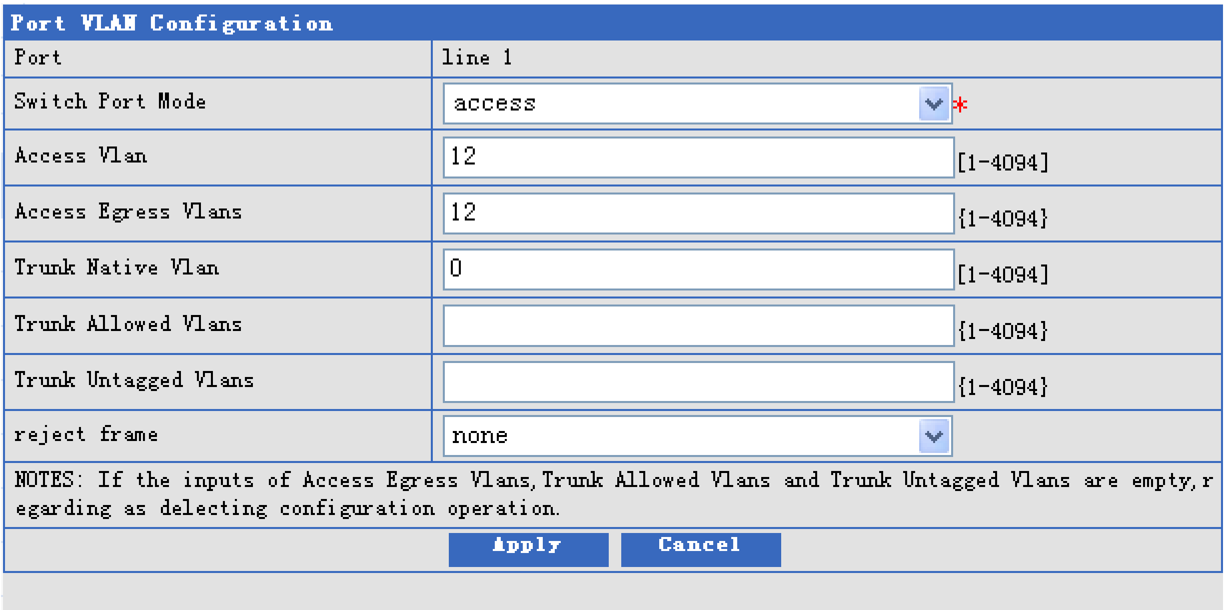


Table 1-10 Configuration items on the Port VLAN Configuration page

Configuration item	Description
Port	Interface name and ID
Switch Port Mode	VLAN mode on the interface • access • trunk By default, it is Access.
Access Vlan	Configure Access interface for VLAN, ranging from 1 to 4094. It is mandatory when the interface is the Access mode.

Access Egress Vlans	Configure list of VLANs allowed on the Access interface, ranging from 1 to 4094. It is optional when it is the Access mode.
Trunk Native Vlan	Configure Native VLAN on the Trunk interface, ranging from 1 to 4094. It is mandatory when it is the Trunk mode.
Trunk Allowed Vlans	Configure list of VLAN allowed on the Trunk interface, ranging from 1 to 4094. It is optional when it is the Trunk mode.
Trunk Untagged Vlans	Configure list of Untagged VLAN on the Trunk interface, ranging from 1 to 4094. It is optional when it is the Trunk mode.
Reject frame	The disapproved packets type • none: packets approved • tag: Tagged packets disapproved • untag: Untagged packets disapproved

1.3.10 Configuring route

Configuring IP basic information

Configure at least a master IP address and associating it with a VLAN for each Layer 3 interface to implement devices management or implement route connectivity among numbers of devices.

Step 1 Click **Route Config > IP Config > IP Base Config**, IP Base Information page appears.

Step 2 In the IP Base Information Config page, you can check IP address and related information about the IP interface. Click **Add**, and IP Base Information appears, where you can configure items, as shown in Table 1-11.

Step 3 After configurations, click **Apply**.

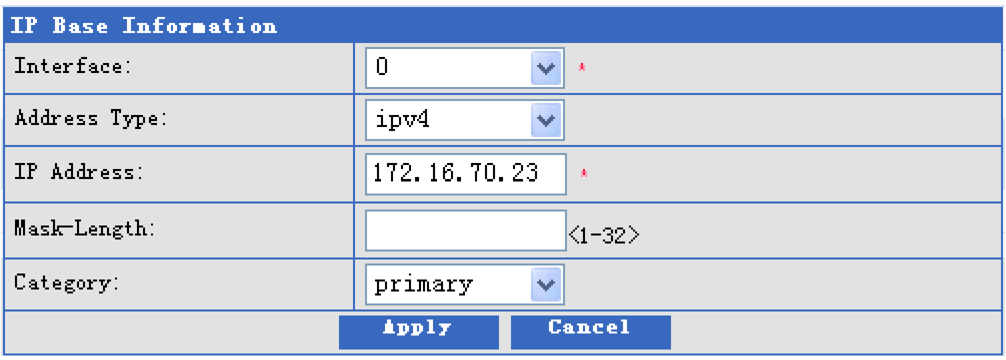


Table 1-11 Configuration items on the IP Base Information page

Configuration item	Description
Port	IP interface ID, ranging from 0 to 14
Address Type	The type of IP address
IP Address	Configuring IP address of the IP interface in dotted decimal notation, such as, 10.10.10.1
Mask-Length	Configuring mask length, ranging from 1 to 32, supporting variable-length mask
Category	Configuring primary-sub IP address • Primary: primary IP address • Sub: sub IP address

Caution

- Each IP interface only has one primary IP address. Before deleting the primary IP address, you must delete corresponding slave IP address.
- When the primary-slave relation is established, it cannot be modified. If you wish to change the relation, you must delete the established primary-slave relation, and reconfigure the relation.

Step 4 In the IP Vlan Information configuration page, you can check VLAN information connected with IP interface. Click **Add**, Vlan Information dialog box appears, where you can configure items, as shown in Table 1-12.

Step 5 After configurations, click **Apply**.

Table 1-12 Configuration items on the VLAN Information page

Configuration item	Description
Port	IP interface ID, ranging from 0 to 14
Vlan ID(1-4094)	The VLAN mapped on the interface, an integer, ranging from 1 to 4094.

Configuring out-of- band interface IP information

Step 1 Click **Route Config** > **IP Config** > **Outband IP Config**, and the Outband IP Base Configuration page appears.

Step 2 In the Outband IP Config configuration panel, you can check the IP address and other configurations of the RAX700. Click **Add**, Outband IP Base Information dialog box appears, where you can configure items, as shown in the Table 1-13.

Step 3 (Optional) in the Outband IP Base Information page, click **Modify** to modify the IP address on the management interface.

Step 4 After configurations, click **Apply**.

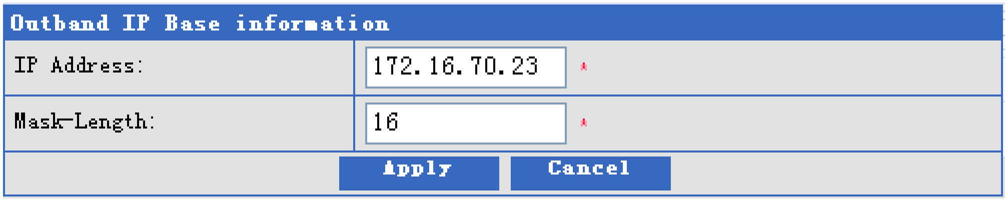


Table 1-13 Configuration items on the IP Base Information page

Configuration item	Description
IP address	The IP Address on the management interface, dotted decimal notation,, such as10.10.10.1
Mask-Length	Mask-length of the IP address, ranging from 1 to 32

1.4 Zero-configuration on the remote devices

With wide application of the Packet Transport Network (PTN) technology in mobile backhaul and professional fields, a great number of the RAX700200 and the RAX700100 devices will be applied in a large scale. However, these devices are scattered at the remote end. When a project is to be implemented, the maintenance personnel must configure then manually. This consumes lots of time and effort. In addition, this may cause errors and influence the working efficiency.

To resolve these problems, the local device automatically configures parameters, such as the IP address and default gateway, for remote devices to manage them. In addition, you can transmit/receive data quickly. That is why zero-configuration is introduced.

With zero-configuration, developed by Raisecom, devices, which support this feature, can be discovered and managed by the NView NNM system once being installed and powered on, without being configured. This simplifies implementation, facilitates wide-scale deployment, and reduces operation and maintenance cost.

1.4.1 Introduction

As a remote device, the RAX711-L realizes zero-configuration through the following methods:

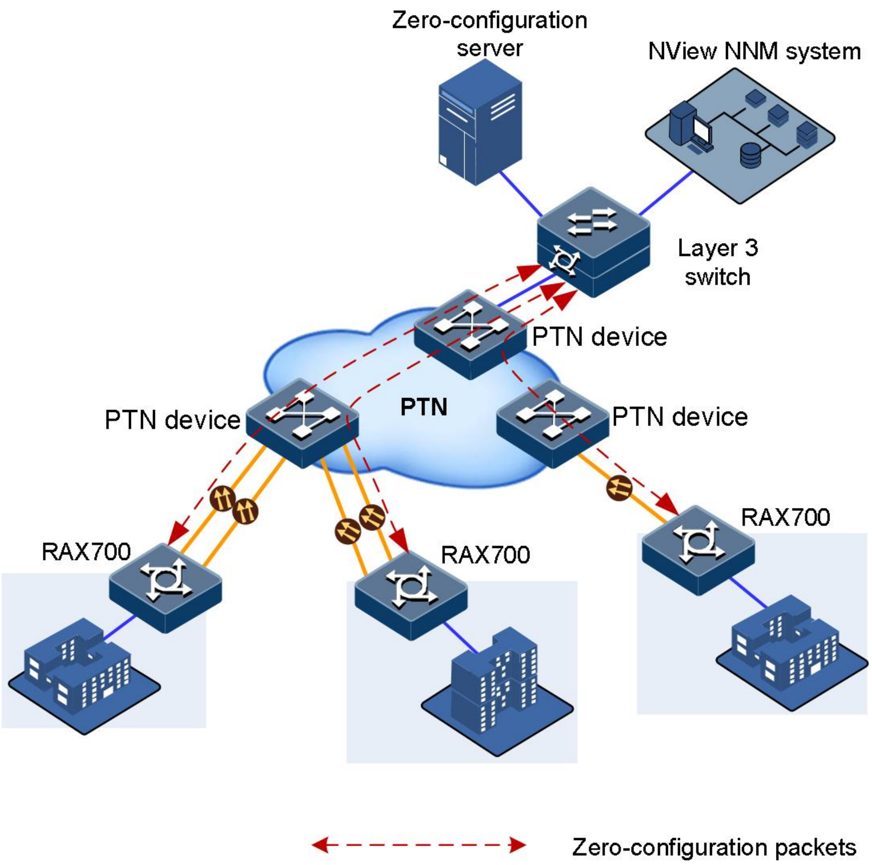
- Zero-configuration server

- Central Office (CO) device, such as the RAX7002100.

Zero-configuration server

Figure 1-10 shows how the RAX711-L realizes zero-configuration through a zero-configuration server.

Figure 1-10 Realizing zero-configuration through a zero-configuration server

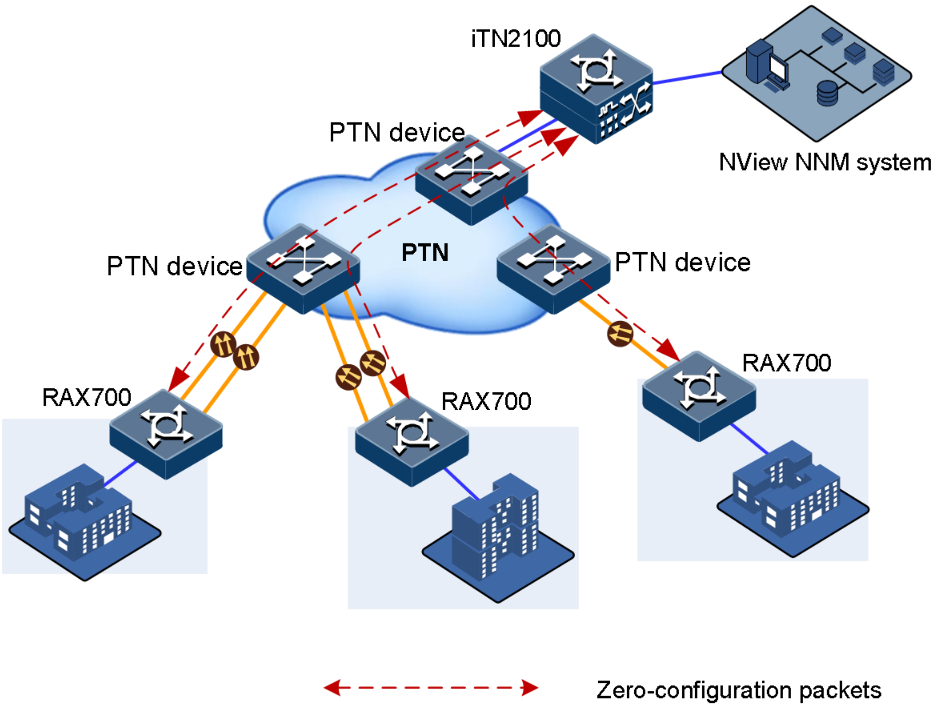


The RAX711-L works as the remote device in the PTN. The zero-configuration server at the NMS side assigns parameters, such as the management IP address, to the remote device. After being powered on, the remote device automatically sends the packet to apply for the IP address. The packet is transmitted to the NMS server through the PTN and Layer 3 switch. And then the zero-configuration server sends the reply packet containing the management IP address, VLAN ID, and default gateway, to the remote device. The remote device will update its configurations automatically after receiving the reply packet, thus realizing the zero-configuration feature.

CO device

Figure 1-10 shows how the RAX711-L realizes zero-configuration through a CO device, such as the RAX7002100.

Figure 1-11 Realizing zero-configuration through a CO device



The RAX711-L works as the remote device in the PTN. The RAX7002100 assigns parameters, such as the management IP address and management VLAN, to the remote device. After being powered on, the RAX711-L establishes an OAM link with the RAX7002100 and obtains required parameters from it through automatic detection to update its configurations automatically. That is, the RAX711-L can be discovered by the NView NNM system to realize the zero-configuration feature.

Note

By default, remote devices are enabled with zero-configuration. After being powered on, they will apply for IP addresses, VLAN IDs, and default gateways automatically. If a remote device is configured with an IP address, it cannot perform zero-configuration operations.

1.4.2 Preparing for zero-configuration

Scenario

In general, after remote devices are connected to the local device and the DHCP Server is configured properly, remote devices can apply for IP addresses automatically once being powered on. When you need to modify parameters about zero-configuration, see this section.

Prerequisite

- Both local and remote devices work in zero-configuration mode.
- IP 0 interface is related to an activated VLAN.
- The physical interface, connected to the zero-configuration server, is added to the VLAN.
- The uplink interface is UP.

1.4.3 Configuring DHCP Client

IP addresses assigned through zero-configuration are valid permanently.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp client mode** { **zeroconfig** | **normal** }	Configure the DHCP Client working as a zero-configuration remote device or a common client. By default, the DHCP Client works as a zero-configuration remote device.
3	Raisecom(config)#**interface ip** *if-number*	Enter IP interface configuration mode. Only IP 0 interface supports being configured with DHCP Client.
4	Raisecom(config-ip)#**ip address dhcp** [**server-ip** *ip-address*]	Enable zero-configuration. Meanwhile, you can specify the IP address of the local DHCP Server. If you specify the IP address of the DHCP Server, you can receive the IP address from the specified DHCP Server only.
5	Raisecom(config-ip)#**ip dhcp client** { **class-id** *class-id* | **client-id** *client-id* | **hostname** *host-name* }	Configure information about the DHCP Client, including the hostname, Class ID, and Client ID. The information is included in the packet sent by the DHCP Client.

Note

- If the IP 0 interface of the remote device has obtained an IP address through DHCP, it is believed that the remote device has obtained the IP address successfully, regardless of whether the default gateway is configured successfully or not.
- The manually-configured IP address of IP 0 interface and the one automatically-obtained through zero-configuration can be mutually overridden.
- IP addresses of other IP interfaces of the remote device cannot be in the same network segment with the one of the IP 0 interface.
- After the IP 0 interface of the remote device has obtained an IP address automatically, if you re-perform this command to make apply for an IP address from another DHCP Server, the remote device will release the original IP address.

1.4.4 (Optional) configuring zero-configuration polling

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp client zeroconfig polling period** *hour*	Configure the zero-configuration polling period. It ranges from 1 to 24 hours. By default, it is set to 2 hours.

1.4.5 Checking configurations

No.	Command	Description
1	Raisecom#**show ip dhcp client**	Show configurations and automatically-obtained information about the DHCP Client.

1.5 Configuring IP address of device

Note

If a remote device has applied an IP address through zero-configuration, there is no need to manually configure an IP address for it.

1.5.1 Configuring IP address of device

The remote device can get an IP address through the following 2 modes:

- Manually configure an IP address.
- Get an IP address through the DHCP Server.

Note

By default, the system has a default VLAN 1. If you need to relate the IP address to another VLAN ID, you must create and activate it in advance.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
3	Raisecom(config-ip)#**ip address** *ip-address* [*ip-mask*] [**sub**] [*vlan-id*] Raisecom(config-ip)#**ipv6 address** *ipv6-address/M* [**eui-64**] [*vlan-list*]	Configure the IP address and related VLAN.
4	Raisecom(config-ip))#**ip address dhcp** [**server-ip** *server-ip-address*] Raisecom(config-ip))#**ipv6 address dhcp** [**server-ip** *ipv6-address*]	Get an IP address through DHCP Server.

1.5.2 Checking configurations

No.	Command	Description
1	Raisecom#**show ip interface brief**	Show basic configurations on the IP interface.
2	Raisecom#**show ip interface ip** *if-number*	Show detailed configurations on the IP interface.
3	Raisecom#**show interface ip vlan**	Show the IP address and its related VLAN.

No.	Command	Description
4	Raisecom#**show ip dhcp client**	Show DHCP Client configurations.
5	Raisecom#show ipv6 interface { brief | ip *if-number* }	Show IPv6 configurations on the IP interface.
6	Raisecom#**show ipv6 dhcp client**	Show the IPv6 configurations on the DHCP Client.

1.6 Configuring time management

1.6.1 Configuring time and time zone

To ensure that the RAX711-L can cooperate with other devices, you need to configure system time and time zone precisely for the RAX711-L.

Step	Command	Description
1	Raisecom#**clock set** *hour minute second year month day*	Configure the system time. By default, the system time is set to 8:00:00, Jan 1, 2000.
2	Raisecom#**clock timezone** { **+** | **-** } *hour minute timezone-name*	Configuring system time zone. By default, it is GMT + 8:00.

1.6.2 Configuring DST

Daylight Saving Time (DST) is set locally to save energy, but vary in details. Thus, you need to consider detailed DST rules locally before configurations.

Step	Command	Description
1	Raisecom#**clock summer-time enable**	Enable DST on the RAX711-L. By default, DST is disabled.
2	Raisecom#**clock summer-time recurring** { *start-week* | **last** } { **sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat** } *start-month hour minute* { *end-week* | **last** } { **sun** | **mon** | **tue** | **wed** | **thu** | **fri** | **sat** } *end-month hour minute offset*	Configure the begin time and end time of DST. By default, the time offset is set to 60 minutes.

Note

- When you configure the system time manually, if the system uses DST, such as DST from 2 a.m. on the second Sunday, April to 2 a.m. on the second Sunday, September every year, you have to advance the clock one hour faster during this period, that is, set the time offset as 60min. So the period from 2 a.m. to 3 a.m. on the second Sunday, April each year is inexistent. Configuring time manually in this period will fail.

- The DST in southern hemisphere is opposite to the northern hemisphere, which is from September to April next year. If the start time is later than end time, the system will suppose that it is in the southern hemisphere. That is to say, the DST is the period from the start time this year to the end time next year.

1.6.3 Configuring NTP/SNTP

Note

SNTP and NTP are mutually exclusive. If you have configured the IP address of the NTP server on the RAX711-L, you cannot configure SNTP on the RAX711-L, and vice versa.

Network Time Protocol (NTP) is a time synchronization protocol defined by RFC1305. It is used to perform time synchronization between the distributed time server and clients. NTP transmits data based on UDP, using UDP port 123.

NTP is used to perform time synchronization on all devices with clocks in the network. Therefore, these devices can provide various applications based on the uniformed time. In addition, NTP can ensure a very high accuracy with an error about 10ms.

Devices, which support NTP, can both be synchronized by other clock sources and can synchronize other devices as the clock source.

The RAX711-L supports performing time synchronization through multiple NTP working modes:

- Server/Client mode

In this mode, the client sends clock synchronization message to different servers. The servers work in server mode automatically after receiving the synchronization message and send response messages. The client receives response messages, performs clock filtering and selection, and is synchronized to the preferred server.

In this mode, the client can be synchronized to the server but the server cannot be synchronized to the client.

- Symmetric peer mode

In this mode, the device working in the symmetric active mode sends clock synchronization messages to the device working in the symmetric passive mode. The device that receives this message automatically enters the symmetric passive mode and sends a reply. By exchanging messages, the symmetric peer mode is established between the two devices. Then, the two devices can synchronize, or be synchronized by each other.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ntp server**{ *ip-address* | *ipv6-address* } [**version** [**v1** | **v2** | **v3**]]	(Optional) configure the NTP server address for the client that works in server/client mode.
3	Raisecom(config)#**ntp peer** { *ip-address* | *ipv6-address* } [**version** [**v1** | **v2** | **v3**]]	(Optional) configure the NTP server address for the RAX711-L that works in symmetric peer mode.

Step	Command	Description
4	Raisecom(config)#**ntp refclock-master** [*clock-source*] [*stratum*]	Configure the NTP reference clock source in server/client mode. **Note** If the RAX711-L is configured as the NTP reference clock source, it cannot be configured as the NTP server or NTP symmetric peer; and vice versa.

SNTP

RFC1361 simplifies NTP and provides Simple Network Time Protocol (SNTP). Compared with NTP, SNTP supports the server/client mode only.

In SNTP mode, the RAX711-L only supports working as the SNTP client to be synchronized by the server.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sntp server** { *ip-address* | *ipv6-address* }	(Optional) configure the SNTP server address for the device that works in symmetric peer mode.

1.6.4 Checking configurations

No.	Command	Description
1	Raisecom#**show clock** [**summer-time recurring**]	Show configurations on the system time, time zone, and DST.
2	Raisecom#**show sntp**	Show SNTP configurations.
3	Raisecom#**show ntp status**	Show NTP configurations.
4	Raisecom#**show ntp associations** [**detail**]	Show NTP association configurations.

1.7 Configuring static route

You can configure static routes for the network with a simple topology. You need to configure static routes manually to create an intercommunication network. Before configuring static routes, configure the IP address of the Layer 3 interface properly.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip route** [*ip-address ip-mask* | *ip-address/0* | *ip-address/M*] *next-hop-ip-address*	Configure the static route to the destination network whose IP address is set to *ip-address*,
3	Raisecom(config)#**ip route static distance** *distance*	Configure the default management distance of the static route. By default, the default management distance is set to 1.
4	Raisecom(config)#**show ip route** [*dest-ip-address* | **detail** | **ip-access-list** *acl-id* | **protocol** { **direct** | **static** } | **statistics**]	Show static routing table configurations.

1.8 NDP

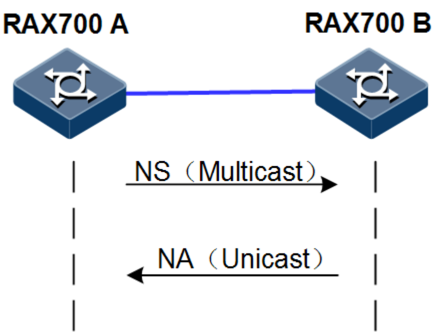
1.8.1 Introduction

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

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

As shown in Figure 1-12, take RAX700 A for example. RAX700 A needs to obtain the data link layer address of RAX700 B, and the detailed procedure is as below.

Figure 1-12 Principle of NDP address resolution



- RAX700 A sends a NS message in multicast mode. The source address of the NS message is the IPv6 address of Layer 3 interface on RAX700 A, and the destination address of the NS message is the multicast address of the requested node of the RAX700 B. The NS message even contains the data link layer address of RAX700 A.
- After receiving the NS message, RAX700 B judges whether the destination address of the NS message is the multicast address of the request node corresponding to the IPv6 address of RAX700 B. If yes, RAX700 B can obtain the data link layer address of

RAX700 A, and sends a NA message which contains its data link layer address in unicast mode.

- After receiving the NA message from RAX700 B, RAX700 A obtains the data link layer address of RAX700 B.

By sending ICMPv6 message, IPv6 NDP even has the following functions:

- Verify whether the neighbor is reachable.
- Detect duplicated addresses.
- Discover routers or prefix.
- Automatically configure addresses.
- Support redirection.

1.8.2 Preparing for configurations

Scenario

IPv6 NDP not only implements IPv4 ARP, ICMP redirection, and ICMP device discovery, but also supports detecting whether the neighbor is reachable.

Prerequisite

- Connect related interfaces and configure physical parameters of them to make the physical layer Up.
- Configure the IPv6 address of the Layer 3 interface.

1.8.3 NDP default configuration

Default configurations of NDP are as below.

Function	Default
Times of sending NS messages for detecting duplicated addresses	1
Maximum number of NDPs allowed to learn	512

1.8.4 Configuring static neighbour entries

To resolute the IPv6 address of a neighbor into the data link layer address, you can use the NS message and NA message, or manually configure static neighbor entries.

Configure static neighbor entries for the RAX700 as below.

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

1.8.5 Configuring times of sending NS messages for detecting duplicated addresses

Configure times of sending NS messages for detecting duplicated addresses for the RAX700 as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
3	Raisecom(config-ip)#**ipv6 nd dad attempts** *value*	Configure times of sending NS messages for detecting duplicated addresses.

Note

When the RAX700 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 a specified times and receiving no response, it determines that the IPv6 address is not duplicated and thus can be used

1.8.6 Configuring maximum number of NDPs allowed to learn on Layer 3 interface

Configure the maximum number of NDPs allowed to learn on the Layer 3 interface for the RAX700 as below.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode
2	Raisecom(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
3	Raisecom(config-ip)#**ipv6 neighbors max-learning-num** *number*	Configure the maximum number of NDPs allowed to learn on the Layer 3 interface.

1.8.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show ipv6 neighbors**	Show all NDP neighbor information.
2	Raisecom#**show ipv6 neighbors** *ipv6-address*	Show neighbor information about a specified IPv6 address.
3	Raisecom#**show ipv6 neighbors ip** *if-number*	Show neighbor information about a specified layer 3 interface.

No.	Command	Description
4	Raisecom#**show ipv6 neighbors static**	Show information about IPv6 static neighbor.
5	Raisecom#**show ipv6 interface prefix** [**ip** *if-number*]	Show prefix information about the IPv6 address.
6	Raisecom#**show ipv6 interface nd** [**ip** *if-number*]	Show ND information configured on the interface.

1.8.8 Maintenance

Maintain the RAX700 as below.

Command	Description
Raisecom(config)#**clear ipv6 neighbors**	Clear all IPv6 neighbor information.

1.9 Configuring Ethernet interface

1.9.1 Configuring basic attributies of interfaces

The interconnected devices cannot communicate normally if their interface attributes, such as Maximum Transmission Unit (MTU), duplex mode, and speed, are inconsistent. You have to adjust the interface attributes to make the devices at two ends match with each other.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**system mtu** *size*	Configure the MTU for all interfaces. MTU is the maximum number of bytes allowed to pass through the interface (without fragmentation). When the length of the forward message exceeds the maximum value, the device will discard this message automatically. By default, the MTU of the interface is set to 1526 bytes.
3	Raisecom(config)#**interface** *interface-type interface-list*	Enter Ethernet electrical interface configuration mode.
4	Raisecom(config-port)#**duplex** { **auto** | **full** | **half** }	Configure the duplex mode of the interface. By default, the duplex mode is set to **auto**.
5	Raisecom(config-port)#**speed** { **auto** | **10** | **100** | **1000** }	Configure the speed of the interface. By default, the speed is automatically negotiated.
6	Raisecom(config-port)#**phy mode** { **auto** | **master** | **slave** }	Configure the Phy mode of the interface. By default, it is auto-negotiation.

1.9.2 Configuring interface statistics

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**dynamic statistics time** *period*	Configure the interval for interface dynamic statistics. By default, the interval is set to 3s.
3	Raisecom(config)#**clear interface** *interface-type interface-number* **statistics**	Clear interface statistics saved at the device.

1.9.3 Configuring flow control on interfaces

When speeds of interface for sending and receiving data are inconsistent, data will overflow. Therefore, there should be a mechanism (flow control) to coordinate the 2 interfaces for sending and receiving data properly.

- Half duplex: back-pressure flow control is adopted to emulate collision in Ethernet. In half duplex Ethernet, when a collision occurs, the Tx host will stop sending data. Emulation makes the host with a greater speed stop sending data to control the traffic. Back-pressure flow control is realized through hardware without being configured manually.
- Full duplex: IEEE 802.3x flow control is adopted. After the client sends a request to the server, when the Autonomous System (AS)/network is congested, the client will sends a PAUSE frame to the server to make the server stop sending data to the client.

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)#**flowcontrol** { **receive** | **send** } **on**	Enable IEEE 802.3x flow control on interfaces. By default, IEEE 802.3x flow control is disabled on interfaces.

1.9.4 Opening/Shuting down interfaces

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)#**shutdown**	Shut down the current interface. By default, the interface is open. You can use the **no shutdown** command to re-open an interface after it is shut down.

Step	Command	Description
4	Raisecom(config-port)#**force-transmit enable**	Enable unidirectional force transmission on interfaces.

1.9.5 Checking configurations

No.	Command	Description
1	Raisecom#**show interface** *interface-type interface-list* [**statistics**]	Show interface status.
2	Raisecom#**show system mtu**	Show the system MTU.
3	Raisecom#**show interface** *interface-type interface-list* **statistics dynamic** [**detail**]	Show interface statistics.
4	Raisecom#**show interface** *interface-type interface-list* **flowcontrol**	Show interface flow control information.
5	Raisecom#**show interface force-transmit**	Show unicast forced transmission configurations.
6	Raisecom#**show interface** { **client** *client-number* | **line** *line-number* } **phy mode**	Show the Phy mode of the interface.
7	Raisecom#**show running interface** [*interface-type interface-list* | **port-channel** *port-channel-id*]	Show operating configurations of the interface.

1.10 Configuring SNMP

1.10.1 Configuring IP address of SNMP interface

To perform out-of-band management on the RAX711-L through the SNMP interface, you should configure the IP address of the SNMP interface.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**management-port ip address** *ip-address* [*ip-mask*]	Configure the IP address of the SNMP interface. By default, it is set to 192.168.4.28 and the subnet mask is set to 255.255.255.0.

1.10.2 Configuring SNMP basic functions

Configuring SNMP v1 and SNMP v2c

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server community** *name* [**view** *view*] { **ro** | **rw** }	Create the community name and configure the related view and authority.
3	Raisecom(config)#**snmp-server contact** *contact*	(Optional) configure the identifier and contact mode of the administrator.
4	Raisecom(config)#**snmp-server group** *name* **user** *user* { **v1sm** | **v2csm** | **usm** }	(Optional) configure the mapping between the user and the access group.
5	Raisecom(config)#**snmp-server location** *location*	(Optional) specify the physical location of the RAX711-L.

Configuring SNMP v3

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** { **authnopriv** | **authpriv** | **noauthnopriv** }	Create and configure the SNMP access group.
3	Raisecom(config)#**snmp-server contact** *syscontact*	(Optional) configure the identifier and contact mode of the administrator.
4	Raisecom(config)#**snmp-server location** *sysLocation*	(Optional) specify the physical location of the RAX711-L.
5	Raisecom(config)#**snmp-server user** *user-name* [**remote** *engine-id*] [{ **authentication** | **authkey** } { **md5** | **sha** } *password* [**privacy** *password*]]	Create the user name and configure the authentication mode.
6	Raisecom(config)#**snmp-server view** *view-name* *oid-tree* [*mask*] { **included** | **excluded** }	Configure the SNMP view.

1.10.3 Configuring Trap

Trap means refers to unrequested information sent to the NView NNM system automatically, which is used to report some critical events.

Before configuring Trap, you should configure the SNMP target host.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server host** { *ip-address* | *ipv6-address* } **version** { **1** | **2c** } *name* [**udpport** *port-id*]	Configure SNMP v1-/SNMP v2c-based Trap target host.
	Raisecom(config)#**snmp-server host** { *ip-address* | *ipv6-address* } **version 3** { **authnopriv** | **authpriv** | **noauthnopriv** } *name* [**udpport** *port-id*]	(Optional) configure SNMP v3-based Trap target host.
3	Raisecom(config)#**snmp-server enable traps**	Enable Trap.
4	Raisecom(config)# **snmp-server keepalive-trap** { **enable** | **disable** | **interval** *interval* | **pause** }	(Optional) configure Keepalive Trap feature.

1.10.4 Checking configurations

No.	Command	Description
1	Raisecom#**show management-port ip-address**	Show the IP address of the SNMP interface.
2	Raisecom#**show snmp access**	Show SNMP access group configurations.
3	Raisecom#**show snmp community**	Show SNMP community configurations.
4	Raisecom#**show snmp config**	Show SNMP basic configurations.
5	Raisecom#**show snmp group**	Show the mapping between SNMP users and the access group.
6	Raisecom#**show snmp host**	Show Trap target host information.
7	Raisecom#**show snmp statistics**	Show SNMP statistics.
8	Raisecom#**show snmp user**	Show SNMP user information.
9	Raisecom#**show snmp view**	Show SNMP view information.

1.11 Configuring Banner

1.11.1 Preparing for configurations

Scenario

Banner is a message to display when you log in to or log out of the RAX711-L, such as the precautions or disclaimer.

You can configure Banner of the RAX711-L as required. After Banner display is enabled, the configured Banner information appears when you log in to or log out of the RAX711-L.

Prerequisite

N/A

1.11.2 Configuring Banner

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**banner login** *word* Enter text message followed by the character '*word*' to finish.User can stop configuration by inputing' Ctrl+c' *message word*	Configure the Banner contents. **Note** • The *word* parameter is a 1-byte character. It is the beginning and end marker of the Banner contents. These 2 marks must be the identical character. • The *message* parameter is the Banner contents. Up to 2560 characters are supported.

1.11.3 Enabling Banner display

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**banner enable**	Enable Banner display. By default, Banner display is disabled.
3	Raisecom(config)#**write**	Save Banner configurations to ensure saving them after the RAX711-L is rebooted.

1.11.4 Checking configurations

No.	Command	Description
1	Raisecom#**show banner login**	View Banner status and configured Banner contents.

1.12 Configuration examples

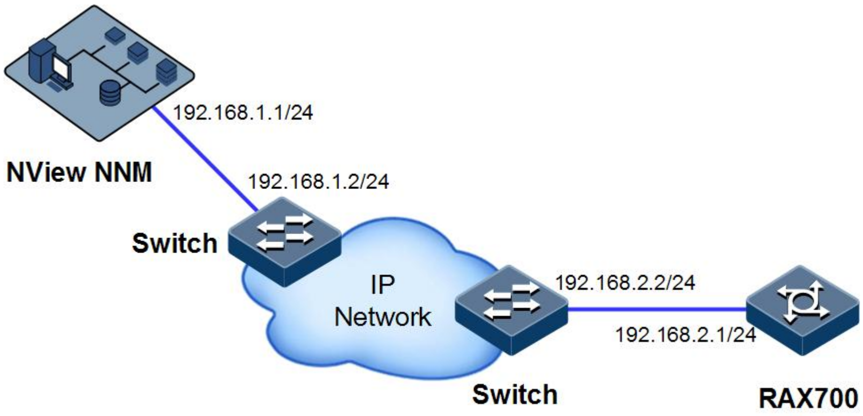
1.12.1 Example for configuring SNMP

Networking requirements

As shown in Figure 1-13, the route between the NView NNM system and RAX711-L is reachable. The IP address and sub-net mask of the NView NNM system are set to 192.168.1.1 and 255.255.255.0 respectively.

The IP address of the RAX711-L Ethernet interface connected to the network is set to 192.168.2.1. The NView NNM system manages the RAX711-L through the switch.

Figure 1-13 Configuring SNMP



Configuration steps

Step 1 Configure the IP address of the SNMP interface.

```
Raisecom#config
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address 192.168.2.1 255.255.255.0 1
```

Step 2 Configure the static route between the NView NNM system and the RAX711-L.

```
Raisecom(config)#ip route 192.168.1.0 255.255.255.0 192.168.2.2
```

Step 3 Configure the SNMP community.

```
Raisecom(config)#snmp-server community raisecom rw
Raisecom(config)#snmp-server community raisecom ro
```

Step 4 Configure the SNMP Trap target address.

```
Raisecom(config)#snmp-server host 192.168.1.1 version 2c raisecom
Raisecom(config)#exit
```

Step 5 Save configurations.

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

Checking results

Use the **show ip route** command to show static route configurations.

```
Raisecom(config)#show ip route
Codes: C - Connected, S - Static, R - RIP, O - OSPF
-----------------------------------------------------------
S   192.168.1.0[255.255.255.0],Via 192.168.2.2
C   192.168.18.0[255.255.255.0],is directly connected , Interface 0
Total route count: 2
```

Use **show snmp community** the command to show SNMP community configurations.

```
Raisecom#show snmp community
Index   Community Name     View Name         Permission
------------------------------------------------------------
1        raisecom           internet          rw
2        raisecom           internet          ro
```

2 Ethernet

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

- Configuring MAC address table
- Configuring VLAN
- Configuring basic QinQ
- Configuring selective QinQ
- Configuring loop detection
- Configuring interface protectionSTP/RSTP
- MSTP
- Configuring port mirroring
- Configuring L2CP
- Maintenance
- Configuration examples

2.1 Configuring MAC address table

2.1.1 Preparing for configurations

Scenario

Static MAC addresses need be set for fixed servers, fixed and important hosts for special persons (managers, financial staffs, etc.), to ensure all data traffic to these MAC addresses are correctly forwarded from the interface that is related to these static MAC addresses.

For interfaces with fixed static MAC addresses, you can disable the MAC address learning to avoid other hosts visiting LAN data from these interfaces.

To avoid the explosive growth of MAC address table entries, you need to configure the aging time for a MAC address table.

Prerequisite

N/A

2.1.2 Configuring static MAC address entries

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`mac-address-table static unicast`** *`mac-address`* **`vlan`** *`vlan-id interface-type interface-number`*	Configure static unicast MAC addresses.

2.1.3 Configuring dynamic MAC address entries

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`mac-address-table learning enable`** `{` *`interface-type interface-number`* `|` **`vlanlist`** *`vlan-list`* `}`	Enable MAC address learning. By default, MAC address learning is enabled on the RAX711-L.
3	`Raisecom(config)#`**`mac-address-table aging-time`** `{` **`0`** `|` *`second`* `}`	Configure the aging time of dynamic MAC addresses. By default, the aging time of dynamic MAC addresses is set to 300s.
4	`Raisecom(config)#`**`mac-address-table threshold`** *`threshold-value`* **`vlan`** *`vlan-id`*	Configure VLAN-based MAC address limit threshold. By default, no VLAN-based MAC address limit threshold is configured.
5	`Raisecom(config)#`**`interface`** *`interface-type interface-number`*	Enter physical layer interface configuration mode.
6	`Raisecom(config-port)#`**`mac-address-table threshold`** *`threshold-value`*	Configure interface-based MAC address limit threshold. By default, no interface-based MAC address limit threshold is configured.

2.1.4 Configuring blackhole MAC address entries

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`mac-address-table blackhole`** *`mac-address`* **`vlan`** *`vlan-id`*	Configure the blackhole MAC address.

2.1.5 Configuring MAC address drifting

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

Step	Configuration	Description
2	Raisecom(config)#**mac-address-table mac-move enable**	Enable the inhibition of global MAC address drifting. By default, it is disabled.
3	Raisecom(config)#**mac-address-table trap enable**	Enable the alarm of global MAC address drifting. By default, it is disabled.

2.1.6 Checking configurations

No.	Command	Description
1	Raisecom#**show mac-address-table static** [*interface-type interface-number* | **vlan** *vlan-id*]	Show static MAC addresses.
2	Raisecom#**show mac-address-table l2-address** [**vlan** *vlan-id* | *interface-type interface-number* | **count**]	Show all MAC addresses.
3	Raisecom#**show mac aging-time**	Show the aging time of MAC addresses.
4	Raisecom#**show mac-address-table threshold** [*interface-type interface-list*]	Show MAC address limit configurations.
5	Raisecom#**show mac-address-table blackhole**	Show information about the blackhole MAC address table.
6	Raisecom#**show mac-address-table learning** [*interface-type interface-list*]	Show enabling information about MAC address learning.

2.2 Configuring VLAN

2.2.1 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. All packets to be forwarded carry VLAN Tags. 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 has to carve up VLAN 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.

When you need to configure an IP address for a VLAN, you can relate a Layer 3 interface to the VLAN. Each Layer 3 interface corresponds to an IP address and is related to a VLAN.

Prerequisite

N/A

2.2.2 Configuring VLAN properties

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**create vlan** *vlan-list* { **active** | **suspend** }	Create one or more VLANs.
3	Raisecom(config)#**vlan** *vlan-id*	Enter VLAN configuration mode.
4	Raisecom(config-vlan)#**name** *string*	(Optional) configure the VLAN name.
5	Raisecom(config-vlan)#**state** { **active** | **suspend** }	Activate/Suspend the VLAN.

Note

- VLANs that are created by using the **vlan** *vlan-id* command are in Suspend status. If you need them to take effect, you need to use the **state** command to activate them.
- By default, there is a VLAN in the system, that is, the default VLAN (VLAN 1). The default VLAN (VLAN 1) cannot be deleted.
- By default, the default VLAN (VLAN 1) is named as "Default" and the cluster VLAN (VLAN 2) has no name. Other VLANs are named as VLAN+4-digit VLAN ID. For example VLAN 3 is names as VLAN 0003 while VLAN 4094 is named as VLAN 4094.
- All configurations of a VLAN cannot take effect until the VLAN is activated. When a VLAN is in Suspend status, you can also configure the VLAN, such as deleting/adding interfaces. The system will save these configurations. Once the VLAN is activated, these configurations will take effect.

2.2.3 Configuring interface modes

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 mode** { **access** | **trunk** }	Set the interface mode to Access or Trunk.

Step	Command	Description
4	Raisecom(config-port)# **switchport reject-frame** { **tagged** | **untagged** }	(Optional) configure the packet type which is not allowed to be received by the interface in ingress direction. Through this configuration, you can directly reject the packet carrying the VLAN Tag or not.

2.2.4 Configuring VLANs based on Access interfaces

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 mode access** Raisecom(config-port)#**switchport access vlan** *vlan-id*	Set the interface mode to Access and add Access interfaces to the VLAN.
4	Raisecom(config-port)#**switchport access egress-allowed vlan** { **all** | [**add** | **remove**] *vlan-list* } [**confirm**]	(Optional) configure the allowed VLANs of the Access interface.

Note

- By default, the Access interface does not belong to any VLAN.
- The interface permits Access VLAN packets passing regardless of configurations for VLAN list on the Access interface. The forwarded packets do not carry VLAN Tag.
- When configuring Access VLAN, the system will automatically create and activate a VLAN if you do not create and activate the VLAN in advance.
- If you manually delete an Access VLAN, the system will automatically configure the Access VLAN as VLAN 0.

2.2.5 Configuring VLANs based on Trunk interfaces

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 mode trunk**	Set the interface mode to Trunk.
4	Raisecom(config-port)#**switchport trunk native vlan** *vlan-list*	Configure interface Native VLAN.
5	Raisecom(config-port)#**switchport trunk allowed vlan** { **all** | *vlan-list* } [**confirm**] Raisecom(config-port)#**switchport trunk allowed vlan** { **add** *add-vlan-list* | **remove** *vlan-list* }	(Optional) configure the allowed VLANs of the Trunk interface.

Step	Command	Description
6	Raisecom(config-port)#**switchport trunk untagged vlan** { **all** | *vlan-list* } [**confirm**] Raisecom(config-port)#**switchport trunk untagged vlan** { **add** *vlan-list* | **remove** *vlan-list* }	(Optional) configure VLANs whose Tags can be deleted on the Trunk interface.

Note

- By default, the Trunk interface does not belong to any VLAN.
- The Trunk interface permits Native VLAN packets passing 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 and activate the VLAN in advance.
- If you manually delete a Native VLAN, the system will automatically set the interface Trunk Native VLAN as the default VLAN 0.
- 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 forwarded as original.
- When configuring a Trunk Untag VLAN list, the system automatically adds all Untagged VLAN to the Trunk allowed VLAN.

2.2.6 Checking configurations

No.	Command	Description
1	Raisecom#**show vlan**	Show VLAN configurations.
2	Raisecom#**show interface** *interface-type interface-number* **switchport**	Show interface VLAN configurations.

2.3 Configuring basic QinQ

2.3.1 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 ISP network can be transparently transmitted, without conflicting with the VLAN ID in Carrier network.

Prerequisite

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

2.3.2 Configuring basic QinQ

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)# **mls double-tagging inner-tpid** *tpid*	(Optional) configure the TPID of the global inner Tag.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#**mls double-tagging tpid** *tpid*	(Optional) configure the outer TPID of the interface.
5	Raisecom(config-port)#**switchport qinq dot1q-tunnel**	Enable basic QinQ on the interface.
6	Raisecom(config-port)#**switchport access vlan** *vlan-id*	Add the Access interface to the VLAN.
7	Raisecom(config-port)#**switchport trunk native vlan** *vlan-id*	Add the Trunk interface to the VLAN.

2.3.3 Configuring egress interface to Trunk 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)#**switchport mode trunk**	Configure the egress interface to Trunk mode, allowing double Tag packets to pass.

2.3.4 Checking configurations

No.	Command	Description
1	Raisecom#**show switchport qinq**	Show basic QinQ configurations.

2.4 Configuring selective QinQ

2.4.1 Preparing for configurations

Scenario

Differentiated from basic QinQ, the outer VLAN Tag for selective QinQ can be selected according to service types. Set different VLAN IDs for services in the user network. Differentiate voice, video and data services in the ISP by adding different outer VLAN Tags to classify services when forwarding them, realizing the VLAN mapping between inner and outer VLAN tags.

Prerequisite

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

2.4.2 Configuring selective QinQ

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls double-tagging inner-tpid** *tpid*	(Optional) configure the TPID value of the inner Tag.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#**mls double-tagging tpid** *tpid*	Configure the TPID value of the outer VLAN Tag on the interface.
5	Raisecom(config-port)#**switchport vlan-mapping cvlan** *vlan-list* [**cos** *cos-value1*] **add-outer** *vlan-id* [**cos** *cos-value2*]	Configure selective QinQ rules on the interface in ingress direction.
	Raisecom(config-port)#**switchport vlan-mapping both cvlan** *vlan-id* [**cos** *cos-value1*] **add-outer** *vlan-id* [**cos** *cos-value2*]	Configure dual-layer VLAN for the Untagged packets on the interface.
	Raisecom(config-port)#**switchport vlan-mapping both cvlan** *vlan-id* **add-outer** *vlan-id* [**cos** *cos-value*] { **translate** *vlan-id* | **remove** }	Configure dual-layer VLAN for the Untagged packets on the interface.
	Raisecom(config-port)#**switchport vlan-mapping both cvlan** *vlan-id* **cos** *cos-value1* **add-outer** *vlan-id* [**cos** *cos-value2*] { **translate** *vlan-id* | **remove** }	Configure outer VLAN for packets with CVLAN and CoS on the interface.
	Raisecom(config-port)#**switchport vlan-mapping both outer** *vlan-id* [**inner** *vlan-id*] **translate** *vlan-id1* [*vlan-id2*] [**cos** *cos-value*]	Configure packets with outer VLAN Tag or dual-layer VLAN Tag on the interface converting as VLAN Tag.

Step	Command	Description
	Raisecom(config-port)#**switchport vlan-mapping both priority-tagged cos** *cos-value1* **add-outer** *vlan-id* [**cos** *cos-value2*]	Configure packets with priority Tag and CoS on the interface adding outer VLAN.
	Raisecom(config-port)#**switchport vlan-mapping both** { **untag** | **priority-tagged** } **add-outer** *vlan-id* [**cos** *cos-value*]	Configure packets with Untagged or priority Tag adding outer VLAN on the interface.
6	Raisecom(config-port)# **switchport vlan-mapping-miss discard**	(Optional) configure discarding unmatched packets on the interface in ingress direction.

Note

If you have configured selective QinQ based on VLAN+CoS, or specified the CoS value of the added outer Tag, you need to use the **no switchport qinq** command on the interface to disable basic QinQ.

2.4.3 Checking configurations

No.	Command	Description
1	Raisecom(config)#**show switchport qinq**	Show basic QinQ configurations.
2	Raisecom(config)#**show interface** *interface-type interface-number* **vlan-mapping add-outer**	Show selective QinQ configurations on the interface.
3	Raisecom(config)#**show vlan-mapping both interface** *interface-type interface-number*	Show QinQ rules in both the ingress and egress direction on the interface.

2.5 Configuring VLAN mapping

2.5.1 Preparing for configurations

Scenario

Differentiated from QinQ, VLAN mapping only changes VLAN tag but does not encapsulate additional multilayer VLAN Tag. You just need to change VLAN Tag to make packets transmitted according to Carrier VLAN mapping rules, without increasing frame length of the original packet. VLAN mapping is used in following situations:

- Map user services into one carrier VLAN ID.
- Map multi-user services into one carrier VLAN ID.

Prerequisite

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

2.5.2 Configuring 1:1 VLAN mapping

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 vlan-mapping** { **ingress** | **egress** } *vlan-list id* **translate** *vlan-id*	Configure 1:1 VLAN mapping rules based on the ingress/egress interface. When configuring 1:1 VLAN mapping, you should configure VLAN mapping rules on both the ingress and egress interfaces.
	Raisecom(config-port)**switchport vlan-mapping egress outer** *vlan-id* [**cos** *cos-value*] [**inner** *vlan-id*] [**cos** *cos-value*] **translate** [**outer-vid** *vlan-id*] [**outer-cos** *cos-value*] [**inner-vid** *vlan-id*] [**inner-cos** *cos-value*]	Configure 1:1 double-Tag VLAN mapping rules based on the egress interface. Configure 1:1 VLAN mapping based on the outer VLAN ID, outer CoS, inner VLAN ID, and inner CoS respectively.
4	Raisecom(config-port)#**switchport vlan-mapping-miss discard**	(Optional) configure discarding unmatched packets on the interface in ingress direction.

Note

For packets complying with the VLAN mapping rules, forward them after VLAN mapping. That is, the forwarded VLAN is the mapped VLAN and the MAC address of the packet is learnt from the mapped VLAN.

2.5.3 Checking configurations

No.	Command	Description
1	Raisecom#**show interface** *interface-type interface-number* **vlan-mapping** { **egress** | **ingress** } **translate**	Show 1:1 VLAN mapping configurations.

2.6 Configuring loop detection

2.6.1 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 loopback is detected on a port, the interface will be blocked.

Prerequisite

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

2.6.2 Configuring loop detection

Note

- Loopback 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 on both ends will be blocked.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**loopback-detection enable** *interface-type interface-list*	Enable loop detection on an interface. By default, enable loop detection on user's interface. Disable loop detection on the line interface and aggregation group interface.
3	Raisecom(config)#**loopback-detection mode** { **port-based** | **vlan-based** }	(Optional) configure the loop detection mode. By default, the loop detection is set to VLAN-based loop detection.
4	Raisecom(config)#**loopback-detection loop** { **discarding** | **trap-only** | **shutdown** } *interface-type interface-list*	(Optional) configure the mode for an interface to process loop detection packets from other interfaces. **Note** To ensure that loop detection runs properly, we recommend selecting the **discarding** mode. In addition, the RAX711-L supports up to 15 VLAN-based loop detection.
5	Raisecom(config)#**loopback-detection hello-time** *period*	Configure the interval for sending loop detection packet. By default, the interval is set to 4s.

Step	Command	Description
6	Raisecom(config)#**loopback-detection down-time** { *second* | **infinite** }	(Optional) configure the time to automatically restore the blocked interface caused by loopback. By default, it is set to **infinite**.
7	Raisecom(config)#**loopback-detection loop upstream** *interface-type interface-list* [**delete-vlan**]	(Optional) configure the processing mode of the uplink interface when it detects a loopback.
8	Raisecom(config)#**loopback-detection port-based vlan** *vlan-id*	(Optional) configure the VLAN ID of the interface enabled with loop detection.
9	Raisecom(config)#**loopback-detection log-interval** *interval*	(Optional) configure the interval for outputting log for the loop detection. By default, it is 0 minute.

2.6.3 Checking configurations

No.	Command	Description
1	Raisecom#**show loopback-detection** [*interface-type interface-list*]	Show interface-based loop detection configurations.
2	Raisecom#**show loopback-detection statistics** [*interface-type interface-list*]	Show loop detection statistics.
3	Raisecom#**show loopback-detection block-vlan** [*interface-type interface-list*]	Show information about the blocked VLAN.
4	Raisecom#**show loopback-detection vlan-list** *vlan-list*	Show VLAN-based loop detection configurations.

2.7 Configuring interface protection

2.7.1 Preparing for configurations

Scenario

To isolate Layer 2/Layer 3 data in an interface protection group and provide physical isolation between interfaces, you need to configure interface protection.

By adding interfaces that need to be controlled to an interface protection group, you can enhance network security and provide flexible networking scheme.

Prerequisite

N/A

2.7.2 Configuring interface protection

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 protect**	Enable interface protection. By default, downlink interfaces are isolated from each other.

2.7.3 Checking configurations

No.	Command	Description
1	Raisecom#**show switchport protect**	Show interface protection configurations.

2.8 STP/RSTP

2.8.1 Introduction

STP

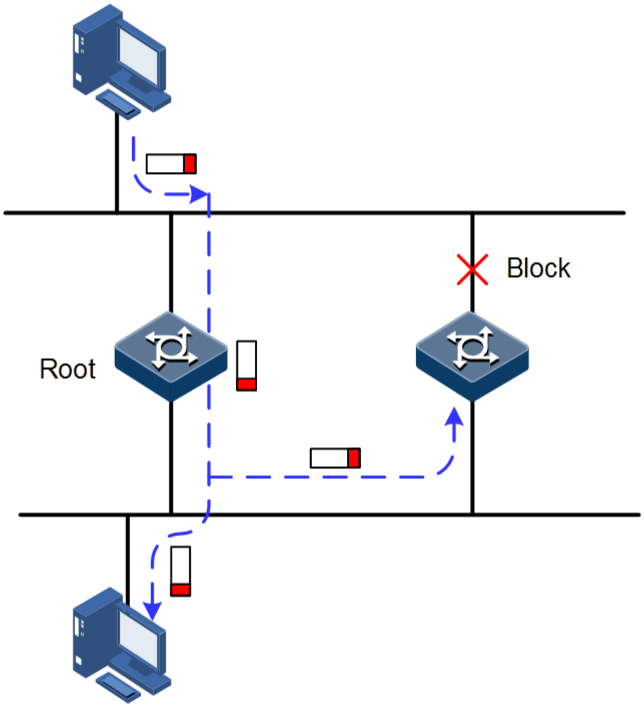
With the increasing complexity of network structure and growing number of switches on the network, the Ethernet network loops become the most prominent problem. Because of the packet broadcast mechanism, a loop causes the network to generate storms, exhaust network resources, and have serious impact to forwarding normal data.

Spanning Tree Protocol (STP) is compliant to IEEE 802.1d standard and used to remove data physical loop in data link layer in the LAN.

The RAX700 running STP can process Bridge Protocol Data Unit (BPDU) with each other for the election of root switch and selection of root port and designated port. It also can block loop interface on the RAX700 logically according to the selection results, and finally trims the loop network structure to tree network structure without loop which takes an RAX700 as root. This prevents the continuous proliferation and limitless circulation of packet on the loop network from causing broadcast storms and avoids declining packet processing capacity caused by receiving the same packets repeatedly.

Figure 2-1 shows loop networking running STP.

Figure 2-1 Loop networking with STP



Although STP can eliminate loop network and prevent broadcast storm well, its shortcomings are still gradually exposed with thorough application and development of network technology.

The major disadvantage of STP is the slow convergent speed.

RSTP

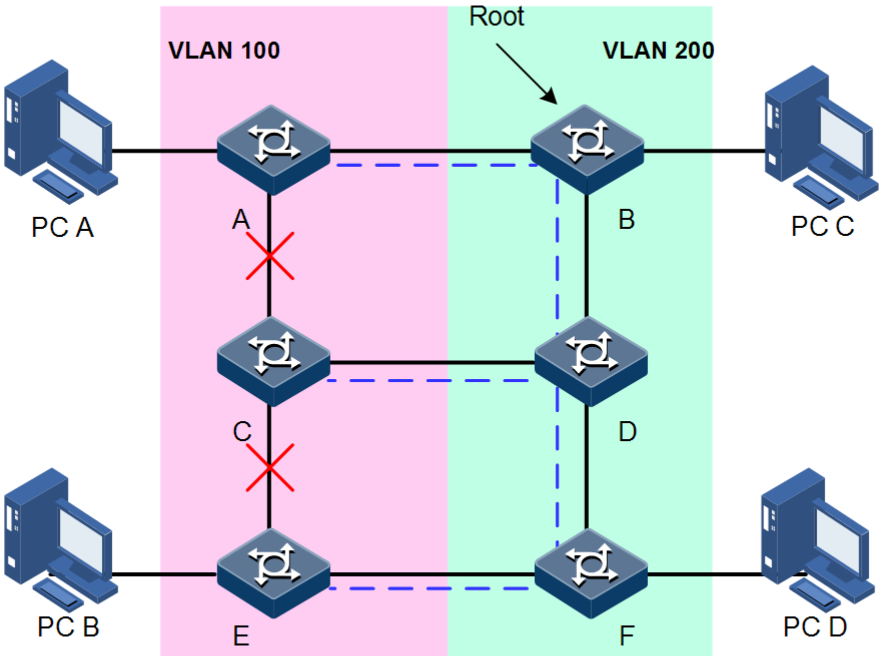
For improving the slow convergent speed of STP, IEEE 802.1w establishes Rapid Spanning Tree Protocol (RSTP), which increases the mechanism to change interface blocking state to forwarding state, speed up the topology convergence rate.

The purpose of STP/RSTP is to simplify a bridge connection LAN to a unitary spanning tree in logical topology and to avoid broadcast storm.

The disadvantages of STP/RSTP are exposed with the rapid development of VLAN technology. The unitary spanning tree simplified from STP/RSTP leads to the following problems:

- The whole switching network has only one spanning tree, which will lead to longer convergence time on a larger network.
- After a link is blocked, it does not carry traffic any more, causing waste of bandwidth.
- Packet of partial VLAN cannot be forwarded when network structure is unsymmetrical. As shown in Figure 2-2 B is the root switch; RSTP blocks the link between A and C logically and makes that the VLAN 100 packet cannot be transmitted, and A and C cannot communicate.

Figure 2-2 packet forward failure due to RSTP



2.8.2 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 loop among them, MAC address learning fault, and broadcast storm and network crash caused by quick copy and transmission of data frames. STP calculation can block one interface in a broken loop and ensure there is only one path for the data flow to be transmitted to the destination host t, which is also the best path.

Prerequisite

Configure interface physical parameters to make it Up.

2.8.3 Enabling STP

Configure STP for the RAX700 as below

Step	**Configuration**	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`spanning-tree enable`**	Enable global STP. By default, disable global STP.
3	`Raisecom(config)#`**`spanning-tree mode`** `{` **`stp`** `|` **`rstp`** `}`	Configure running mode of the spanning tree
4	`Raisecom(config)#`**`interface`** *`interface-type interface-number`*	Enter configuration mode on the physical layer interface.

Step	Configuration	Description
5	Raisecom(config-port)#**spanning-tree enable**	Enable STP on the interface. By default, enable STP on the interface.

2.8.4 Configuring STP parameters

Configure STP parameters for the RAX700 as below

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**spanning-tree priority** *priority-value*	(Optional) configure device priority. By default, it is 32768.
4	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**spanning-tree priority** *priority-value*	(Optional) configure priority on the interface. By default, it is 128.
5	Raisecom(config-port)#**spanning-tree extern-path-cost** *cost-value* Raisecom(config-port)#**exit**	(Optional) configure extern-path cost of the interface. By default, it is 200000.
6	Raisecom(config)#**spanning-tree hello-time** *value*	(Optional) configure Hello Time. By default, it is 2s.
7	Raisecom(config)#**spanning-tree transit-limit** *value*	(Optional) configure maximum transmission rate of interface. By default, Hello Time send up to three BPDU packets.
8	Raisecom(config)#**spanning-tree forward-delay** *value*	(Optional) configure Forward Delay. By default, it is 15s.
9	Raisecom(config)#**spanning-tree max-age** *value*	(Optional) configure Max Age. By default, it is 20s.

2.8.5 (Optional) configuring RSTP edge interface

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

The edge interface can change the interface status to forward quickly without any waiting time. You had better set the Ethernet interface connected to user client as edge interface to make it quick to change to forward status.

The edge interface attribute depends on actual condition when it is in auto-detection mode; the real port will change to false edge interface after receiving BPDU when it is in force-true mode; when the interface is in force-false mode, whether it is true or false edge interface in real operation, it will maintain the force-false mode until the configuration is changed.

By default, all interfaces on the RAX are set in auto-detection attribute.

Step	Configuration	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 RSTP edge interface.

2.8.6 (Optional) configure RSTP link type

Two interfaces connected by a point-to-point link can quickly transit to forward 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 configure this item in auto status and the system will automatically detect whether the interface is connected to a point-to-point link.

Configure link type for the RAX as below

Step	Configuration	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 link type for interface.

2.8.7 Checking configurations

Use the following commands to check configuration results

No.	Command	Description
1	`Raisecom#`**`show spanning-tree`** `[` **`instance`** *`instance-id`* `] [` **`detail`** `]`	Show basic STP configuration.
2	`Raisecom#`**`show spanning-tree`** `[` **`instance`** *`instance-id`* `]` *`interface-type interface-list`* `[` **`detail`** `]`	Show spanning tree configuration on the interface.

2.9 MSTP

2.9.1 Introduction

Multiple Spanning Tree Protocol (MSTP) is defined by the IEEE 802.1s standard.

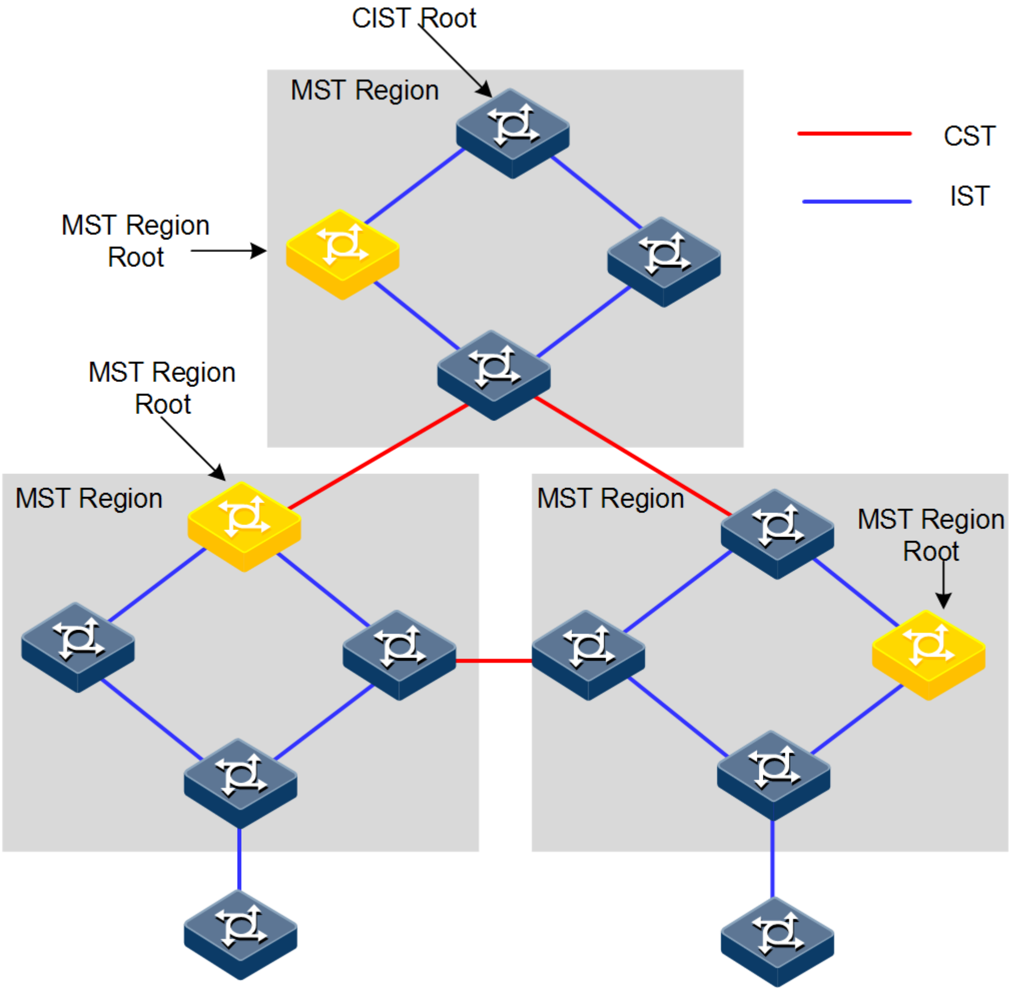
Recovering the disadvantages of STP and RSTP, the MSTP realizes fast convergence and distributes different VLAN flows following their own paths to provide an excellent load sharing mechanism

MSTP divides a switching network into multiple domains, called MST domain. Each MST domain contains several spanning trees but the trees are independent from each other. Each spanning tree is called a Multiple Spanning Tree Instance (MSTI).

MSTP protocol introduces Common Spanning Tree (CST) and Internal Spanning Tree (IST) concepts. CST refers to taking MST domain as a whole to calculate and generating a spanning tree. IST refers to generating spanning tree in internal MST domain.

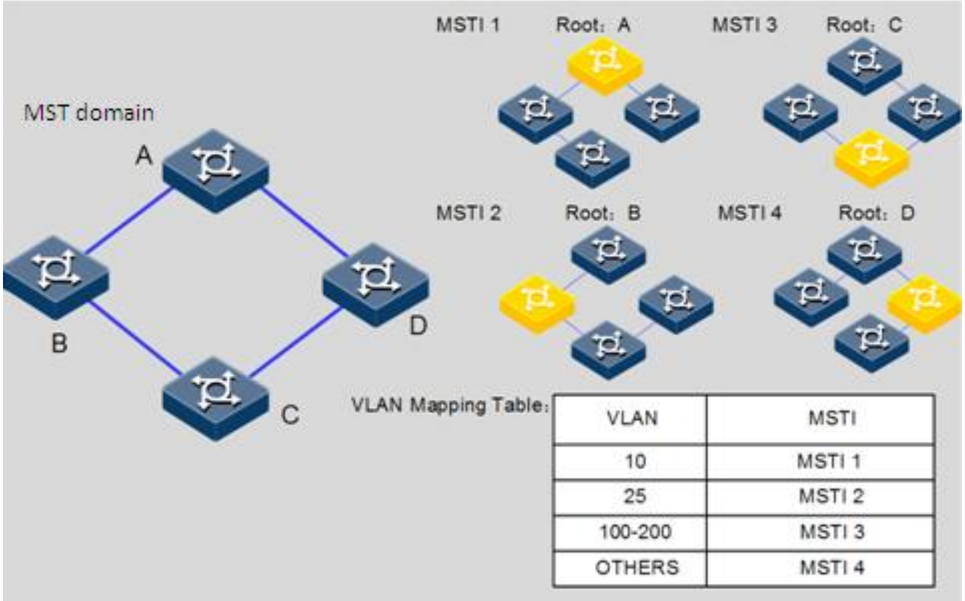
Compared with STP and RSTP, MSTP also introduces a CIST root and MST region root. The CIST root is a global concept; all switches running STP/RSTP/MSTP can have only one CIST Root. The MST region root is a local concept, which is relative to an instance in a domain. As shown in Figure 2-3, all connected devices only have one total root, and the number of domain root contained in each domain is associated with the number of instances.

Figure 2-3 Basic concepts of MSTP network



There can be different MST instance in each MST domain, which associates VLAN and MSTI by setting VLAN mapping table (relationship table of VLAN and MSTI). The concept sketch map of MSTI is shown in Figure 2-4.

Figure 2-4 Basic concepts of MSTI network



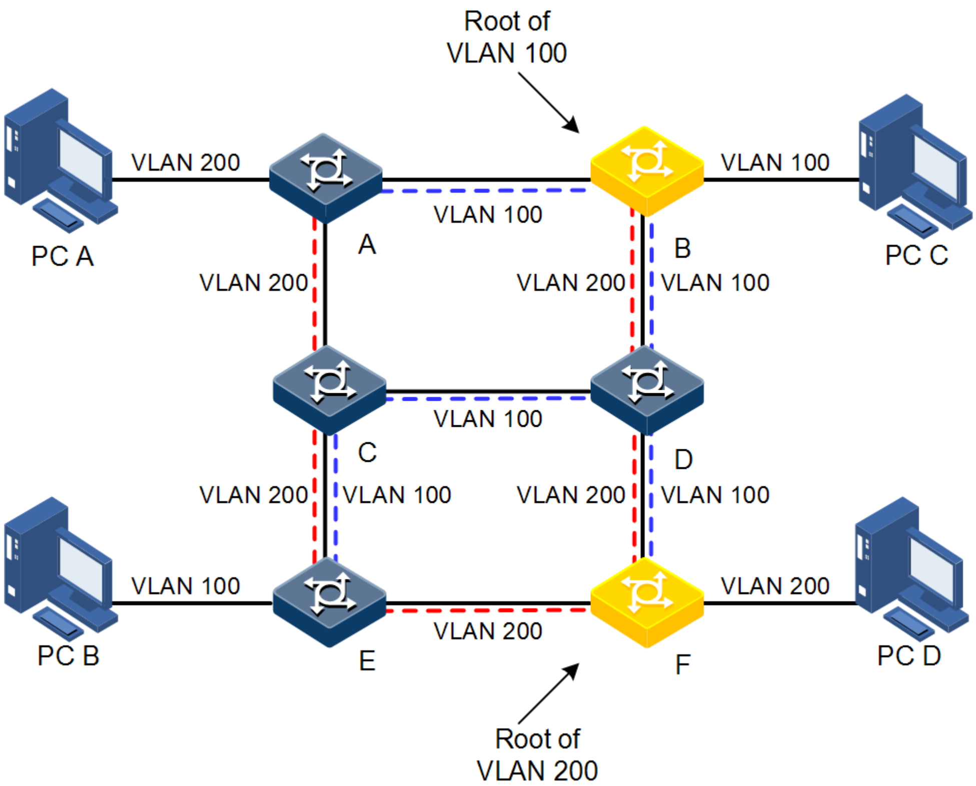
VLAN	MSTI
10	MSTI 1
25	MSTI 2
100-200	MSTI 3
OTHERS	MSTI 4

Note

Each VLAN can map to one MSTI; that is to say, data of one VLAN can only be transmitted in one MSTI while one MSTI may correspond to several VLANs.

Compared with the previous STP and RSTP, MSTP has obvious advantages, including cognitive ability of VLAN, load balance sharing ability, similar RSTP port status switching ability as well as binding multiple VLANs to one MSTI to reduce resource occupancy rate. In addition, MSTP running devices on the network are also compatible with the devices running STP and RSTP.

Figure 2-5 Networking of multiple spanning trees instances in MST domain



Applying MSTP in the network, as shown in Figure 2-5, after calculation, there are two spanning trees generated at last (two MSTIs):

- MSTI 1 takes B as the root switch, forwarding packets of VLAN 100.
- MSTI 2 takes F as the root switch, forwarding packets of VLAN 200.

In this way, all VLANs can communicate internally, different VLAN packets are forwarded in different paths to share load.

2.9.2 Preparing for configurations

Scenario

In big LAN or residential region aggregation, the aggregation devices make up a ring for link backup, at the same time avoid loop and realize service load sharing. MSTP can select different and unique forwarding path for each one or a group of VLANs.

Prerequisite

Configure interface physical parameters to make it Up.

2.9.3 Enabling MSTP

Configure MSTP for the RAX700 as below.

Step	Configuration	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 global STP.
4	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
5	Raisecom(config-port)#**spanning-tree enable**	Enable STP on the interface.

2.9.4 Configuring MST domain and its maximum number of hops

You can set domain information about the RAX700 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 set current device in a specific MST domain through following configuration.

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 once it is forwarded passing a device; the RAX700 discards the configuration message whose number of hops is 0. The device exceeding the maximum number of hops cannot join spanning tree calculation and then restrict MST domain scale.

Configure MSTP domain and its maximum number of hops for the RAX700 as below

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
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*	Set revision level for MST domain.
5	Raisecom(config-region)#**instance** *instance-id* **vlan** *vlan-list* Raisecom(config-region)#**exit**	Set mapping from MST domain VLAN to instance.
6	Raisecom(config)#**spanning-tree max-hops** *hops-value*	Configure the maximum number of hops for 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.

2.9.5 Configuring device interface and system priority

Whether the interface is selected as the root interface depends on interface priority. Under the identical 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 RAX700 can be selected as the root of the spanning tree. Configuring smaller priority helps obtain smaller Bridge ID and designate the RAX700 as the root. If priorities of two RAX700 devices are identical, the RAX700 with smaller MAC address will be selected as the root.

Similar to configuring root and backup root, priority is mutually independent in different instances. You can confirm priority instance through the **instance** *instance-id* parameter. Configure 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 RAX700 as below.

Step	Configuration	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**	Set interface priority for a STP instance.
4	Raisecom(config)#**spanning-tree** [**instance** *instance-id*] **priority** *priority-value*	Set system priority for a STP instance.

Note

The value of priority must be multiples of 4096, like 0, 4096, 8192, etc. It is 32768 by default.

2.9.6 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 CIST, and invalid to MSTI instance. No matter how many nodes in a path in one domain, it is considered as just one node. Actually, network diameter should be defined as the domain number 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 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 RAX700 is configured as the CIST root device can this configuration take effect. MSTP will automatically set the Hello Time, Forward Delay and Max Age parameters to a privileged value through calculation when configuring the network diameter.

Configure the network diameter for the switching network as below.

Step	Configuration	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.

2.9.7 Configuring inner path cost for 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 independently mutually in different instances. You can configure inner path cost for instance through the **instance** *instance-id* parameter. Configure inner path cost of interface for 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 inner path cost for the RAX700 as below.

Step	Configuration	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 inner path cost on the interface. By default, it is 200000.

2.9.8 Configuring external path cost on interface

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 RAX700 as below.

Step	Configuration	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 on interface. By default, it is 200000.

2.9.9 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 RAX700 as below.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**spanning-tree transit-limit** *value*	Configure interface maximum transmission rate. By default, transmit up to three packets.

2.9.10 Configuring MSTP timer

- Hello Time: the RAX700 sends the interval of bridge configurations (BPDU) regularly to check whether there is failure in detection link of the RAX700. The RAX700 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. 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 status remove system: before the root interface and designated interface starts forwarding data, it needs a medium status (learning status); after delay for the interval of Forward Delay, it enters forwarding status. The delay guarantees the new configuration message to be transmitted through whole network. You can adjust the delay according to actual condition; namely, reduce it when 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 RAX700 will discard outdated

configurations and STP will recalculate spanning tree. The default value is 20s. Over short age may cause frequent recalculation of the spanning tree, while over greater age value will make STP not adapt to network topology change timely.

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

Configure the MSTP timer for the RAX700 as below.

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

2.9.11 Configuring edge interface

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

The edge interface can change the interface status to forward quickly without any waiting time. You had better set the Ethernet interface connected to user client as edge interface to make it quick to change to forward status.

The edge interface attribute depends on actual condition when it is in auto-detection mode; the real port will change to false edge interface after receiving BPDU when it is in force-true mode; when the interface is in force-false mode, whether it is true or false edge interface in real operation, it will maintain the force-false mode until the configuration is changed.

By default, all interfaces on the RAX700 are set in auto-detection attribute.

Configure the edge interface for the RAX700 as below.

Step	Configuration	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 RSTP edge interface.

2.9.12 Configuring BPDU filtering

When the BPDU filtering on the edge interface is enabled, edge interface does not send BPDU packets or deal with the received BPDU packets.

Configure the BPDU filtering for the RAX700 as below.

Step	Configuration	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`spanning-tree edged-port bpdu-filter enable`** *`interface-type interface-number`*	Enable the BPDU filtering on the edged interface. By default, disable the BPDU filtering on the edged-port.

2.9.13 Configuring BPDU Guard

Generally, on a switch, interfaces are directly connected with terminals (such as a PC) or file servers are set to an edge interfaces. Therefore, these interfaces can be moved quickly.

In normal status, these edge interfaces will not receive BPDU packets. If somebody attacks the switch by forging the BPDU packet, the device will set these edge interfaces to non-edge interfaces when these edge interfaces receive the forged BPDU packet and re-perform spanning tree calculation. This may cause network vibration.

BPDU Guard provided by MSTP can prevent this attack. After BPDU Guard is enabled, edge interfaces can avoid attack from forged BPDU packets.

After BPDU Guard is enabled, the device will shut down the edge interfaces if they receive BPDUs and notify the NView NNM system of the case. The blocked edge interface is restored only by the administrator through the CLI.

Configure the BPDU guard for the RAX700 as below

Step	Configuration	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`spanning-tree bpduguard enable`**	Enable BPDU guard. By default, disable BPDU guard.
3	`Raisecom(config)#`**`interface`** *`interface-type interface-number`*	Enter physical layer interface configuration mode.
4	`Raisecom(config-port)#`**`no spanning-tree bpduguard shutdown port`**	Manually restore interfaces that are shut down by BPDU Guard.

Note

When the edge interface is enabled with BPDU filtering and the device is enabled with BPDU Guard, BPDU Guard takes effect first. Therefore, an edge interface is shut down if it receives a BPDU packet.

2.9.14 Configuring STP/RSTP/MSTP mode switching

When STP is enabled, three spanning tree modes are supported as below:

- STP compatible mode: the RAX700 does not implement fast switching from the replacement interface to the root interface and fast forwarding by a specified interface;

instead it sends STP configuration BPDU and STP Topology Change Notification (TCN) BPDU. After receiving MST BPDU, it discards unidentifiable part.

- RSTP mode: the RAX700 implements fast switching from the replacement interface to the root interface and fast forwarding by a specified interface. It sends RST BPDUs. After receiving MST BPDUs, it discards unidentifiable part. If the peer device runs STP, the local interface is switched to STP compatible mode. If the peer device runs MSTP, the local interface remains in RSTP mode.
- MSTP mode: the RAX700 sends MST BPDU. If the peer device runs STP, the local interface is switched to STP compatible mode. If the peer device runs MSTP, the local interface remains in RSTP mode, and process packets as external information of domain.

Configure the RAX700 as below.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**spanning-tree mode** { **stp** | **rstp** | **mstp** }	Configure spanning tree mode.

2.9.15 Configuring link type

Two interfaces connected by a point-to-point link can quickly transit to forward 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 configure this item in auto status and the system will automatically detect whether the interface is connected to a point-to-point link.

Configure link type for the RAX700 as below.

Step	Configuration	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 link type for interface.

2.9.16 Configuring root interface protection

The network will select a bridge again when it receives a packet with higher priority, which influents network connectivity and also consumes CPU resource. For the MSTP network, if someone sends BPDU packets with higher priority, the network may become unstable for the continuous election. Generally, 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. So the downlink interface cannot receive the packets higher than bridge priority unless under someone 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 other attacks from attacking sources and damaging the upper layer link.

Configure root interface protection for the RAX700 as below.

Step	Configuration	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**	Enable/Disable root interface protection.

2.9.17 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 link in the topology if link backup is required. Spanning tree can avoid loop by blocking the redundant link and enable link backup function by opening redundant link when the link breaks down.

The spanning tree module exchanges packets periodically, and the link has failed if it has not received packet in a period. Then select a new link and enable backup interface. In actual networking, the cause to failure in receiving packets may not link fault. In this case, enabling the backup interface may lead to loop.

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

Note

Loopguard and link backup are mutually exclusive; namely, loopguard is implemented on the cost of disabling link backup.

Configure interface loop protection for the RAX700 as below.

Step	Configuration	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**	Configure interface loopguard attributes. By default, disable loopguard.

2.9.18 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show spanning-tree** [**instance** *instance-id*] [**detail**]	Show basic configurations of STP.
2	Raisecom#**show spanning-tree** [**instance** *instance-id*] *interface-type interface-list* [**detail**]	Show configurations of spanning tree on the interface.
3	Raisecom#**show spanning-tree region-operation**	Show configurations of the MST domain.
4	Raisecom(config-region)#**show spanning-tree region-configuration**	Show configurations of MST domain.

2.9.19 Maintenance

Use the following commands to maintain.

Command	Description
Raisecom(config-port)#**spanning-tree clear statistics**	Clear statistics of spanning tree on the interface.

2.9.20 Preparing for configurations

Scenario

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

In general, ARP address entries are dynamically maintained by the device. The device automatically finds the mapping between IP addresses and MAC addresses based on ARP. You can manually configure the device just for preventing ARP spoofing and for adding static ARP address entries.

Prerequisite

N/A

2.9.21 Configuring ARP address entries

Caution

When you configure static ARP address entries, IP addresses of these static ARP address entries must be at the IP network of Layer 3 interfaces on the RAX711-L.

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

Step	Command	Description
2	Raisecom(config)#**interface ip** *interface-number* Raisecom(config-ip)#**ip address** *ip-address* Raisecom(config-ip)#**exit**	Enter IP interface configuration mode and configure the IP address of the IP interface.
3	Raisecom(config)#**arp** *ip-address mac-address*	Configure static ARP address entries. The IP address of the statically added ARP entry should be in the same IP network segment with that of the IP interface.
4	Raisecom(config)#**arp aging-time** *second*	Configure the aging time of dynamic ARP address entries. By default, the aging time is set to 1200s.
5	Raisecom(config)#**arp detect-times** *time*	Configure times of aging detection of neighbor information table entries. By default, it is 3.
6	Raisecom(config)#**arp mode** { **learn-all** | **learn-reply-only** }	Configure the ARP learning mode. By default, the ARP learning mode is set to **learn-reply-only**.
7	Raisecom(config)#**interface ip** *interface-number*	Enter IP interface configuration mode.
8	Raisecom(config-ip)#**arp learning enable**	Enable ARP dynamic learning on the IP interface. By default, ARP dynamic learning is enabled.
9	Raisecom(config-ip)#**arp max-learning-num** *max-learning-num*	Configure the threshold of dynamically-learned ARP address entries.

2.9.22 Checking configurations

No.	Command	Description
1	Raisecom#**show arp**	Show configurations on all entries in the ARP address table.
2	Raisecom#**show arp** *ip-address*	Show configurations on ARP address entries related to a specified IP address.
3	Raisecom#**show arp ip** *if-number*	Show configurations on ARP address entries related to Layer 3 interfaces.
4	Raisecom#**show arp static**	Show configurations on static ARP address entries.
	Raisecom#**show arp dynamic**	Show configurations on dynamic ARP address entries.

2.10 Configuring port mirroring

2.10.1 Preparing for configurations

Scenario

Port mirroring is used for the administrator to monitor data traffic in a network. By mirroring traffic on a mirroring port to a monitor port, the administrator can get traffics that have fault and anomaly. The port mirroring is used to locate, analyse, and resolve faults.

Prerequisite

N/A

2.10.2 Configuring port mirroring

Caution

- There can be multiple mirroring ports. However, there is only one monitor port.
- After port mirroring takes effect, packets on both ingress and egress ports will be copied to the monitor port.
- The mirroring port and the monitor port should not be the same one.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mirror enable**	Enable the port mirroring. By default, the port mirroring is disabled.
3	Raisecom(config)#**mirror monitor-port** *interface-type interface-number*	Configure the monitor port. By default, the monitor port index is set to 1. **Note** Packets that are mirrored to the monitor port will not follow VLAN configurations on the mirroring port and all packets can pass the interface.
4	Raisecom(config)#**mirror source-port-list** { **both** | **ingress** | **egress** } *interface-type interface-list*	Configure the mirroring port and the mirroring rules. By default, there is no mirroring port. **Note** When a mirroring port list is configured in one direction, the mirroring port list in the other direction will be cleared automatically.

2.10.3 Checking configurations

No.	Command	Description
1	Raisecom(config)#**show mirror**	Show port mirroring configurations.

2.11 Configuring L2CP

2.11.1 Preparing for configurations

Scenario

On the access device in the Metropolitan Area Network (MAN), you need to make different configurations of the processing methods towards Layer 2 control packets in the user network, which can be realized through configuring the L2CP profile on the interface at the user network side.

Prerequisite

N/A

2.11.2 Configuring L2CP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**l2cp-process tunnel destination-address** *mac-address*	Configure the destination multicast MAC address of the transparently transmitted packet.

2.11.3 Configuring L2CP profile

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**l2cp-process profile** *profile-id*	Create a L2CP profile and enter L2CP profile configuration mode.
3	Raisecom(config-l2cp-profile)#**name** *string*	(Optional) add the name of the L2CP profile.
4	Raisecom(config-l2cp-profile)#**l2cp-process mac-address** *mac-address* [*ether-type*] **action** [**drop**| **peer** | **tunnel**]	(Optional) configure the action to process the L2CP of a specified destination MAC address.

Step	Command	Description
5	Raisecom(config-l2cp-profile)#**l2cp-process protocol** { **all** | **cdp** | **dot1x** | **lacp** | **lldp** | **oam** | **pvst** | **stp** | **vtp** } **action** [**drop**| **peer** | **tunnel**]	(Optional) configure the action to process the L2CP of a specified protocol type.
6	Raisecom(config-l2cp-profile)#**tunnel tunnel-type** { **mac** | **mpls** }	(Optional) configure the specified channel to transparently transmit the L2CP.
7	Raisecom(config-l2cp-profile)#**tunnel mpls vlan** *vlan-id*	(Optional) configure the MPLS channel to transparently transmit L2CP packets in the specified VLAN.
8	Raisecom(config-l2cp-profile)#**tunnel vlan** *vlan-id*	(Optional) configure the MAC channel to transparently transmit L2CP packets in the specified VLAN.

2.11.4 Applying L2CP profile to interfaces

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)#**l2cp-process profile** *profile-id*	Apply the L2CP profile to the interface.

Note

Only when the L2CP profile is enabled globally can the L2CP profile applied to the interface take effect. Otherwise, configurations cannot take effect.

2.11.5 Checking configurations

No.	Command	Description
1	Raisecom#**show l2cp-process profile** [*profile-id*]	Show information about the created L2CP profile.
2	Raisecom#**show l2cp-process** [*interface-type interface-list*]	Show configurations of the L2CP on the interface.
3	Raisecom#**show l2cp-process tunnel statistic** [*interface-type interface-list*]	Show L2CP statistics on the interface.

2.12 Maintenance

Command	Description
Raisecom(config)#**clear mac-address-table** { **all** | **dynamic** | **static** }	Clear MAC addresses.
Raisecom(config)#**search mac-address** *mac-address* { **all** | **dynamic** | **static** } [*interace-type interface-number*] [**vlan** *vlan-id*]	Search MAC addresses.
Raisecom(config-port)#**clear loopback-detection statistic**	Clear loop detection statistics.
Raisecom(config)#**clear l2cp-process tunnel statistics** [*interface-type interface-list*]	Clear L2CP statistics on the interface.

2.13 Configuration examples

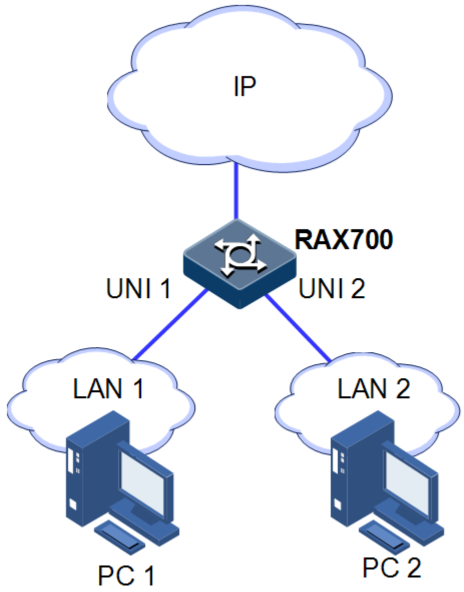
2.13.1 Example for configuring MAC address table

Networking requirements

As shown in Figure 2-6, LAN 1 and LAN 2 are in VLAN 10. The MAC address of PC 1 is 000e.5e01.0105 and the MAC address of PC 2 is 000e.5e02.0207. PC 2 accessed the network illegally by using the MAC address of PC 1. To prevent PC 2 from accessing the network without influencing other devices accessing the network through UNI 2, perform the following operations.

- On UNI 1 of the RAX711-L, configure a static MAC address entry that is related to the MAC address of PC 1 and disable dynamic MAC address learning.
- On UNI 2 of the RAX711-L, set the MAC address of PC 2 to a blackhole MAC address and enable dynamic MAC address learning. Set the aging time to 400s.

Figure 2-6 Configuring MAC address table



Configuration steps

Step 1 Create VLAN 10 and then add interfaces to VLAN 10.

```
Raisecom#config
Raisecom(config)#create vlan 10 active
Raisecom(config)#interface uni 1
Raisecom(config-port)#switchport mode access
Raisecom(config-port)#switchport access vlan 10
Raisecom(config-port)#exit
Raisecom(config-port)#interface uni 2
Raisecom(config-port)#switchport mode access
Raisecom(config-port)#switchport access vlan 10
Raisecom(config-port)#exit
```

Step 2 On UNI 1, configure a static unicast MAC address (000e.5e01.0105), which belongs to VLAN 10 and disable dynamic MAC address learning.

```
Raisecom(config)#mac-address-table static unicast 000e.5e01.0105 vlan 10
uni 1
Raisecom(config)#mac-address-table learning disable uni 1
```

Step 3 On UNI 2, configure a blackhole MAC address (000e.5e02.0207), which belongs to VLAN 10, enable dynamic MAC address learning, and set the aging time to 400s.

```
Raisecom(config)#mac-address-table blackhole 000e.5e02.0207 vlan 10
Raisecom(config)#mac-address-table learning enable uni 2
Raisecom(config)#mac-address-table aging-time 400
```

Step 4 Save configurations.

```
Raisecom#write
```

Checking results

Use the **show mac-address-table l2-address** command to show MAC address configurations.

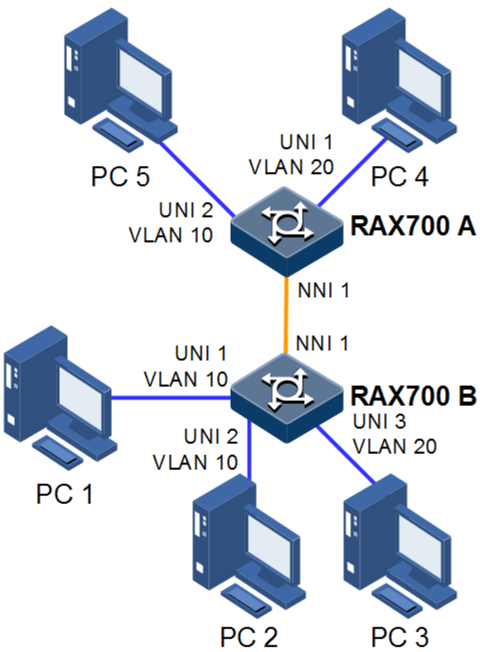
```
Raisecom#show mac-address-table l2-address
Aging time:400 seconds
Mac Address       Port        Vlan    Flags
---------------------------------------------
000E.5E01.0105   uni1      10      static
000E.5E02.0207    --          10      blackhole
```

2.13.2 Example for configuring VLAN and interface protection

Networking requirements

As shown in Figure 2-7, PC 1, PC 2, and PC 5 are in VLAN 10; PC 3 and PC 4 are in VLAN 20. RAX700 A and RAX700 B are connected through a Trunk interface and packets of VLAN 20 are disallowed to pass. Therefore, PC 3 and PC 4 cannot communicate with each other. Enable interface protection on PC 1 and PC 2 to make them fail to communicate. However, PC 1 and PC 2 can communicate with PC 5 respectively.

Figure 2-7 Configuring VLAN



Configuration steps

Step 1 Create and activate VLAN 10 and VLAN 20 on RAX700 A and RAX700 B respectively.

- Configure RAX700 A.

```
RAX700A#config
RAX700A(config)#create vlan 10,20 active
```

- Configure RAX700 B.

```
RAX700B#config
RAX700B(config)#create vlan 10,20 active
```

Step 2 Add UNI 1 (Access) and UNI 2 (Access) of RAX700 B to VLAN 10. Add UNI 3 (Access) to VLAN 20. NNI 1 is in Trunk mode and allows packets of VLAN 10 to pass.

```
RAX700B(config)#interface uni 1
RAX700B(config-port)#switchport mode access
RAX700B(config-port)#switchport access vlan 10
RAX700B(config-port)#exit
RAX700B(config)#interface uni 2
RAX700B(config-port)#switchport mode access
RAX700B(config-port)#switchport access vlan 10
RAX700B(config-port)#exit
RAX700B(config)#interface uni 3
RAX700B(config-port)#switchport mode access
RAX700B(config-port)#switchport access vlan 20
RAX700B(config-port)#exit
RAX700B(config)#interface nni 1
RAX700B(config-port)#switchport mode trunk
RAX700B(config-port)#switchport trunk allow vlan 10
RAX700B(config-port)#exit
```

Step 3 Add UNI 2 (Access) of RAX700 A to VLAN 10. Add UNI 1 (Trunk) to VLAN 20. NNI 1 is in Trunk mode and allows packets of VLAN 10 to pass.

```
RAX700A(config)#interface uni 2
RAX700A(config-port)#switchport mode access
RAX700A(config-port)#switchport access vlan 10
RAX700A(config-port)#exit
RAX700A(config)#interface uni 1
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#switchport trunk native vlan 20
RAX700A(config-port)#exit
RAX700A(config)#interface nni 1
```

```
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#switchport trunk allow vlan 10
```

Step 4 Enable interface protection on UNI 1 and UNI 2 of RAX700 B.

```
RAX700B(config)#interface uni 1
RAX700B(config-port)#switchport protect
RAX700B(config-port)#exit
RAX700B(config)#interface uni 2
RAX700B(config-port)#switchport protect
```

Step 5 Save configurations of RAX700 A and RAX700 B, taking RAX700 A for example.

```
RAX700A#write
```

Checking results

Use the **show vlan** command to show VLAN configurations.

Take RAX700 B for example.

```
RAX700B#show vlan
Switch Mode: --
VLAN  Name     State   Status  Priority   Member-Ports
---------------------------------------------------------------------
1   Default   active  static   --        L:1,2;C:1-4 L:1,2;C:1-4
2             active  other    --         L:1,2;C:1-4 n/a
10   VLAN0010  active  static   --         L:1;C:1,2   C:1,2
20   VLAN0020  active  static   --         C:3         C:3
```

Use the **show interface** *interface-type interface-number* **switchport** command to show VLAN configurations on an interface.

Take RAX700 B for example.

```
RAX700B#show interface uni 1 switchport
Interface: uni 1
Reject frame type: none
Administrative Mode: access
Operational Mode: access
Access Mode VLAN: 10
Administrative Access Egress VLANs: 1
Operational Access Egress VLANs: 1,10
Trunk Native Mode VLAN: 1
Administrative Trunk Allowed VLANs: 1-4094
```

```
Operational Trunk Allowed VLANs: n/a
Administrative Trunk Untagged VLANs: 1
Operational Trunk Untagged VLANs: 1
```

Use the **show switchport protect** command to show interface protection configuration.

Take RAX700 B for example.

```
RAX700B#show switchport protect
Port     Protected State
--------------------------
L:1        disable
L:2        disable
C:1        enable
C:2        enable
C:3        disable
```

By executing the ping command between PC 1 and PC 5, PC 2 and PC 5, PC 3 and PC 4 to check VLAN configurations on the Trunk interface.

- If PC 1 can ping through PC 5, VLAN 10 communicates properly.
- If PC 2 can ping through PC 5, VLAN 10 communicates properly.
- If PC 3 cannot ping through PC 4, VLAN 20 communicates improperly.

By executing the ping command between PC 1 and PC 2, check interface protection configurations.

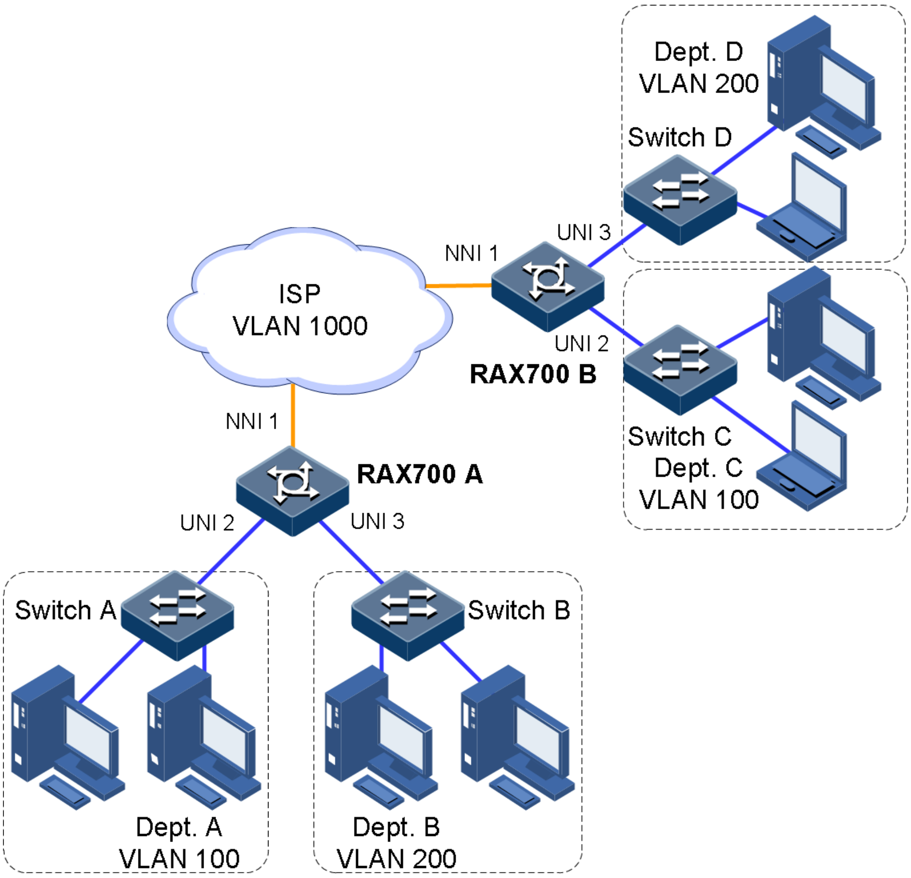
- If PC 1 cannot ping through PC 2, interface protection takes effect.

2.13.3 Example for configuring basic QinQ

Networking requirements

As shown in Figure 2-8, RAX700 A and RAX700 B are connected to VLAN 100 and VLAN 200 respectively. To communicate through the ISP network, Department A and Department C, Department B and Department D should set the outer Tag to VLAN 1000. Configure UNI 2 and UNI 3 on RAX700 A and RAX700 B working in dot1q-tunnel mode and being connected to VLAN 100 and VLAN 200. NNI 1 is used to connect the ISP network, which works in Trunk mode and allows packets with double tag to pass. The TPID is set to 0x9100.

Figure 2-8 Configuring basic QinQ



Configuration steps

Step 1 Create and activate VLAN 100, VLAN 200, and VLAN 1000.

- Configure RAX700 A.

```
RAX700A#config
RAX700A(config)#create vlan 100,200,1000 active
```

- Configure RAX700 B.

```
RAX700B#config
RAX700B(config)#create vlan 100,200,1000 active
```

Step 2 Configure UNI 2 and UNI 3 working in dot1q-tunnel mode.

- Configure RAX700 A.

```
RAX700A(config)#interface uni 2
RAX700A(config-port)#switchport mode access
RAX700A(config-port)#switchport access vlan 1000
```

```
RAX700A(config-port)#switchport qinq dot1q-tunnel
RAX700A(config-port)#exit
RAX700A(config)#interface uni 3
RAX700A(config-port)#switchport mode access
RAX700A(config-port)#switchport access vlan 1000
RAX700A(config-port)#switchport qinq dot1q-tunnel
RAX700A(config-port)#exit
```

- Configure RAX700 B.

```
RAX700B(config)#interface uni 2
RAX700B(config-port)#switchport mode access
RAX700B(config-port)#switchport access vlan 1000
RAX700B(config-port)#switchport qinq dot1q-tunnel
RAX700B(config-port)#exit
RAX700B(config)#interface uni 3
RAX700B(config-port)#switchport mode access
RAX700B(config-port)#switchport access vlan 1000
RAX700B(config-port)#switchport qinq dot1q-tunnel
RAX700B(config-port)#exit
```

Step 3 Configure NNI 1 allowing packets with double Tag to pass. Set the TPID value to 0x9100.

- Configure RAX700 A.

```
RAX700A(config)#interface nni 1
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#mls double-tagging tpid 9100
RAX700A(config-port)#switchport trunk allowed vlan 1000
RAX700A(config-port)#exit
```

- Configure RAX700 B.

```
RAX700B(config)#interface nni 1
RAX700B(config-port)#switchport mode trunk
RAX700B(config-port)#mls double-tagging tpid 9100
RAX700B(config-port)#switchport trunk allowed vlan 1000
RAX700B(config-port)#exit
```

Step 4 Save configurations of RAX700 A and RAX700 B, taking RAX700 A for example.

```
RAX700A#write
```

Checking results

Use the **show switchport qinq** command to show QinQ configurations.

Take RAX700 A for example.

```
RAX700A#show switchport qinq
Inner TPID:: 0x8100
Interface   QinQ Status   Outer TPID on port  Cos override Vlan-map-miss
drop
-----------------------------------------------------------------------
---
  nni1      --           0x9100          --        disable
  nni2      --           0x8100           --        disable
  uni1    --            0x8100          --        disable
  uni2    Dot1q-tunnel   0x8100          --        disable
  uni3    Dot1q-tunnel   0x8100          --        disable
  uni4    --          0x8100           --        disable
Notice: Only 2 TPID values can be used as outer TPID on ports(Except
0x8100 and 0x9100),
Already used 0 TPID values: --, left:2 TPID value can be use.
```

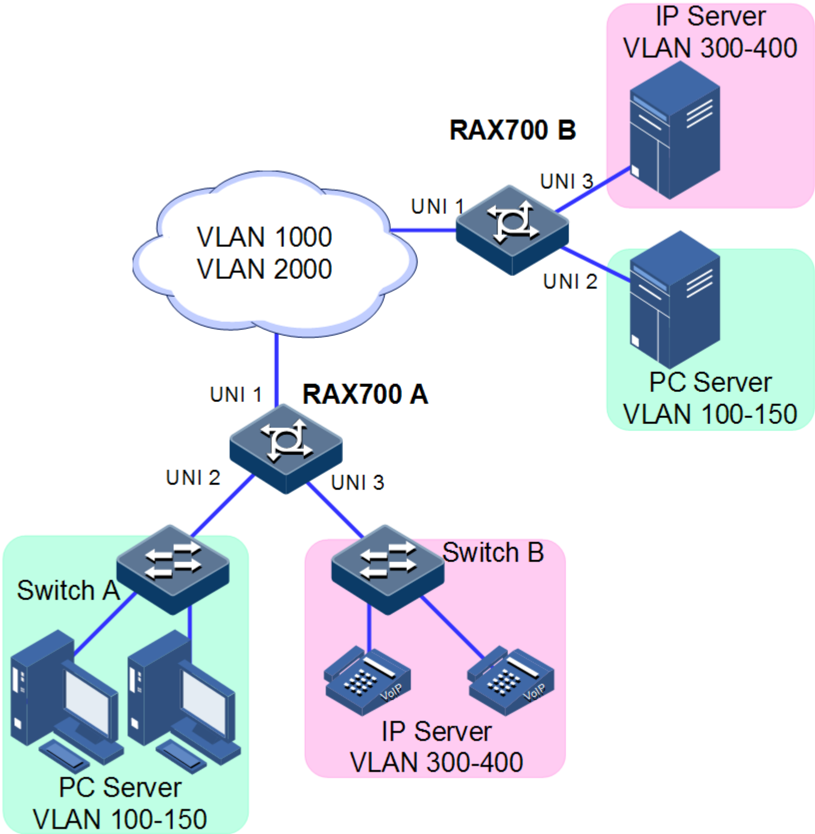
2.13.4 Example for configuring selective QinQ

Networking requirements

As shown in Figure 2-9, services in the ISP network are divided into PC service and IP service. Therefore, configure the PC service with VLAN 1000 and configure the IP service with VLAN 2000. Perform following configurations on RAX700 A and RAX700 B respectively:

Add outer Tag VLAN 1000 to VLANs 100–150 assigned to PC service. Add outer Tag VLAN 2000 to VLANs 300–400 assigned to IP service. Make users properly communicate with the server through the ISP network. The TPID is set to 0x9100.

Figure 2-9 Configuring selective QinQ



Configuration steps

Step 1 Create and activate VLANs.

- Configure RAX700 A.

```
RAX700A#config
RAX700A(config)#create vlan 100-150,300-400,1000,2000 active
```

- Configure RAX700 B.

```
RAX700B#config
RAX700B(config)#create vlan 100-150,300-400,1000,2000 active
```

Step 2 Configure UNI 2 and UNI 3 working in dot1q-tunnel mode.

- Configure RAX700 A.

```
RAX700A(config)#interface uni 2
RAX700A(config-port)#switchport mode trunk
```

```
RAX700A(config-port)#switchport vlan-mapping cvlan 100-150 add-outer 1000
RAX700A(config-port)#switchport trunk untagged vlan 1000,2000 confirm
RAX700A(config-port)#exit
RAX700A(config)#interface uni3
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#switchport vlan-mapping cvlan 300-400 add-outer 2000
RAX700A(config-port)#switchport trunk untagged vlan 1000,2000 confirm
RAX700A(config-port)#exit
```

- Configure RAX700 B.

```
RAX700B(config)#interface uni 2
RAX700B(config-port)#switchport mode trunk
RAX700B(config-port)#switchport vlan-mapping cvlan 100-150 add-outer 1000
RAX700B(config-port)#switchport trunk untagged vlan 1000,2000 confirm
RAX700B(config-port)#exit
RAX700B(config)#interface uni 3
RAX700B(config-port)#switchport mode trunk
RAX700B(config-port)#switchport vlan-mapping cvlan 300-400 add-outer 2000
RAX700B(config-port)#switchport trunk untagged vlan 1000,2000 confirm
RAX700B(config-port)#exit
```

Step 3 Configure UNI 1 allowing packets with double Tag to pass. Set the TPID value to 0x9100.

- Configure RAX700 A.

```
RAX700A(config)#interface uni 1
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#mls double-tagging tpid 9100
RAX700A(config-port)#switchport trunk allowed vlan 1000,2000 confirm
RAX700A(config-port)#exit
```

- Configure RAX700 B.

```
RAX700B(config)#interface uni 1
RAX700B(config-port)#switchport mode trunk
RAX700B(config-port)#mls double-tagging tpid 9100
RAX700B(config-port)#switchport trunk allowed vlan 1000,2000 confirm
RAX700B(config-port)#exit
```

Step 4 Save configurations of RAX700 A and RAX700 B, taking RAX700 A for example.

```
RAX700A#write
```

Checking results

Use the **show interface** *interface-type* [*interface-number*] **vlan-mapping add-outer** command to show QinQ configurations.

Take RAX700 A for example.

```
RAX700A#show interface uni 2 vlan-mapping add-outer
Based outer VLAN QinQ mapping rule:
      Original   Original Add-outer Add-outer Add-Local Hardware Hardware
Port  Outer VLAN  COS      VLAN      COS       Proi      Status   ID
-----------------------------------------------------------------------
U2   100-150       --      1000      --        --        Enable     1

RAX700A#show interface uni 3 vlan-mapping add-outer
Based outer VLAN QinQ mapping rule:
      Original   Original Add-outer Add-outer Add-Local Hardware Hardware
Port  Outer VLAN  COS      VLAN      COS       Proi      Status   ID
-----------------------------------------------------------------------
U3   300-400       --      2000      --        --       Enable     2
```

2.13.5 Example for configuring VLAN mapping

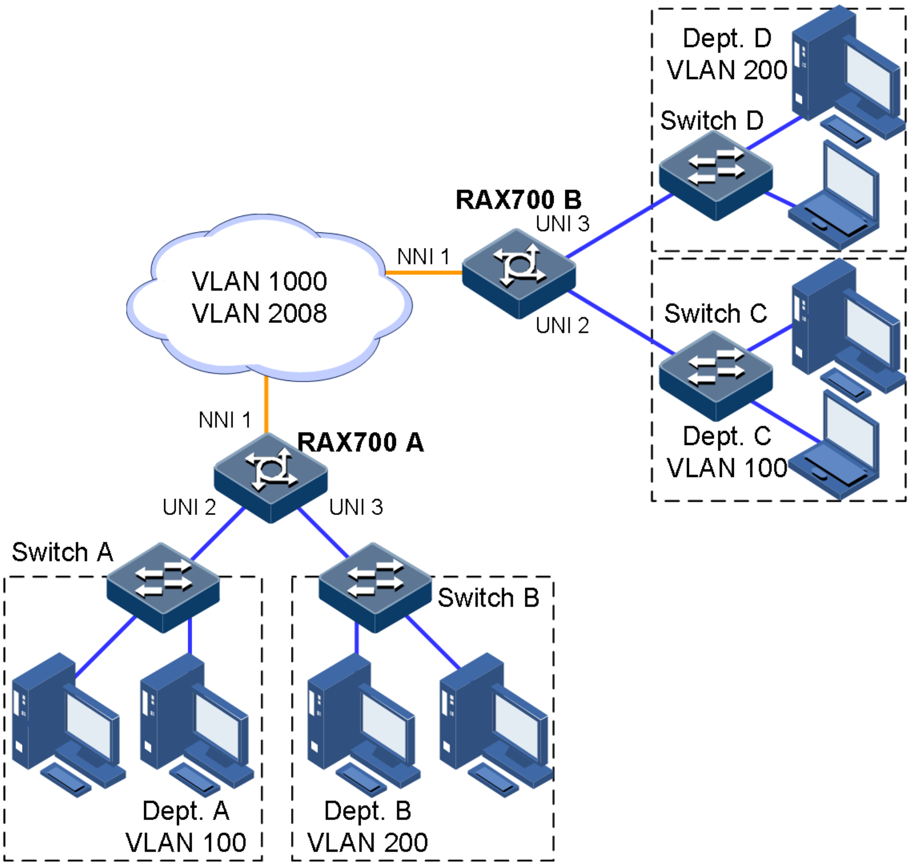
Networking requirements

As shown in Figure 2-10, UNI 2 and UNI 3 of RAX700 A is connected to Department A and Department B. Department A is in VLAN 100 and Department B is in VLAN 200.

UNI 2 and UNI 3 of RAX700 B are connected to Department C and Department D. Department C is in VLAN 100 and Department D is in VLAN 200.

To make Departments A and C and Departments B and D communicate with each other, you can configure 1:1 VLAN mapping on RAX700 A and RAX700 B. In the ISP, VLAN 1000 is assigned to Department A and Department C for transmitting data. VLAN 2008 is assigned to Department B and Department D for transmitting data.

Figure 2-10 Configuring VLAN mapping



Configuration steps

Configurations on RAX700 A and RAX700 B are identical. Therefore, only configurations on RAX700 A are described.

Step 1 Create and activate VLANs.

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

Step 2 Configure NNI 1 to work in Trunk mode, allowing packets of VLAN 100, VLAN 200, VLAN 1000, and VLAN 2008 to pass. Enable VLAN mapping on NNI 1.

```
RAX700A(config)#interface nni 1
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#switchport trunk allowed vlan 100,200,1000,2008
RAX700A(config-port)#switchport vlan-mapping egress 100 translate 1000
RAX700A(config-port)#switchport vlan-mapping egress 200 translate 2008
RAX700A(config-port)#exit
```

Step 3 Configure UNI 2 working in Access mode, allowing packets of VLAN 100 and VLAN 1000 to pass. Enable VLAN mapping on UNI 2.

```
RAX700A(config)#interface uni 2
RAX700A(config-port)#switchport mode access
RAX700A(config-port)#switchport access vlan 100
RAX700A(config-port)#switchport access vlan 1000
RAX700A(config-port)#switchport vlan-mapping egress 1000 translate 100
RAX700A(config-port)#exit
```

Step 4 Configure UNI 3 working in Trunk mode, allowing packets of VLAN 200 and VLAN 2008 to pass. Enable VLAN mapping on UNI 3.

```
RAX700A(config)#interface uni 3
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#switchport trunk allowed vlan 200,2008
RAX700A(config-port)#switchport vlan-mapping egress outer 2008 outer
translate 200
RAX700A(config-port)#exit
```

Step 5 Save configurations of RAX700 A and RAX700 B, taking RAX700 A for example.

```
RAX700A#write
```

Checking results

Use the **show interface** *interface-type interface-number* **vlan-mapping egress translate** command to show 1:1 VLAN mapping configurations.

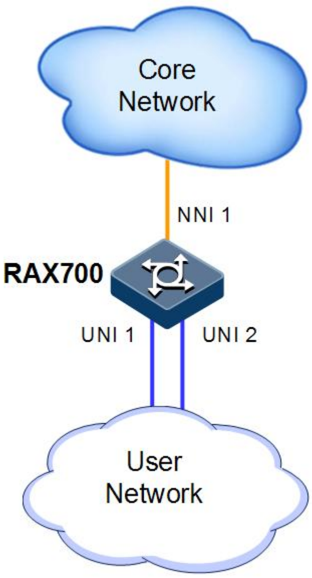
```
RAX700A(config)#show interface uni 2 vlan-mapping egress translate
Direction: Egress
Based outer-inner VLAN QinQ mapping rule:
-----------------------------------------
Interface  : U2
Hardware-ID: 5
Original Outer VLANs: 1000
Original Outer COS:   --
Original Inner VLANs: --
Original Inner COS:   --
Outer-tag Mode:     Translate
New Outer-VID:      100
New Outer-COS:      --
Inner-tag Mode:     --
New Inner-VID:      --
New Inner-COS:      --
```

2.13.6 Example for configuring loop detection

Networking requirements

As shown in Figure 2-11, NNI 1 of the RAX711-L is connected to the core network. UNI 1 and UNI 2 of the RAX711-L are connected to the user network. Enable loop detection on the RAX711-L to detect the loop generated in the user network immediately and block the related interface.

Figure 2-11 Configuring loop detection



Configuration steps

Step 1 Create VLAN 3 and add UNI 1 and UNI 2 to VLAN 3.

```
Raisecom(config)#create vlan 3 active
Raisecom(config)#interface uni 1
Raisecom(config-port)#switchport access vlan 3
Raisecom(config-port)#exit
Raisecom(config)#interface uni 2
Raisecom(config-port)#switchport access vlan 3
Raisecom(config-port)#exit
```

Step 2 Enable loop detection on UNI 1 and UNI 2.

```
Raisecom(config)#loopback-detection enable uni 1-2
Raisecom(config)#loopback-detection hello-time 3
```

Step 3 Save configurations.

```
Raisecom#write
```

Checking results

Use the **show loopback-detection** command to show loop detection status on UNI 2.

```
Raisecom#show loopback-detection uni 2
Destination address: ffff.ffff.ffff
Mode:Vlan-based
Port mode vlan:3
Period of loopback-detection:3s
Restore time:infinite
Port     PortState  State    Status      loop-act          vlanlist
----------------------------------------------------------------------
U2        Down      Ena      no       trap-only         --
```

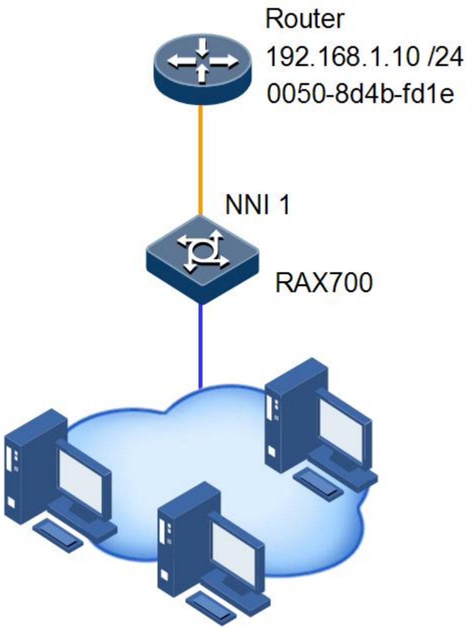
2.13.7 Example for configuring ARP

Networking requirements

As shown in Figure 2-12, the RAX711-L is connected to PCs. The RAX711-L is connected to the Router through NNI 1. The IP address of the Router is set to 192.168.1.10/24 and the MAC address is set to 0050.8D4B.FD1E.

Set the aging time of dynamic ARP address entries to 600s. To improve the security on communication between the RAX711-L and Router, you need to configure the related static ARP entry on the RAX711-L.

Figure 2-12 Configuring ARP



Configuration steps

Step 1 Add a static ARP entry.

```
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address 192.168.1.2
Raisecom(config-ip)#exit
Raisecom(config)#arp 192.168.1.10 0050.8d4b.fd1e
```

Step 2 Set the aging time of dynamic ARP address entries to 600s.

```
Raisecom(config)#arp aging-time 600
```

Step 3 Save configurations.

```
Raisecom#write
```

Checking results

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

```
Raisecom#show arp
ARP table aging-time: 600 seconds(default: 1200s)
ARP mode: Learn reply only

IP Address       Mac Address      Interface   Type     Age(s)
----------------------------------------------------------------
172.16.70.66     7845.C404.CD34    outband0    dynamic   1106
192.168.1.10     0050.8D4B.FD1E    ip0        static    600

Total:  2
Static: 1
Dynamic:1
```

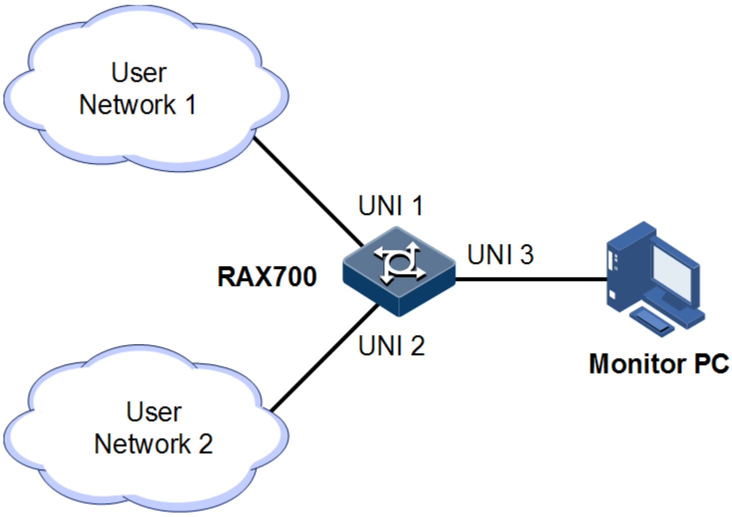
2.13.8 Example for configuring port mirroring

Networking requirements

As shown in Figure 2-13, user network 1 is connected to the RAX711-L through UNI 1 and user network 2 is connected to the RAX711-L through UNI 2. The network administrator needs to monitor packets transmitted to and sent by user network 1 through the monitor PC, and then gets anomalous data traffic, analyzes causes, and addresses problems.

The monitor PC is connected to the RAX711-L through UNI 3.

Figure 2-13 Configuring port mirroring



Configuration steps

Step 1 Enable port mirroring.

```
Raisecom#config
Raisecom(config)#mirror enable
```

Step 2 Set UNI 3 to the monitor port.

```
Raisecom(config)#mirror monitor-port uni 3
```

Step 3 Set UNI 1 to the mirroring port and set the mirroring rule to **both**.

```
Raisecom(config)#mirror source-port-list both uni 1
```

Step 4 Save configurations.

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

Checking results

Use the **show mirror** command to show port mirroring configurations.

```
Raisecom(config)#show mirror
Mirror: Enable
Monitor port: uni 3
-----------the ingress mirror rule-----------
Mirrored ports: uni 1
-----------the egress mirror rule-----------
Mirrored ports: uni 1
```

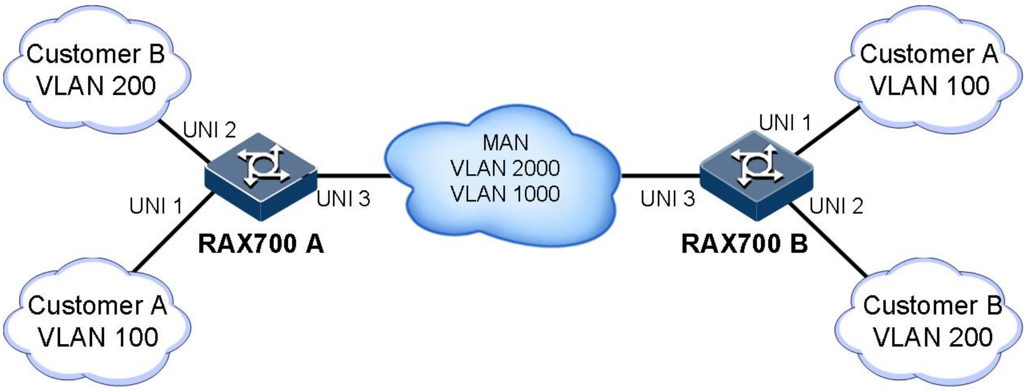
2.13.9 Example for configuring L2CP

Networking requirements

As shown in Figure 2-14, configure the L2CP feature on RAX700 A and RAX700 B as below:

- Specify the multicast destination MAC address as 000e.5e34.0003 for RAX700 A and RAX700 B.
- The STP packets of Customer A can be transmitted through the MAN. Other packets are discarded.
- The STP and VTP packets of Customer B can be transmitted through the MAN. The LLDP packets are uploaded to the CPU. Other packets are discarded.

Figure 2-14 Configuring L2CP



Configuration steps

Configure RAX700 A and RAX700 B.

Configurations on RAX700 A and RAX700 B are identical. Therefore, only configurations on RAX700 A are described.

Step 1 Configure L2CP profile 1 and apply the profile to UNI 1 (suitable for Customer A).

```
Raisecom#config
Raisecom(config)#l2cp-process profile 1
Raisecom(config-l2cp-proflie)#name CustomerA
Raisecom(config-l2cp-proflie)#l2cp-process protocol all action drop
Raisecom(config-l2cp-proflie)#l2cp-process protocol stp action tunnel
Raisecom(config-l2cp-profile)#tunnel tunnel-type mac
Raisecom(config-l2cp-proflie)#exit
```

```
Raisecom(config)#interface uni 1
Raisecom(config-port)#l2cp-process profile 1
Raisecom(config-port)#exit
```

Step 2 Configure L2CP profile 2 and apply the interface to UNI 2 (suitable for Customer B).

```
Raisecom(config)#l2cp-process profile 2
Raisecom(config-l2cp-proflie)#name CustomerB
Raisecom(config-l2cp-proflie)#l2cp-process protocol all action drop
Raisecom(config-l2cp-proflie)#l2cp-process protocol stp action tunnel
Raisecom(config-l2cp-proflie)#l2cp-process protocol vtp action tunnel
Raisecom(config-l2cp-proflie)#l2cp-process protocol lldp action peer
Raisecom(config-l2cp-profile)#tunnel tunnel-type mac
Raisecom(config-l2cp-proflie)#exit
Raisecom(config)#interface uni 2
Raisecom(config-port)#l2cp-process profile 2
Raisecom(config-port)#exit
```

Checking results

Use the **show l2cp-process** command to show L2CP configurations.

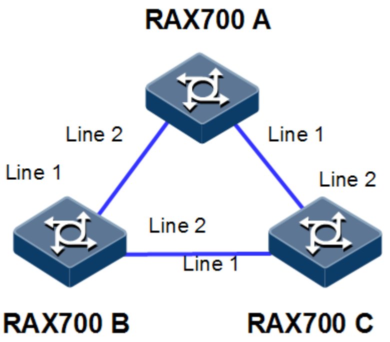
```
Raisecom#show l2cp-process
L2CP running informatiom
Port   ProfileID   BpduType   mac-address   l2cp-process
---------------------------------------------------------
nni1    --         --         --            --
nni2    --         --         --            --
uni1   1         stp       0180.C200.0000   tunnel
                    dot1x      0180.C200.0003   drop
                    lacp       0180.C200.0002   drop
                    oam        0180.C200.0002   drop
                    cdp        0100.0CCC.CCCC   drop
                    vtp        0100.0CCC.CCCC   drop
                    pvst       0100.0CCC.CCCD   drop
                    lldp       0180.C200.000E   drop
uni2   2         stp       0180.C200.0000   tunnel
                    dot1x      0180.C200.0003   drop
                    lacp       0180.C200.0002   drop
                    oam        0180.C200.0002   drop
                    cdp        0100.0CCC.CCCC   drop
                    vtp        0100.0CCC.CCCC   tunnel
                    pvst       0100.0CCC.CCCD   drop
                    lldp       0180.C200.000E   peer
uni3   --         --         --            --
```

2.13.10 Example for configuring STP

Networking requirements

As shown in Figure 2-15, RAX700 A, RAX700 B, and RAX700 C forms a ring network, so the loopback problem must be solved in the situation of a physical ring. Enable STP on them, set the priority of RAX700 A to 0, and path cost from RAX700 B to RAX700 A to 10.

Figure 2-15 STP networking



Configuration steps

Step 1 Enable STP on RAX700 A, RAX700 B, and RAX700 C.

Configure RAX700 A.

```
Raisecom#hostname RAX700A
RAX700A#config
RAX700A(config)#spanning-tree enable
RAX700A(config)#spanning-tree mode stp
```

Configure RAX700 B.

```
Raisecom#hostname RAX700B
RAX700B#config
RAX700B(config)#spanning-tree enable
RAX700B(config)#spanning-tree mode stp
```

Configure RAX700 C.

```
Raisecom#hostname RAX700C
RAX700C#config
RAX700C(config)#spanning-tree enable
RAX700C(config)#spanning-tree mode stp
```

Step 2 Configure interface mode on three devices.

Configure RAX700 A.

```
RAX700A(config)#interface line 1
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#exit
RAX700A(config)#interface line 2
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#exit
```

Configure RAX700 B.

```
RAX700B(config)#interface line 1
RAX700B(config-port)#switchport mode trunk
RAX700B(config-port)#exit
RAX700B(config)#interface line 2
RAX700B(config-port)#switchport mode trunk
RAX700B(config-port)#exit
```

Configure RAX700 C.

```
RAX700C(config)#interface line 1
RAX700C(config-port)#switchport mode trunk
RAX700C(config-port)#exit
RAX700C(config)#interface line 2
RAX700C(config-port)#switchport mode trunk
RAX700C(config-port)#exit
```

Step 3 Configure priority of spanning tree and interface path cost.

Configure RAX700 A.

```
RAX700A(config)#spanning-tree priority 0
RAX700A(config)#interface line 2
RAX700A(config-port)#spanning-tree extern-path-cost 10
```

Configure RAX700 B.

```
RAX700B(config)#interface line 1
RAX700B(config-port)#spanning-tree extern-path-cost 10
```

Checking results

Use the **show spanning-tree** command to show bridge status. Take the RAX700 A as an example.

```
RAX700A#show spanning-tree
Spanning-tree admin state: enable
Spanning-tree protocol mode: STP

BridgeId:    Mac 000E.5E7B.C557  Priority 0
Root:        Mac 000E.5E7B.C557  Priority 0   RootCost 0
Operational:  HelloTime 2, ForwardDelay 15, MaxAge 20
Configured:   HelloTime 2, ForwardDelay 15, MaxAge 20 TransmitLimit 3
           MaxHops   20  Diameter 7
```

Use the **spanning-tree** *interface-type interface-number* to show bridge status. Take the RAX700 A as an example.

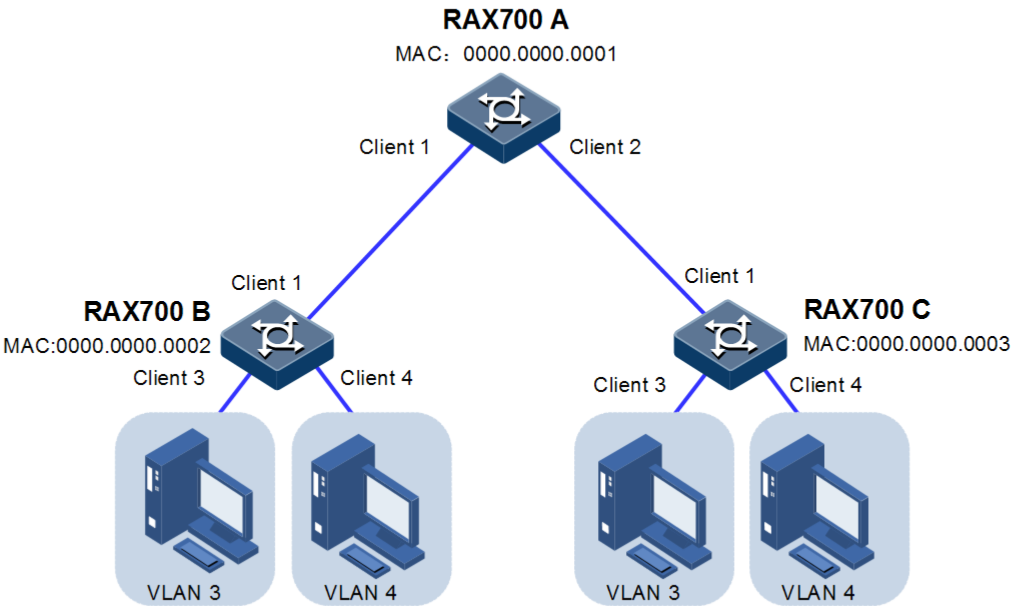
```
RAX700A#show spanning-tree line 1-2
line 1
PortEnable: admin: enable       oper: enable
Rootguard:  disable
Loopguard:  disable
Bpduguard:  disable
ExternPathCost:10
Partner STP Mode: stp
Bpdus send:   279  (TCN<0>    Config<279>  RST<0>  MST<0>)
Bpdus received:13  (TCN<13>    Config<0>  RST<0>  MST<0>)
State:forwarding  Role:designated     Priority:128   Cost: 200000
Root:        Mac 000E.5E7B.C557  Priority 0   RootCost 0
DesignatedBridge: Mac 000E.5E7B.C557  Priority 0   DesignatedPort 32777

Line 2
PortEnable: admin: enable       oper: enable
Rootguard:  disable
Loopguard:  disable
ExternPathCost:200000
Partner STP Mode: stp
Bpdus send:    279  (TCN<0>    Config<279>  RST<0>  MST<0>)
Bpdus received:6  (TCN<6>    Config<0>  RST<0>  MST<0>)
State:forwarding  Role:designated     Priority:128   Cost: 200000
Root:        Mac 000E.5E7B.C557  Priority 0   RootCost 0
DesignatedBridge: Mac 000E.5E7B.C557  Priority 0   DesignatedPort 32778
```

2.13.11 Example for configuring MSTP

Networking requirements

As shown in Figure 2-16, three RAX700 devices are connected to form a ring network through MSTP, with the domain name aaa. RAX700 B, connected with a PC, belongs to VLAN 3. RAX700 C, connected with another PC, belongs to VLAN 4. Instant 3 is related to VLAN 3. Instant 4 is related to VLAN 4. Configure the path cost of instance 3 on RAX700 B so that packets of VLAN 3 and VLAN 4 are forwarded respectively in two paths, which eliminates loopback and implements load sharing.

Figure 2-16 MSTP networking



Configuration steps

Step 1 Create VLAN 3 and VLAN 4 on RAX700 A, RAX700 B, and RAX700 C respectively, and activate them

Configure RAX700 A.

```
Raisecom#hostname RAX700A
RAX700A#config
RAX700A(config)#create vlan 3-4 active
```

Configure RAX700 B.

```
Raisecom#hostname RAX700B
RAX700B#config
RAX700B(config)#create vlan 3-4 active
```

Configure RAX700 C.

```
Raisecom#hostname RAX700C
RAX700C#config
RAX700C(config)#create vlan 3-4 active
```

Step 2 Configure Client 1 and Client 2 on RAX700 A to allow all VLAN packets to pass in Trunk mode. Configure Client 1 and Client 2 on RAX700 B to allow all VLAN packets to pass in Trunk mode. Configure Client 1 and Client 2 on RAX700 C to allow all VLAN packets to pass in Trunk mode. Configure Client 3 and Client 4 on RAX700 B and RAX700 C to allow packets of VLAN 3 and VLAN 4 to pass in Access mode.

Configure RAX700 A.

```
RAX700A(config)#interface client 1
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#exit
RAX700A(config)#interface client 2
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#exit
```

Configure RAX700 B.

```
RAX700B(config)#interface client 1
RAX700B(config-port)#switchport mode trunk
RAX700B(config-port)#exit
RAX700B(config)#interface client 3
RAX700B(config-port)#switchport access vlan 3
RAX700B(config-port)#exit
RAX700B(config)#interface client 4
RAX700B(config-port)#switchport access vlan 4
RAX700B(config-port)#exit
```

Configure RAX700 B.

```
RAX700C(config)#interface client 1
RAX700C(config-port)#switchport mode trunk
RAX700C(config-port)#exit
RAX700C(config)#interface client 3
RAX700C(config-port)#switchport access vlan 3
RAX700C(config-port)#exit
RAX700C(config)#interface client 4
RAX700C(config-port)#switchport access vlan 4
RAX700C(config-port)#exit
```

Step 3 Set spanning tree mode of RAX700 A, RAX700 B, and RAX700 C to MSTP, and enable STP. Enter MSTP configuration mode, and set the domain name to aaa, revised version to 0. Map instance 3 to VLAN 3, and instance 4 to VLAN 4. Exist from MST configuration mode.

Configure RAX700 A.

```
RAX700A(config)#spanning-tree mode mstp
RAX700A(config)#spanning-tree enable
RAX700A(config)#spanning-tree region-configuration
RAX700A(config-region)#name aaa
RAX700A(config-region)#revision-level 0
RAX700A(config-region)#instance 3 vlan 3
RAX700A(config-region)#instance 4 vlan 4
RAX700A(config-region)#exit
```

Configure RAX700 B.

```
RAX700B(config)#spanning-tree mode mstp
RAX700B(config)#spanning-tree enable
RAX700B(config)#spanning-tree region-configuration
RAX700B(config-region)#name aaa
RAX700B(config-region)#revision-level 0
RAX700B(config-region)#instance 3 vlan 3
RAX700B(config-region)#instance 4 vlan 4
RAX700B(config-region)#exit
```

Configure RAX700 C.

```
RAX700C(config)#spanning-tree mode mstp
RAX700C(config)#spanning-tree enable
RAX700C(config)#spanning-tree region-configuration
RAX700C(config-region)#name aaa
RAX700C(config-region)#revision-level 0
RAX700C(config-region)#instance 3 vlan 3
RAX700C(config-region)#instance 4 vlan 4
RAX700C(config-region)#exit
```

Step 4 Set the inner path coast of Client 1 of spanning tree instance 3 to 100000 on RAX700 B.

```
RAX700B(config)#interface client 1
RAX700B(config-port)#spanning-tree instance 3 inter-path-cost 100000
```

Checking configurations

Use the **show spanning-tree region-operation** command to show configurations of the MST domain. Take RAX700 A as an example.

```
RAX700A#show spanning-tree region-operation
Operational Information:
-----------------------------------------------
Name: aaa
Revision level: 0
Instances running: 3
Digest: 0X7D28E66FDC1C693C1CC1F6B61C1431C4
Instance     Vlans Mapped
--------     ----------------------
0          1,2,5-4094
3          3
4          4
```

Use the **show spanning-tree instance 3** command to check whether basic information about spanning tree instance 3 is correct. Take RAX700 A as an example.

```
RAX700A#show spanning-tree instance 3
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
MST ID: 3
-----------------------------------------------------------
BridgeId:    Mac 0000.0000.0001  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost 0
PortId  PortState   PortRole   PathCost  PortPriority  LinkType
-------------------------------------------------------------------------
Client1     forwarding  designated 200000   128     point-to-point
Client2     forwarding  designated 200000   128     point-to-point
```

Use the **show spanning-tree instance 4** command to check whether basic information about spanning tree instance 4 is correct. Take RAX700 A as an example.

```
RAX700A#show spanning-tree instance 4
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
MST ID: 4
-----------------------------------------------------------
BridgeId:    Mac 000E.5E00.0000  Priority 32768
RegionalRoot: Mac 000E.5E00.0000  Priority 32768  InternalRootCost 0
Port    PortState  PortRole   PathCost  PortPriority  LinkType
-------------------------------------------------------------------------
Client1    forwarding designated   200000    128      point-to-point
Client2    forwarding designated    200000    128          point-to-point
```

3 Clock synchronization

Note

The RAX711-L-4GC4E1-S and RAX711-L-4GC4E1-BL-S support this feature.

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

- Configuring clock synchronization based on synchronous Ethernet
- Configuring clock synchronization based on PTP
- Maintenance
- Configuration examples

3.1 Configuring clock synchronization based on synchronous Ethernet

3.1.1 Preparing for configurations

Scenario

In the PTN, to communicate properly, the sender must put the pulse in the specified timeslot when sending the digital pulse signal and the receiver can extract the pulse from the specified timeslot. To realize this, you must resolve the synchronization problem.

The synchronous Ethernet technology can perform clock synchronization in the PTN. Because it does not support phase synchronization, synchronous Ethernet technology is applied for the base station, fixed network TDM relay, leased clock network relay, and wireless base stations which have no requirement on phase synchronization, such as Global System for Mobile Communications (GSM) and Wideband Code Division Multiple Access (WCDMA).

The RAX711-L supports selecting the optimum clock source automatically or selecting the specified clock source manually.

Prerequisite

N/A

3.1.2 Configuring clock source properties

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**synce enable**	Enable synchronous Ethernet. By default, synchronous Ethernet is disabled on the RAX711-L.
3	Raisecom(config)#**synce source** { **nni** *interface-number* | **external 2m** *interface-number* | **internal** | **pdh** *interface-number* } **priority** *priority*	Configure the priority of the clock source. By default, the local crystal oscillator has the lowest priority and other clock sources are not configured with priority.
4	Raisecom(config)# **synce quality-level** { **standard** | **extend** | **disable**}	(Optional) enable SSM quality level. By default, the RAX711-L uses the standard SSM quality level to select the clock source.
5	Raisecom(config)#**synce source** { **nni** *interface-number* | **external 2m** *interface-number* | **internal** | **pdh** *interface-number* } **quality-level** { **dnu** | **prc** | **sec** | **ssua** | **ssub** }	Configure the clock source management quality level. By default, the quality level of the internal clock source is 11 (referring to the received clock quality level). Other clock sources have no quality level.
6	Raisecom(config)#**synce operation-type** { **auto-select** | **forced-freerun** }	Configure the status of synchronous Ethernet phased-locked loop. By default, the RAX711-L selects the **forced-freerun** mode. It means the RAX711-L uses the local crystal oscillator as the clock source.
7	Raisecom(config)#**synce source nni** *interface-number* **ring-outside**	Configure the RAX711-L to search a line clock source from the outside of the ring network. By default, the RAX711-L does not search a line clock source from the outside of the ring network.
8	Raisecom(config)#**synce revertive enable**	Enable auto reverse mode. By default, auto reverse mode is enabled.
9	Raisecom(config)#**synce source** { **nni** *interface-number* | **external 2m** *interface-number* | **pdh** *interface-number* } **wait-to-restore-time** *minutes*	Configure the WTR time of the clock source. By default, the WTR time of the clock source is set to 5 minutes.
10	Raisecom(config)#**synce source** { **nni** *interface-number* | **external 2m** *interface-number* | **pdh** *interface-number* } **hold-off-time** *time*	Configure the hold-off time of the clock source. By default, the hold-off time of the clock source is set to 1800ms.

Step	Command	Description
11	Raisecom(config)#**synce quality-level transmit-threshold** *threshold*	Configure the quality level threshold of the synchronous Ethernet packets. By default, the quality level threshold of the synchronous Ethernet packets is set to 0.
12	Raisecom(config)#**synce trap enable**	Enable synchronous Ethernet Trap. By default, synchronous Ethernet Trap is enabled.

3.1.3 Operating clock source manually

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**synce manual-source** { **nni** *interface-number* | **external 2m** *interface-number* | **internal** | **pdh** *interface-number* }	Switch the clock source manually.
3	Raisecom(config)#**synce forced-source** { **nni** *interface-number* | **external 2m** *interface-number* | **internal** | **pdh** *interface-number* }	Switch the clock source forcibly.
4	Raisecom(config)#**synce lockout-source** { **nni** *interface-number* | **external 2m** *interface-number* | **pdh** *interface-number* }	Lock out the clock source manually.

3.1.4 Configuring clock signal input/output

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**clock-mgmt slot** *slot-number*	Enter clock configuration mode.
3	Raisecom(config-clock)#**external-2m** *interface-number* **mode** { { **e1** | **e1-crc** } [**sa** *sa-value*] | **2mhz** }	(Optional) enable 2 Mbit/s clock signal input and configure its mode. By default, 2 Mbit/s clock signal input is enabled on the RAX711-L.
4	Raisecom(config-clock)# **external-2m** *interface-number* **output shutdown-threshold quality-level** *quality-level*	Configure the quality level threshold of output 2 Mbit/s clock signals. By default, no threshold is configured.

3.1.5 Checking configurations

No.	Command	Description
1	Raisecom#**show synce** [**source**]	Show configurations on clock synchronization based on synchronous Ethernet.

No.	Command	Description
2	Raisecom#**show synce ssm [source | statistic]**	Show synchronization status message based on synchronous Ethernet.
3	Raisecom#**show clock-mgmt slot** *slot-id*	Show clock signal configurations.
4	Raisecom#**show synce source extend-ssm**	Show extended SSM information of the synchronous Ethernet clock source.

3.2 Configuring clock synchronization based on PTP

3.2.1 Preparing for configurations

Scenario

The synchronous Ethernet can implement frequency synchronization only while the PTP can implement both frequency and phase synchronization, which is suitable for the scenario with requirements on frequency and phase synchronization, such as clock synchronization of the TD-SCDMA or CDMA2000 Base Station (BS).

Generally, you only need to configure PTP clock synchronization in global and interface configuration modes, specify the PTP clock type, and configure input/output clock signals of the subcard on the clock, then the RAX711-L can perform PTP clock synchronization with upstream and downstream devices. If there is no external clock source, the RAX711-L provides clock signals through the internal crystal oscillator clock.

According to the network location of the RAX711-L and configurations of upstream and downstream devices, you may need to configure PTP clock proprieties, packet transmission properties, interface properties of the PTP clock, and so on.

Prerequisite

Add the VLAN ID of the 1588v2 packet processed on the interface to the allowed VLAN list of the interface. Otherwise, the RAX711-L cannot process the packet properly.

3.2.2 Configuring PTP clock mode

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)#**ptp mode e2etransparent**	Configure clock synchronization based on PTP.
4	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical interface configuration mode.

Step	Command	Description
5	Raisecom(config-port)#**ptp enable**	Enable PTP on the interface. By default, PTP on the interface is disabled.

3.2.3 (Optional) configuring PTP clock properties

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ptp adjust-frequency enable**	Enable frequency adjustment of the PTP clock. By default, the RAX711-L is enabled with frequency adjustment of the PTP clock.

3.2.4 (Optional) configuring packet transmission properties

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ptp transmit** { **appropriate** | **multicast** | **unicast** }	Configure the mode for sending 1588v2 packets. By default, the RAX711-L sends 1588v2 packets in broadcast.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical interface configuration mode.
4	Raisecom(config-port)#**ptp protocol** { **ethernet** | **udp** | **ipv6** }	Specify the protocol type of transmitting 1588v2 packets. By default, the RAX711-L transmits 1588v2 packets based on Ethernet protocol.
9	Raisecom(config-port)#**ptp vlan** *vlan-id*	Configure the VLAN ID of 1588v2 packets encapsulated by the RAX711-L.

3.2.5 (Optional) configuring interface properties of PTP clock

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)#**ptp asymmetry** *nanosecond*	Configure the asymmetric delay check time of sending 1588v2 packets from the interface. By default, the asymmetric delay check time of sending 1588v2 packets from the interface is 0; namely, no asymmetric delay check is performed.

3.2.6 Checking configurations

No.	Command	Description
1	Raisecom#**show ptp** [*interface-type interface-number*]	Show global or interface PTP configurations.
2	Raisecom#**show ptp statistics** *interface-type interface-number*	Show 1588v2 packet statistics of the specified interface on the PTP clock device in slave mode.
3	Raisecom#**show ptp clock**	Show local clock configurations of the PTP clock device.

3.3 Maintenance

Command	Description
Raisecom(config)#**clear synce ssm statistic**	Clear synchronization status statistics of synchronous Ethernet.
Raisecom(config)#**clock-mgmt trap enable**	Enable clock sub-card Trap.

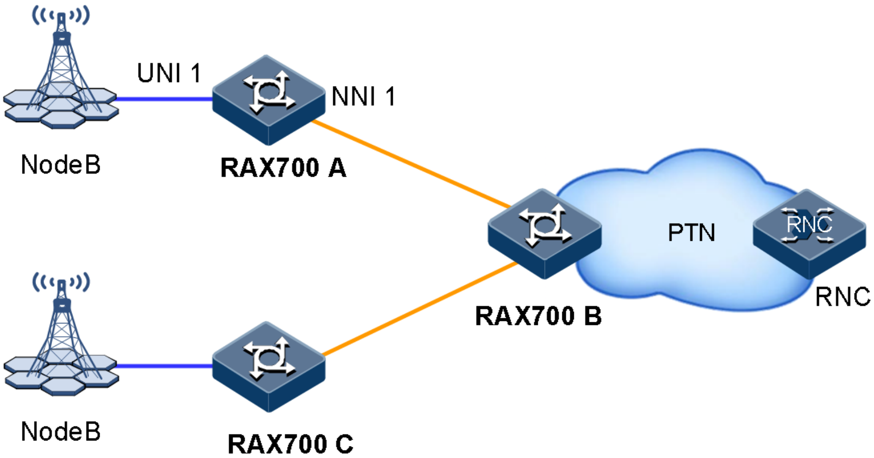
3.4 Configuration examples

3.4.1 Example for configuring clock synchronization based on synchronous Ethernet

Networking requirements

As shown in Figure 3-1, RAX700 B accesses RNC through the 2 Mbit/s clock interface to get high-accurate clock signals and then transmits these clock signals to RAX700 A through NNI 1. After receiving the clock signals, RAX700 A transmits them to NodeB through UNI 1.

Figure 3-1 Configuring clock synchronization based on synchronous Ethernet



Configuration steps

Step 1 Configure clock source properties.

- Configure RAX700 A.

```
Raisecom#hostname RAX700A
RAX700A#config
RAX700A(config)#synce enable
RAX700A(config)#synce operation-type auto-select
RAX700A(config)#synce source nni 1 priority 1
RAX700A(config)#synce source nni 1 wait-to-restore-time 0
```

- Configure RAX700 B.

```
Raisecom#hostname RAX700B
RAX700B#config
RAX700B(config)#synce enable
RAX700B(config)#synce operation-type auto-select
RAX700B(config)#synce source external 2m 1 priority 1
RAX700B(config)#synce source external 2m 1 wait-to-restore-time 0
RAX700B(config)#synce source external 2m 1 quality-level 0
```

Step 2 Save configurations of RAX700 A and RAX700 B, taking RAX700 A for example.

```
RAX700A#write
```

Checking results

Use the **show synce** command to show clock synchronization configurations of the synchronous Ethernet.

- Show clock synchronization configurations on RAX700 A.

```
RAX700A#show synce
Synce            : enable
Synce running status(PLL): freerun(auto-select)
Current clock source: internal(Ql:11)
Previous clock source: internal(Ql:11)
Synce trap        : enable
Revertive mode     : enable
Transmit quality level threshold: 0
Latest switch time  : 2106-02-06,17:52:12.116
Ql degradation to eec1 mode : lock
```

- Show clock synchronization configurations on RAX700 B.

```
RAX700B#show synce
Synce            : enable
Synce running status(PLL):freerun(auto-select)
Current clock source: internal(Ql:11)
Previous clock source: internal(Ql:11)
Synce trap        : enable
Revertive mode     : enable
Transmit quality level threshold: 0
Latest switch time  : 2106-02-06,17:52:12.116
Ql degradation to eec1 mode : lock
```

Use the **show synce ssm** command to show SSM status of the synchronous Ethernet.

- Show SSM status on RAX700 A.

```
RAX700A#show synce ssm
Quality level mode  : enable
Ssm source name    : nni 1
Ssm state         : locked
Ssm quality level   : 0
```

- Show SSM status on RAX700 B.

```
RAX700B#show synce ssm
Quality level mode  : enable
Ssm source name    : external 2m 1
Ssm state         : locked
```

```
Ssm quality level   : 0
```

4 MPLS-TP

This chapter describes principles and configuration procedures of MPLS-TP, as well as related configuration examples, including following sections:

- Configuring basic functions of MPLS
- Configuring static LSP
- Configuring MPLS L2VPN
- Configuring MPLS-TP OAM
- Configuring MPLS-TP linear protection switching
- Configuring PW dual-homed protection switching
- Maintenance
- Configuration examples

4.1 Configuring basic functions of MPLS

4.1.1 Preparing for configurations

Scenario

Basic functions of MPLS are the basis for other MPLS functions taking effect. Basic functions of MPLS include enabling global MPLS and enabling MPLS on the interface. And configuring the LSR ID is the basis for enabling global MPLS.

Prerequisite

Only after you have enabled MPLS in global configuration mode, configured the IP address of the IP interface of the device, and associated the IP interface to a VLAN, can the MPLS feature on the interface take effect.

4.1.2 Configuring basic functions of MPLS

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

Step	Command	Description
2	Raisecom(config)#**mpls lsr-id** *lsr-id*	Configure the LSR ID. In general, use the IP address of some IP interface on the device as the LSR ID. By default, no LSR ID is configured.
3	Raisecom(config)#**mpls enable**	Enable global MPLS. By default, global MPLS is disabled.
4	Raisecom(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
5	Raisecom(config-ip)#**mpls enable**	Enable MPLS on the Layer 3 interface. By default, MPLS on the interface is enabled.

4.1.3 Checking configurations

No.	Command	Description
1	Raisecom#**show mpls**	Show global MPLS configurations.

4.2 Configuring static LSP

4.2.1 Preparing for configurations

Scenario

The static LSP is established by manually assigning labels for all FECs. It is suitable for simple and stable small-size network. To manually assign labels, the outgoing label value of the last node is the incoming label value of the next node.

The static LSP does not use the label distribution protocol and does not exchange the control packet. Therefore, it consumes fewer resources. However, the LSP, established by statically assigning labels, cannot be dynamically adjusted according to the network topology changes. The administrator needs to manually adjust the static LSP.

Prerequisite

Configure basic functions of MPLS.

4.2.2 Configuring static LSP

Configuring static LSP on Ingress node

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

Step	Command	Description
2	Raisecom(config)# **mpls static-lsp ingress** *lsp-name ip-address* [*mask*] **nexthop-mac** *mac-address* **vlan** *vlan-id interface-type interface-number* **out-label** *out-label* **lsr-id** *egress-lsr-id* **tunnel-id** *tunnel-id*	Configure the static LSP on the Ingress node.

Configuring static LSP on Transit node

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)# **mpls static-lsp transit** *lsp-name* **in-label** *in-label* **nexthop-mac** *mac-address* **vlan** *vlan-id interface-type interface-number* **out-label** *out-label* **lsr-id** *ingress-lsr-id egress-lsr-id* **tunnel-id** *tunnel-id* [**standby**]	Configure the static LSP on the Transit node.

Configuring static LSP on Egress node

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)# **mpls static-lsp egress** *lsp-name* **in-label** *in-label* **lsr-id** *ingress-lsr-id* **tunnel-id** *tunnel-id*	Configure the static LSP on the Egress node.

4.2.3 Configuring static bidirectional corouted LSP

Note

After configuring the static bidirectional corouted LSP, you need to configure the forward LSP and backward LSP in the ingress and egress directions respectively in bidirectional corouted LSP configuration mode.

- In ingress direction, the received MPLS packet carries the incoming label.
- In egress direction, the sent MPLS packet carries the outgoing label.

Configuring static bidirectional LSP on Ingress node

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls bidirectional static-lsp ingress** *lsp-name* **lsr-id** *egress-lsr-id* **tunnel-id** *tunnel-id*	Create a static bidirectional corouted LSP on the Ingress node and enter bidirectional Ingress configuration mode.

Step	Command	Description
3	Raisecom(config-ingress-lsp)#**forward** *dest-network* [*mask*] **nexthop-mac** *mac-address* **vlan** *vlan-id interface-type interface-number* **out-label** *out-label*	Configure the forward egress LSP which does not have the IP capability in bidirectional Ingress configuration mode.
4	Raisecom(config-ingress-lsp)#**backward in-label** *in-label*	Configure the backward ingress LSP in bidirectional Ingress configuration mode.

Configuring static bidirectional LSP on Transit node

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls bidirectional static-lsp transit** *lsp-name* **lsr-id** *ingress-lsr-id egress-lsr-id* **tunnel-id** *tunnel-id* [**standby**]	Create a static bidirectional corouted LSP on the Transit node and enter bidirectional Transit configuration mode.
3	Raisecom(config-transit-lsp)#**forward in-label** *in-label* **nexthop-mac** *mac-address* **vlan** *vlan-id interface-type interface-number* **out-label** *out-label*	Configure the forward LSP which does not have the IP capability in bidirectional Transit configuration mode.
4	Raisecom(config-transit-lsp)#**backward in-label** *in-label* **nexthop-mac** *mac-address* **vlan** *vlan-id interface-type interface-number* **out-label** *out-label*	Configure the backward LSP which does not have the IP capability in bidirectional Transit configuration mode.

Configuring static bidirectional LSP on Egress node

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls bidirectional static-lsp egress** *lsp-name* [**lsr-id** *ingress-lsr-id* **tunnel-id** *tunnel-id*]	Create a static bidirectional corouted LSP on the Ingress node and enter bidirectional Egress configuration mode.
3	Raisecom(config-egress-lsp)#**forward in-label** *in-label*	Configure the forward ingress LSP in bidirectional Egress configuration mode.
4	Raisecom(config-egress-lsp)#**backward** *dest-network* [*mask*] **nexthop-mac** *mac-address* **vlan** *vlan-id interface-type interface-number* **out-label** *out-label*	Configure the backward egress LSP which does not have the IP capability in bidirectional Egress configuration mode.

4.2.4 Configuring Tunnel

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface tunnel** *tunnel-number*	Enter Tunnel interface configuration mode. By default, the static MPLS Tunnel is not configured.
3	Raisecom(config-tunnelif)#**destination** *destination-ip-address*	Configure the destination IP address.
4	Raisecom(config-tunnelif)#**mpls tunnel-id** *tunnel-id*	Configure binding the MPLS Tunnel ID.

4.2.5 Checking configurations

No.	Command	Description
1	Raisecom#**show mpls lsp statistics**	Show LSP statistics.
2	Raisecom#**show mpls bidirectional static-lsp** [*lsp-name*]	Show bidirectional LSP configurations.
3	Raisecom#**show mpls statistics bidirectional lsp**	Show MPLS packet statistics of the bidirectional LSP.
4	Raisecom#**show mpls static-lsp** [**egress** | **ingress** | **transit** | *lsp-name*]	Show static LSP configurations.
5	Raisecom#**show mpls statistics lsp** [*lsp-name*]	Show LSP-based MPLS packet statistics.
6	Raisecom#**show mpls label** [*label-id* [**to** *label-id*]]	Show information about assigned MPLS label or status about a specified label.
7	Raisecom#**show mpls tunnel** [*tunnel-name*]	Show Tunnel configurations.

4.3 Configuring MPLS L2VPN

4.3.1 Preparing for configurations

Scenario

With MPLS L2VPN, the carrier can provide Layer 2 VPN services with different media on a uniform MPLS network, including VLAN and Ethernet. The MPLS network can still provide traditional services, such as IP, MPLS L3VPN, traffic engineering, and QoS.

Prerequisite

Since the RAX711-L does not support dynamic routing at present, when it is interconnected with another device supporting dynamic routing, you need to add the route to the RAX711-L on the device.

4.3.2 Configuring MPLS L2VPN

L2VC is required when you configuring Martini/SVC MPLS L2VPN.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls l2vpn**	Enable global MPLS L2VPN. By default, global MPLS L2VPN is enabled.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#**mpls l2vpn**	Enable MPLS L2VPN on an interface. By default, MPLS L2VPN on an interface is enabled.
5	Raisecom(config-port)#**mpls static-l2vc** { **vlan** *vlan-id* | **cvlan** *cvlan-id* } **destination** *ip-address* **raw vc-id** *vc-id* **in-label** *in-label* **out-label** *out-label* [**tunnel-policy** *policy-name* | **tunnel-interface** *tunnel-number*] [**priority** *priority*] [**no-control-word**] [**mtu** *mtu*] [**tpid** { **0x8100** | **0x9100** | **0x88a8** }] [**bandwidth cir** *cir* **pir** *pir*]	Configure static L2VC after extracting services based on interface+VLAN or interface+CVLAN, and use Raw encapsulation.
	Raisecom(config-port)#**mpls static-l2vc** { **vlan** *vlan-id* | **cvlan** *cvlan-id* } **destination** *ip-address* **tagged vc-id** *vc-id* **in-label** *in-label* **out-label** *out-label* [**tunnel-policy** *policy-name* | **tunnel-interface** *tunnel-number*] [**priority** *priority*] [**no-control-word**] [**mtu** *mtu*] [**tpid** { **0x8100** | **0x9100** | **0x88a8** }] [**svlan** *svlan-id*] [**bandwidth cir** *cir* **pir** *pir*]	Configure static L2VC after extracting services based on interface+VLAN or interface+CVLAN, and use Tagged encapsulation (based on SVLAN).
	Raisecom(config-port)#**mpls static-l2vc destination** *ip-address* **raw vc-id** *vc-id* **in-label** *in-label* **out-label** *out-label* [**tunnel-policy** *policy-name* | **tunnel-interface** *tunnel-number*] [**priority** *priority*] [**no-control-word**] [**mtu** *mtu*] [**tpid** { **0x8100** | **0x9100** | **0x88a8** }] [**bandwidth cir** *cir* **pir** *pir*]	Configure static L2VC after extracting services based on interface, and use Raw encapsulation.

<table>
<tr><th>Step</th><th>Command</th><th>Description</th></tr>
<tr><td></td><td>Raisecom(config-port)#mpls static-l2vc destination ip-address ethernet-vlan vc-id vc-id in-label in-label out-label out-label [tunnel-policy policy-name | tunnel-interface tunnel-number] [priority priority] [no-control-word] [mtu mtu] [tpid { 0x8100 | 0x9100 | 0x88a8 }] [svlan svlan-id] [bandwidth cir cir pir pir]</td><td>Configure static L2VC after extracting services based on interface, and use Ethernet VLAN encapsulation (based on SVLAN).</td></tr>
<tr><td></td><td>Raisecom(config-port)#mpls static-l2vc destination ip-address vc-id vc-id in-label in-label out-label out-label [tunnel-policy policy-name | tunnel-interface tunnel-number] { backup | bypass]</td><td>Create the backup PW and bypass PW (that is, DNI PW) in the PW protection group.</td></tr>
<tr><td>6</td><td>Raisecom(config-port)#no mpls static-l2vc [backup | bypass]</td><td>(Optional) delete the backup or bypass static L2VC which extracts services based on interface.</td></tr>
<tr><td></td><td>Raisecom(config-port)#no mpls static-l2vc [vlan vlan-id] [backup | bypass]</td><td>(Optional) delete the backup or bypass static L2VC which extracts services based on interface+VLAN or interface+CVLAN.</td></tr>
</table>

Note

- When the existing service is bound with any other VPN Tunnel, it does not support this configuration.
- When the encapsulation mode of packets is **raw**, in the ingress PW direction, if the TPID carried by the packet received by the PE is identical with the interface TPID, the Tag is deleted automatically; otherwise, the Tag remains unchanged. In the egress PW direction, the PE directly sends the packet to the AC.
- When the encapsulation mode of packets is **tagged**, in the ingress PW direction, if the TPID carried by the packet received by the PE is identical with the interface TPID, the Tag remains unchanged; otherwise, the default VLAN Tag is added. In the egress PW direction, the PE directly sends the packet to the AC.
- When configuring static L2VC, you need to configure it to carry the control word generally. Only when the related function of PW OAM is not needed, the control word may be not carried.

4.3.3 Checking configurations

<table>
<tr><th>No.</th><th>Command</th><th>Description</th></tr>
<tr><td>1</td><td>Raisecom#show mpls l2vc [static] [statistic] [interface-type interface-list] [vlan vlan-id | cvlan-list cvlan-list]</td><td>Show L2VC configurations.</td></tr>
<tr><td>2</td><td>Raisecom#show mpls l2vpn</td><td>Show L2VPN configurations.</td></tr>
</table>

4.4 Configuring MPLS-TP OAM

4.4.1 Preparing for configurations

Scenario

To extend the application of MPLS-TP technology in carrier-grade network, the MPLS-TP network needs to achieve the same service level as the carrier-grade transport network. Connectivity Fault Management (CFM) helps the MPLS-TP network to resolve the problem by providing complete OAM tools.

CFM can provide the following OAM functions for the MPLS-TP network:

- Fault detection (Continuity Check, CC)
- Fault acknowledgement (LoopBack, LB)
- Fault location (LinkTrace, LT)
- Alarm Indication Signal (AIS)
- Client Signal Fail (CSF)
- Lock (LCK)
- Packet Delay and Packet Delay Variation Measurements (DM)
- Frame Loss Measurements (LM)

The principle of MPLS-TP OAM is similar to the one of Ethernet-based OAM. Only the carrying modes of related packets are different.

To ensure that users can get qualified network services. The Carrier and users sign a Service Level Agreement (SLA). To effectively fulfil the SLA, the Carrier needs to deploy the SLA feature on the device to measure the network performance and takes the measurement result as the basis for ensuring the network performance.

SLA selects 2 detection points, configures, and schedules the SLA operation on one detection point to detect the network performance between the 2 detection points.

The SLA feature counts the round-trip packet loss ratio, round-trip/unidirectional (SD/DS) delay, jitter, jitter variance, and jitter distribution and reports them to the upper monitoring software (such as the NView NNM system). And then the upper monitoring software analyses the network performance to get a data meeting users' requirements.

Prerequisite

- Connect the interface, configure its physical parameters, and make it Up at the physical layer.
- Configure basic functions of MPLS.
- Before configuring SLA, you need to deploy CFM between devices that need to detect the network performance.

4.4.2 Enabling MPLS-TP CFM

Note

- The fault detection and fault location cannot take effect unless CFM is enabled.

- Before enabling the CFM packet delivery feature, you should configure the relationship between the service instance and static L2VC.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)# **mpls-tp cfm enable**	Enable global MPLS-TP CFM. By default, global MPLS-TP CFM is disabled.

4.4.3 Configuring MPLS-TP CFM

Associating service instance to LSP/PW/Section layer

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls-tp cfm channel-type** { **0X7FFA** | **0X8902** | *channel-type* }	(Optional) configure the MPLS-TP CFM control channel type. By default, the MPLS-TP CFM control channel type is set to 0X7FFA. **Note** Modifying the control channel type is only for the device communicating with devices from other vendors. Upon no specific requirements, we do not recommend modifying the configuration.
3	Raisecom(config)#**mpls-tp cfm domain level** *level*	Create a MPLS-TP Maintenance Domain (MD).
4	Raisecom(config)#**mpls-tp service** *cis-id* **level** *level*	Create a service instance and enter service instance configuration mode.
5	Raisecom(config-service)#**service lsp** { **bidirection** *lsp-name* | **ingress** *in-lsp-name* [**egress** *out-lsp-name*] | **egress** *out-lsp-name* }	(Optional) associate the service instance to a static LSP based on the static bidirectional LSP, ingress static LSP, or egress static LSP.
6	Raisecom(config-service)#**service lsp transit forward** *lsp-in* **backward** *lsp-out* **ttl** *ttl*	(Optional) configure the server instance connected by the subnet based on the ingress static LSP or egress static LSP.
7	Raisecom(config-service)#**service lsp transit bidirection** *lsp-name* **lsr-id** *lsr-id* **ttl** *ttl*	Configure the service instance based on the subnet connection of the bidirectional LSP.
8	Raisecom(config-service)#**service pw transit forward vc-id** *vc-id* **destination** *ip-address* **backward vc-id** *vc-id* **destination** *ip-address*	(Optional) associate the service instance to the Transit PW.
9	Raisecom(config-service)#**service section** *interface-type interface-number*	(Optional) associate the service instance to the Section.

Step	Command	Description
10	Raisecom(config-service)#**service section dest-mac** *mac-address*	(Optional) configure the destination MAC address of the Section-layer CC.

Configuring MEPs based on MPLS-TP service instances

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls-tp cfm domain level** *level*	Create a MPLS-TP MD.
3	Raisecom(config)#**mpls-tp service** *csi-id* **level** *level*	Create a service instance and enter service instance configuration mode.
4	Raisecom(config-service)#**service vc-id** *vc-id* **destination** *ip-address*	Configure the VC ID associated to the service instance.
5	Raisecom(config-service)#**service mep mpid** *mep-id*	Configure a MEP based on the service instance.

Note

Before enabling the CFM packet delivery feature, you should configure the relationship between the service instance and static L2VC.

4.4.4 Configuring fault detection

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls-tp cfm remote mep age-time** *minute*	(Optional) configure the aging time of the Remote MEP (RMEP). By default, the aging time of the learned RMEP is set to 100min. **Note** This configuration takes effect on the dynamic RMEP only.
3	Raisecom(config)#**mpls-tp cfm errors archive-hold-time** *minute*	(Optional) configure the hold time of error CC packets. By default, the hold time of error CC packets is set to 100min. When the new hold time is configured, the system will check the database immediately. If any data exceeds the hold time, it will be deleted from the database.
4	Raisecom(config)#**mpls-tp service** *cis-id* **level** *level*	Enter service instance configuration mode.

Step	Command	Description
5	Raisecom(config-service)#**service cc interval** { **1** | **10** | **60** | **600** | **3ms** | **10ms** | **100ms** }	(Optional) configure the interval for sending service instance CC packet. By default, the interval for sending service instance CC packet is set to 1s. When the CC packet delivery is enabled, the interval for sending CC packet cannot be modified.
6	Raisecom(config-service)#**service cc enable mep** { *mep-id-list* | **all** }	Enable MEP sending CC packet. By default, the MEP does not send CC packet. You can use the **service cc disable mep** { *mepid-list* | **all** } command to disable CC packet delivery.
7	Raisecom(config-service)#**service remote-mep** *mep-id* [**remote-mac** *mac-address*]	(Optional) configure the static RMEP. It cooperates with CC packet detection feature.
8	Raisecom(config-service)#**service remote-mep cc-check enable**	(Optional) enable REMP CC packet check. After REMP CC packet check is enabled, once receiving the CC packet, the service instance will check whether the dynamically learned RMEP ID is identical to the statically-configured one. If they are inconsistent, the service instance takes the CC packet as an errored one. By default, REMP CC packet check is disabled.
9	Raisecom(config-service)#**service remote-mep learning active**	(Optional) enable RMEP learning dynamic import. After RMEP learning dynamic import is enabled, once receiving the CC packet, the service instance will automatically translate the learned dynamic RMEP into static RMEP. By default, RMEP learning dynamic import is disabled.
10	Raisecom(config-service)#**service priority** *priority*	(Optional) configure CFM OAM packet priority. After the CFM OAM packet priority is configured, CCM, LBM, LTM, DDM packets sent by all MEPs in a service instance will use the specified priority. By default, the CFM OAM packet priority is set to 7.

4.4.5 Configuring fault acknowledgement

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls-tp service** *cis-id* **level** *level*	Enter service instance configuration mode.

Step	Command	Description
3	Raisecom(config-service)#**ping** { **egress** | **ingress** } **ttl** *time* [**count** *count*] [**size** *size*][**source** *mep-id*] [**timeout** *time*] [**padding** { **null** | **null-crc** | **prbs** | **prbs-crc** }]	Execute MPLS-TP layer Ping to acknowledge the fault. By default, the number of transmitted LBM packets is set to 5. The packet TLV is set to 64. In addition, the service instance automatically searches for an available source MEP.

Note

- Before executing this command, you must ensure that the global CFM is enabled. Otherwise, the Ping operation fails.
- If no MEP is configured for the service instance, the Ping operation will fails because no source MEP is found.
- The 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.
- The Ping operation will fail if another user is using the specified source MEP to initiate the Ping operation.

4.4.6 Configuring fault location

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls-tp service** *cis-id* **level** *level*	Enter service instance configuration mode.
3	Raisecom(config-service)#**traceroute mep** *mep-id* [**ttl** *ttl*] [**source** *mep-id*] [**interface-mode**] [**timeout** *time*] Raisecom(config-service)#**traceroute mip icc** *icc node-id* [**ttl** *ttl*] [**interface-num** *number*] [**timeout** *time*] Raisecom(config-service)#**traceroute ttl** *ttl* [**interface-mode**] [**timeout** *time*]	Execute MPLS-TP layer Traceroute to locate the fault. By default, the packet TLV is set to 64. In addition, the service instance automatically searches for an available source MEP.

Note

- Before executing this command, you must ensure that the global CFM is enabled. Otherwise, the Traceroute operation fails.
- The 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.

- The Traceroute operation will fail if another user is using the specified source MEP to initiate the Ping operation.

4.4.7 Configuring AIS

Steps 6 is optional and perform it as required.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls-tp service** *cis-id* **level** *level*	Enter service instance configuration mode.
3	Raisecom(config-service)#**service ais enable**	Enable AIS delivery. By default, AIS delivery is disabled. You can use the **service ais disable** command to disable AIS delivery.
4	Raisecom(config-service)#**service ais period** { **1** | **60** }	Configure the AIS delivery period. By default, the AIS delivery period is set to 1s.
5	Raisecom(config-service)#**service ais level** *level* [**vlan** *vlan-id*]	Configure the level of client-layer MD to which the AIS is sent.
6	Raisecom(config-service)#**service suppress-alarms enable mep** { **all** | *mep-list* }	Enable MEP alarm inhibition.

4.4.8 Configuring signal locking

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls-tp service** *cis-id* **level** *level*	Enter service instance configuration mode.
3	Raisecom(config-service)#**service lck start mep** { *mep-id* | **all** }	Enable sending the LCK packet. By default, sending the LCK packet is disabled.
4	Raisecom(config-service)#**service lck period** { **1** | **60** }	Configure the sending interval of the LCK packet. By default, the sending interval is 1s.
5	Raisecom(config-service)#**service lck level** *level* [**vlan** *vlan-id*]	Configure the service instance level of the LCK packet sent by the MEP.

4.4.9 Configuring basic information about MPLS-TP SLA operation

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

Step	Command	Description
2	Raisecom(config)#**sla** oper-num **mpls-y1731-echo level** level { **section** interface-type interface-number | **lsp-ingress** lsp-egress-name **lsp-egress** lsp-ingress-name | **vcid** vc-id **peer-address** ip-address } [**tc** tc-id]	Create mpls-y1731-echo operations based on Section layer, LSP layer, or PW layer.
3	Raisecom(config)#**sla** oper-num **mpls-y1731-jitter level** level { **section** interface-type interface-number | **lsp-ingress** lsp-egress-name **lsp-egress** lsp-ingress-name | **vcid** vc-id **peer-address** ip-address } [**tc** tc-id] [**interval** period] [**packets** packets-num]	Create mpls-y1731-jitter operations based on Section layer, LSP layer, or PW layer.
4	Raisecom(config)#**sla mpls-y1731-echo quick-input** [**level** level { **section** interface-type interface-number | **lsp-ingress** lsp-egress-name **lsp-egress** lsp-ingress-name | **vcid** vc-id **peer-address** ip-address }]	Quickly create mpls-y1731-echo operations based on Section layer, LSP layer, or PW layer.
5	Raisecom(config)#**sla mpls-y1731-jitter quick-input** [**level** level { **section** interface-type interface-number | **lsp-ingress** lsp-egress-name **lsp-egress** lsp-ingress-name | **vcid** vc-id **peer-address** ip-address }]	Quickly create mpls-y1731-jitter operations based on Section layer, LSP layer, or PW layer.
6	Raisecom(config)#**sla** oper-num **mpls-y1731-pkt-loss level** level { **section** interface-type interface-number | **lsp-ingress** lsp-egress-name **lsp-egress** lsp-ingress-name | **vcid** vc-id **peer-address** ip-address } [**tc** tc-id] [**interval** period] [**packets** packets-num]	Create mpls-y1731-pkt-loss operations based on Section layer, LSP layer, or PW layer.
7	Raisecom(config)#**sla** oper-num **mpls-y1731-pkt-loss level** level **lsp-ingress** lsp-egress-name **lsp-egress** lsp-ingress-name [**tc** tc-id] **sd**	Create mpls-y1731-pkt-loss signal degradation operations based on LSP layer.
8	Raisecom(config)#**sla schedule** oper-num [**life** { **forever** | life-time }] [**period** period]	Configure SLA scheduling information and enable SLA operation scheduling. By default, SLA operation scheduling is disabled.

4.4.10 Configuring SLA shceduling information and enabling SLA operation scheduling

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla schedule** *oper-num* [**life** { **forever** | *life-time* }] [**period** *period*]	Configure SLA scheduling information and enable SLA operation scheduling. By default, SLA operation scheduling is disabled.

Note

- The interval to send signal degradation operation packets is fixed to 500ms and the number of detection packets is fixed to 2.
- After SAL scheduling is enabled, the period of the signal degradation operation must be configured as 1s and the life time must be configured as forever.

4.4.11 Checking configurations

No.	Command	Description
1	Raisecom#**show mpls-tp cfm**	Show MPLS-TP CFM global configurations.
2	Raisecom#**show mpls-tp cfm domain** [**level** *level*]	Show MD and service instance configurations.
3	Raisecom#**show mpls-tp cfm errors** [**level** *level*]	Show error CCM database information.
4	Raisecom#**show mpls-tp cfm ais** [**level** *level*]	Show AIS configurations.
5	Raisecom#**show mpls-tp cfm lck** [**level** *level*]	Show LCK configurations.
6	Raisecom#**show mpls-tp cfm local-mp** [**level** *level*]	Show local MEP configurations.
7	Raisecom#**show mpls-tp cfm remote-mep static**	Show static RMEP configurations.
8	Raisecom#**show mpls-tp cfm remote-mep** [**level** *level* [**service** *service-instance* [**mepid** *mep-id*]]]	Show RMEP discovery information.
9	Raisecom#**show mpls-tp cfm suppress-alarms** [**level** *level*]	Show CFM alarm inhibition configurations.
10	Raisecom#**show sla** { **all** | *oper-num* } **configuration**	Show SLA configurations.
11	Raisecom#**show sla** { **all** | *oper-num* } **result**	Show the last test information of the operation.
12	Raisecom#**show sla** { **all** | *oper-num* } **statistic**	Show operation scheduling statistics. Statistics of an operation (identified by the operation ID) is recorded up to 5 groups. If the number exceeds 5, the most aged (calculated based on the begin time of the operation scheduling) statistics will be aged.

4.5 Configuring MPLS-TP linear protection switching

4.5.1 Preparing for configurations

Scenario

MPLS-TP linear protection switching protects the primary link by providing a backup link. Therefore, it provides end-to-end protection for LSP links between devices.

Prerequisite

- Configure MPLS basic functions.
- Configure the static LSP.
- Configure MPLS-TP OAM.
- Create the working PW/LSP and protection PW/LSP.

4.5.2 Configuring LSP-based 1:1 linear protection switching

Before configuring MPLS-TP linear protection switching, you should attach the bidirectional/ingress/egress static LSP to the related service instance.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls-tp line-protection association** *aps-name level ma-name*	Configure the information about service instance associated to MPLS-TP APS. Create association information about service instances and APS of working line and protection line.
3	Raisecom(config)#**mpls-tp line-protection** *aps-id* **lsp working** *ingress-aps-name egress-aps-name* **protection** *ingress-aps-name egress-aps-name* **one-to-one** [**non-revertive**]	Create the LSP-based 1:1 linear protection line.

Caution

After you perform the MS-W operation(traffic is switched from the protection line back to the working line manually), if the device fails, recovers from a fault, or performs other protection group commands, such as **lockout**, **force-switch**, or **manual-switch**, both devices of the protection group may select different lines. In this case, you should use the **clear mpls-tp line-protection** aps-id **command** command to clear the configured protection group command, making devices select the same line.

4.5.3 Configuring PW-based 1:1 linear protection switching

Before configuring PW-based 1:1 linear protection switching, perform the following operations in advance:

- Configure basic functions of MPLS; create the LSP; relate the Tunnel interface.
- Create the working PW and protection PW.
- Configure MPLS-TP CFM; relate the PW to the related service instance; configure the service instance.

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

Step	Command	Description
2	Raisecom(config)#**mpls-tp line-protection association** *aps-name level ma-name*	Configure the information about service instances associated to MPLS-TP APS. Create association information about service instances and APS of the working line and protection line.
3	Raisecom(config)#**mpls-tp line-protection** *aps-id* **pw working** *association-name* **protection** *association-name* **one-to-one** [**non-revertive**]	Create the PW-based 1:1 linear protection line.

4.5.4 Configuring operation properties of LSP-/PW-based linear protection switching

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls-tp line-protection** *aps-id* **name** *string*	(Optional) configure the name of the MPLS-TP linear protection line.
3	Raisecom(config)#**mpls-tp line-protection** *aps-id* { **working** | **protection** } **failure-detect** { **cc** | **phisycal-lsp** | **sd** }	Configure the fault detection mode of the MPLS-TP working/protection line, including CC fault detection, physical line fault detection, and SD fault detection. This command format is based on one detection mode.
	Raisecom(config)# **mpls-tp line-protection** *aps-id* { **working** | **protection** } **failure-detect** { **cc phisycal-lsp** | **cc sd** | **phisycal-lsp sd** }	This command format is based on two detection modes.
	Raisecom(config)#**mpls-tp line-protection** *aps-id* { **working** | **protection** } **failure-detect cc phisycal-lsp sd**	This command format is based on three detection modes.
4	Raisecom(config)#**mpls-tp line-protection trap enable**	Enable MPLS-TP linear protection Trap.
5	Raisecom(config)#**mpls-tp line-protection** *aps-id* **force-switch**	Switch the traffic from the working line to the protection line forcedly.
6	Raisecom(config)#**mpls-tp line-protection** *aps-id* **hold-off-timer** *hold-off-timer*	Configure the HOLD-OFF timer.
7	Raisecom(config)#**mpls-tp line-protection** *aps-id* **lockout**	Lock the protection switching feature of the lines.
8	Raisecom(config)#**mpls-tp line-protection** *aps-id* **manual-switch**	Switch the traffic from the working line to the protection line manually.
9	Raisecom(config)#**mpls-tp line-protection** *aps-id* **manual-switch-to-work**	Switch the traffic from the protection line back to the working line manually.

Step	Command	Description
10	Raisecom(config)#**clear mpls-tp line-protection** *aps-id* **command**	Clear MPLS-TP linear protection switching operations, including Lockout, Manual-switch, and Manual-switch-to-work.
11	Raisecom(config)#**mpls-tp line-protection** *aps-id* **wtr-timer** *wtr-timer*	(Optional) configure the WTR timer. By default, the value of the WTR timer is set to 5min.

4.5.5 Checking configurations

No.	Command	Description
1	Raisecom#**show mpls-tp line-protection association**	Show APS association information of MPLS-TP linear protection switching.
2	Raisecom#**show mpls-tp line-protection** [*aps-id*] **config**	Show MPLS-TP linear protection switching configurations.
3	Raisecom#**show mpls-tp line-protection** [*aps-id*] **statistics**	Show MPLS-TP linear protection switching statistics.
4	Raisecom#**show mpls-tp line-protection** [*aps-id*] **status**	Show APS information of MPLS-TP linear protection switching.

4.6 Configuring PW dual-homed protection switching

4.6.1 Preparing for configurations

Scenario

PW dual-homed protection switching refers to protecting access links between the local device and PTN through cooperation of the working PW, protection PW, and Dual Node Interconnection Pseudo Wire (DNI-PW). Moreover, it can provide protection when the local PE node fails.

Prerequisite

- Configure the IP address of the device, and associate the IP address to the corresponding VLAN.
- Configure basic functions of MPLS, create the LSP, and associate the LSP to the Tunnel interface.
- Create the working PW, protection PW, and DNI-PW.
- Configure MPLS-TP CFM. Associate the PW to the corresponding service instance and configure information about the service instance.
- Create the Inter-Chassis Communication Protocol (ICCP) channel.

4.6.2 Configuring ICCP channel

In the application scenario of the PW dual-homed protection switching, the local device accesses the PTN through two PE devices. An ICCP channel should be established between the two PE devices to carry the DNI-PW.

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. This IP address must be identical with some IP address of the device.
3	Raisecom(config)#**iccp channel** *channel-id*	Create the ICCP channel and enter ICCP configuration mode.
4	Raisecom(config-iccp)#**member-ip** *ip-address*	Configure the peer IP address of the ICCP channel.
5	Raisecom(config-iccp)#**iccp enable**	Enable the ICCP channel.

4.6.3 Configuring PW dual-homed protection switching

Configuring working PW

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls-tp line-protection association** *aps-name level ma-name*	Associate the working PW in the PW dual-homed protection group to the CFM service instance. **Note** Before the configuration, you need to use the **mpls-tp service** and **service vc-id** commands to configure information about the CFM service instance related to the working PW.
3	Raisecom(config)#**mpls-tp line-protection** *aps-id* **mc-pw working** *aps-name*	Configure the protection PW for the working node and associate it to the working PW.
4	Raisecom(config)#**mpls-tp line-protection** *aps-id* **binding-channel** *channel-id*	Bind the working PW with the ICCP channel on the working node. **Note** After step 2 and step 3, step 4 establishes the association between the working PW and DNI-PW actually.

Configuring protection PW

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls-tp line-protection association** *aps-name level ma-name*	Associate the protection PW in the PW dual-homed protection group to the CFM service instance. **Note** Before the configuration, you need to use the **mpls-tp service** and **service vc-id** commands to configure information about the CFM service instance related to the protection PW.
3	Raisecom(config)#**mpls-tp line-protection** *aps-id* **mc-pw protection** *aps-name* **one-to-one** [**non-revertive**]	Configure the protection PW in the PW dual-homed protection group.
4	Raisecom(config)#**mpls-tp line-protection** *aps-id* **binding-channel** *channel-id*	Bind the protection PW with the ICCP channel. **Note** After step 2 and step 3, step 4 establishes the association between the protection PW and DNI-PW actually.

4.6.4 Checking configurations

No.	Command	Description
1	Raisecom(config)#**show iccp channel** [*channel-id*] **statistics**	Show statistics of received and sent packets of the ICCP channel.
2	Raisecom(config)#**show iccp channel** *channel-id*	Show configurations and operation information about the ICCP channel.
3	Raisecom(config)#**show mpls-tp line-protection** [*aps-id*] { **config** | **statistics** | **status** }	Show configurations, statistics, and status of the PW dual-homed protection switching.

4.7 Maintenance

Command	Description
Raisecom(config)#**clear mpls-tp cfm errors** [**level** *md-level*]	Clear wrong CCM records.

Command	Description
Raisecom(config)#**clear mpls-tp cfm remote-mep** [**level** *md-level*]	Clear information about the RMEP. **Note** This configuration takes effect on the dynamic RMEP only.
Raisecom(config)#**clear mpls statistics lsp** [*lsp-name*] Raisecom(config)#**clear mpls pw** { *ip-address vc-id* **statistic** | **statistic** }	Clear static LSP/PW statistics.
Raisecom(config)#**clear mpls-tp line-protection** *aps-id* **command**	Clear protection switching operations.
Raisecom(config)# **clear mpls-tp line-protection** [*aps-id*] **statistics**	Clear MPLS-TP linear protection switching statistics.

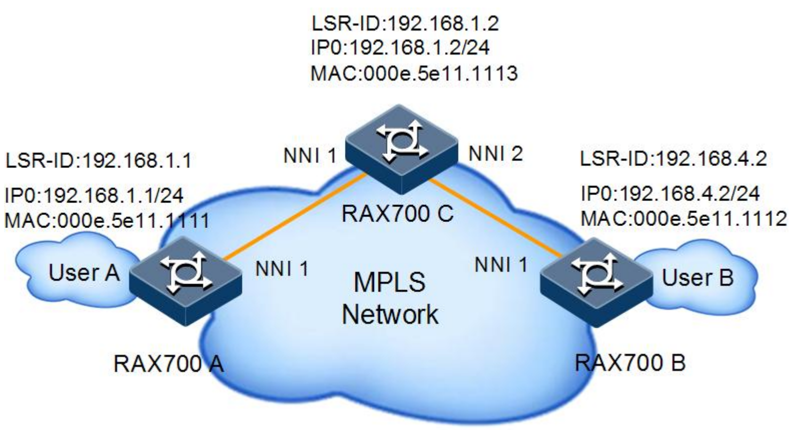
4.8 Configuration examples

4.8.1 Example for configuring bidirectional static LSP

Networking requirements

As shown in Figure 4-1, User A has branches at 2 locations. You need to establish VPN between the 2 locations. Therefore, devices at these 2 locations can communicate with each other. Because the network is small and stable, you can configure the bidirectional static LSP between RAX700 A and RAX700 B and take it as the public Tunnel of the L2VPN.

Figure 4-1 Configuring the bidirectional static LSP



Configuration steps

Step 1 Configure MPLS basic functions.

- Configure RAX700 A.

```
RAX700A(config)#mpls lsr-id 192.168.1.1
RAX700A(config)#mpls enable
```

- Configure RAX700 B.

```
RAX700B(config)#mpls lsr-id 192.168.4.2
RAX700B(config)#mpls enable
```

- Configure RAX700 C.

```
RAX700C(config)#mpls lsr-id 192.168.1.2
RAX700C(config)#mpls enable
```

Step 2 Configure the bidirectional static LSP between RAX700 A and RAX700 B.

- Configure RAX700 A.

```
RAX700A(config)#mpls bidirectional static-lsp ingress lspAB lsr-id
192.168.4.2 tunnel-id 1
RAX700A(config-ingress-lsp)#forward 192.168.4.0 nexthop-mac
000e.5e11.1113 vlan 1 nni 1 out-label 1001
RAX700A(config-ingress-lsp)#backward in-label 2001
```

- Configure RAX700 C.

```
RAX700C(config)#mpls bidirectional static-lsp transit lspAB lsr-id
192.168.1.1 192.168.4.2 tunnel-id 1
RAX700C(config-transit-lsp)#forward in-label 1001 nexthop-mac
000e.5e11.1112 vlan 1 nni 2 out-label 1002
RAX700C(config-transit-lsp)#backward in-label 2002 nexthop-mac
000e.5e11.1111 vlan 1 nni 1 out-label 2001
```

- Configure RAX700 B.

```
RAX700B(config)#mpls bidirectional static-lsp egress lspAB lsr-id
192.168.1.1 tunnel-id 1
RAX700B(config-egress-lsp)#forward in-label 1002
RAX700B(config-egress-lsp)#backward 192.168.1.0 nexthop-mac
000e.5e11.1113 vlan 1 nni 1 out-label 2002
```

Checking results

Use the **show mpls bidirectional static-lsp** command to show bidirectional static LSP configurations on RAX700 A, RAX700 B, and RAX700 C.

- Show bidirectional static LSP configurations on RAX700 A.

```
RAX700A(config)#show mpls bidirectional static-lsp lspAB
LSP-Index:            1
LSP-Name:             lspAB
LSR-Role:             Ingress
LSP-Flag:             Working
Ingress-Lsr-Id:        1.1.1.1
Egress-Lsr-Id:        192.168.4.2
Forward Destination:    192.168.4.0
Forward In-Label:      --
Forward Out-Label:      1001
Forward In-Interface:   --
Forward Out-Interface:   nni 1
Forward Next-Hop:      --
Forward Next-Mac:      000E.5E11.1113
Forward Vlan-Id:       1
Backward Destination:   --
Backward In-Label:      2001
Backward Out-Label:     --
Backward In-Interface:   all interfaces
Backward Out-Interface:  --
Backward Next-Hop:      --
Backward Next-Mac:      --
Backward Vlan-Id:      --
Tunnel-Id:            1
LSP Status:           Up
```

- Show bidirectional static LSP configurations on RAX700 B.

```
RAX700B(config)#show mpls bidirectional static-lsp lspAB
LSP-Index:            2
LSP-Name:             lspAB
LSR-Role:             Egress
LSP-Flag:             Working
Ingress-Lsr-Id:        192.168.1.1
Egress-Lsr-Id:        1.1.1.1
Forward Destination:    --
Forward In-Label:      1002
Forward Out-Label:      --
Forward In-Interface:   all interfaces
Forward Out-Interface:  --
Forward Next-Hop:      --
Forward Next-Mac:      --
Forward Vlan-Id:       --
Backward Destination:   192.168.1.0
Backward In-Label:      --
```

```
Backward Out-Label:     2002
Backward In-Interface:   --
Backward Out-Interface:  nni 1
Backward Next-Hop:      --
Backward Next-Mac:      000E.5E11.1113
Backward Vlan-Id:       1
Tunnel-Id:            1
LSP Status:           Up
```

- Show bidirectional static LSP configurations on RAX700 C.

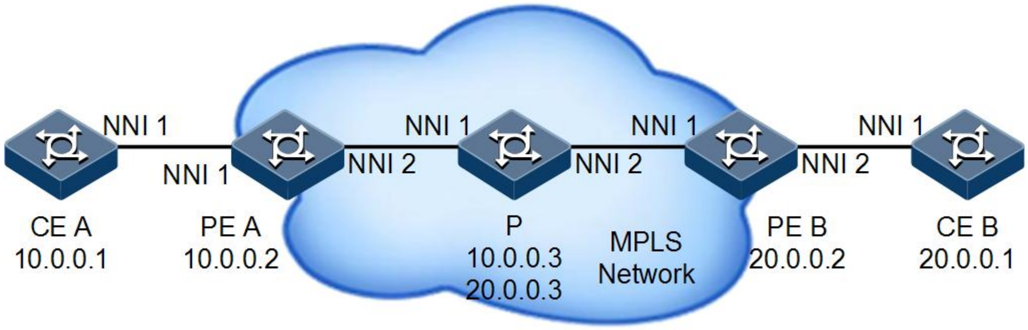
```
RAX700C(config)#show mpls bidirectional static-lsp lspAB
LSP-Index:            3
LSP-Name:             lspAB
LSR-Role:             Transit
LSP-Flag:             Working
Ingress-Lsr-Id:        192.168.1.1
Egress-Lsr-Id:         192.168.4.2
Forward Destination:    --
Forward In-Label:      1001
Forward Out-Label:     1002
Forward In-Interface:   all interfaces
Forward Out-Interface:  nni 2
Forward Next-Hop:      --
Forward Next-Mac:      000E.5E11.1112
Forward Vlan-Id:       1
Backward Destination:   --
Backward In-Label:     2002
Backward Out-Label:     2001
Backward In-Interface:   all interfaces
Backward Out-Interface:  nni 1
Backward Next-Hop:      --
Backward Next-Mac:      000E.5E11.1111
Backward Vlan-Id:       1
Tunnel-Id:            1
LSP Status:           Up
```

4.8.2 Example for configuring static LSP to carry static L2VC

Networking requirements

As shown in Figure 4-2, CE devices and PE devices are connected through Line interfaces. To make CE A and CE B communicate with each other, you should create the static L2VC based on the static LSP between PE A and PE B.

Figure 4-2 Configuring the static LSP to carry the static L2VC



Configuration steps

Step 1 Configure CE A. Create VLANs and add the specified interface to VLANs. Configure the IP address. Configuration s steps for CE B are identical to the ones for CE A.

```
Raisecom#hostname CEA
CEA#config
CEA(config)#create vlan 2-4 active
CEA(config)#interface ip 0
CEA(config-ip)#ip address 10.0.0.1 3
CEA(config-ip)#exit
CEA(config)#interface nni 1
CEA(config-port)#switchport mode trunk
```

Step 2 Configure IP addresses for PE A and PE B and create VLANs for PE A, PE B, and P.

- Configure PE A.

```
Raisecom#hostname PEA
PEA#config
PEA(config)#create vlan 2-4 active
PEA(config)#interface ip 0
PEA(config-ip)#ip address 10.0.0.2 4
PEA(config-ip)#exit
PEA(config-port)#interface nni 2
PEA(config-port)#switchport mode trunk
PEA(config-port)#switchport trunk allowed vlan 2-4
PEA(config-port)#exit
```

- Configure PE B.

```
Raisecom#hostname PEB
PEB#config
PEB(config)#create vlan 2-4 active
PEB(config)#interface ip 0
```

```
PEB(config-ip)#ip address 20.0.0.2 4
PEB(config-ip)#exit
PEB(config)#interface nni 1
PEB(config-port)#switchport mode trunk
PEB(config-port)#switchport trunk allowed vlan 2-4
PEB(config-port)#exit
```

- Configure P.

```
Raisecom#hostname P
P#config
P(config)#create vlan 2-4 active
P(config)#interface nni 1
P(config-port)#switchport mode trunk
P(config-port)#switchport trunk allowed vlan 2-4
P(config-port)#interface nni 2
P(config-port)#switchport mode trunk
P(config-port)#switchport trunk allowed vlan 2-4
P(config-port)#exit
```

Step 3 Enable MPLS on PE A, PE B, and P and configure the static LSP. Create the Tunnel between PE A and PE B and configure the static L2VC.

- Configure PE A.

```
PEA(config)#mpls lsr-id 10.0.0.2
PEA(config)#mpls enable
PEA(config)#mpls static-lsp ingress a2b 20.0.0.2 255.255.255.255 nexthop-
mac 000e.5e11.1113 vlan 4 nni 2 out-label 301 lsr-id 20.0.0.2 tunnel-id 1
PEA(config)#mpls static-lsp egress b2a in-label 201 lsr-id 20.0.0.2
tunnel-id 2
PEA(config)#interface tunnel 1
PEA(config-tunnelif)#destination 20.0.0.2
PEA(config-tunnelif)#mpls tunnel-id 1
PEA(config-tunnelif)#exit
PEA(config)#mpls l2vpn
PEA(config)#interface nni 1
PEA(config-port)#mpls static-l2vc destination 20.0.0.2 raw vc-id 1 vc-
label 401 tunnel-interface 1
PEA(config-port)#exit
```

- Configure PE B.

```
PEB(config)#mpls lsr-id 20.0.0.2
PEB(config)#mpls enable
PEB(config)#mpls static-lsp egress a2b in-label 302 lsr-id 10.0.0.2
tunnel-id 1
```

```
PEB(config)#mpls static-lsp ingress b2a 10.0.0.2 255.255.255.255 nexthop-
mac 000e.5e11.1113 vlan 4 nni 1 out-label 202 lsr-id 10.0.0.2 tunnel-id 2
PEB(config)#interface tunnel 1
PEB(config-tunnelif)#destination 10.0.0.2
PEB(config-tunnelif)#mpls tunnel-id 1
PEB(config-tunnelif)#exit
PEB(config)#mpls l2vpn
PEB(config)#interface nni 1
PEB(config-port)#mpls static-l2vc destination 10.0.0.2 raw vc-id 1 vc-
label 401 tunnel-interface 2
PEB(config-port)#exit
```

- Configure P.

```
P(config)#mpls lsr-id 10.0.0.3
P(config)#mpls enable
P(config)#mpls static-lsp transit a2b in-label 301 nexthop-mac
000e.5e11.1112 vlan 4 nni 2 out-label 302 lsr-id 10.0.0.2 20.0.0.2
tunnel-id 1
P(config)#mpls static-lsp transit b2a in-label 202 nexthop-mac
000e.5e11.1111 vlan 4 nni 1 out-label 201 lsr-id 20.0.0.2 10.0.0.2
tunnel-id 2
```

Checking results

Use the **show mpls static-lsp** command to show static LSP configurations, taking PE A for an example.

```
PEA(config)#show mpls static-lsp
LSP-Index:            2
LSP-Name:            b2a
LSR-Role:            Ingress
LSP-Flag:            Working
Ingress-Lsr-Id:        10.0.0.2
Egress-Lsr-Id:        20.0.0.2
FEC:               20.0.0.2
In-Label:            --
Out-Label:            201
In-Interface:          --
Out-Interface:         nni 1
Next-Hop:            --
Next-Mac:            000E.5E12.1113
Vlan-Id:            4
Tunnel-Id:            2
LSP Status:           Down
LSP-Index:            3
LSP-Name:            a2b
LSR-Role:            Egress
LSP-Flag:            Working
```

```
Ingress-Lsr-Id:        20.0.0.2
Egress-Lsr-Id:         10.0.0.2
FEC:                 --
In-Label:             301
Out-Label:            --
In-Interface:          all interfaces
Out-Interface:         --
Next-Hop:             --
Next-Mac:             --
Vlan-Id:              --
Tunnel-Id:            1
LSP Status:           Up
```

Use the **show interface tunnel** command to show whether the Tunnel is created successfully, taking PE A for example.

```
PEA(config)#show interface tunnel
Interface tunnel 1
Encapsulation is MPLS
Tunnel source 10.0.0.2, destination 20.0.0.2,
Tunnel protocol static, tunnel id 1 ,explicit-path:--,
Tunnel related LSP Type: Unidirectinal, LSP-name: a2b,
Tunnel current state : UP
Last up time: 2013-3-16, 12:26:17
```

Use the **show mpls l2vc** command to show static L2VC configurations, taking PE A for example.

```
PEA(config-port)#show mpls l2vc
  Client Interface  : nni 1
  Client Vlan      : All
  VC ID           : 1
  Encapsulation Type: raw
  Tunnel Type      : mplsNonTe
  Destination      : 20.0.0.2
  Tunnel Policy     : --
  Tunnel Number     : 1
  Local VC Label    : 401
  Remote VC Label   : 401
  AC Status        : down
  VC State         : lowerLayerDown
  VC Signal        : manual
  PW Control Word   : enable
  Local VC MTU      : 1500
  Remote VC MTU     : --
  TPID            : 0x8100
  SVLAN           : --
  Create Time      : 1970-01-01,09:02:37
  Up Time         : 0 days, 0 hours, 0 minutes 0.0 second
  Last Change Time  : 1970-01-01,09:02:37
```

```
----------------------------------------
Total l2vc : 1    0 up    1 down
```

4.8.3 Example for configuring MPLS-TP linear protection switching

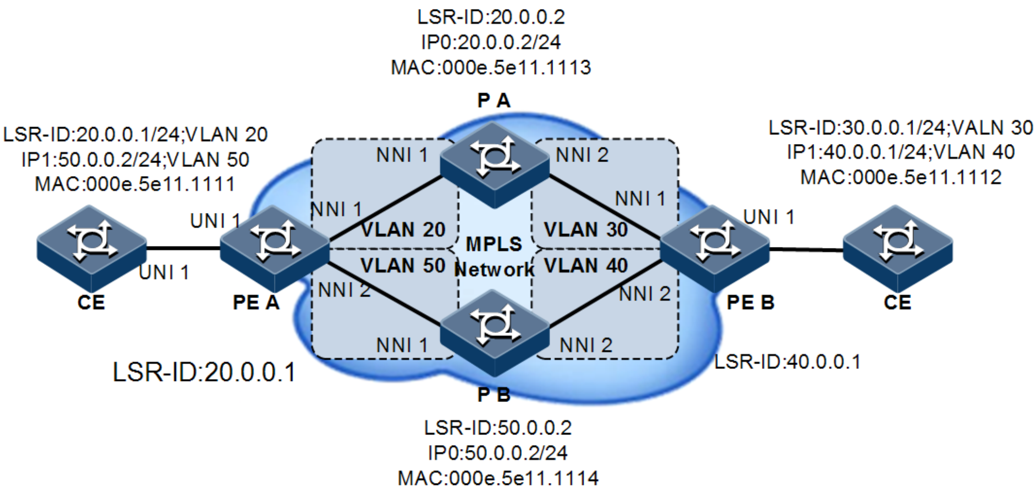
Networking requirements

As shown in Figure 4-3, PE A and PE B communicate with each other through the MPLS network. To enhance the link reliability, you need to configure linear protection switching between PE A and PE B.

LSPs among PE A, P A, and PE B are working lines. LSPs among PE A, P B, and PE B are protection lines. It requires that service can be quickly switched to the protection line for transmission when the working line fails.

- The static LSP among PE A, P A, and PE B is named as a2bA.
- The static LSP among PE A, P B, and PE B is named as a2bB.
- The static LSP among PE B, P A, and PE B is named as b2aA.
- The static LSP among PE B, P B, and PE A is named as b2aB.

Figure 4-3 Configuring MPLS-TP linear protection switching



Configuration steps

Step 1 Configure VLANs and add specified interfaces to VLANs. Configure IP addresses and static routes. Configurations on CE devices are not described in this guide.

- Configure PE A.

```
Raisecom#hostname PEA
PEA#config
PEA(config)#create vlan 20,30,40,50 active
PEA(config)#interface ip 0
PEA(config-ip)#ip address 20.0.0.1 20
PEA(config-ip)#interface ip 1
```

```
PEA(config-ip)#ip address 50.0.0.1 50
PEA(config-ip)#exit
PEA(config)#interface nni 1
PEA(config-port)#switchport access vlan 20
PEA(config-port)#interface nni 2
PEA(config-port)#switchport access vlan 50
PEA(config-port)#exit
```

- Configure PE B.

```
Raisecom#hostname PEB
PEB#config
PEB(config)#create vlan 20,30,40,50 active
PEB(config)#interface ip 0
PEB(config-ip)#ip address 30.0.0.1 30
PEB(config-ip)#interface ip 1
PEB(config-ip)#ip address 40.0.0.1 40
PEB(config-ip)#exit
PEB(config)#interface nni 1
PEB(config-port)#switchport access vlan 30
PEB(config-port)#interface nni 2
PEB(config-port)#switchport access vlan 40
PEB(config-port)#exit
```

- Configure P A.

```
Raisecom#hostname PA
PA#config
PA(config)#create vlan 20,30,40,50 active
PA(config)#interface ip 0
PA(config-ip)#ip address 20.0.0.2 20
PA(config)#interface nni 1
PA(config-port)#switchport mode trunk
PA(config-port)#switchport trunk allowed vlan 20-50
PA(config-port)#interface nni 2
PA(config-port)#switchport mode trunk
PA(config-port)#switchport trunk allowed vlan 20-50
PA(config-port)#exit
```

- Configure P B.

```
Raisecom#hostname PB
PB#config
PB(config)#create vlan 20-70 active
PB(config)#interface ip 0
PB(config-ip)#ip address 50.0.0.2 50
PB(config-ip)#exit
```

```
PB(config)#interface nni 1
PA(config-port)#switchport mode trunk
PA(config-port)#switchport trunk allowed vlan 20-50
PB(config-port)#interface nni 2
PA(config-port)#switchport mode trunk
PA(config-port)#switchport trunk allowed vlan 20-50
PB(config-port)#exit
```

Step 2 Enable MPLS on PE A, PE B, P A, and P B. Configure static LSPs from PE A to PE B, as well as from PE B to PE A. Create Tunnels between PE A and PE B and configure the static L2VC.

- Configure PE A.

```
PEA(config)#mpls lsr-id 20.0.0.1
PEA(config)#mpls enable
PEA(config)#interface ip 0
PEA(config-ip)#mpls enable
PEA(config-ip)#interface ip 1
PEA(config-ip)#mpls enable
PEA(config-ip)#exit
PEA(config)#mpls static-lsp ingress a2bA 30.0.0.1 nexthop-mac
000e.5e11.1113 vlan 20 nni 1 out-label 103 lsr-id 40.0.0.1 tunnel-id 1
PEA(config)#mpls static-lsp egress b2aA in-label 301 lsr-id 40.0.0.1
tunnel-id 1
PEA(config)#interface tunnel 1
PEA(config-tunnelif)#destination 30.0.0.1
PEA(config-tunnelif)#mpls tunnel-id 1
PEA(config-tunnelif)#exit
PEA(config)#mpls static-lsp ingress a2bB 40.0.0.1 nexthop-mac
000e.5e11.1114 vlan 50 nni 2 out-label 104 lsr-id 40.0.0.1 tunnel-id 3
PEA(config)#mpls static-lsp egress b2aB in-label 401 lsr-id 40.0.0.1
tunnel-id 3
PEA(config)#mpls l2vpn
PEA(config)#interface uni 1
PEA(config-port)#mpls l2vpn
PEA(config-port)#mpls static-l2vc destination 30.0.0.1 raw vc-id 1 vc-
label 100 tunnel-interface 1
PEA(config-port)#exit
```

- Configure PE B.

```
PEB(config)#mpls lsr-id 60.0.0.1
PEB(config)#mpls enable
PEB(config)#interface ip 0
PEB(config-ip)#mpls enable
PEB(config-ip)#interface ip 1
PEB(config-ip)#mpls enable
PEB(config-ip)#exit
```

```
PEB(config)#mpls static-lsp egress a2bA in-label 302 lsr-id 20.0.0.1
tunnel-id 1
PEB(config)#mpls static-lsp ingress b2aA 20.0.0.1 nexthop-mac
000e.5e11.1113 vlan 30 nni 1 out-label 203 lsr-id 20.0.0.1 tunnel-id 1
PEB(config)#interface tunnel 1
PEB(config-tunnelif)#destination 20.0.0.1
PEB(config-tunnelif)#mpls tunnel-id 1
PEB(config-tunnelif)#exit
PEB(config)#mpls static-lsp egress a2bB in-label 402 lsr-id 20.0.0.1
tunnel-id 3
PEB(config)#mpls static-lsp ingress b2aB 50.0.0.1 nexthop-mac
000e.5e11.1114 vlan 40 nni 2 out-label 204 lsr-id 20.0.0.1 tunnel-id 3
PEB(config)#mpls l2vpn
PEB(config)#interface uni 1
PEB(config-port)#mpls static-l2vc destination 50.0.0.1 raw vc-id 2 vc-
label 200 tunnel-interface 1
PEB(config-port)#exit
```

- Configure P A.

```
PA(config)#mpls lsr-id 20.0.0.2
PA(config)#mpls enable
PA(config)#interface ip 0
PA(config-ip)#mpls enable
PA(config-ip)#exit
PA(config)#mpls static-lsp transit a2bA in-label 103 nexthop-mac
000e.5e11.1112 vlan 30 nni 2 out-label 302 lsr-id 20.0.0.1 40.0.0.1
tunnel-id 1
PA(config)#mpls static-lsp transit b2aA in-label 203 nexthop-mac
000e.5e11.1111 vlan 20 nni 1 out-label 301 lsr-id 40.0.0.1 20.0.0.1
tunnel-id 2
```

- Configure P B.

```
PB(config)#mpls lsr-id 50.0.0.2
PB(config)#mpls enable
PB(config)#interface ip 0
PB(config-ip)#mpls enable
PB(config-ip)#exit
PB(config)#mpls static-lsp transit a2bB in-label 103 nexthop-mac
000e.5e11.1112 vlan 40 nni 2 out-label 302 lsr-id 20.0.0.1 40.0.0.1
tunnel-id 3
PA(config)#mpls static-lsp transit b2aB in-label 203 nexthop-mac
000e.5e11.1111 vlan 50 nni 1 out-label 301 lsr-id 40.0.0.1 20.0.0.1
tunnel-id 4
```

Step 3 Configure CFM on PE A and PE B.

- Configure PE A.

```
PEA(config)#mpls-tp cfm domain level 7
PEA(config)#mpls-tp service ma1 level 7
PEA(config-service)#service lsp ingress a2bA egress b2aA
PEA(config-service)#service mep mpid 1
PEA(config-service)#service cc enable mep 1
PEA(config-service)#mpls-tp service ma2 level 7
PEA(config-service)#service lsp ingress a2bB egress b2aB
PEA(config-service)#service mep mpid 3
PEA(config-service)#service cc enable mep 3
PEA(config-service)#service remote-mep 4
PEA(config-service)#exit
PEA(config)#mpls-tp cfm enable
```

- Configure PE B.

```
PEB(config)#mpls-tp cfm domain level 7
PEB(config)#mpls-tp service ma1 level 7
PEB(config-service)#service lsp ingress b2aA egress a2bA
PEB(config-service)#service mep mpid 2
PEB(config-service)#service cc enable mep 2
PEB(config-service)#mpls-tp service ma2 level 7
PEB(config-service)#service lsp ingress b2aB egress a2bB
PEB(config-service)#service mep mpid 4
PEB(config-service)#service cc enable mep 4
PEB(config-service)#service remote-mep 3
PEB(config-service)#exit
PEB(config)#mpls-tp cfm enable
```

Step 4 Configure MPLS-TP linear protection switching on PE A and PE B.

- Configure PE A.

```
PEA(config)#mpls-tp line-protection association 1 apsab1 7 ma1
PEA(config)#mpls-tp line-protection association 1 apsab2 7 ma2
PEA(config)#mpls-tp line-protection 1 working apsa2b1 apsab1 protection
apsa2b2 apsab2 one-to-one
```

- Configure PE B.

```
PEB(config)#mpls-tp line-protection association 2 apsba1 7 ma1
PEB(config)#mpls-tp line-protection association 2 apsba2 7 ma2
PEB(config)#mpls-tp line-protection 2 working apsba1 apsba1 protection
apsba2 apsba2 one-to-one
```

Checking results

Use the **show mpls-tp line-protection status** command to show the MPLS-TP linear protection group status, taking PE A for example.

```
PEA(config)#show mpls-tp line-protection status
Id      Type    Direction(Configured) Direction(Negotiated) Revert Aps
State Signal(Requested/Bridged)
-----------------------------------------------------------------------
1-Local  1:1     bi             bi             yes    yes NR-W  null/null
1-Remote 1:1     --             bi             yes    yes NR-W  null/null
```

5 TDMoP

This chapter describes principles and configuration procedures of Time Division Multiplex over Packet (TDMoP), as well as related configuration examples, including following sections:

- Configuring TDM interfaces
- Configuring PW
- Configuring TDMoP clock
- Maintenance
- Configuration examples

5.1 Configuring TDM interfaces

5.1.1 Preparing for configurations

Scenario

The RAX711-L accesses TDM services through the TDM interface. Before enabling circuit emulation services, you need to configure basic properties and related features of TDM interfaces, such as the link type and Tx clock source of TDM interfaces, and codes of TDM idle timeslots.

Circuit emulation services are encapsulated based on the TDM interface type. When a TDM interface is in framed/multiframed mode, TDM frame structure can be recognized and structured encapsulation mode is adopted. When a TDM interface is in unframed mode, unstructured encapsulation mode is adopted.

In structured encapsulation mode, PW can be only related to timeslots that carry services. Timeslots related to the PW are occupied timeslots and the ones does not carry services are idle timeslots.

Prerequisite

N/A

5.1.2 Configuring E1 interfaces

Note

These configurations are available for the device whose TDM interface is an E1 interface.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface tdm`** *`interface-number`*	Enter TDM interface configuration mode.
3	`Raisecom(config-tdm-port)#`**`tdm-type`** { **`e1-unframed`** | **`e1-framed`** | **`e1-crc-framed`** }	Configure the link type of the TDM interface (E1 interface). By default, the link type is set to E1 unframed mode.

5.1.3 Checking configurations

No.	Command	Description
1	`Raisecom(config-tdm)#`**`show tdm interface`**	Show configurations of the current TDM interface.
2	`Raisecom(config-tdm)#`**`show pw-status`**	Show the status of the PW associated to the current TDM interface.

5.2 Configuring PW

5.2.1 Preparing for configurations

Scenario

TDM service data flow is received by the TDM interface and then is encapsulated to PW packets via a protocol. PW packets of the same type form the PW service flow, which is transmitted through the Tunnel to traverse the PSN. After reaching the peer device, PW service flow is decapsulated to the original TDM service data flow and the TDM service data flow is forwarded through the TDM interface.

The RAX711-L supports MPLS-/MEF-/IP-based PSN. Therefore, Tunnels are grouped in these 3 types. Properties of a MPLS Tunnel are defined by the LSP and Tunnel of the MPLS protocol. For details about how to create a MPLS Tunnel, see related configurations.

MPLS/IP-based PW packets select a transport path based on the IP address. The source IP address of a PW packet is the IP address of the TDMoP system.

Prerequisite

N/A

5.2.2 Configuring TDMoP system parameters

Note

The IP address of the TDMoP system and the management IP address of the RAX711-L should be in different network segments.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**tdmop-ip-address** *ip-address* [*ip-mask*]	Configure the IP address of the TDMoP system.
3	Raisecom(config)#**tdmop-svlan-tpid** *tpid*	Configure the TPID of the outer VLAN Tag.
4	Raisecom(config)#**tdmop-udp-multiplex** { **src** / **dest** }	When the PSN is based on UDP/IP, configure the multiplex mode of the UDP port and PW label.

5.2.3 Creating Tunnel

The Tunnel is a tunnel to carry PWs to traverse the PSN. Before configuring PWs, you must configure the Tunnel.

Note

- When Tunnel packets are Tag ones, CVLAN ID and priority are required parameters while SVLAN ID and priority are not needed to be configured.
- When Tunnel packets are Double-tag ones, CVLAN ID, SVLAN ID, and priority are required parameters.
- When Tunnel packets are Untag ones, you do not need to configure the CVLAN ID and SVLAN ID.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mef tunnel** *tunnel-name* **dest-mac-address** *mac-address* **tag-vlan-mode** { **double-tag** | **tag** | **untag** } [**cvlan-id** *vlan-id* **pri** *pri-value*] [**svlan-id** *vlan-id* **pri** *pri-value*]	Create a MEF Tunnel and configure basic properties of the Tunnel, including the destination MAC address, VLAN mode, VLAN ID, and priority. **Note** The destination MAC address of a MEF Tunnel is the MAC address of the peer TDMoP system.
	Raisecom(config)#**mef tunnel** *tunnel-name* **dest-mac-addr** *mac-address* **tag-vlan-mode double-tag cvlan-id** *vlan-id* **pri** *pri-value* **svlan-id** *vlan-id* **pri** *pri-value*	

Step	Command	Description
	Raisecom(config)#**mef tunnel** *tunnel-name* **dest-mac-addr** *mac-address* **tag-vlan-mode untag**	
	Raisecom(config)#**ip tunnel** *tunnel-name slot-id* **dest-ip-address** *ip-address* [**ip-ttl** *ttl-value*] [**ip-tos** *tos-value*] [**nexthop-type** { **ip nexthop-addr** *ip-address* / **mac nexthop-addr** *mac-address* }] **tag-vlan-mode** { **double-tag** | **tag** | **untag** } [**cvlan-id** *vlan-id* **pri** *pri-value*] [**svlan-id** *vlan-id* **pri** *pri-value*]	Create an IP Tunnel and configure basic properties of the Tunnel, including the destination IP address, TTL, ToS, next-hop address and type, VLAN mode, VLAN ID, and priority. You can use the **no tunnel** *tunnel-name* command to delete a created Tunnel. **Note** The destination IP address of an IP Tunnel is the IP address of the peer TDMoP system.
	Raisecom(config)#**ip tunnel** *tunnel-name* **dest-ip-addr** *ip-address* [**ip-ttl** *ttl-value*] [**ip-tos** *tos-value*] [**nexthop-type** { **ip nexthop-addr** *ip-address* / **mac nexthop-addr** *mac-address* }] **tag-vlan-mode tag cvlan-id** *vlan-id* **pri** *pri-value*	
	Raisecom(config)# **ip tunnel** *tunnel-name* **dest-ip-addr** *ip-address* [**ip-ttl** *ttl-value*] [**ip-tos** *tos-value*] [**nexthop-type** { **ip nexthop-addr** *ip-address* / **mac nexthop-addr** *mac-address* }] **tag-vlan-mode untag**	

5.2.4 Creating PW and configuring PW properties

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mpls cespw** *pw-name* **vc-id** *vc-id* **type** { **cesop** | **satop** } **tdmport** *interface-number* **timeslot** { **all** | *tsstring* } **in-label** *label-value* **out-label** *label-value* **destination** *ip-address* [**tunnel-interface** *interface-number*]	Create a MPLS PW and configure basic properties of the PW, including the encapsulation protocol type, incoming label value, outgoing label value, related TDM interface ID, timeslot ID, and destination IP address.
	Raisecom(config)#**mef cespw** *pw-name* **type** { **cesop** | **satop** } **tdmport** *interface-number* **timeslot** { **all** | *tsstring* } **in-label** *label-value* **out-label** *label-value* **tunnel** *tunnel-name*	Create a MEF PW and configure basic properties of the PW, including the encapsulation protocol type, related TDM interface ID, bound timeslot ID, incoming label value, outgoing label value, and bound Tunnel name.

Step	Command	Description
	Raisecom(config)#**ip cespw** *pw-name* **type** { **cesop** | **satop** } **tdmport** *interface-number* **timeslot** { **all** | *tsstring* } **in-label** *label-value* **out-label** *label-value* **tunnel** *tunnel-name*	Create an IP PW and configure basic properties of the PW, including the encapsulation protocol type, related TDM interface ID, bound timeslot ID, incoming label value, outgoing label value, and bound Tunnel name.
3	Raisecom(config)#**cespw** *pw-name*	Enter PW configuration mode.
4	Raisecom(config-pw)#**load-time** *load-time*	Configure the PW packet encapsulation time, the PW packet encapsulation time is a multiple of 125μs. By default, the PW packet encapsulation time is 1000μs.
5	Raisecom(config-pw)#**frame-size** *size-value*	(Optional) configure the number of TDM frames encapsulated into PW packets. Note The function of this command is identical to the one of the **load-time** *load-time* command. The latter configured one takes effect.
6	Raisecom(config-pw)#**jitter-buffer** *jitter-buffer*	Configure the PW Jitter Buffer size. By default, the PW Jitter Buffer size is set to 8000μs.
7	Raisecom(config-pw)#**rtp-header enable**	Enable RTP of the PW packet header. Note When the TDMoP system adopts the differential clock mechanism, you must enable RTP of the PW packet header.
8	Raisecom(config-pw)#**ses-threshold** *ses-threshold*	Configure the packet loss ratio threshold for a PW entering Severely Errored Second (SES) status. By default, the packet loss ratio threshold for a PW entering SES status is set to 30%.
9	Raisecom(config-cespw)#**cespw-exp** *exp-priority*	Configure the EXP priority of the PW packets. By default, the PW EXP priority is set to 0.
10	Raisecom(config-pw)#**out-synch-threshord** *out-synch-threshord*	Configure the sequential frame loss threshold. By default, the sequential frame loss threshold is set to 15.
11	Raisecom(config-pw)#**connect enable**	Enable PW connection. Services cannot be transmitted unless the PW connection is created. By default, PW connection is disabled.

Note

- Values of the incoming label and outgoing label of a PW must be different.
- The PW Jitter Buffer size must be equal to or greater than the PW packet encapsulation time.

- The number of payloads encapsulated in the PW packet is related to the encapsulation protocol. The number of payloads encapsulated in the PW packet by SAToP protocol = frame - size × 32 Bytes. The number of payloads encapsulated in the PW packet by CESoPSN protocol = frame - size × the number of encapsulated timeslots (Bytes).

5.2.5 Cheking configurations

No.	Command	Description
1	Raisecom(config-cespw)#**show cespw interface**	Show PW interface configurations and status.
2	Raisecom(config)#**show tunnel** *tunnel-name*	Show Tunnel configurations.
3	Raisecom(config)#**show tdmop info**	Show TDMoP global configurations.

5.3 Configuring TDMoP clock

5.3.1 Preparing for configurations

Scenario

The TDMoP system supports clock synchronization in nature. The PTN is an STDM-based best-effort network. It may cause end-to-end delay TDM services are encapsulated into Ethernet packets and then are transmitted cross the PTN. This also influences the performance for de-encapsulating TDM services. However, TDMoP clock recovery technology can reduce impact caused by PTN delay.

The clock recovery mechanism adopted by the TDMoP system depends on the Tx clock source of the TDM interface.

Prerequisite

Create a PW.

5.3.2 Configuring Tx clock source of TDM interfaces

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface tdm** *interface-number*	Enter TDM interface configuration mode.
3	Raisecom(config-tdm)#**tx-clock-src { adaptive | differential | external | loopback | system }**	Configure the Tx clock source of a TDM interface. Each interface on the RAX711-L supports one PW only. WHne the clock source type is configured as **adaptive** or **differential**, the PW on this interface works as the recovery clock source. By default, the clock source type is external clock.

5.3.3 Checking configurations

No.	Command	Description
1	Raisecom(config-tdm)#**show tdm interface**	Show clock configurations of the current TDM interface.

5.4 Maintenance

Command	Description
Raisecom(config-tdm-port)#**loopback** { **internal** | **external** | **bidirectional** }	Configure loopback mode of a TDM interface. By default, no loopback is configured the TDM interface.
Raisecom(config-tdm-port)#**clear-statistics**	Clear TDM interface statistics.
Raisecom(config-cespw)#**clear-statistics**	Clear PW statistics.

5.5 Configuration examples

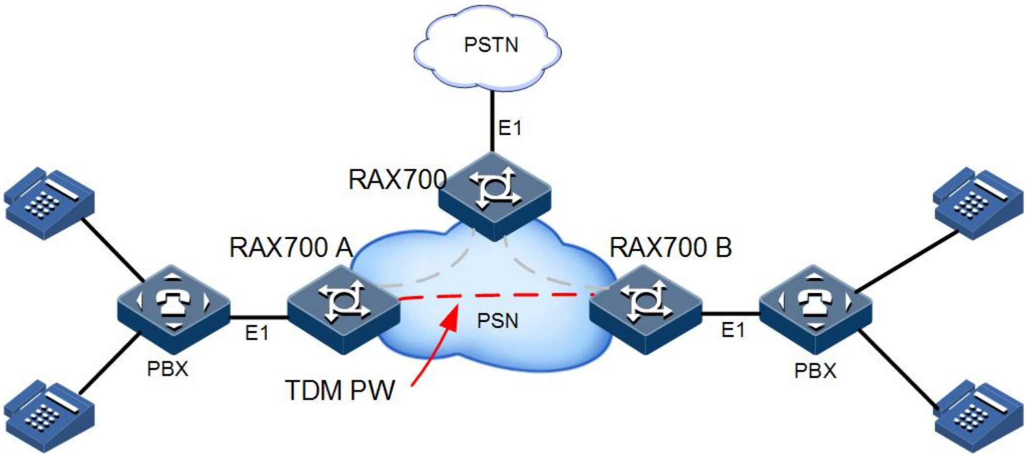
5.5.1 Example for configuring CESoPSN emulation services

Networking requirements

As shown in Figure 5-1, the user has offices in sites A and B. Telephones of sites A and B access the PTN through RAX700 A and RAX700 B respectively. Telephones of sites A and B need to communicate with each other through the PTN. Configurations are shown as below:

- Site A:
  - Occupied timeslots: TS6–TS10 and TS17–TS31
  - Idle timeslots: TS1–TS5 and TS11–TS15
- Site B:
  - Occupied timeslots: TS6–TS10 and TS17–TS31
  - Idle timeslots: TS1–TS5 and TS11–TS15
- IP address of RAX700 B: 192.168.10.1 (configured on the RAX700 A)
- Encapsulation protocol: CESoPSN protocol
- LSR ID of RAX700 A: 10.1.1.1
- LSR ID of RAX700 B: 192.168.10.1

Figure 5-1 Configuring CESoPSN emulation services



Configuration steps

Configuration steps of RAX700 A are identical to the ones of RAX700 B. In this guide, only configurations on RAX700 A are described.

Step 1 Configure the TDM interface.

```
Raisecom#config
Raisecom(config)#interface tdm 1
Raisecom(config-tdm-port)#tdm-type e1-crc-framed-cas
Raisecom(config-tdm-port)#exit
```

Step 2 Create a PW and configure basic properties of the PW.

```
Raisecom(config)#mpls lsr-id 10.1.1.1
Raisecom(config)#mpls enable
Raisecom(config)#mpls static-lsp ingress a2b 192.168.10.1 255.255.255.255
nexthop-mac 000e.5e11.1113 vlan 1 nni 1 out-label 102 lsr-id 192.168.10.1
tunnel-id 1
Raisecom(config)#interface tunnel 1
Raisecom(config-tunnelif)#destination 192.168.10.1
Raisecom(config-tunnelif)#mpls tunnel-id 1
Raisecom(config-tunnelif)#exit
Raisecom(config)#mpls cespw 100 vc-id 1 type cesop tdmport 1 timeslot 6-
10,17-31 in-label 100 out-label 200 destination 192.168.10.1 tunnel-
interface 1
Raisecom(config)#cespw 100
Raisecom(config-cespw)#load-time 1000
Raisecom(config-cespw)#jitter-buffer 8000
Raisecom(config-cespw)#rtp-header enable
Raisecom(config-cespw)#ses-threshold 35
Raisecom(config-cespw)#out-synch-threshold 10
Raisecom(config-cespw)#exit
```

Step 3 Configure the TDMoP clock.

```
Raisecom(config)#interface tdm 1
Raisecom(config-tdm)#tx-clock-src differential
Raisecom(config-tdm)#exit
```

Step 4 Enable PW connection.

```
Raisecom(config)#cespw 100
Raisecom(config-cespw)#connect enable
```

Checking results

Use the **show tdm interface** command to show TDM interface configurations.

```
Raisecom(config-tdm)#show tdm interface
tdm port                        ...(1)
tdm identifier                   ...(TDM1)
tdm type                        ...(e1-crc-framed-cas)
line coding                      ...(HDB3)
loopback                        ...(no loopback)
idle code                       ...(0x20)
tx clock source                  ...( external)
alarm                          ...( los lof )
Statistics:
ES                             ...(10)
SES                            ...(10)
UAS                            ...(18887)
```

Use the **show cespw interface** command to show PW configurations.

```
Raisecom(config-cespw)#show cespw interface
pw id                        ...(1)
pw name                     ...(100)
pw payload type                ...(cesop)
TDM port index                 ...(1/2)
TDM ds0 number                 ...(4)
   1    2    3    4    5    6    7    8
   9   10   11   12   13   14   15   16
  17   18   19   20   21   22   23   24
  25   26   27   28   29   30   31

pw in label                   ...(100)
pw out label                  ...(200)
pw load time                  ...(1000)
```

```
jitter buffer                  ...(8000)
ses threshold                  ...(35%)
pw exp                        ...(0)
pw rtp-header                  ...(enable)
out-synch-threshold             ...(10)
pw oos-act                    ...(oos-suppression)
pw connection config            ...(enable)
pw oper status                 ...(up)
pw local status                ...(normal)
RX PKTS                       ...(167)
TX PKTS                       ...(167)
```

5.5.2 Example for configuring SAToP emulation services

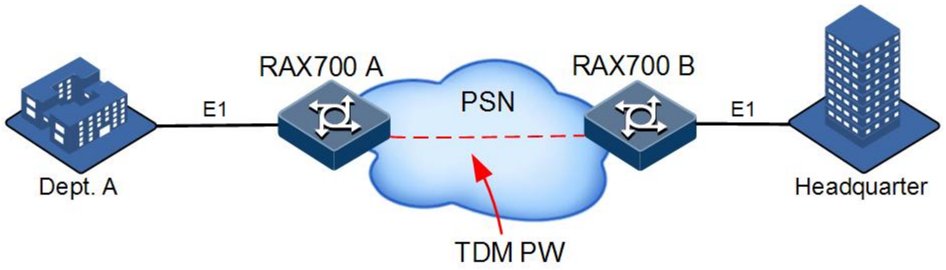
Networking requirements

As shown in Figure 5-2, a company has many branches in multiple cities. Branches and the headquarter are connected through the PTN to transmit services. After being connected to RAX700 A through the E1 lease cable, Department A accesses the PTN. And then services of Department A traverse the PTN through the transparent transmission feature of TDM emulation services to realize data communication among all branches.

Perform the following configurations on RAX700 A:

- IP address of RAX700 B: 192.168.11.1
- Encapsulation protocol: SAToP
- LSR ID of RAX700 A: 10.1.1.1
- LSR ID of RAX700 B: 192.168.11.1

Figure 5-2 Configuring SAToP emulation services



Configuration steps

Configuration steps of RAX700 A are identical to the ones of RAX700 B. In this guide, only configurations on RAX700 A are described.

Step 1 Configure the TDM interface (this step can be ignored).

```
Raisecom#config
Raisecom(config)#interface tdm 1
Raisecom(config-tdm)#tdm-type e1-unframed
Raisecom(config-tdm)#exit
```

Step 2 Configure the PW.

```
Raisecom(config)#mpls lsr-id 10.1.1.1
Raisecom(config)#mpls enable
Raisecom(config)#mpls static-lsp ingress a2b 192.168.11.1 255.255.255.255
nexthop-mac 000e.5e11.1113 vlan 1 nni 1 out-label 102 lsr-id 192.168.11.1
tunnel-id 1
Raisecom(config)#interface tunnel 1
Raisecom(config-tunnelif)#destination 192.168.11.1
Raisecom(config-tunnelif)#mpls tunnel-id 1
Raisecom(config-tunnelif)#exit
Raisecom(config)#mpls cespw 60 vc-id 1 type satop tdmport 1 timeslot all
in-label 100 out-label 200 destination 192.168.11.1 tunnel-interface 1
Raisecom(config)#cespw 60
Raisecom(config-pw)#load-time 1500
Raisecom(config-pw)#jitter-buffer 6000
Raisecom(config-pw)#rtp-header enable
Raisecom(config-pw)#ses-threshold 40
Raisecom(config-pw)#out-synch-threshord 10
Raisecom(config-pw)#exit
```

Step 3 Configure the TDMoP clock.

```
Raisecom(config)#interface tdm 1
Raisecom(config-tdm)#tx-clock-src differential
Raisecom(config-tdm)#exit
```

Step 4 Enable PW connection.

```
Raisecom(config)#cespw 60
Raisecom(config-pw)#connect enable
```

Checking results

Use the **show tdm interface** command to show TDM interface configurations.

```
Raisecom(config-tdm)#show tdm interface
tdm port                        ...(1)
tdm identifier                   ...(TDM1)
tdm type                        ...(e1-unframed)
line coding                      ...(HDB3)
loopback                        ...(no loopback)
tx clock source                  ...(differential)
alarm                          ...( los )
Statistics:
```

```
ES                              ...(10)
SES                             ...(10)
UAS                             ...(19472)
```

Use the **show cespw interface** command to show PW configurations.

```
Raisecom(config-pw)#show cespw interface
pw id                         ...(64)
pw name                       ...(60)
pw payload type                ...(satop)
TDM port index                 ...(1/4)
pw in label                   ...(100)
pw out label                  ...(200)
pw load time                  ...(1500)
jitter buffer                 ...(6000)
ses threshold                 ...(40%)
pw exp                        ...(0)
pw rtp-header                  ...(enable)
out-synch-threshold            ...(10)
pw connection config           ...(enable)
pw oper status                 ...(up)
pw local status                ...(normal)
RX PKTS                       ...(0)
TX PKTS                       ...(0)
```

6 Network 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 failover
- Maintenance
- Configuration examples

6.1 Configuring link aggregation

6.1.1 Preparing for configurations

Scenario

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

The RAX711-L supports the following 2 link aggregation modes:

- Manual link aggregation mode
- Static LACP aggregation mode

Prerequisite

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

6.1.2 Configuring manual link aggregation

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

Step	Command	Description
2	Raisecom(config)#**interface port-channel** *port-channel-number*	Enter aggregation group configuration mode.
3	Raisecom(config-aggregator)#**mode manual**	Configure manual link aggregation.
4	Raisecom(config-aggregator)#**exit**	Return to global configuration mode.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
6	Raisecom(config-port)#**channel group** *port-channel-number*	Add member interfaces to the LAG.
7	Raisecom(config-port)#**exit**	Exit global configuration mode.
8	Raisecom(config)#**link-aggregation enable**	(Optional) enable link aggregation. By default, link aggregation is enabled.
9	Raisecom(config)#**link-aggregation load-sharing mode { dip | dmac | smac | sip | sxordip | sxordmac }**	(Optional) configuring the load-sharing mode of the LAG. By default, load sharing mode is set to **sxordmac**, which means selecting the forwarding interface according to the OR operation result of source MAC address and destination MAC address.

Note

In a LAG, member interfaces that share loads must be identically configured. Otherwise, data cannot be forwarded properly. 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 and Access) on the interface, and whether VLAN packets carry Tags.
- Interface properties: speed, duplex mode, and link Up/Down status.
- MAC address learning: MAC address learning status and MAC address limit.

6.1.3 Configuring static LACP link aggregation

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

Step	Command	Description
2	Raisecom(config)#**lacp system-priority** *system-priority*	(Optional) configure the system LACP priority. By default, the system LACP priority is set to 32768. **Note** 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.
3	Raisecom(config)#**lacp timeout** { **fast** | **slow** }	(Optional) configure the LACP timeout mode.
4	Raisecom(config)#**interface port-channel** *port-channel-number*	Enter aggregation group configuration mode.
5	Raisecom(config-aggregator)#**mode lacp-static**	Configure the static LACP LAG.
6	Raisecom(config-aggregator)#{ **max-active** | **min-active** } **links** *threshold*	(Optional) configure the maximum/minimum number of active links in the LACP LAG.
7	Raisecom(config-aggregator)#**exit**	Return to global configuration mode.
8	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
9	Raisecom(config-port)#**channel group** *port-channel-number*	Add member interfaces to the LACP LAG.
10	Raisecom(config-port)#**lacp mode** { **active** | **passive** }	(Optional) configure the LACP mode of member interfaces. By default, the LACP mode is set to active. LACP connection fails if both ends of a link are in passive mode.
11	Raisecom(config-port)#**lacp port-priority** *port-priority*	(Optional) configure the interface LACP priority.
12	Raisecom(config-port)#**exit**	Return to global configuration mode.
13	Raisecom(config)#**link-aggregation enable**	(Optional) enable link aggregation. By default, link aggregation is enabled.

Note

- 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 the following conditions in order: whether the neighbour is discovered, maximum interface speed, highest interface LACP priority, 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.

6.1.4 Checking configurations

No.	Command	Description
1	Raisecom#**show lacp internal**	Show local system LACP configurations.
2	Raisecom#**show lacp neighbor**	Show the neighbour LACP configurations
3	Raisecom#**show lacp statistics**	Show interface LACP statistics.
4	Raisecom#**show lacp sys-id**	Show local system LACP global enabling status, device ID.
5	Raisecom#**show link-aggregation**	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 aggregation groups.

6.2 Configuring interface backup

6.2.1 Preparing for configurations

Scenario

Interface backup can realize redundancy backup and fast switching of primary and backup links, VLAN-based interface backup can realize load-sharing among different interfaces.

Interface backup ensures millisecond level switching and simplifies configurations.

Prerequisite

- Create a VLAN.
- Add interfaces to the VLAN.

6.2.2 Configuring basic functions of interface backup

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type primary-interface-number*	Enter physical layer interface configuration mode. The interface is the primary interface for interface backup.

Step	Command	Description
3	Raisecom(config-port)#**switchport backup** { *interface-type interface-number* | **port-channel** *port-channel-list* } [**vlanlist** *vlan-list*]	Configure the interface backup group. If the interface backup group specifies no VLAN list, VLAN IDs ranges from 1 to 4094 by default. Note When aggregation group interfaces of the devices on both ends back up each other, these interfaces cannot be configured to work in manual aggregation mode at the same time.
4	Raisecom(config-port)#**exit**	Return to global configuration mode.
5	Raisecom(config)#**switchport backup restore-delay** *period*	(Optional) configure the restore delay. By default, the restore delay is set to 15s.
6	Raisecom(config)#**switchport backup restore-mode** { **disable** | **mep-up** | **port-up** }	(Optional) configure the restore mode. • **port-up**: the link recovers once the interface in Up status. • **mep-up**: MEP connection mode. Some RMEP considers that the link recovers. • **disable**: disable backup restore. By default, the restore mode is set to **port-up**.

Note

- In an interface backup group, an interface is a primary interface or a backup interface.
- In a VLAN, an interface/LAG is a member of only one interface backup group.
- If you set a LAG to a member of the interface backup group, you need to set the interface with the smallest interface ID in the LAG to the member of the interface backup interface. When the member interface is in Up status, all interfaces in the aggregation group are in Up status. When the member interface is in Down status, all interfaces in the aggregation group are in Down status.

6.2.3 (Optional) configuring interface forced switch

Caution

- After forced switch is successfully configured, the primary and backup lines will be switched. The working line is switched to the protection line. For example, when both the primary and backup interfaces are in Up status, if the data is being transmitted through the primary line, data will be transmitted to the primary line to the backup line after forced switch is performed.
- In the CLI, the backup interface ID is an optional parameter. If the primary interface is configured with multiple interface backup pairs, you should input the backup interface ID.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type primary-interface-number*	Enter physical layer interface configuration mode. The interface is the primary interface for interface backup.
3	Raisecom(config-port)#**switchport backup** [*interface-type backup-interface-number*] **force-switch**	Configure interface forced switch. **Note** When aggregation group interfaces of the devices on both ends back up each other, these interfaces cannot be configured to work in manual aggregation mode at the same time.

6.2.4 Checking configurations

No.	Command	Description
1	Raisecom#**show switchport backup**	Show interface backup information.

6.3 Configuring ELPS

6.3.1 Preparing for configurations

Scenario

To make the Ethernet reliability up to carrier 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.

Prerequisite

- Connect the interface, configure its physical parameters, and make it Up at the physical layer.
- Create the management VLAN and VLANs of the working and protection interfaces.
- Configure CFM detection between devices (preparing for CFM detection mode).

6.3.2 Creating protection lines

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

Step	Command	Description
2	Raisecom(config)#**ethernet line-protection** *line-id* **working** *interface-type interface-number vlanlist* **protection** *interface-type interface-number vlanlist* **one-to-one** [**non-revertive**] [**protocol-vlan** *vlan-id*]	Create the ELPS protection line 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, the protection group is in revertive mode.
3	Raisecom(config)#**ethernet line-protection** *line-id* **name** *string*	(Optional) configure a name for the ELPS protection line.
4	Raisecom(config)#**ethernet line-protection** *line-id* **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 time value is set to 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-id* **hold-off-timer** *holdoff-timer*	(Optional) configure the HOLDOFF timer. Hold-off timer configurations on both ends should be consistent. By default, the HOLDOFF timer value is set to 0. **Note** If the HOLDOFF timer value is over great, it may influence 50ms switching performance. Therefore, we recommend setting the HOLDOFF timer value to 0.
6	Raisecom(config)#**ethernet line-protection trap enable**	(Optional) enable ELPS Trap. By default, ELPS Trap is disabled.

6.3.3 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.
2	Raisecom(config)#**ethernet line-protection** *line-id* { **working** | **protection** } **failure-detect physical-link**	Set the fault detection mode of the working line/protection line to **failure-detect physical-link**. By default, the fault detection mode is set to **failure-detect physical-link**.
	Raisecom(config)#**ethernet line-protection** *line-id* { **working** | **protection** } **failure-detect cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	Set 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-id* { **working** | **protection** } **failure-detect physical-link-or-cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	Set the fault detection mode of the working line/protection line to **failure-detect physical-link-or-cc**. In this mode, a Trap is reported when a fault is detected on the physical link/CC. This fault detection mode cannot take effect unless you finish related configurations on CFM.

6.3.4 (Optional) configuring ELPS control

Note

By default, traffic is automatically switched to the protection line when the working line fails. Therefore, you need to configure ELPS control in some special cases.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet line-protection** *line-id* **lockout**	Lock protection switching. After this configuration, the traffic is not switched to the protection line even the working line fails.
3	Raisecom(config)#**ethernet line-protection** *line-id* **force-switch**	Switch the traffic from the working line to the protection line forcedly.
4	Raisecom(config)#**ethernet line-protection** *line-id* **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.
5	Raisecom(config)#**ethernet line-protection** *line-id* **manual-switch-to-work**	In non-revertive mode, switch the traffic from the protection line to the working line.

6.3.5 Checking configurations

No.	Command	Description
1	Raisecom#**show ethernet line-protection** [*line-id*]	Show protection line configurations.
2	Raisecom#**show ethernet line-protection** [*line-id*] **statistics**	Show protection line statistics.
3	Raisecom#**show ethernet line-protection** [*line-id*] **aps**	Show APS information.

6.4 Configuring ERPS

6.4.1 Preparing for configurations

Scenario

With development of Ethernet to carrier-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 RAX711-L supports the single ring, intersecting ring, and tangent ring.

ERPS provides 2 modes to detect a fault:

- Detect faults based on the 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.

Prerequisite

- Connect the interface, configure its physical parameters, and make it Up at the physical layer.
- Create the management VLAN and VLANs of the working and protection interfaces.
- Configure CFM detection between devices (preparing for CFM detection mode).

6.4.2 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 set to RPL Neighbour. 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 master ring and a sub-ring. Configurations on the master ring are identical to the ones on the common single ring. For details about configurations on the sub-ring, see section 6.4.3 (Optional) creating ERPS protection sub-ring.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet ring-protection** *ring-id* **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** *vlanlist*]	Create a protection ring and set the node to the RPL Owner. By default, the protocol VLAN is set to 1. Blocked VLANs ranges from 1 to 4094. **Note** The east and west interfaces cannot be the same one.
	Raisecom(config)#**ethernet ring-protection** *ring-id* **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** *vlanlist*]	Create a protection ring and set the node to the RPL Neighbour.
	Raisecom(config)#**ethernet ring-protection** *ring-id* **east** *interface-type interface-number* **west** *interface-type interface-number* [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlanlist*]	Create a protection line and set the node to the protection forwarding node.
3	Raisecom(config)#**ethernet ring-protection** *ring-id* **name** *string*	(Optional) configure a name for the protection ring. Up to 32 bytes are supported.
4	Raisecom(config)#**ethernet ring-protection** *ring-id* **version** { **1** | **2** }	(Optional) configure the protocol version.
5	Raisecom(config)#**ethernet ring-protection** *ring-id* **guard-time** *guard-time*	(Optional) after the ring Guard timer is configured, the failed node does not process APS packets during a period. By default, the ring Guard timer is set to 500ms.
6	Raisecom(config)#**ethernet ring-protection** *ring-id* **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 set to 5min.

Step	Command	Description
7	Raisecom(config)#**ethernet ring-protection** *ring-id* **holdoff-time** *holdoff-time*	(Optional) configure the ring HOLDOFF timer. Hold-off timer configurations on both ends should be consistent. By default, the ring HOLDOFF timer value is set to 0. Note If the ring HOLDOFF timer value is over great, it may influence 50ms switching performance. Therefore, we recommend setting the ring HOLDOFF timer value to 0.
8	Raisecom(config)#**ethernet ring-protection trape nable**	(Optional) enable ERPS Trap. By default, ERPS Trap is disabled.

6.4.3 (Optional) creating ERPS protection sub-ring

Caution

- Only the intersecting ring consists of a master ring and a sub-ring.
- Configurations on the master ring are identical to the ones on the single ring/tangent ring. For details, see section 6.4.2 Creating ERPS protection ring.
- Configurations of non-intersecting nodes of the intersecting ring are identical to the ones on the single ring/tagent ring. For details, see section 6.4.2 Creating ERPS protection ring.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet ring-protection** *ring-id* { **east** *interface-type interface-number* | **west** *interface-type interface-number* } **node-type rpl-owner** [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlanlist*]	Create the sub-ring on the intersecting node and set the intersecting node to the RPL Owner. By default, the protocol VLAN is set to 1. Blocked VLANs ranges from 1 to 4094. Note The links between 2 intersecting nodes belong to the master ring. Therefore, when you configure the sub-ring on the intersecting node, you can only configure the west or east interface.
	Raisecom(config)#**ethernet ring-protection** *ring-id* { **east** *interface-type interface-number* | **west** *interface-type interface-number* } **node-type rpl-neighbour** [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlanlist*]	Create the sub-ring on the intersecting node and set the intersecting node to the RPL Neighbour.

Step	Command	Description
	Raisecom(config)#**ethernet ring-protection** *ring-id* { **east** *interface-type interface-number* | **west** *interface-type interface-number* } [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlanlist*]	Create the sub-ring on the intersecting node and set the intersecting node to the protection forwarding node.
3	Raisecom(config)#**ethernet ring-protection** *ring-id* **raps-vc** { **with** | **without** }	(Optional) configure the sub-ring virtual channel mode on the intersecting node. By default, the sub-ring virtual channel adopts the **with** mode. **Note** Transmission modes on 2 intersecting nodes must be identical.
4	Raisecom(config)#**ethernet ring-protection** *ring-id* **propagate enable**	Enable the ring Propagate switch on the intersecting node. By default, the ring Propagate switch is disabled.

6.4.4 Configuring ERPS fault detection modes

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } **failure-detect physical-link**	Set the ERPS fault detection mode to **failure-detect physical-link**. By default, the ERPS fault detection mode is set to **failure-detect physical-link**.
	Raisecom(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } **failure-detect cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	Set 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-id* { **east**| **west** } **failure-detect physical-link-or-cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	Set the ERPS fault detection mode to **failure-detect physical-link-or-cc**. In this mode, a Trap is reported 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.

6.4.5 (Optional) configuring ERPS control

Note

By default, traffic is automatically switched to the protection line when the working line fails. Therefore, you need to configure ERPS control in some special cases.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet ring-protection** *ring-id* **force-switch { east | west }**	Switch the traffic on the protection ring to the west/east interface forcedly. • **east**: block the east interface and switch the traffic to the west interface forcedly. • **west**: block the west interface and switch the traffic to the east interface forcedly.
3	Raisecom(config)#**ethernet ring-protection** *ring-id* **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.

6.4.6 Checking configurations

No.	Command	Description
1	Raisecom)#**show ethernet ring-protection**	Show ERPS configurations.
2	Raisecom)#**show ethernet ring-protection status**	Show ERPS status.
3	Raisecom)#**show ethernet ring-protection statistics**	Show ERPS statistics.

6.5 Configuring failover

6.5.1 Preparing for configurations

Scenario

When the uplink of the middle device fails and the middle device fails to inform the downstream devices of the fault, the traffic cannot be switched to the backup line. This may cause traffic break.

The failover feature is used to add the upstream interfaces and downstream interfaces of the middle device to a failover group. In addition, it is used to monitor the upstream interfaces.

When all upstream interfaces fail, downstream interfaces are in Down status. When one failed upstream interface recovers from the fault, all downstream interfaces are in Up status. Therefore, faults of the uplinks can be notified to the downstream devices in time. If downstream interfaces fail, upstream interfaces still work properly.

Prerequisite

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

6.5.2 Configuring failover

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**link-state-tracking group** *group-number*	Create an interface-based failover group.
	Raisecom(config)#**link-state-tracking group** *group-number* **upstream ma-name** *ma-name* **cfm-mepid** *mep-id* **level** *level*	Create a MEP- based failover group.
	Raisecom(config)#**link-state-tracking group** *group-number* **upstream mlacp** *mlacp-id*	Create a MC- based failover group.
	Raisecom(config)#**link-state-tracking group** *group-number* **upstream elps-8031-link** *line-id*	Create a ELPS- based failover group.
3	Raisecom(config)#**interface** *interface-type primary-interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#**link-state-tracking group** *group-number* { **upstream** | **downstream** }	Configure the failover group to which the interface belongs and the interface type.
5	Raisecom(config-port)#**exit** Raisecom(config)#**link-state-tracking group** *group-number* **trap enable**	Configure the Trap of the failover group. By default, it is disabled.
6	Raisecom(config)#**link-state-tracking group** *group-number* **action** { **block-vlan** *vlan-list interface-type interface-number* | **delete-vlan** *vlan-id* | **flush-erps** *ring-id* | **modify-pvid** *vlan-id interface-type interface-number* | **suspend-vlan** *vlan-id* }	Configure failover processing action. **Note** Configure the processing action when the source of failover is MEP or ELPS.

6.5.3 Checking configurations

No.	Command	Description
1	Raisecom#**show link-state-tracking group** *group-number*	Show configurations of a failover group.

6.6 Maintenance

Command	Description
Raisecom(config)#**clear ethernet line-protection** *ring-id* **end-to-end command**	Clear end-to-end protection switching commands, including the **lockout**, **force-switch**, **manual-switch**, and **manual-switch-to-work** commands.
Raisecom(config)#**clear ethernet line-protection statistics**	Clear protection line statistics, including the number of Tx APS packets, Rx APS packets, last switching time, and last status switching time.
Raisecom(config)#**clear ethernet ring-protection** *ring-id* **command**	Clear protection switching commands, including the **force-switch** and **manual-switch** commands.
Raisecom(config)#**clear ethernet ring-protection** *ring-id* **statistics**	Clear protection ring statistics.

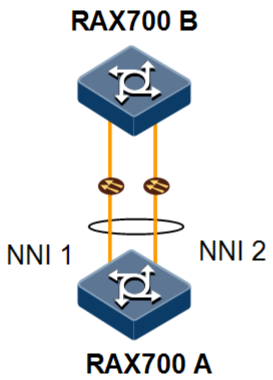
6.7 Configuration examples

6.7.1 Example for configuring manual link aggregation

Networking requirements

As shown in Figure 6-1, to improve reliability of the link between RAX700 A and RAX700 B, you can configure manual link aggregation on RAX700 A and RAX700 B. Add NNI 1 and NNI 2 to a LAG to form a single logical interface. The LAG performs load-sharing to the source MAC address.

Figure 6-1 Configuring manual link aggregation



Configuration steps

Step 1 Create a manual LAG.

- Configure RAX700 A.

```
Raisecom#hostname RAX700A
RAX700A#config
```

```
RAX700A(config)#interface port-channel 1
RAX700A(config-aggregator)#mode manual
RAX700A(config-aggregator)#exit
```

- Configure RAX700 B.

```
Raisecom#hostname RAX700B
RAX700B#config
RAX700B(config)#interface port-channel 1
RAX700B(config-aggregator)#mode manual
RAX700B(config-aggregator)#exit
```

Step 2 Add interfaces to the LAG.

- Configure RAX700 A.

```
RAX700A(config)#interface nni 1
RAX700A(config-port)#channel group 1
RAX700A(config-port)#exit
RAX700A(config)#interface nni 2
RAX700A(config-port)#channel group 1
RAX700A(config-port)#exit
```

- Configure RAX700 B.

```
RAX700B(config)#interface nni 1
RAX700B(config-port)#channel group 1
RAX700B(config-port)#exit
RAX700B(config)#interface nni 2
RAX700B(config-port)#channel group 1
RAX700B(config-port)#exit
```

Step 3 Configure the load-sharing mode of the LAG and enable link aggregation, taking RAX700 A for example.

```
RAX700A(config)#link-aggregation load-sharing mode smac
RAX700A(config)#link-aggregation enable
```

Step 4 Save configurations, taking RAX700 A for example.

```
RAX700A#write
```

Checking results

Use the **showlink-aggregation** command to show global configurations on manual link aggregation.

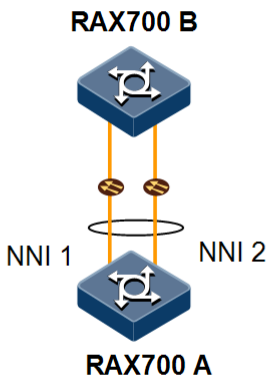
```
RAX700A#show link-aggregation
Link aggregation status:Enable
Load sharing mode:SMAC
Load sharing ticket generation algorithm:Direct-map
M - Manual    S - Static-Lacp    D - Dynamic-Lacp
GroupID       : 1                  Mode          : Manual
MinLinks      : 1                  MaxLinks       : 1
UpLinks       : 2                  Master Port    :
Restore Mode   : non-revertive        Restore delay(s): 1800
Member Port    : nni 1-2
Efficient Port :
```

6.7.2 Example for configuring static LACP link aggregation

Networking requirements

As shown in Figure 6-2, to improve the reliability of the link between RAX700 A and RAX700 B, you can configure static LACP link aggregation on RAX700 A and RAX700 B. Add NNI 1 and NNI 2 to a LAG to form a logical interface.

Figure 6-2 Configuring static LACP link aggregation



Configuration steps

Step 1 Configure the static LACP LAG on RAX700 A and set RAX700 A to the active end.

```
Raisecom#hostname RAX700A
RAX700A#config
RAX700A(config)#lacp system-priority 1000
RAX700A(config)#interface port-channel 1
RAX700A(config-aggregator)#mode lacp-static
RAX700A(config-aggregator)#exit
```

```
RAX700A(config)#interface nni 1
RAX700A(config-port)#channel group 1
RAX700A(config-port)#lacp port-priority 1000
RAX700A(config-port)#lacp mode active
RAX700A(config-port)#exit
RAX700A(config)#interface nni 2
RAX700A(config-port)#channel group 1
RAX700A(config-port)#lacp mode active
RAX700A(config-port)#exit
RAX700A(config)#link-aggregation enable
```

Step 2 Configure the static LACP LAG on RAX700 B.

```
Raisecom#hostname RAX700B
RAX700B#config
RAX700B(config)#interface port-channel 1
RAX700B(config-aggregator)#mode lacp-static
RAX700B(config-aggregator)#exit
RAX700B(config)#interface nni 1
RAX700B(config-port)#channel group 1
RAX700B(config-port)#exit
RAX700B(config)#interface nni 2
RAX700B(config-port)#channel group 1
RAX700B(config-port)#exit
RAX700B(config)#link-aggregation enable
```

Step 3 Save configurations, taking RAX700 A for example.

```
RAX700A#write
```

Checking results

Use the **showlink-aggregation** command on RAX700 A to show global configurations on static LACP link aggregation.

```
RAX700A#show link-aggregation
Link aggregation status:Enable
Load sharing mode:SXORDMAC
Load sharing ticket generation algorithm:Direct-map
M - Manual   S - Static-Lacp   D - Dynamic-Lacp
GroupID      : 1               Mode         : Static-Lacp
MinLinks     : 1               MaxLinks      : 4
UpLinks      : 0               Master Port   :
Restore Mode   : non-revertive      Restore delay(s): 1800
Member Port   : nni 1-2
Efficient Port :
```

Use the **show lacp internal** command on RAX700 A to show the local system LACP interface status, flag, interface priority, administration key, operation key, and interface state machine status.

```
RAX700A#show lacp internal
Flags:
  S - Device is requesting Slow LACPDUs  F - Device is requesting Fast 
LACPDUs
  A - Device in Active mode  P - Device in Passive mode   MP - MLACP Peer 
Port
Interface State      Flag   Port-Priority   Admin-key  Oper-key  Port-State
--------------------------------------------------------------------------
N1      Active       SA     1000          1           1        0x45
N2      Standby      SA     32768          1           1        0x45
```

Use the **show lacp neighbor** command on RAX700 A to show the remote system LACP interface status, flag, interface priority, administration key, operation key, and interface state machine status.

6.7.3 Example for configuring interface backup

Networking requirements

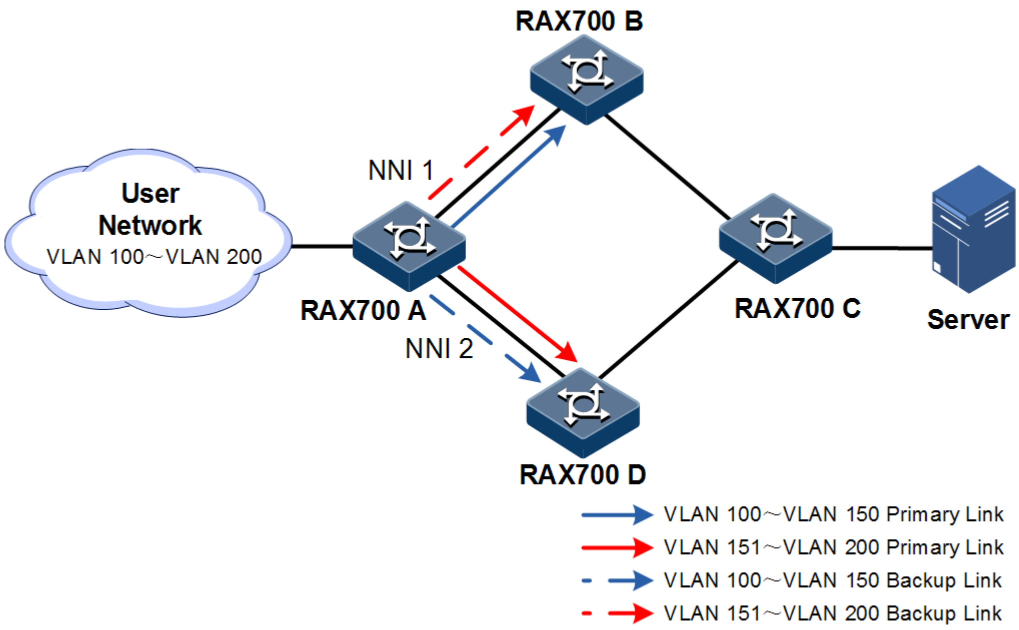
As shown in Figure 6-3, to make the PC access the server reliably, you need to configure the interface backup group on RAX700 A and back up services from VLANs 100–200 for achieving link protection. Configurations are shown as below:

- In VLANs 100–150, set NNI 1 of RAX700 A to the primary interface and NNI 2 of RAX700 A to the backup interface.
- In VLANs 151–200, set NNI 2 of RAX700 A to the primary interface and NNI 1 of RAX700 A to the backup interface.

When NNI 1 fails, the traffic is switched to NNI 2 to keep the link normal.

The RAX700 A should support interface backup while RAX700 B, RAX700 C, and RAX700 D do not need to support interface backup.

Figure 6-3 Configuring interface backup



Configuration steps

Step 1 Creates VLANs 100–200 and add NNI 1 and NNI 2 to VLANs 100–200.

```
Raisecom#config
Raisecom(config)#create vlan 100-200 active
Raisecom(config)#interface nni 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 100-200 confirm
Raisecom(config-port)#exit
Raisecom(config)#interface nni 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 100-200 confirm
Raisecom(config-port)#exit
```

Step 2 In VLANs 100–150, set NNI 1 to the primary interface and NNI 2 to the backup interface.

```
Raisecom(config)#interface nni 1
Raisecom(config-port)#switchport backup nni 2 vlanlist 100-150
Raisecom(config-port)#exit
```

Step 3 In VLANs 151–200, set NNI 2 to the primary interface and NNI 1 to the backup interface.

```
Raisecom(config)#interface nni 2
Raisecom(config-port)#switchport backup nni 1 vlanlist 151-200
```

Step 4 Save configurations.

```
Raisecom#write
```

Checking results

Use the **show switchport backup** command to show interface backup configurations in normal state and in link-failure state.

When both NNI 1 and NNI 2 are in Up status, NNI 1 forwards the traffic in VLANs 100–150 and NNI 2 forwards the traffic in VLANs 151–200.

```
Raisecom#show switchport backup
Restore delay: 15s.
Restore mode: port-up.
Active Port(State)  Backup Port(State)  Vlanlist  Active MAID  MEL  Lmpid
Rmpid  Backup MAID  MEL  Lmpid  Rmpid
-----------------------------------------------------------------
nni1(Up)         nni2(Standby)       100-150      N/A   0    0      0
N/A      0          0       0
nni2(Up)         nni1(Standby)       151-200      N/A   0    0      0
N/A      0          0       0
```

Manually break the link between RAX700 A and RAX700 B to emulate a fault. At this time, NNI 1 is in Down status and NNI 2 is responsible for forwarding the traffic in VLANs 100–200.

```
Raisecom#show switchport backup
Restore delay: 15s
Restore mode: port-up
Active Port(State)  Backup Port(State)  Vlanlist  Active MAID  MEL  Lmpid
Rmpid  Backup MAID  MEL  Lmpid  Rmpid
-----------------------------------------------------------------
nni1(Down)         nni2(Up)       100-150      N/A   0    0      0    N/A
0         0       0
nni2(Up)          nni1(Down)      100-200      N/A   0    0      0    N/A
0         0       0
```

When NNI 1 recovers from a fault, during the WTR time, NNI 1 is the standby interface and NNI 2 is responsible for forwarding the traffic in VLANs 100–200.

```
Raisecom#show switchport backup
Restore delay: 15s.
Restore mode: port-up.
Active Port(State)  Backup Port(State)  Vlanlist  Active MAID  MEL  Lmpid
Rmpid  Backup MAID  MEL  Lmpid  Rmpid
-----------------------------------------------------------------
```

```
nni1(Standby)         nni2(Up)       100-150      N/A   0     0      0
N/A       0         0       0
nni2(Up)           nni1(Standby)      151-200      N/A   0     0      0
N/A  0         0       0
```

When NNI 1 recovers to the Up status and keeps for 15s (restore-delay), NNI 1 forwards the traffic in VLANs 100–150 and NNI 2 forwards the traffic in VLANs 151–200.

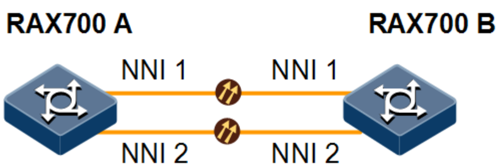
```
Raisecom#show switchport backup
Restore delay: 15s.
Restore mode: port-up.
Active Port(State)  Backup Port(State)  Vlanlist  Active MAID  MEL  Lmpid
Rmpid  Backup MAID  MEL  Lmpid  Rmpid
-----------------------------------------------------------------
nni1(Up)          nni2(Standby)      100-150      N/A   0     0      0
N/A       0         0       0
nni2(Up)           nni1(Standby)      151-200      N/A   0     0      0
N/A  0         0       0
```

6.7.4 Example for configuring 1:1 ELPS

Networking requirements

As shown in Figure 6-4, to enhance reliability of the link between RAX700 A and RAX700 B, you need to configure 1:1 ELPS on RAX700 A and RAX700 B and detect the fault based on the physical interface status. The working interface NNI 1 and protection interface NNI 2 are in VLANs 100–200.

Figure 6-4 Configuring 1:1 ELPS



Configuration steps

Step 1 Create VLANs 100–200 and add NNI 1 and NNI 2 to VLANs 100–200.

- Configure RAX700 A.

```
Raisecom#hostname RAX700A
RAX700A#config
RAX700A(config)#create vlan 100-200 active
RAX700A(config)#interface nni 1
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#switchport trunk allowed vlan 100-200 confirm
RAX700A(config-port)#exit
```

```
RAX700A(config)#interface nni 2
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#switchport trunk allowed vlan 100-200 confirm
RAX700A(config-port)#exit
```

- Configure RAX700 B.

```
Raisecom#hostname RAX700B
RAX700B#config
RAX700B(config)#create vlan 100-200 active
RAX700B(config)#interface nni 1
RAX700B(config-port)#switchport mode trunk
RAX700B(config-port)#switchport trunk allowed vlan 100-200 confirm
RAX700B(config-port)#exit
RAX700B(config)#interface nni 2
RAX700B(config-port)#switchport mode trunk
RAX700B(config-port)#switchport trunk allowed vlan 100-200 confirm
RAX700B(config-port)#exit
```

Step 2 Create the 1:1 ELPS protection line.

- Configure RAX700 A.

```
RAX700A(config)#ethernet line-protection 1 working line 1 1,100-200
protection line 2 1,100-200 one-to-one 150
```

- Configure RAX700 B.

```
RAX700B(config)#ethernet line-protection 1 working line 1 1,100-200
protection line 2 1,100-200 one-to-one 150
```

Step 3 Configure the fault detection mode.

- Configure RAX700 A.

```
RAX700A(config)#ethernet line-protection 1 working failure-detect
physical-link
RAX700A(config)#ethernet line-protection 1 protection failure-detect
physical-link
```

- Configure RAX700 B.

```
RAX700B(config)#ethernet line-protection 1 working failure-detect
physical-link
```

```
RAX700B(config)#ethernet line-protection 1 protection failure-detect
physical-link
```

Step 4 Save configurations, taking RAX700 A for example.

```
RAX700A#write
```

Checking results

Use the **show ethernet line-protection** command to show 1:1 ELPS configurations, taking RAX700 A for example.

```
RAX700A#show ethernet line-protection 1
Id:1
Name:--
ProtocolVlan: 150
Working Entity Information:
Port:    nni1
Vlanlist: 100-200
FaiureDetect:physical
MAID:    --
MdLevel:  0
LocalMep: 0
RemoteMep:0
State/LCK:Active/N
Protection Entity Information:
Port:    nni2
Vlanlist: 100-200
FaiureDetect:physical
MAID:    --
MdLevel:  0
LocalMep: 0
RemoteMep:0
State/F/M:Standby/N/N
Wtr(m):5
Holdoff(100ms):0
```

Use the **show ethernet line-protection aps** command to show 1:1 ELPS APS information, taking RAX700 A for example.

```
RAX700A#show ethernet line-protection 1 aps
Id      Type    Direction Revert Aps State Signal(Requested/Bridged)
-----------------------------------------------------------------------
1-Local  1:1     bi       yes    yes NR-W  null/null
1-Remote 1:1     bi       yes    yes NR-W  null/null
```

6.7.5 Example for configuring single-ring ERPS

Networking requirements

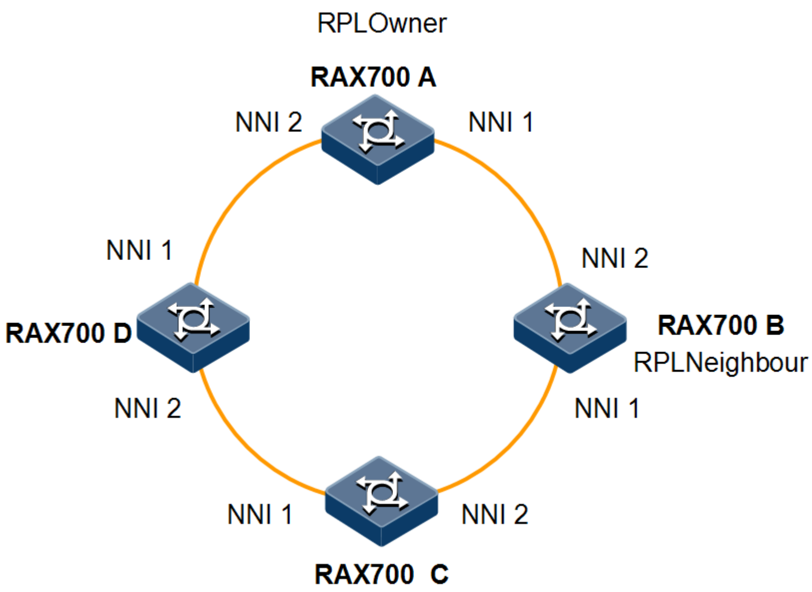
As shown in Figure 6-5, to enhance Ethernet reliability, RAX700 A, RAX700 B, RAX700 C, and RAX700 D form an ERPS single ring.

RAX700 A is the RPL Owner and RAX700 B is the RPL neighbour. The link between RAX700 A and RAX700 B are blocked.

The fault detection mode on the link between RAX700 A and RAX700 D is set to physical-link-or-cc. The default detection mode on other links is set to physical-link.

The default value of protocol VLAN is set to 1. Blocked VLAN IDs ranges from 1 to 4094.

Figure 6-5 Configuring single-ring ERPS



Configuration steps

Step 1 Add interfaces to VLANs 1–4094.

- Configure RAX700 A.

```
Raisecom#hostname RAX700A
RAX700A#config
RAX700A(config)#interface nni 1
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#exit
RAX700A(config)#interface nni 2
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#exit
```

- Configure RAX700 B.

```
Raisecom#hostname RAX700B
RAX700B#config
RAX700B(config)#interface nni 1
RAX700B(config-port)#switchport mode trunk
RAX700B(config-port)#exit
RAX700B(config)#interface nni 2
RAX700B(config-port)#switchport mode trunk
RAX700B(config-port)#exit
```

- Configure RAX700 C.

```
Raisecom#hostname RAX700C
RAX700C#config
RAX700C(config)#interface nni 1
RAX700C(config-port)#switchport mode trunk
RAX700C(config-port)#exit
RAX700C(config)#interface nni 2
RAX700C(config-port)#switchport mode trunk
RAX700C(config-port)#exit
```

- Configure RAX700 D.

```
Raisecom#hostname RAX700D
RAX700D#config
RAX700D(config)#interface nni 1
RAX700D(config-port)#switchport mode trunk
RAX700D(config-port)#exit
RAX700D(config)#interface nni 2
RAX700D(config-port)#switchport mode trunk
RAX700D(config-port)#exit
```

Step 2 Configure CFM.

- Configure RAX700 A.

```
RAX700A(config)#cfm domain md-name md1 level 7
RAX700A(config)#service ma1 level 7
RAX700A(config-service)#service vlan-list 1
RAX700A(config-service)#service mep down mpid 1 nni 2
RAX700A(config-service)#service remote-mep 2 nni 2
RAX700A(config-service)#service cc enable mep 1
RAX700A(config-service)#exit
RAX700A(config)#cfm enable
```

- Configure RAX700 D.

```
RAX700D(config)#cfm domain md-name md1 level 7
RAX700D(config)#service ma1 level 7
RAX700D(config-service)#service vlan-list 1
RAX700D(config-service)#service mep down mpid 2 nni 1
RAX700D(config-service)#service remote-mep1 nni 1
RAX700D(config-service)#service cc enable mep 2
RAX700D(config-service)#exit
RAX700D(config)#cfm enable
```

Step 3 Create the ERPS protection ring.

- Configure RAX700 A.

```
RAX700A(config)#ethernet ring-protection 1 east nni 1 west nni 2 node-
type rpl-owner rpl east
```

- Configure RAX700 B.

```
RAX700B(config)#ethernet ring-protection 1 east nni 1 west nni 2 node-
type rpl-neighbour rplwest
```

- Configure RAX700 C.

```
RAX700C(config)#ethernet ring-protection 1 east nni 1 west nni 2
```

- Configure RAX700 D.

```
RAX700D(config)#ethernet ring-protection 1 east nni 1 west nni 2
```

Step 4 Configure the fault detection mode.

- Configure RAX700 A.

```
RAX700A(config)#ethernet ring-protection 1 west failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 12 22
```

- Configure RAX700 D.

```
RAX700D(config)#ethernet ring-protection 1 east failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 21 32
```

Step 5 Save configurations, taking RAX700 A for example.

```
RAX700A#write
```

Checking results

Use the **show ethernet ring-protection status** command to show ERPS protection ring configurations, taking RAX700 A for example. RPLs are blocked to avoid a loop.

```
RAX700A#show ethernet ring-protection status
Id/Name  Bridge-State   Last Occur(ago)   East-State West-State sc Traffic-vlanlist
--------------------------------------------------------------------------
1       idle 0 day 0:0:50:750  block  forwarding  1  1-4094
```

Manually break the link between RAX700 B and RAX700 C to emulate a fault. Use the **show ethernet ring-protection status** command on RAX700 A again to show ERPS protection ring status. RPLs are in forwarding status.

```
RAX700A#show ethernet ring-protection status
Id/Name  Bridge-State   Last Occur(ago)   East-State West-State sc Traffic-vlanlist
--------------------------------------------------------------------------
1      Protection0 day 0:0:55:950  forwardingforwarding  1  1-4094
```

6.7.6 Example for configuring intersecting-ring ERPS

Networking requirements

As shown in Figure 6-6, to enhance Ethernet reliability, RAX700 A, RAX700 B, RAX700 C, RAX700 D, RAX700 E, and RAX700 F form an ERPS intersecting ring.

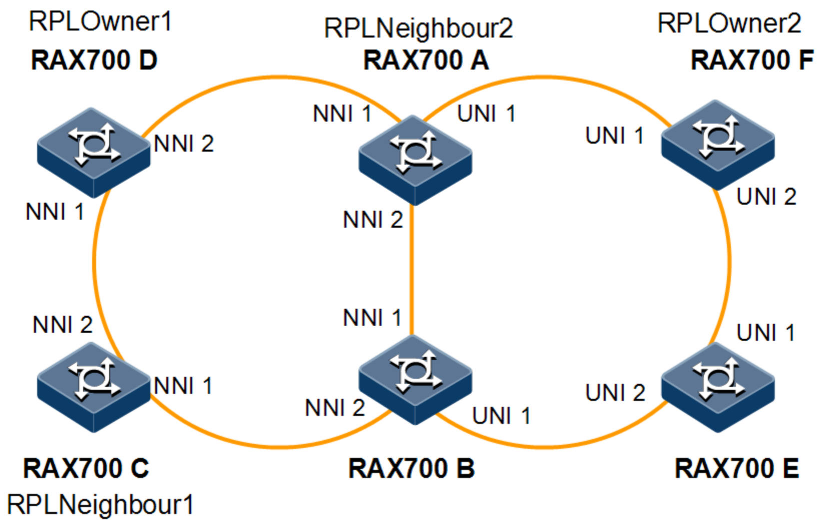
RAX700 A, RAX700 B, RAX700 C, and RAX700 D form the master ring. RAX700 D is the RPL Owner of the master ring and RAX700 C is the RPL neighbour of the master ring. The blocked interface is NNI 1 of RAX700 D. The default value of protocol VLAN is set to 1.

RAX700 A, RAX700 B, RAX700 E, and RAX700 F form the sub-ring. RAX700 F is the RPL Owner of the sub-ring and RAX700 A is the RPL neighbour of the sub-ring. The blocked interface is UNI 1 of RAX700 F. The default value of protocol VLAN is set to 4094. The virtual channel mode of the sub-ring is set to **with** mode.

Blocked VLAN IDs ranges from 1 to 4094 for both the master ring and the sub-ring.

Devices on the master ring adopt the physical-link-or-cc fault detection mode while devices on the sub-ring adopt the physical-link fault detection mode.

Figure 6-6 Configuring intersecting-ring ERPS



Configuration steps

Step 1 Add interfaces to VLANs 1–4094.

- Configure RAX700 A.

```
Raisecom#hostname RAX700A
RAX700A#config
RAX700A(config)#interface nni 1
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#exit
RAX700A(config)#interface nni 2
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#exit
RAX700A(config)#interface uni 1
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#exit
```

- Configure RAX700 B.

```
Raisecom#hostname RAX700B
RAX700B#config
RAX700B(config)#interface nni 1
RAX700B(config-port)#switchport mode trunk
RAX700B(config-port)#exit
RAX700B(config)#interface nni 2
RAX700B(config-port)#switchport mode trunk
RAX700B(config-port)#exit
RAX700B(config)#interface uni 1
RAX700B(config-port)#switchport mode trunk
RAX700B(config-port)#exit
```

- Configure RAX700 C.

```
Raisecom#hostname RAX700C
RAX700C#config
RAX700C(config)#interface nni 1
RAX700C(config-port)#switchport mode trunk
RAX700C(config-port)#exit
RAX700C(config)#interface nni 2
RAX700C(config-port)#switchport mode trunk
RAX700C(config-port)#exit
```

- Configure RAX700 D.

```
Raisecom#hostname RAX700D
RAX700D#config
RAX700D(config)#interface nni 1
RAX700D(config-port)#switchport mode trunk
RAX700D(config-port)#exit
RAX700D(config)#interface nni 2
RAX700D(config-port)#switchport mode trunk
RAX700D(config-port)#exit
```

- Configure RAX700 E.

```
Raisecom#hostname RAX700E
RAX700E#config
RAX700E(config)#interface uni 1
RAX700E(config-port)#switchport mode trunk
RAX700E(config-port)#exit
RAX700E(config)#interface uni 2
RAX700E(config-port)#switchport mode trunk
RAX700E(config-port)#exit
```

- Configure RAX700 F.

```
Raisecom#hostname RAX700F
RAX700F#config
RAX700F(config)#interface uni 1
RAX700F(config-port)#switchport mode trunk
RAX700F(config-port)#exit
RAX700F(config)#interface uni 2
RAX700F(config-port)#switchport mode trunk
RAX700F(config-port)#exit
```

Step 2 Configure CFM detection on the master ring.

- Configure RAX700 A.

```
RAX700A(config)#cfm domain md-name md1 level 7
RAX700A(config)#service ma1 level 7
RAX700A(config-service)#service vlan-list 1
RAX700A(config-service)#service mep down mpid 1 nni 1
RAX700A(config-service)#service mep down mpid 2 nni 2
RAX700A(config-service)#service cc enable mep 1
RAX700A(config-service)#service cc enable mep 2
RAX700A(config-service)#exit
RAX700A(config)#cfm enable
```

- Configure RAX700 B.

```
RAX700B(config)#cfm domain md-name md1 level 7
RAX700B(config)#service ma1 level 7
RAX700B(config-service)#service vlan-list 1
RAX700B(config-service)#service mep down mpid 3 nni 1
RAX700B(config-service)#service mep down mpid 4 nni 2
RAX700B(config-service)#service cc enable mep 3
RAX700B(config-service)#service cc enable mep 4
RAX700B(config-service)#exit
RAX700B(config)#cfm enable
```

- Configure RAX700 C.

```
RAX700C(config)#cfm domain md-name md1 level 7
RAX700C(config)#service ma1 level 7
RAX700C(config-service)#service vlan-list 1
RAX700C(config-service)#service mep down mpid 5 nni 1
RAX700C(config-service)#service mep down mpid 6 nni 2
RAX700C(config-service)#service cc enable mep 5
RAX700C(config-service)#service cc enable mep 6
RAX700C(config-service)#exit
RAX700C(config)#ethernet cfm enable
```

- Configure RAX700 D.

```
RAX700D(config)#cfm domain md-name md1 level 7
RAX700D(config)#service ma1 level 7
RAX700D(config-service)#service vlan-list 1
RAX700D(config-service)#service mep down mpid 7 nni 1
RAX700D(config-service)#service mep down mpid 8 nni 2
RAX700D(config-service)#service cc enable mep 7
RAX700D(config-service)#service cc enable mep 8
RAX700D(config-service)#exit
```

```
RAX700D(config)#ethernet cfm enable
```

Step 3 Create the ERPS master ring.

- Configure RAX700 A.

```
RAX700A(config)#ethernet ring-protection 1 east nni 1 west nni 2
```

- Configure RAX700 B.

```
RAX700B(config)#ethernet ring-protection 1 east nni 1 west nni 2
```

- Configure RAX700 C.

```
RAX700C(config)#ethernet ring-protection 1 east nni 1 west nni 2 node-
type rpl-neighbour rpl west
```

- Configure RAX700 D.

```
RAX700D(config)#ethernet ring-protection 1 east nni 1 west nni 2 node-
type rpl-owner rpl east
```

Step 4 Configure the fault detection mode of the master ring.

- Configure RAX700 A.

```
RAX700A(config)#ethernet ring-protection 1 east failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 1 8
RAX700A(config)#ethernet ring-protection 1 west failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 2 3
```

- Configure RAX700 B.

```
RAX700B(config)#ethernet ring-protection 1 east failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 3 2
RAX700B(config)#ethernet ring-protection 1 west failure-detect physical-
link-or-cc md md1 ma ma1 level 7 mep 4 5
```

- Configure RAX700 C.

```
RAX700C(config)#ethernet ring-protection 1 east failure-detect physical-link-or-cc md md1 ma ma1 level 7 mep 5 4
RAX700C(config)#ethernet ring-protection 1 west failure-detect physical-link-or-cc md md1 ma ma1 level 7 mep 6 7
```

- Configure RAX700 D.

```
RAX700D(config)#ethernet ring-protection 1 east failure-detect physical-link-or-cc md md1 ma ma1 level 7 mep 7 6
RAX700D(config)#ethernet ring-protection 1 west failure-detect physical-link-or-cc md md1 ma ma1 level 7 mep 8 1
```

Step 5 Configure the ERPS sub-ring.

- Configure RAX700 A.

```
RAX700A(config)#ethernet ring-protection 2 east uni 1 node-type rpl-neighbour protocol-vlan 4094
RAX700A(config)#ethernet ring-protection 2 propagate enable
```

- Configure RAX700 B.

```
RAX700B(config)#ethernet ring-protection 2 east uni 1 protocol-vlan 4094
RAX700B(config)#ethernet ring-protection 2 propagate enable
```

- Configure RAX700 E.

```
RAX700E(config)#ethernet ring-protection 2 east uni 1 west uni 2 protocol-vlan 4094
```

- Configure RAX700 F.

```
RAX700F(config)#ethernet ring-protection 2 east uni 1 west uni 2 node-type rpl-owner rpl east protocol-vlan 4094
```

Step 6 Save configurations, taking RAX700 A for example.

```
RAX700A#write
```

Checking results

Use the **show ethernet ring-protection status** command on RAX700 A, RAX700 D, and RAX700 F to show ERPS protection ring configurations.

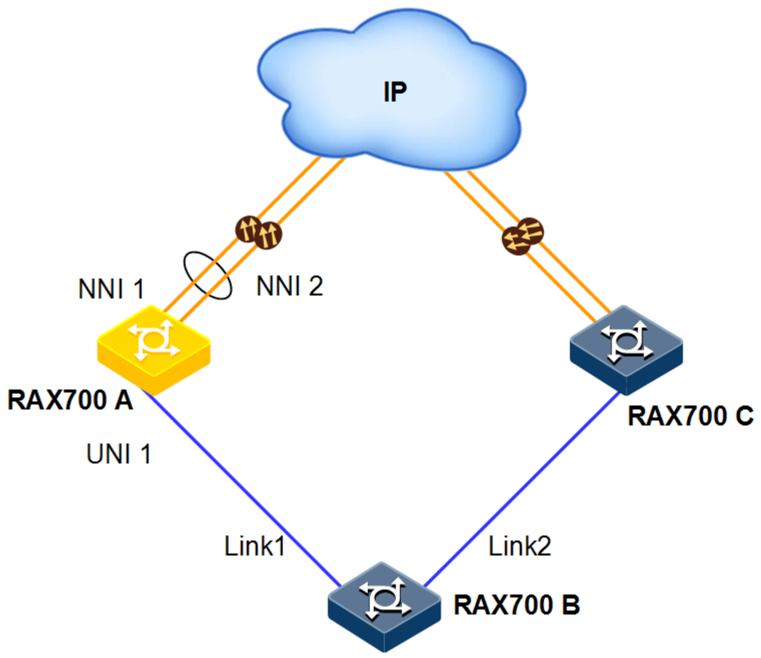
```
RAX700A#show ethernet ring-protection status
Id/Name  Bridge-State  Last Occur(ago)East-State West-State sc   Traffic-
vlanlist
---------------------------------------------------------------------
1       idle 0 day 0:0:50:750  forwarding  forwarding 1    1-4094
Id/Name  Status  Last Occur(ago)East-State West-State sc   Traffic-
vlanlist
---------------------------------------------------------------------
2       idle 0 day 0:0:50:750  forwarding  forwarding 1    1-4094

RAX700D#show ethernet ring-protection status
Id/Name  Bridge-State  Last Occur(ago)  East-State West-State sc Traffic-
vlanlist
---------------------------------------------------------------------
1       idle 0 day 0:0:50:750  block forwarding  1  1-4094

RAX700F#show ethernet ring-protection status
Id/Name  Bridge-State  Last Occur(ago)  East-State West-State sc Traffic-
vlanlist
---------------------------------------------------------------------
2 idle 0 day 0:0:50:750  block forwarding  1  1-4094
```

6.7.7 Example for configuring failover

Networking requirements

As shown in Figure 6-7, to improve network reliability, RAX700 B is connected to RAX700 A and RAX700 C through Link 1 and Link 2 separately. Link 1 is the working line and Link 2 is the protection line. Link 2 does not forward data unless Link 1 fails. RAX700 A is connected uplink to the IP network in the link aggregation mode. When all uplinks of RAX700 A fail, you need to make RAX700 B sense the fault immediately to switch traffic to the protection line in time. Therefore, you need to deploy failover on RAX700 A.

Figure 6-7 Configuring failover



Configuration steps

Step 1 Create a failover group.

```
Raisecom(config)#link-state-tracking group 1
```

Step 2 Add the uplink interface to the failover group.

```
Raisecom(config)#interface nni 1
Raisecom(config-port)#link-state-tracking group 1 upstream
```

Step 3 Add the downlink interface to the failover group.

```
Raisecom(config)#interface uni 1
Raisecom(config-port)#link-state-tracking group 1 downstream
```

Checking results

Use the **show link-state-tracking group** command to show configurations on the failover group.

```
Raisecom(config)#show link-state-tracking group 1
```

```
Link State Tracking Group: 1(enable)
Status:  Normal
Upstream Interfaces:  nni1(Up)
Upsteam Mep:   --
Upsteam aps-8031:     --
Downstream Interfaces:      uni1(Up)
```

After all uplinks of RAX700 A fail, use the **show link-state-tracking group** command to show configurations on the failover group. In this case, you can learn that the downlink interface UNI 1 is disabled.

```
Raisecom(config)#show link-state-tracking group 1
Link State Tracking Group: 1(enable)
Status:  Normal
Upstream Interfaces:  nni1(Down)
Upsteam Mep:   --
Upsteam aps-8031:     --
Downstream Interfaces:      uni1(Down)
```

7 DHCP Client

This chapter describes principles and configuration procedures of DHCP Client, as well as related configuration examples, including following sections:

- Configuring DHCP Client
- Configuration examples

7.1 Configuring DHCP Client

7.1.1 Preparing for configurations

Scenario

When the RAX711-L acts as a DHCP client, it obtains an IP address from the specified DHCP server. The IP address is used to perform follow-up management on the RAX711-L.

When the IP address of the DHCP client is dynamically assigned, it has the lease time. When the lease time expires, the DHCP server will withdraw the IP address. The DHCP client needs to renew the IP address if it continues to use the IP address. If the lease time does not expire and the DHCP client does not need to use the IP address, it can release the IP address.

Note

The RAX711-L supports related configurations of DHCP Client on IP interface 0 only.

Prerequisite

The RAX711-L is not enabled with DHCP Server.

7.1.2 (Optional) configuring DHCP Client information

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface ip 0**	Enter Layer 3 interface configuration mode.

Step	Command	Description
3	Raisecom(config-ip)#**ip dhcp client** { **class-id** *class-id* | **client-id** *client-id* | **hostname** *hostname* }	Configure DHCP Client information, including class identifier, client identifier, and host name. **Note** If the RAX711-L is enabled with DHCP Client, you cannot configure the DHCPv4 Client information.

7.1.3 Enabling DHCPClient

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface ip 0**	Enter Layer 3 interface configuration mode.
3	Raisecom(config-ip)#**ip address dhcp** [**server-ip** *ip-address*]	Enable DHCPv4 Client and specify the DHCPv4 Server address. It means enabling DHCPv4 Client applying for the IP address.
	Raisecom(config-ip)#**ipv6 address dhcp** [**server-ip** *ipv6-address*]	Enable DHCPv6 Client and specify the DHCPv6 Server address. It means enabling DHCPv6 Client applying for the IP address

7.1.4 (Optional) renewing IPv4 addresses

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface ip 0**	Enter Layer 3 interface configuration mode.
3	Raisecom(config-ip)#**ip dhcp client renew**	Renew the IPv4 address.
	Raisecom(config-ip)#**ipv6 dhcp client renew**	Renew the IPv6 address
4	Raisecom(config-ip)#**ipv6 dhcp client rapid-commit**	Enable the rapid interactivity of the DHCPv6 Client. By default, it is disabled.

7.1.5 Checking configurations

No.	Command	Description
1	Raisecom#**show ip dhcp client**	Show DHCPv4 Client configurations.
	Raisecom#**show ipv6 dhcp client**	Show DHCPv6 Client configurations.

7.2 Configuration examples

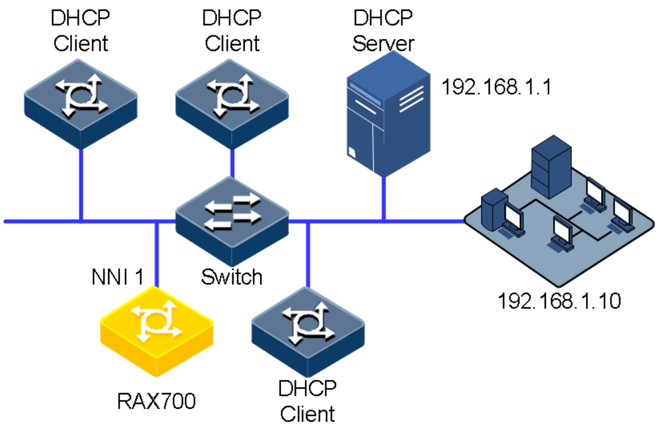
7.2.1 Example for configuring DHCPv4 Client

Networking requirements

As shown in Figure 7-1, the RAX711-Lworks as the DHCP client. The DHCP server needs to assign an IP address to the RAX711-L. Therefore, the NView NNM system can discover and manage the RAX711-L.

The hostname is set to raisecom.

Figure 7-1 Configuring DHCPv4 Client



Configuration steps

Step 1 Configure DHCP Client (the RAX711-L) information.

```
Raisecom#config
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip dhcp client hostname raisecom
```

Step 2 Apply an IP address in the DHCP mode.

```
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address dhcp server-ip 192.168.1.1
```

Step 3 Save configurations.

```
Raisecom#write
```

Checking results

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

```
Raisecom#show ip dhcp client
  Hostname:               raisecom
  Class-ID:               Raisecom-ROS_RAX711-L_2.0.8.20140109
  Client-ID:              Raisecom-ff00537bc000-IF0
  DHCP Client is requesting for a lease.
  Assigned IP Addr:        0.0.0.0
  Subnet mask:            0.0.0.0
  Default Gateway:         --
  Client lease Starts:      Jan-01-2010 08:00:00
  Client lease Ends:       Jan-01-2011 08:00:00
  Client lease duration:    0(sec)
  DHCP Server:            192.168.1.1
  Tftp server name:        --
  Tftp server IP Addr:      --
  Startup_config filename:   --
  NTP server IP Addr:       --
  Root path:             -
```

8 OAM

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

- RSOM
- Configuring EFM
- Configuring CFM
- Configuring SLA
- Configuring Y.1564
- Configuring RSOM
- Maintenance
- Configuration examples

8.1 RSOM

Raisecom Service Oriented Management (RSOM) is based on the MEF40, and aims to promote usability of the Ethernet, and open, manage the Ethernet PLS.

The services type of the Ethernet includes E-Line, E-Lan, and E-Tree.

RSOM includes the services transmission and test and measurement of the Ethernet.

Ethernet services include Ethernet Virtual Connection (EVC) and the UNI corresponding to the EVC. Each EVC is corresponding to a service.

Services transmission of the Ethernet service

Based on the different profiles, services transmission of the Ethernet service matches the packets entering the service and deal with them according to rules. The Ethernet service supports the following profiles.

- L2CP profile: it supports configuring the protocol for matching packets and corresponding action for processing them. It also supports configuring transparent transmission of L2CP packets to the specified destination MAC address.
- CoS profile: it is namely the QoS profile. It is used for the bandwidth profile. It supports configuring CoS and traffic classification rules. Packets enter the quene and are transmitted according to traffic classification rule. Because according to different

classification rules, the rules of priority mapping are different, thus packets enter the quene configured through Ethernet QoS to schedule according to different priority mapping rules.

- Bandwidth profile: it supports configuring coupling function and color aware mode, and supports configuring rate limiting rule.

Test and measurement of the Ethernet service

Test and measurement of the Ethernet service function is achieved by the SLA, Y.1564, Loopback, and CFM.

After you configure the threshold profile and information about remote devices, the measurement through SLA is available for delay, jitter, packet loss ratio, and availability test. After you configure the basic test information (frame type of the test traffic, frame size, etc.), test bandwidth ratio, information about remote devices, and quoting Y.1564 threshold profile through Y.1564 to enable Y.1564 test. Loopback function can be used with Y.1564 test only by configuring loopback packets. CFM function can start CC detection only by configuring information on the devices.

8.2 Configuring EFM

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

8.2.2 Configuring basic functions of EFM

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**oam send-period** *coefficient*	(Optional) OAM link connection is established by both ends sending INFO packet to each other. You can use this command to set the interval for sending INFO packets to control the communicate period of the link. By default, the interval is set to 1s (10×100ms).
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#**oam** { **active** | **passive** }	Configure a working mode of EFM. When configuring EFM OAM, you must ensure that at least one end is in active mode. Otherwise, you cannot successfully detect a link.

Step	Command	Description
5	Raisecom(config-port)#**oam enable**	Enable OAM on An interface. By default, OAM is disabled on the interface.

8.2.3 Configuring active functions of EFM

Note

Active functions of EFM must be configured when the RAX711-L is in active mode.

(Optional)configuring RAX711-L initiating 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 a remote loopback status, the RAX711-L 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** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**oam remote-loopback**	Initiate EFM remote loopback on an interface. The remote loopback can be initiated only when EFM connection is established. In addition, only the active end can initiate EFM remote loopback.
4	Raisecom(config-port)#**no oam remote-loopback**	(Optional) disable EFM remote loopback immediately after EFM loop detection is finished.

(Optional) configuring peer OAM event Trap

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)#**oam peer event trap enable**	Enable peer OAM event Trap to report link monitoring events to the NView NNM system immediately. By default, peer OAM event Trap is disabled.

(Optional) viewing current variable values of peer device

Note

After EFM connection is established, you can get current link status by getting the current variable values of the peer.

Step	Command	Description
1	Raisecom#**show oam peer** [**link-statistic** | **oam-info**] *interface-type interface-number-list*	Get OAM information or variable values about the peer device.

8.2.4 Configuring passive functions of EFM

Note

The passive functions of EFM can be configured regardless of the RAX711-L is in active or passive mode.

(Optional) configuring device responding to EFM remote loopback

Note

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** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**oam loopback** { **ignore** | **process** }	Ignore/Respond to EFM remote loopback. By default, the RAX711-L responds to EFM remote loopback.

(Optional) configuring OAM link monitoring

Note

OAM link monitoring is used to detect and report link errors in different conditions. When detecting a fault on a link, the RAX711-L 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 via SNMP Trap. Besides, the local device can directly report events to the NView NNM system via 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.

Step	Command	Description
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**oam errored-frame window** *window* **threshold** *threshold*	Configure the monitor window and threshold for an error frame event. By default, the monitor window is set to 1s and the threshold is set to 1 error frame.
4	Raisecom(config-port)#**oam errored-frame-period window** *window* **threshold** *threshold*	Configure the monitor window and threshold for an error frame period event. By default, the monitor window is set to 100ms and the threshold is set to 1 error frame.
5	Raisecom(config-port)#**oam errored-frame-seconds window** *window* **threshold** *threshold*	Configure the monitor window and threshold for an error frame seconds event. By default, the monitor window is set to 60s and the threshold is set to 1s.
6	Raisecom(config-port)#**oam errored-symbol-period window** *window* **threshold** *threshold*	Configure the monitor window and threshold for an error symbol event. By default, the monitor window is set to 60s and the threshold is set to 1s.

(Optional) configuring OAM fault indication

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)#**oam notify** { **critical-event** | **dying-gasp** | **errored-frame** | **errored-symbol-period** | **errored-frame-seconds** | **errored-frame-period** } **enable**	Enable OAM fault indication mechanism, which is used to inform the peer when the local device fails. By default, OAM fault indication is enabled.

(Optional) configuring local OAM event Trap

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)#**oam event trap enable**	Enable local OAM event Trap to report link monitoring events to the NView NNM system immediately. By default, local OAM event Trap is disabled.

8.2.5 Configuring loopback timeout

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)#**oam loopback timeout** *second*	Configure OAM loopback timeout. By default, OAM loopback timeout is set to 3s.
4	Raisecom(config-port)#**oam loopback retry** *retry-number*	Configure OAM loopback packet retry times. By default, OAM loopback packet retry times are set to 2.
5	Raisecom(config-port)#**oam loopback** { **ignore** | **process** }	(Optional) ignore/respond to the peer OAM loopback establishment request. By default, the peer OAM loopback establishment request is ignored.

8.2.6 Checking configurations

No.	Command	Description
1	Raisecom#**show oam** [*interface-type interface-list*]	Show EFM basic configurations.
2	Raisecom#**show oam loopback** [*interface-type interface-list*]	Show EFM remote loopback configurations.
3	Raisecom#**show oam notify** [*interface-type interface-list*]	Show OAM link monitoring and fault indication configurations.
4	Raisecom#**show oam statistics** [*interface-type interface-list*]	Show OAM statistics.
5	Raisecom#**show oam trap** [*interface-type interface-list*]	Show OAM event Trap configurations.
6	Raisecom#**show oam event** [*interface-type interface-list*] [**critical**]	Show local OAM link events detected on an interface.

8.3 Configuring CFM

8.3.1 Preparing for configurations

Scenario

To expand application of Ethernet technologies at a carrier-grade network, the Ethernet must ensure the same QoS as the carrier-grade transport network. CFM solves this problem by providing overall OAM tools for the carrier-grade Ethernet.

Prerequisite

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

8.3.2 Enabling CFM

Note

CFM fault detection and CFM fault location functions cannot take effect until the CFM is enabled.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet cfm enable**	Enable global CFM. By default, global CFM is disabled.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
	Raisecom(config)#**interface port-channel** *port-channel*	Enter aggregation group configuration mode.
4	Raisecom(config-port)#**ethernet cfm enable**	(Optional) enable CFM on an interface. By default, CFM is enabled on the interface.
	Raisecom(config-aggregator)#**ethernet cfm enable**	Enable CFM on the aggregation group. By default, the CFM is disabled on the aggregation group.

8.3.3 Configuring basic functions of CFM

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet cfm domain** [**md-name** *domain-name*] **level** *level*	Create a MD. If a MD name is assigned by the **md-name** parameter, it indicates that the MD is in IEEE 802.1ag style. And all MAs and CCMs in the MD are in 802.1ag style. Otherwise, the MD is in Y.1731 style and all MAs and CCMs in the MD are in Y.1731 style. If a name is specified for a MD, the name must be unique in global. Otherwise the MD is configured unsuccessfully. **Note** Levels of different MDs must be different. Otherwise the MD is not successfully configured.

Step	Command	Description
3	Raisecom(config)#**service** *cis-id* **level** *level*	Create a service instance and enter service instance configuration mode. Character strings composed by MD name/service instance name are unique in global. If a service instance existed, you can use this command to enter service instance configuration mode directly.
4	Raisecom(config-service)#**service vlan-list** *vlan-list* [**primary-vlan** *vlan-id*]	Configure VLAN mapping based on the service instance. The VLAN list contains up to 32 VLANs. If you do not use the **primary-vlan** parameter to specify the primary VLAN, the minimum VLAN is taken as the primary VLAN of the service instance. All MEPs in the service instance send and receive packets through this primary VLAN. **Note** The primary VLAN is used to send and receive packets. Therefore, all non-primary VLANs are mapped to the primary VLAN in logical. This logical VLAN mapping relationship is global, but VLANs cannot be crossed. For example, service instance 1 is mapped to VLANs 12–20 and service instance 2 is mapped to VLANs 15–30. Therefore, VLANs 15–20 are crossed. This configuration is illegal.
5	Raisecom(config-service)#**service mep** [**up** | **down**] **mpid** *mep-id* [*interface-type interface-number* | **port-channel** *port-channel*] [**priority** *priority*]	Configure MEPs based on a service instance. When configuring a MEP based on a service instance, you must ensure that the service instance is mapped to a VLAN. By default, the MEP is Up. It indicates detecting the fault in uplink direction.
6	Raisecom(config-service)#**service sdp** { *interface-type backup-interface-number* | **port-channel** *port-channel-list* } { *interface-type backup-interface-number* | **port-channel** *port-channel-list* } **secondary**	Configure sending interface based on a service instance. The uplink interface only can be configured as the sending interface.

8.3.4 Configuirng fault detection

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

Step	Command	Description
2	Raisecom(config)#**ethernet cfm remote mep age-time** *minute*	(Optional) configure the aging time of RMEP. By default, the aging time of RMEP is set to 100min. **Note** This configuration takes effect on the dynamic RMEP only.
3	Raisecom(config)#**ethernet cfm errors archive-hold-time** *minute*	(Optional) configure the hold time of error CCMs. Fault information reported by all MEPs is saved on the RAX711-L. By default, the hold time OF error CCMs is 100min. When a new holdtime is configured, the system will detect the database immediately. The data will be removed if exceeds the time.
4	Raisecom(config)#**service** *cis-id* **level** *level*	Enter service instance configuration mode.
5	Raisecom(config-service)#**service cc interval** { **1** | **10** | **60** | **600** | **3ms** | **10ms** | **100ms** }	(Optional) configure the interval for sending CCMs. By default, the interval for sending CCMs is 10s. The interval for sending CCM packets cannot be modified when CCM delivery is enabled. **Note** Only when hardware CC is performed during the device sends packets in Down direction, Parameters **3ms** | **10ms** | **100ms** are available. These parameters are not available when software CC is performed.
6	Raisecom(config-service)#**service cc enable mep** { *mep-id-list* | **all** }	Enable MEPs sending CCMs. By default, MEPs do not sending CCMs.
7	Raisecom(config-service)#**service remote-mep** *mep-id* [**remote-mac** *mac-address*] [*interface-type interface-number*]	(Optional) configure the static RMEP, which cooperates with cc check. The **remote-mac** *mac-address* parameter is used to specify the MAC address of the RMEP.
8	Raisecom(config-service)#**service remote-mep learning active**	(Optional) configure REMP learning dynamic import. After REMP learning dynamic import is enabled, when receiving a CCM, the service instance will automatically translate the dynamically-learned REMP into the statically-configured RMEP. By default, REMP learning dynamic import is disabled.
9	Raisecom(config-service)#**service remote-mep cc-check enable**	(Optional) enable cc check of the REMP. By default, cc check of the RMEP is disabled.

Step	Command	Description
10	Raisecom(config-service)#**service cvlan** *vlan-id*	(Optional) configure the CVLAN of a CFM OAM packet, which needs to be configured only in QinQ networking environment. By default, the CFM OAM packet does not carry the C-TAG. After the CVLAN is configured for a service instance, CCMs, LBMs, LTMs, and DMMs sent by MEPs in the service instance will carry double Tags, where the C-T-TAG is the CVLAN configured by this command.
11	Raisecom(config-service)#**service priority** *priority*	(Optional) configure the priority of CFM OAM packet. After the priority is configured, CCMs, LBMs, LTMs, and DMMs sent by MEPs in a service instance will use the assigned priority. By default, the priority is set to 7.

8.3.5 Configuring fault acknowledgement

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**service** *cis-id* **level** *level*	Enter service instance configuration mode.
3	Raisecom(config-service)#**ping** { *mac-address* | **mep** *mep-id* } [**count** *count*] [**size** *packet-size*] [**source** *mep-id*] [**timeout** *time*] [**padding** { **prbs** | **pbrs-crc** | **null** | **null-crc** }] Raisecom(config-service)#**ping ethernet multicast** [**size** *packet-size*] [**timeout** *time*] [**padding** { **prbs** | **pbrs-crc** | **null** | **null-crc** }]	Perform Layer 2 Ping for acknowledging faults. By default, 5 LBMs are sent. The TLV length of a packet is set to 64. The RAX711-L automatically looks for an available source MEP. If Layer 2 Ping is performed by specifying the destination MEP ID, CFM cannot finish Ping operation unless it finds the MAC address of the destination MEP based on the MEP ID. The source MEP will save RMEP data in the source MEP database after discovering and stabilizing the RMEP. And then according to MEP ID, the source MEP can find the MAC address of the RMEP in the RMEP database.

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 the specified destination MEP ID and the MAC address of destination is not found based on the MEP ID.
- Ping operation will fail if other users are using the specified source MEP to perform Ping operation.

8.3.6 Configuring fault location

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet cfm traceroute cache enable**	(Optional) enable the traceroute cache switch. When the traceroute cache switch is disabled, the result will be automatically erased by the **traceroute** command. By default, the traceroute cache switch is disabled.
3	Raisecom(config)#**ethernet cfm traceroute cache hold-time** *minute*	(Optional) configure the hold time of data in the traceroute cache. You can configure the hold time when the traceroute cache is enabled. By default, the hold time is set to 100min.
4	Raisecom(config)#**ethernet cfm traceroute cache size** *size*	(Optional) configure the traceroute cache size. You can configure the traceroute cache size when the traceroute cache is enabled. By default, the traceroute cache size is set to 100. The data are not saved when the traceroute cache is disabled.
5	Raisecom(config)#**service** *cis-id* **level** *level*	Enter service instance configuration mode.
6	Raisecom(config-service)# **traceroute** { *mac-address* [**ttl** *ttl*] [**source** *mep-id*] [**size** *packet-size*] | **mep** *mep -id* [**ttl** *ttl*] [**source** *mep-id*] [**interface-mode**]: [**timeout** *second*] [**size** *packet-size*] | **mip icc** *icc-code node-id* [**ttl** *ttl*] [**interface-num** *interface-num*] [**timeout** *second*] | **ttl** *ttl* [**interface-mode**] [**timeout** *second*] [**size** *packet-size*] }	Perform Layer 2 Traceroute for locating faults. By default, the TLV length of a packet is set to 64. The RAX711-L automatically looks for an available source MEP.

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 the specified destination MEP ID and the MAC address of destination is not found based on the 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.

8.3.7 ConfiguringAIS

Configuring AIS on server-layer devices

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**service** *cis-id* **level** *level*	Enter service instance configuration mode.
3	Raisecom(config-service)#**service ais enable**	Enable AIS delivery. By default, AIS delivery is disabled.
4	Raisecom(config-service)#**service ais period** { **1** | **60** }	Configure the AIS delivery period. By default, the AIS delivery period is set to 1s.
5	Raisecom(config-service)#**service ais level** *level*	Configure the level of the customer-layer MD to which AIS is sent.

Configuring AIS on customer-layer devices

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**service** *cis-id* **level** *level*	Enter service instance configuration mode.
3	Raisecom(config-service)#**service suppress-alarms enable mep** { *mep-id* | **all** }	Enable alarm inhibition. By default, alarm inhibition is enabled.

8.3.8 Configuring ETH-LCK

Configuring ETH-LCK on server-layer devices

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**service** *cis-id* **level** *level*	Enter service instance configuration mode.
3	Raisecom(config-service)#**service lck start mep** { *mep-id* | **all** }	Enable LCK delivery. By default, LCK delivery is disabled.

Step	Command	Description
4	Raisecom(config-service)#**service lck period** { **1** | **60** }	Configure the LCK delivery period. By default, the LCK delivery period is set to 1s.
5	Raisecom(config-service)#**service lck level** *level* [**vlan** *vlan-id*]	Configure the level of the customer-layer MD to which LCK is sent.

Configuring ETH-LCK on customer-layer devices

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**service** *cis-id* **level** *level*	Enter service instance configuration mode.
3	Raisecom(config-service)#**service suppress-alarms enable mep** { *mep-id* | **all** }	Enable alarm inhibition. By default, alarm inhibition is enabled.

8.3.9 Configuring Ethernet CSF

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**service** *csi-id* **level** *ma-level*	Enter MA configuration mode.
3	Raisecom(config-service)#**service csf enable mpid** *mep-id*	Enable to send CSF packets. By default, the RAX711-L is not enabled to send CSF packets.
4	Raisecom(config-service)#**service csf period** { **1** | **60** }	Configure the period to send CSF packets, suitable for PW OAM only. By default, the period is 1s.
5	Raisecom(config-service)#**service csf trap enable**	Enable Trap report of the CSF module, suitable for PW OAM only. By default, Trap report of the CSF module is disabled.

8.3.10 Configuring performance monitor

Configure performance monitor for the RAX700 as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**service** *csi-id* **level** *ma-level*	Enter MA configuration mode.

Step	Command	Description
3	Raisecom(config-service)#**service pm enable mep** { **all** | *mep-id* }	Enable the performance monitor of the MEP.

8.3.11 Checking configurations

No.	Command	Description
1	Raisecom#**show ethernet cfm**	Show CFM global configurations.
2	Raisecom#**show ethernet cfm domain** [**level** *level*]	Show configurations on MDs and service instances.
3	Raisecom#**show ethernet cfm errors** [**level** *level*]	Show error CCM database information.
4	Raisecom#**show ethernet cfm lck** [**level** *level*] [**source**]	Show ETH-LCK signals.
5	Raisecom#**show ethernet cfm local-mp** [**interface** *interface-type interface-number* | **level** *level*]	Show local MEP configurations.
6	Raisecom#**show ethernet cfm remote-mep** [**level** *level*] **static**	Show static RMEP information.
7	Raisecom#**show ethernet cfm remote-mep** [**level** *level* [**service** *service-instance* [**mpid** *mep-id*]]]	Show RMEP delivery information.
8	Raisecom#**show ethernet cfm suppress-alarms** [**level** *level*]	Show CFM alarm inhibition configurations.
9	Raisecom#**show ethernet cfm traceroute-cache**	Show Link-Trace cache route discovery information.

8.4 Configuring SLA

8.4.1 Preparing for configurations

Scenario

To provide users with qualified network services, the SP signs a SLA with users. To carry out SLA effectively, the SP 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 this 2 detection points can be detected.

SLA makes a statistics on round-trip packet loss ratio, round-trip/unidirectional (SD/DS) delay, jitter, jitter variance, jitter distribution, throughput, and LM packet loss test. In addition, it reports these data to the upper monitoring software (such as the NView NNM system) to help analyze network performance for getting an expected result.

Prerequisite

- When you configure Layer 2 test operations, 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 test operations (icmp-echo and icmp-jitter), Layer 3 Ping operation succeeds between local and remote devices.
- When you configure Layer 4 test operations, local and remote devices can be in the same network segment. Otherwise, routes must be reachable.

8.4.2 Configuring basic SLA operation information

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla** *oper-num* **y1731-echo remote-mep** *mep-id* **level** *level* **svlan** *vlan-id* [**cvlan** *vlan-id*] [**cos** *cos-value*] [**dm**]	Configure the SLA y1731-echo operation based on the destination MEP ID.
3	Raisecom(config)#**sla** *oper-num* **y1731-echo remote-mac** *mac-address* **level** *level* **svlan** *vlan-id* [**cvlan** *vlan-id*] [**cos** *cos-value*] [**dm**]	Configure the SLA y1731-echo operation based on the destination MAC address.
4	Raisecom(config)#**sla** *oper-num* **y1731-jitter remote-mep** *mep-id* **level** *level* **svlan** *vlan-id* [**cvlan** *vlan-id*] [**interval** *period*] [**packets** *packets-num*] [**cos** *cos-value*] [**dm**]	Configure the SLA y1731-jitter operation based on the destination MEP ID.
5	Raisecom(config)#**sla** *oper-num* **y1731-jitter remote-mac** *mac-address* **level** *level* **svlan** *vlan-id* [**cvlan** *vlan-id*] [**interval** *period*] [**packets** *packets-num*] [**cos** *cos-value*] [**dm**]	Configure the SLA y1731-jitter operation based on the destination MAC address.
6	Raisecom(config)#**sla** *oper-num* **icmp-echo dest-ipaddr***ip-address* [**dscp** *dscp-value*]	Configure basic information of the SLA icmp-echo operation.
7	Raisecom(config)#**sla** *oper-num* **icmp-jitter dest-ipaddr** *ip-address* [**dscp** *dscp-value*] [**interval** *period*] [**packets** *packets-nums*]	Configure basic information of the SLA icmp-jitter operation.
8	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*] [**packets** *packet-num*]	Configure the SLA y1731-pkt-loss packet loss test operation based on the MEP ID. **Note** When you perform packet loss ratio test based on the MEP ID, we recommend specifying the MAC address when you use the **service remote-mep** command to configure the RMEP.

Step	Command	Description
9	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*] [**packets** *packet-num*]	Configure the SLA y1731-pkt-loss packet loss test operation based on the destination MAC address.
10	Raisecom(config)#**sla y1731-echo quick-input** [**level** *level* [**svlan** *vlan-id*]] [**dm**]	Create the y1731-echo operation quickly.
11	Raisecom(config)#**sla y1731-jitter quick-input** [**level** *level* [**svlan** *vlan-id*]] [**dm**]	Create the y1731-jitter operation quickly.
12	Raisecom(config)#**sla private-tlv enable**	(Optional) configure whether the SLA operation is padded with the private TLV. By default, the SLA operation is not padded with the private TLV.
13	Raisecom(config)# **sla** *oper-num* { **loss-rate-threshold** | **delay-threshold** | **jitter-threshold** } { **current** | **average** } [**ds** | **sd** | **two-way**] *threshold-value*	Configure the delay threshold, jitter threshold, and packet loss ratio threshold.
14	Raisecom(config)#**sla** *oper-num* **loss-pkt-trap** { **current** | **average** } **enable** Raisecom(config)#**sla** *oper-num* { **delay-trap** | **jitter-trap** } { **current** | **average** } [**ds** | **sd** | **two-way**] **enable**	Enable sending Trap when the test result exceeds the threshold.
15	Raisecom(config)#**sla maintenance start**	Start emergency maintenance window.

Note

- After configuring one operation (identified 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 100 operations at one 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.
- The private TLV is designed for Raisecom devices. When SLA operations are padded with the private TLV, you can configure and schedule any operations. When SLA operations are not padded with the private TLV, VLANs of DMs and LMs should be different. In addition, LB packets cannot be co-scheduled with DMs and LMs.
- If SLA operations are padded with the private TLV, if may influence communicated with devices from other vendors.

8.4.3 Configuring SLA scheduling information and enabling operation scheduling

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla schedule** *oper-num* [**life** { **forever** | *life-time* }] [**period** *period*] [**begin**]	Configure SLA scheduling information, including the life time and execution interval. Enable SLA operation scheduling. By default, operation scheduling is disabled.

Note

- The operation life time should not be smaller than the interval for performing SAL operations.
- The interval for performing SLA operations should not be smaller than 20s.

8.4.4 Configuring basic ETH-Test throughput test operation information and enabling operation scheduling

Note

The prerequisites for configuring throughput test are shown as below:

- CFM is deployed on local and remote devices.
- Ping operation succeeds between local and remote devices.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla y1731-throughput enable**	Enable ETH-Test throughput test. By default, ETH-Test throughput test is disabled.
3	Raisecom(config)#**sla schedule y1731-throughput** *oper-id* { **rx** | **tx** | **tx-rx** } **start**	Configure the mode for scheduling the ETH-Test between the RAX711-L and the tester.
4	Raisecom(config)#**sla y1731-throughput** *oper-id* { **local-mep** *mep-id* **remote-mep** *mep-id* | **remote-mac** *mac-address* } **level** *level-id* **svlan** *vlan-id* [**cvlan** *vlan-id*] [**cos** *cos-value*] [**cfi** *cfi-value*]	Create the ETH-Test throughput test operation, including the test operation ID, local MEP ID, remote MEP ID, remote MAC address, MEG level, SVLAN ID, CVLAN ID, and CoS priority.

Step	Command	Description
5	Raisecom(config)#**sla y1731-throughput** *oper-id* { **one-way** | **two-way** } **object** *band-width* **packet-size** *pkt-length* **pattern** { **null** | **null-crc** | **prbs** | **prbs-crc** } **duration** *lasting-time*	(Optional) configure parameters of the ETH-Test throughput test operation, including the test operation ID, test direction (unidirectional/bidirectional), destination test bandwidth, test packet size, padding mode of the test packet payload, and hold time. By default, the test operation is a unidirectional one. • Destination test bandwidth: 100 Mbit/s • Test packet size: 1024 bytes • Padding mode of the test packet payload: null • Hold time: 30s.
6	Raisecom(config)#**sla schedule y1731-throughput** *oper-id*	Enable ETH-Test throughput test operation scheduling. By default, ETH-Test throughput test operation scheduling is disabled.

Note

- ETH-Test does not support testing multiple operations at one time. If multiple operations are scheduled, they are tested in order based on the scheduling time.
- Up to 10 ETH-Test test operations are supported. Operations are distinguished by the operation ID.
- ETH-Test supports MEP in Down direction only.

8.4.5 Configuring TWAMP test operation and enabling operation scheduling

Note

The prerequisite to configure the TWAMP test is that the Ping operation succeeds between local and remote devices.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla** *oper-num* **twamp source-ip** *ip-address* **dst-ip** *ip-address* [**udp-port** *port-id*] **outer-vlan** *vlan-id* [**outer-cos** *cos-value*] [**inner-vlan** *vlan-id*] [**inner-cos** *cos-value*] [**dscp** *dscp-value*] [**interval** *interval-num*] [**size** *packet-size*]	Create a SLA TWAMP test operation on the local device. **Note** The value of the outer VLAN must be identical to that of VLAN associated to the IP interface.
3	Raisecom(config)#**sla** *oper-num* **sender timeout** *timeout*	Configure the timer for sending packets from the SLA TWAMP test operation sender on the local device. By default, the timer is 5000ms.

Step	Command	Description
4	Raisecom(config)#**twamp monitor udp-port** *port-id*	Configure the response interface of the SLA TWAMP test operation on the remote device. By default, the response interface ID of the SLA TWAMP test operation is 862. **Note** The response UDP interface ID must be identical to that of the SLA TWAMP test operation created on the local device.
5	Raisecom(config)#**twamp reflector enable**	Enable response of the remote device. By default, response of the remote device is disabled.
6	Raisecom(config)#**sla schedule** *oper-num* [**life** { **forever** | *life-time* }] [**period** *period*] [**begin**]	Configure SLA scheduling on the local device, including the operation lifetime and execution interval, and enable SLA operation scheduling. By default, the SLA operation scheduling is disabled.

8.4.6 Configuring availability test

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sla** *oper-num* **availability-num-consecutive-meas-pdus** *number*	Configure the number of test packets sent within a SLA availability test period.
3	Raisecom(config)#**sla** *oper-num* **availability-flr-threshold** *threshold*	Configure the threshold of packet loss rate in the SLA availability test.
4	Raisecom(config)#**sla** *oper-num* **availability-num-consecutive-intervals** *number*	Configure the number of consecutive indicators of the SLA availability test.
5	Raisecom(config)#**sla** *oper-num* **availability-measurement-interval** *minute*	Configure the interval of the SLA availability test.
6	Raisecom(config)#**sla** *oper-num* **availability-num-consecutive-high-flr** *number*	(Optional) configure the number of the CHLI availability indicators of the SLA availability test.
7	Raisecom(config)#**sla** *oper-num* **availability-threshold** [**sd** | **ds**] *threshold*	Configure the threshold of the SLA availability test.
8	Raisecom(config)#**sla** *oper-num* { **availability-trap** | **availabilitychange-trap** } [**ds** | **sd**] **enable**	Enable SLA availability threshold alarm or SLA availability threshold changing alarm. By default, it is disabled.

8.4.7 Checking configurations

No.	Command	Description
1	Raisecom#**show sla** { **all** | *oper-num* } **configuration**	Show SLA configurations.
2	Raisecom#**show sla** { **all** | *oper-num* } **result**	Show the last test information of an operation.
3	Raisecom#**show sla** { **all** | *oper-num* } **statistic**	Show operation scheduling statistics.
4	Raisecom#**show sla y1731-throughput** *oper-id* **configuration**	Show ETH-Test throughput test operation configurations.
5	Raisecom#**show sla y1731-throughput** *oper-id* **result**	Show test result of the ETH-Test throughput test operation.
6	Raisecom#**show sla twamp reflector** [**udp-port** *port-id*]	Show the remote device of the SLA TWAMP operation and packet statistics of the response UDP interface.
7	Raisecom#**show sla** { **all** | *oper-num* } **threshold**	Show operation scheduling threshold configurations and Trap status.
8	Raisecom#**show sla** *oper-num* **current packet**	Show the present operations scheduling frame.
9	Raisecom#**show sla** *oper-num* **latest statistic**	Show the scheduling statistics of the latest operation.
10	Raisecom#**show sla maintanence**	Show the maintenance window.

Note

The **show sla y1731-throughput** *oper-id* **result** command can be used to show statistics of ETH-Test throughput test operation test results. For an operation, up to 5 groups of statistics are supported. If it is over 5, the oldest statistics (from the starting time of the scheduling) will be aged.

8.5 Configuring Y.1564

8.5.1 Preparing for configurations

Scenario

To learn about configuration parameters and performance of Ethernet services, you can make related configurations of Raisecom Service Activation Measurement (RCSAM) on the RAX711-L.

On the same device, RCSAM, RFC2544, MPLS-TP OAM, and Loopback are mutually exclusive.

Prerequisite

The remote device is enabled with loopback based on SMAC.

8.5.2 Configuring test task

Configuring test types of RCSAM

Note

- Use step 4 to configure the test type as configuration test.
- Use step 5 to configure the test type as service test.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**rcsam cir step** *step1* [*step2*] [*step3*] [*step4*]	Configure the step of the CIR test packet in RCSAM. By default, values of steps 1–4 are 25, 50, 75, and 100 respectively, indicating that 25%, 50%, 75%, or 100% of the current CIR is being tested.
3	Raisecom(config)#**rcsam step-time** *second*	Configure the test time step of RCSAM.
4	Raisecom(config)#**rcsam configuration-test enable**	Enable the configuration test of the global RCSAM. By default, the configuration test is enabled.
5	Raisecom(config)#**rcsam performance-test duration** *minute*	Configure the performance test duration of RCSAM. By default, the performance test duration is 15min.
	Raisecom(config)#**rcsam performance-test enable**	Enable the performance test of the global RCSAM. By default, the performance test is enabled.
6	Raisecom(config)#**rcsam service-identify type vlan** [**cos** | **dscp**]	Configure the RCSAM test services based on the VLAN and CoS or based on the VLAN and DSCP.

Creating RCSAM service and configuring properties of test packets

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**rcsam service** *service-id* { **ipv4-udp** | **l2-eth** | **video-udp** | **voice-udp** }	Create the RCSAM service, specify the service ID, configure the test packet type, and enter corresponding service instance configuration mode.
3	Raisecom(config-rcsamservice)#**name** *name*	Configure the name of the RCSAM service.

<table>
<tr><th>Step</th><th>Command</th><th>Description</th></tr>
<tr><td></td><td>Raisecom(config-rcsamservice)#mpls static-lsp ingress lsp-name</td><td>Configure the name of the LSP of the RCSAM test traffic.</td></tr>
<tr><td>4</td><td>Raisecom(config-rcsamservice)#dmac mac-address</td><td>Configure the MAC address of the RCSAM service packet.
Note
The test packet based on L2-ETH or IPv4-UDP needs to be configured with the destination MAC address.</td></tr>
<tr><td>5</td><td>Raisecom(config-rcsamservice)#smac mac-address</td><td>Configure the source MAC address of the RCSAM services packets.</td></tr>
<tr><td>6</td><td>Raisecom(config-rcsamservice)#static-l2vc destination ip-address vc-id vc-id</td><td>Configure the destination IP address and VC ID of the RCSAM test traffic.</td></tr>
<tr><td>7</td><td>Raisecom(config-rcsamservice)#dest-ip ip-address [source-ip ip-address] [dest-udp-port port-id] [source-udp-port port-id] [tos { ip-precedence ip-precedence | dscp dscp-value }] [ttl ttl]</td><td>Configure the source/destination IP address, source/destination UDP port ID, TOS type and value, and TTL of the RCSAM service packet.
Note
Only the test packet based on IPv4-UDP needs to be configured with the destination IP address.</td></tr>
<tr><td>8</td><td>Raisecom(config-rcsamservice)#nexthop-ip ip-address</td><td>Configure the IP address of the next hop of the RCSAM test traffic.</td></tr>
<tr><td>9</td><td>Raisecom(config-rcsamservice)#svlan vlan-id [tpid tpid] [cos cos-value] [cfi cfi-value]</td><td>Configure the SVLAN of the RCSAM service packet.</td></tr>
<tr><td>10</td><td>Raisecom(config-rcsamservice)#cvlan vlan-id [tpid tpid] [cos cos-value] [cfi cfi-value]</td><td>Configure the CVLAN of the RCSAM service packet.</td></tr>
<tr><td>11</td><td>Raisecom(config-rcsamservice)#frame-size { fix size | radom }fix size</td><td>Configure the size of the RCSAM service packet.
By default, the size of the packet is 12 Bytes.</td></tr>
<tr><td>12</td><td>Raisecom(config-rcsamservice)#uni interface-type interface-number</td><td>Configure the UNI corresponding to the RCSAM service.</td></tr>
<tr><td>13</td><td>Raisecom(config-rcsamservice)#cir cir cbs cbs [eir eir ebs ebs]</td><td>Configure the rate of the CIR/EIR test.</td></tr>
<tr><td>14</td><td>Raisecom(config-rcsamservice)#traffic-policing rate rate</td><td>Configure the rate of the traffic policing test.
By default, the rate is 0, indicating that there is no limit.</td></tr>
<tr><td>15</td><td>Raisecom(config-rcsamservice)#latency-threshold threshold</td><td>Configure the latency threshold of the RCSAM service packet.
By default, the latency threshold is 10ms.</td></tr>
</table>

Step	Command	Description
16	Raisecom(config-rcsamservice)#**jitter-threshold** *threshold*	Configure the jitter threshold of the RCSAM service packet. By default, the jitter threshold is 5ms.
17	Raisecom(config-rcsamservice)#**frame-loss-threshold** *threshold*	Configure the packet loss threshold of the RCSAM service. By default, the packet loss threshold is 10, that is, 0.01%.
18	Raisecom(config-rcsamservice)#**eir-test enable**	(Optional) enable the EIR test. By default, the EIR test is enabled.
19	Raisecom(config-rcsamservice)#**traffic-policing-test enable**	(Optional) enable the traffic policing test. By default, the traffic policing test is enabled.
20	Raisecom(config-rcsamservice)#**performace-test cir** *cir*	(Optional) configure the performance test bandwidth of the RCSAM test.
21	Raisecom(config-rcsamservice)#**service enable**	Enable the RCSAM service. By default, this service is disabled.

Note

When the test is being performed, all parameters above cannot be configured.

Enabling RCSAM

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**rcsam test { start | stop }**	Enable RCSAM.

8.5.3 Checking configurations

No.	Command	Description
1	Raisecom#**show rcsam configuration { global | service {** *service-list* **| all } }**	Show RCSAM configurations.
2	Raisecom#**show rcsam result { detail | summary }**	Show RCSAM results.

8.6 Configuring RSOM

8.6.1 Preparing for configurations

Scenario

- RSOM includes services transport and services test measurement.
- When configuring transmission of the service, you need to configure L2CP, CoS bandwidth profile, and connect the services with each profile. Packets entering the services will deal with corresponding packets according to each profile.
- When configuring services test and measurement, you need to configure the SLA, Y.1564, and Loopback, connect the services with each function, and test in the services.

Prerequisite

- N/A

8.6.2 Configuring L2CP profile

Configure the L2CP profile as below.

Step	Configuration	Description
1	Raisecom#**config** Raisecom(config)#**mefservice**	Enter the RSOM configuration mode.
2	Raisecom(mefservice)#**l2cp-profile** *l2cp-profile-id*	Create the L2CP profile group, and enter the L2CPprofile group configuration mode. By default, the system has 3 profiles, but the default profile cannot be deteled and modified.
3	Raisecom(mefservice-l2cpprofile)#**description** *string*	Configure the L2CP profile group description. By default, it is mef-l2cp-profile-group--*l2cp-profile-id*.
4	Raisecom(mefservice-l2cpprofile)#**l2cp-item** *l2cp-item-id*	Create the L2CP bandwidth profile.
5	Raisecom(mefservice-l2cpitem)#**l2cp-protocol** { **stp** | **lacp** | **lamp** | **link-oam** | **esmc** | **dot1x** | **elmi** | **lldp** | **ptp** | **cdp** | **vtp** | **pvst** | **udld** | **pagp** } **action** { **discard** | **forward** | **peer** | **tunnel** }	Configure protocol rules and processing command of the packets corresponding to the L2CP bandwidth profile.
6	Raisecom(mefservice-l2cpitem)#**dest-mac** *mac-address* [**ethertype** *value* [**sub-type** *value*]] **action** { **discard** | **forward** | **peer** | **tunnel** } Raisecom(mefservice-l2cpitem)#**exit**	Configure the destination MAC rules and processing command of the packets corresponding to the L2CP bandwidth profile. By default, processing action is Tunnel.

Step	Configuration	Description
7	Raisecom(mefservice-l2cpprofile)# **exit** Raisecom(mefservice)#**l2cp-process tunnel destination** *mac-address*	Configure transparent transmission of the L2CP packets with the specified destination MAC address. By default, transparent transport the L2CP packets with destination MAC address 010e.5e00.0003.

8.6.3 Configure CoS profile

Configure the CoS profile as below.

Step	Configuration	Description
1	Raisecom#**config** Raisecom(config)#**mefservice**	Enter RSOM configuration mode.
2	Raisecom(mefservice)#**cos-profile** *cos-profile-id*	Create CoS profile group, and enter CoS profile configuration mode.
3	Raisecom(mefservice-cosprofile)#**name** *name*	Configure CoS profile group description. By default, CoS profile group description is *cos-profile-id*.
4	Raisecom(mefservice-cosprofile)#**coslable** *cos-value* [**remark-pcp** *pcp-value*]	Configure CoS value of CoS profile. By default, it is 0. Re-mark PCP is 0.
5	Raisecom(mefservice-cosprofile)#**type** { **evc** | **dscp** *dscp-list* | **pcp** *pcp-list* } Raisecom(mefservice-cosprofile)#**type** { **evc** | **dscp** *dscp-list* | **pcp** *pcp-list* } **l2cp** { *l2cp-profile-id* | **default1** | **default2** | **default3** } Raisecom(mefservice-cosprofile)#**type l2cp** { *l2cp-profile-id* | **default1** | **default2** | **default3** }	Configure services traffic offload mode of the CoS profile. After service traffic is classified, it will be transmitted according to QoS rule of the Ethernet. By default, it is PCP mode Cos is from 0 to 7.

Note

In the EVC configuration mode, the association way between UNI and EVC is different, and traffic classification is different.

- When the association mode is All-To-One and Bundling, the packets carrying interface priority, Untagged packets, and packets carrying C-Tag enter the same line, namely line 1.
- When the association way is Bundling-Multipex or Multipex, all the packets enter the same line, namely line 1.

In the DSCP configuration mode, the association way between UNI and EVC is different, and traffic classification is different.

- When the association way is All-To-One, Layer 3 packets is mapped to the local priority according to carried DSCP, and enter the corresponding line; Non-Layer 3 packets is mapped to the local priority according to services Default-DSCP configured by the **default-dscp** command, and enter the corresponding line. If DSCP is full mapping, do not discard the packets.

- When the association way is Bundling, Bundling-Multipex, and Multipex, Layer 3 packets is mapped to the local priority according to carried DSCP, and enter the corresponding line; Non-Layer 3 packets is mapped to the local priority according to services Default-DSCP configured by the **default-dscp** command, and enter the corresponding line. When the DSCP carried on the Layer 3 does not match with services DSCP, discard the packets.

In the PCP configuration mode, the association way between UNI and EVC is different, and traffic classification is different.

- When the association way is All-To-One, the packets carrying interface priority and the packet carrying C-Tag according to configured PCP are mapped to the local priority; Untagged packets is mapped to the local priority according to Default-cepriority configured by the **default-cepriority** command.

In the L2CP configuration mode, the packets are matched and processed according to L2CP profile attribute.

In the L2CP and DACP, PCP or EVC mixed mode, classification follows L2CP, DSCP, PCP, and EVC in descending priority.

8.6.4 Configuring bandwidth profile

Configure bandwidth profile as below.

Step	Configuration	Description
1	Raisecom#**config** Raisecom(config)#**mefservice**	Enter RSOM configuration mode.
2	Raisecom(mefservice)#**bandwidth enable**	Enable global bandwidth. By default, it is enabled.
3	Raisecom(mefservice)#**bandwidth-profile** *bandwidth-profile-id*	Create a bandwidth profile group, and enter bandwidth profile group configuration.
4	Raisecom(mefservice-bwpprofile)#**bandwidth-item** *bandwidth-item-id*	Create bandwidth profile group, and enter bandwidth profile group configuration. By default, bandwidth profile is coming with system, and profile ID is 1. CIR is 512 kbit/s, and committed burst size is 512kB. It is color blind mode, and disabling the coupling function.
	Raisecom(mefservice-bwpitem)#**bandwidth-hierachy**	Create hierarchical bandwidth profile, and enter hierarchical bandwidth profile configuration mode. By default, the new hierarchical bandwidth profile does not limit on the speed and color blind mode.
5	Raisecom(mefservice-bwpitem)#**name** *name*	Configure bandwidth profile description. By default, it is 123.
6	Raisecom(mefservice-bwpitem)#**cir** *cir* **cbs** *cbs* [**eir** *eir* **ebs** *ebs*]	Configure speed-limit rule for the bandwidth profile.
	Raisecom(mefservice-bwpitem)#**cir unlimited**	

Step	Configuration	Description
7	Raisecom(mefservice-bwpitem)#**color-mode** { **aware** | **blind** }	Configure color aware mode for the bandwidth profile.
8	Raisecom(mefservice-bwpitem)#**coupling enable**	Enable bandwidth coupling.
9	Raisecom(mefservice-bwpitem)#**cos-profile** *cos-profile-id*	Configure bandwidth profile to quote the CoS profile.

8.6.5 Configuring interfaces

Configure interfaces as below.

Step	Configuration	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)#**mef-type uni** Raisecom(config-port)#**mef-type nni**	Configure physical interface type. By default, the interface of Line is NNI; the interface of Client is UNI.
4	Raisecom(config-port)#**exit** Raisecom(config)# **mefservice**	Enter RSOM configuration mode.
5	Raisecom(mefservice)#**interface** *interface-type interface-number*	Enter RSOM UNI configuration mode.
6	Raisecom(mefservice-interface)#**uni-id** *string*	Configure UNI interface identification.
7	Raisecom(mefservice-interface)#**bandwidth-profile** { **ingress** | **egress** } *bandwidth-profile-id*	Configure the association between interface and bandwidth group.
8	Raisecom(mefservice-interface)#**l2cp-profile** { *l2cp-profile-id* | **default1** | **default2** | **default3** } **service** *service-id*	Configure the association between the UNI interface and L2CP profile group.
9	Raisecom(mefservice-interface)#**bundling-type** { **all-to-one** | **bundling** | **bundling-multiplex** | **multiplex** }	Configure association rules between the CE VLAN on the UNI and services. By default, it is All-To-One.
10	Raisecom(mefservice- interface)#**default-cevlan** *vlan-id*	Configure the default CE VLAN of the Untagged packets. By default, it is VLAN 1.
11	Raisecom(mefservice- interface)#**default-cepriority** *priority*	Configure the default CE VLAN priority of the Untagged packets. By default, it is 0.

8.6.6 Configuring SLA

Configuring SLA threshold profile

Configure SLA threshold profile as below.

Step	Configuration	Description
1	Raisecom#**config** Raisecom(config)#**mefservice**	Enter RSOM configuration mode.
2	Raisecom(mefservice)#**performance-tier** *performance-tier-id*	Create threshold configuration profile, and enter threshold configuration profile mode.
3	Raisecom(mefservice-thresholdprofile)#**description** *string*	Configure profile description. By default, it is PT*performance-tier-id*.
4	Raisecom(mefservice-thresholdprofile)#**cos-lable** *cos-value* { **availability** | **delay** | **jitter** | **loss-rate** } *threshold-value*	Configure each threshold information and CoS in the SLA threshold profile.

Configuring SLA test

Configure SLA test as below.

Step	Configuration	Description
1	Raisecom#**config** Raisecom(config)#**mefservice**	Enter RSOM configuration mode.
2	Raisecom(mefservice)#**service** *service-id*	Enter EVC configuration mode.
3	Raisecom(mefservice-evc)#**performance-tier** *performance-tier-id*	Configure association between service and threshold profile.
4	Raisecom(mefservice-evc)#**sla remote-ip** *ip-address*	Configure the IP address of the remote device for the SLA test.
5	Raisecom(mefservice-evc)#**sla remote-mep** { **all** | *mep-list* } [**size** *size*]	Configure remote devices MEP of the SLA test.
6	Raisecom(mefservice-evc)#**sla start**	Start the SLA test.
7	Raisecom(mefservice-evc)#**exit** Raisecom(mefservice)#**sla archive enable**	(Optional) enable SLA archiving. By default, it is disabled.

8.6.7 Configuring Y.1564

Configuring Y.1564 test traffic profile

Configure Y.1564 test traffic profile as below.

Step	Configuration	Description
1	Raisecom#**config** Raisecom(config)#**mefservice**	Enter RSOM configuration mode.
2	Raisecom(mefservice)#**flow profile** *flow-profile-id*	Create Y.1564 traffic profile, and enter traffic profile configuration mode.
3	Raisecom(mefservice-flowprofile)#**description** *string*	Configure Y.1564 traffic profile description. By default, description about traffic profile is FLOW-*flow-profile-id*.
4	Raisecom(mefservice-flowprofile)#**frame type** { **vsm** | **udp source-port** *port-number* **dest-port** *port-number* }	Configure Y.1564 test traffic type. By default, it is VSM packet.
5	Raisecom(mefservice-flowprofile)#**nexthop ip-address** *ip-address*	Configure next hop IP address of Y.1564 test traffic only when the packet of Y.1564 test is UDP.
6	Raisecom(mefservice-flowprofile)# **frame length** { **mix** | **single** *length* }	Configure the frame size of Y.1564 test traffic. By default, it is uniframe and it is 512 bytes.
7	Raisecom(mefservice-flowprofile)# **frame pattern prbs**	Configure Y.1564 test traffic calibration.
8	Raisecom(mefservice-flowprofile)#**source-ip** *ip-address*	Configure the source IP address of Y.1564 test traffic.
9	Raisecom(mefservice-flowprofile)#**source-mac** *mac-address*	Configure the source MAC address of Y.1564 traffic.

Configuring Y.1564 test

Configure Y.1564 test as below.

Step	Configuration	Description
1	Raisecom#**config** Raisecom(config)#**mefservice**	Enter RSOM configuration mode.
2	Raisecom(mefservice)#**service** *service-id*	Enter EVC configuration mode.
3	Raisecom(mefservice-evc)#**rcsam flow-profile** *flow-profile-id*	Configure association between service and Y.1564 traffic profile.
4	Raisecom(mefservice-evc)#**performance-tier** *performance-tier-id*	Configure association between services and threshold profile.
5	Raisecom(mefservice-evc)#**rcsam duration** { **forever** | *period* }	Configure Y.1564 test period. By default, it is 15 minutes.

Step	Configuration	Description
6	Raisecom(mefservice-evc)#**rcsam performance cir ratio** *ratio*	Configure Y.1564 performance test bandwidth ratio. By default, it is 100.
7	Raisecom(mefservice-evc)#**rcsam** { **remote-mac** *mac-address* | **remote-mep** { **all** | *mep-id* } }	Configure remote devices information of the Layer 2 Y.1564 test based on CFM or remote devices MAC.
	Raisecom(mefservice-evc)#**rcsam remote-ip** *ip-address*	Configure information, carried in emulated user packets, about the remote device for the Layer 3 Y.1564 test on Internet leased line services.
8	Raisecom(mefservice-evc)#**rcsam start** { **both** | **configuration** | **performance** }	Start Y.1564 test.

Note

The SLA test and Y.1564 test share threshold profile. During the test, it needs to bind respective threshold profile.

8.6.8 Configuring loopback

Configure the loopback test as below.

Step	Configuration	Description
1	Raisecom#**config** Raisecom(config)#**mefservice**	Enter RSOM configuration mode.
2	Raisecom(mefservice)#**service** *service-id*	Create the service, and enter EVC configuration mode.
3	Raisecom(mefservice-evc)#**loopback type** { **vsm** | **udp source-port** *port-number* **dest-port** *port-number* }	Configure the type of loopback packets. By default, it is VSM.
4	Raisecom(mefservice-evc)#**loopback enable**	Enable service loopback.

Note

- The loopback and Y.1564 test needs to cooperate with each other.
- Be cautious about starting service loopback because it can have influence on normal services.
- After loopback test is finished, disable loopback immediately by using the **loopback disable** command.

8.6.9 Configuring CFM

Configure CFM for RAX700 as below.

Step	Configuration	Description
1	Raisecom#**config** Raisecom(config)#**mefservice**	Enter RSOM configuration mode.
2	Raisecom(mefservice)#**service** *service-id*	Enter service configuration mode.
3	Raisecom(mefservice-evc)#**md level** *level*	Configure the MD level. By default, it is level 5.
4	Raisecom(mefservice-evc)#**cfm local-mep** *mep-id*	Configure the local MEP ID.
5	Raisecom(mefservice-evc)#**far-end** *remote-uni-id* { **ip-address** *ip-address* | **mac** *mac-address* | **remote-mep** *mep-id* }	Configure UNI interface information on the service remote devices.
6	Raisecom(mefservice-evc)#**cc enable**	Enable transmitting CCM. By default, it is disabled.
7	Raisecom(mefservice-evc)#**cc interval** { **1** | **10** | **60** | **600** | **3ms** | **10ms** | **100ms** }	Configure the transmission period of the CCM, By default, it is 3.3s.
8	Raisecom(mefservice-evc)#**ping** { **remote-mep** *mep-id* | *mac-address* } [**size** *size*]	Configure PING RMEP.
9	Raisecom(mefservice-evc)#**traceroute** { **remote-mep** *mep-id* | *mac-address* } [**size** *size*]	Configure Traceroute RMEP.

Note

Parameters related to CFM on the service are calculated automatically by the system, such as MD name, MA name, etc.

8.6.10 Configuring services

Configure services for the RAX700 as below.

Step	Configuration	Description
1	Raisecom#**config** Raisecom(config)#**mefservice**	Enter RSOM configuration mode.
2	Raisecom(mefservice)#**service** *service-id*	Enter service configuration mode.
3	Raisecom(mefservice-evc)#**id** *string*	Configure the service ID. By default, it is service-*service-id*.
4	Raisecom(mefservice-evc)#**type** { **eline** | **elan** | **etree** }	Configure the type of the Ethernet type. By default, it is Ethernet LAN mode.
5	Raisecom(mefservice-evc)#**cevlan-cos preservation**	Enable keeping the CE VLAN and CoS label of the packets. By default, it is enabled.

Step	Configuration	Description
6	Raisecom(mefservice-evc)#**default-dscp** *dscp*	Configure default DSCP priority of the non-IP packets. By default, it is 0.
7	Raisecom(mefservice-evc)#**encapsulate-mode** { **forward** | **svlan** }	Configure the processing mode about packets received on the service. By default, service adds a LAN to received packets.
8	Raisecom(mefservice-evc)#**primary-vid** *vlan-id*	Configure SVLAN for the service. By default, it is VLAN 1.
9	Raisecom(mefservice-evc)#**sdp** *interface-type interface-number* [*interface-type backup-interface-number*]	Configure association between service and SDP interface.
10	Raisecom(mefservice-evc)#**sap** *interface-type interface-number*	Configure the association between service and SAP, and enter service UNI configuration mode,
11	Raisecom(mefservice-evcuni)#**cevlan-map** *vlan-list*	Configure the CE VLAN on the service UNI.
12	Raisecom(mefservice-evcuni)#**type** { **leaf** | **root** }	Configure UNI interface type of the E-Tree services only when the Ethernet services type is configured as the E-Tree service.
13	Raisecom(mefservice-evcuni)#**bandwidth-profile** { **ingress** | **egress** } *bandwidth-profile-id*	Configure association between UNI of the service and bandwidth profile group.
14	Raisecom(mefservice-evcuni)#**exit** Raisecom(mefservice-evc)#**link-state-tracking enable**	Enable service failover
15	Raisecom(mefservice-evc)#**statistics enable**	Enable service statistics.
16	Raisecom(mefservice-evc)#**no shutdown**	Configure starting service.

Note

Test and measurement of the service mainly aim at test of the EVC on the network side.

Services include EVC and corresponding UNI. When configuring the EVC UNI, you need to operate as follows:

- Enter interface configuration mode, and configure interface type of the physical layer according to the **mef-type** command. For example, configure the physical interface as UNI or NNI.
- In the RSOM configuration mode, enter the UNI interface configuration mode by using command **interface**, and configure the interface attributes of the UNI.
- Enter the EVC mode; associate the EVC and UNI by using the **sap** command. The SAP interface is the UNI of the service.

8.6.11 Checking configurations

No.	Configuration	Description
1	Raisecom#**show rsom l2cp-profile** [*l2cp-profile-id* / **default1** | **default2** | **default3**]	Show configurations of the L2CP profile group.
2	Raisecom#**show rsom cos-profile** [*cos-profile-id*]	Show the CoS profile group configuration.
3	Raisecom#**show rsom bandwidth-profile** *bandwidth-profile-id*	Show bandwidth profile group configuration.
4	Raisecom#**show rsom uni interface [** *interface-type interface-number*]	Show the UNI interface.
5	Raisecom#**show rsom statistics interface** **[** *interface-type interface-number*]	Show the UNI interface statistics.
6	Raisecom#**show rsom service** *service-id* **performance** { **remote-ip** *ip-address* | **remote-mep** *mep-id* }	Show the SLA test statistics.
7	Raisecom#**show rsom service statistics** [*service-id*]	Show the service statistics.
8	Raisecom#**show rsom service** [*service-id*] **status**	Show the service state.

8.7 Maintenance

Command	Description
Raisecom(config-port)#**clear oam** { **event** | **statistics** }	Clear EFM OAM interface link statistics/OAM frame statistics.
Raisecom(config)#**clear oam config**	Clear EFM OAM configurations to return to Passive and Disable status.
Raisecom(config)#**clear ethernet cfm errors** [level *level*]	Clear CCM error database information.
Raisecom(config)#**clear ethernet cfm remote-mep** [**level** *level*]	Clear RMEPs. **Note** This configuration takes effect on the dynamic RMEP only.
Raisecom(config)#**clear ethernet cfm traceroute-cache**	Clear traceroute cache database.

8.8 Configuration examples

8.8.1 Example for configuring EFM

Networking requirements

As shown in Figure 8-1, to enhance the management and maintenance capability of the Ethernet link between RAX700 A and RAX700 B, you need to deploy EFM on RAX700 A and RAX700 B. The RAX700 A is the active end and the RAX700 B is the passive end. In addition, you need to deploy OAM event Trap on RAX700 A.

Figure 8-1 Configuring EFM

Configuration steps

Step 1 Configure RAX700 A.

```
Raisecom#hostname RAX700A
RAX700A#config
RAX700A(config)#oam active
RAX700A(config)#interface nni 1
RAX700A(config-port)#oam enable
RAX700A(config-port)#oam event trap enable
RAX700A(config-port)#oam peer event trap enable
```

Step 2 Configure RAX700 B.

```
Raisecom#hostname RAX700B
RAX700B#config
RAX700B(config)#interface nni 1
RAX700B(config-port)#oam enable
```

Step 3 Save configurations.

- Save configurations of RAX700 A.

```
RAX700A#write
```

- Save configurations of RAX700 B.

```
RAX700B#write
```

Checking results

Use the **show oam** command on RAX700 A to show EFM configurations.

```
RAX700A#show oam nni 1
Port:              nni 1
Mode:              Active
Administrate state:   Enable
Operation state:     Operational
Max OAMPDU size:     1518
Send period:        1000 ms
Link timeout :       10 s
Config revision:     1
Supported functions:  Loopback, Event, Variable
```

Use the **show oam trap** command on RAX700 A to show OAM event Trap configurations.

```
RAX700A#show oam trap nni 1
Port:nni 1
Event trap:Enable
Peer event trap:Enable
Discovery trap total:0
Discovery trap timestamp:0 days, 0 hours, 0 minutes
Lost trap total:0
Lost trap timestamp:0 days, 0 hours, 0 minutes
```

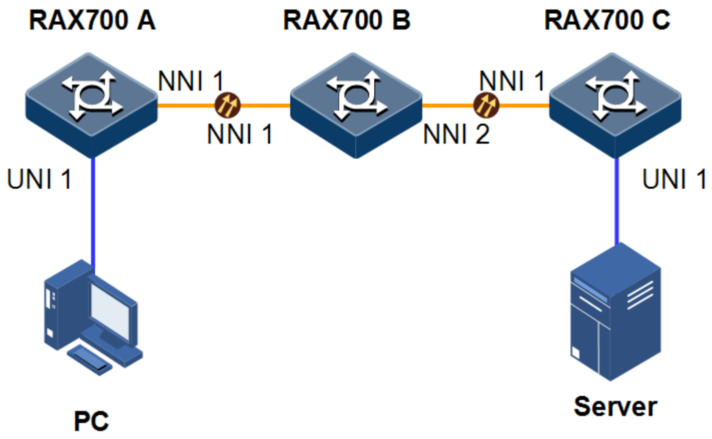
8.8.2 Example for configuring CFM

Networking requirements

As shown in Figure 8-2, the PC communicates with the server through the network where RAX700 A, RAX700 B, and RAX700 C are located. To ensure that the link between the PC and the server provide Carrier-grade service, you need to enable CFM on RAX700 A, RAX700 B, and RAX700 C. CFM is used to detect fault actively, as well as acknowledge and locate these faults. UNI 1 of RAX700 A and UNI 1 of RAX700 C are MEPs. RAX700 B is the MIP.

Detect Ethernet faults on the link between RAX700 A UNI 1 and RAX700 C UNI 1. The MD level is set to 3.

Figure 8-2 Configuring CFM



Configuration steps

Step 1 Add interfaces to the VLAN.

- Configure RAX700 A.

```
Raisecom#hostname RAX700A
RAX700A#config
RAX700A(config)#create vlan 100 active
RAX700A(config)#interface uni 1
RAX700A(config-port)#switchport access vlan 100
RAX700A(config-port)#exit
RAX700A(config)#interface nni 1
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#switchport trunk allowed vlan 100
RAX700A(config-port)#exit
```

- Configure RAX700 B.

```
Raisecom#hostname RAX700B
RAX700B#config
RAX700B(config)#create vlan 100 active
RAX700B(config)#interface nni 1
RAX700B(config-port)#switchport mode trunk
RAX700B(config-port)#switchport trunk allowed vlan 100
RAX700B(config-port)#exit
RAX700B(config)#interface nni 2
RAX700B(config-port)#switchport mode trunk
RAX700B(config-port)#switchport trunk allowed vlan 100
RAX700B(config-port)#exit
```

- Configure RAX700 C.

```
Raisecom#hostname RAX700C
RAX700C#config
RAX700C(config)#create vlan 100 active
RAX700C(config)#interface uni 1
RAX700C(config-port)#switchport access vlan 100
RAX700C(config-port)#exit
RAX700C(config)#interface nni 1
RAX700C(config-port)#switchport mode trunk
RAX700C(config-port)#switchport trunk allowed vlan 100
RAX700C(config-port)#exit
```

Step 2 Configure CFM fault detection.

- Configure RAX700 A.

```
RAX700A(config)#ethernet cfm domain level 3
RAX700A(config)#service ma1 level 3
RAX700A(config-service)#service vlan-list 100
RAX700A(config-service)#service mep up mpid 301 uni 1
RAX700A(config-service)#service remote-mep learning active
RAX700A(config-service)#service cc enable mep all
RAX700A(config-service)#exit
RAX700A(config)#ethernet cfm enable
RAX700A(config)#interface nni 1
RAX700A(config-port)#ethernet cfm enable
RAX700A(config-port)#interface uni 1
RAX700A(config-port)#ethernet cfm enable
```

- Configure RAX700 B.

```
RAX700B(config)#ethernet cfm domain level 3
RAX700B(config)#service ma1 level 3
RAX700B(config-service)#service vlan-list 100
RAX700B(config-service)#exit
RAX700B(config)#ethernet cfm enable
RAX700B(config)#interface nni 1
RAX700B(config-port)#ethernet cfm enable
RAX700B(config-port)#interface nni 2
RAX700B(config-port)#ethernet cfm enable
```

- Configure RAX700 C.

```
RAX700C(config)#ethernet cfm domain level 3
RAX700C(config)#service ma1 level 3
RAX700C(config-service)#service vlan-list 100
RAX700C(config-service)#service mep up mpid 302 uni 1
RAX700C(config-service)#service remote-mep learning active
RAX700C(config-service)#service cc enable mep all
```

```
RAX700C(config-service)#exit
RAX700C(config)#ethernet cfm enable
RAX700C(config)#interface nni 1
RAX700C(config-port)#ethernet cfm enable
RAX700C(config-port)#interface uni 1
RAX700C(config-port)#ethernet cfm enable
```

Step 3 Perform CFM fault acknowledgement, taking RAX700 A for example.

```
RAX700A(config)#service ma1 level 3
RAX700A(config-service)#ping mep 302 source 301
Type CTRL+C to abort
Sending 5 Ethernet CFM loopback messages to 000E.5E00.0001, timeout is 5
s:
Reply from MEP 302: time<1ms
Reply from MEP 302: time<1ms
Reply from MEP 302: time=17ms
Reply from MEP 302: time<1ms
Reply from MEP 302: time=16ms

------ PING Statistics ------
Success rate is 100 percent (5/5).
Ping statistics from 000E.5E00.0002:
Received loopback replys:<5 /0 /0 > (In order/Out of order/Error)
```

Step 4 Perform CFM fault location, taking RAX700 A for example.

```
RAX700A(config)#service ma1 level 3
RAX700A(config-service)#traceroute mep 302 source 301
TTL: <64>
Tracing the route to 000E.5E00.0002 on level 3, service ma1.
Traceroute send via uni1.
-------------------------------------------------------------------------
Hops  HostMac        Ingress/EgressPort  IsForwarded  RelayAction  NextHop
-------------------------------------------------------------------------
1    000E.5E00.0003    U1/N1               Yes     rlyFdb   000E.5E00.0003
2    000E.5E00.0003    N1/N2               Yes     rlyFdb   000E.5E00.0001
!3    000E.5E00.0001    N1/-               No     rlyHit   000E.5E00.0002
```

Step 5 Save configurations, taking RAX700 A for example.

```
RAX700A#write
```

Checking configurations

Use the **show ethernet cfm** command on RAX700 devices to show CFM configurations, taking RAX700 A for example.

```
RAX700A#show ethernet cfm
Port cfm enabled portlist:nni:1-4 uni:1-12 PC:1-8
Global cfm status: Enable
Archive hold time of error CCMs: 100(Min)
Remote mep aging time: 100(Min)
Device mode: Slave
```

8.8.3 Example for configuring SLA

Networking requirements

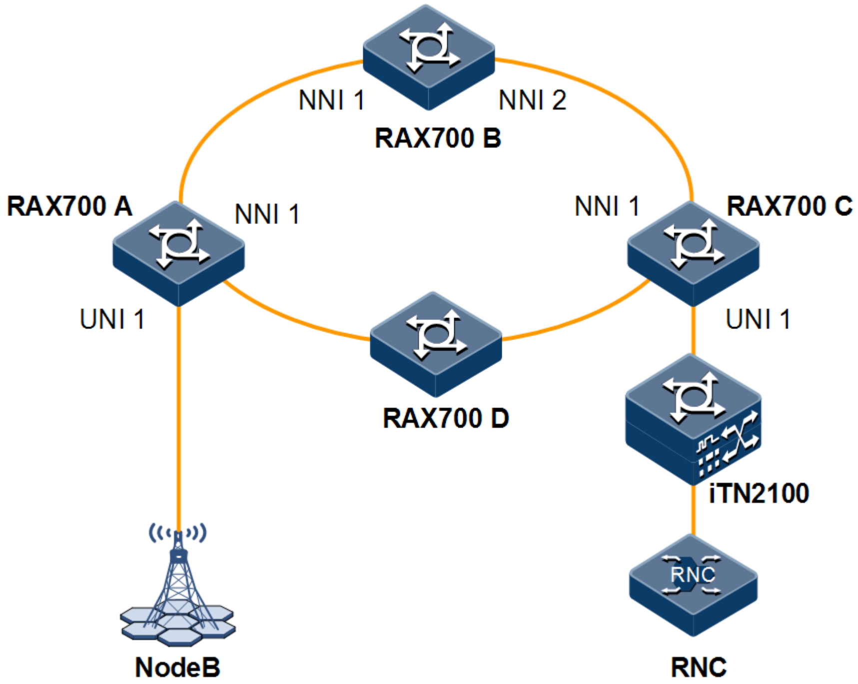
As shown in Figure 8-3, NodeB communicates with the RNC through RAX700 A, RAX700 B, and RAX700 C at the ring network, as well as the RAX7002100.

To make the Ethernet link between RNC and NodeB provide carrier-grade services, you need to deploy CFM on RAX700 devices. To effectively fulfil the SLA signed with users, the Carrier deploys SLA on RAX700 A and schedules it periodically. SLA is used to detect the network performance between RAX700 A and RAX700 C in time.

Perform Layer 2 delay test from RAX700 C to RAX700 A. Configure the y1731-echo operation on RAX700 C as below:

- Operation ID: 2
- RMEP ID: 2
- MD level: 3
- VLAN ID: 100
- CoS priority: 0
- Scheduling lifetime: 20s
- Test period: 10s

Figure 8-3 Configuring SLA



Configuration steps

Step 1 Configure CFM on RAX700 devices.

For detailed configurations, see section 8.8.2 Example for configuring CFM.

Step 2 Configure the y1731-echo operation on RAX700 C and enable operation scheduling.

```
RAX700C#config
RAX700C(config)#sla 2 y1731-echo remote-mep 2 level 3 svlan 100 cos 0
RAX700C(config)#sla schedule 2 life 20 period 10
```

Step 3 Save configurations, taking RAX700 C for example.

```
RAX700C#write
```

Checking results

Use the **show sla configuration** command on RAX700 C to show SLA configurations.

```
RAX700C(config)#show sla 2 configuration
------------------------------------------------------------------------
Operation <2>:
   Type: Y.1731 echo
```

```
   StartTime:  0 days, 0 : 0 : 50
------------------------------------------------------------------------
   Cos:                   0
   Service Vlan ID:         100
   Customer Vlan ID:         0
   MD Level:               3
   Remote MEP ID:           2
   Timeout(sec):            5
   Schedule Life(sec):       20
   Schedule Period(sec):      10
   Schedule Status:         active
```

Use the **show sla result** command on RAX700 C to show SLA scheduling results.

```
RAX700C(config)#show sla 2 result
------------------------------------------------------------------------
Operation <1026>: Success
   Info of Latest Test:  TWO-WAY    ONE-WAY(SD) ONE-WAY(DS)
------------------------------------------------------------------------
   Delay(usec):        < 1       ---       ---
```

8.8.4 Example for configuring ETH-Test throughput test

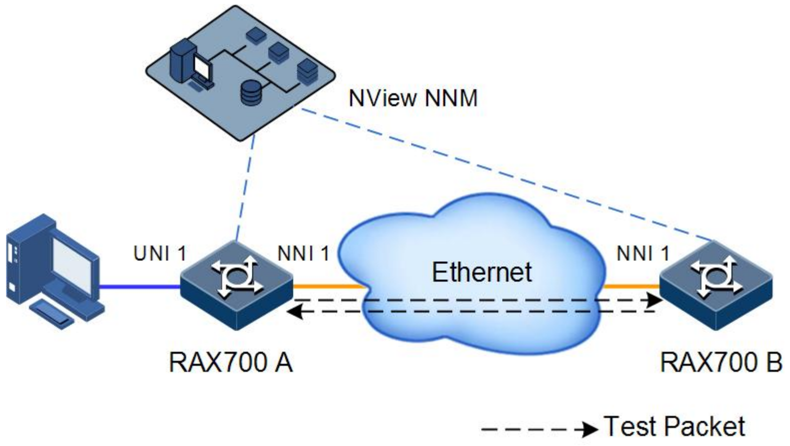
Networking requirements

As shown in Figure 8-4, RAX700 A and RAX700 B access the Ethernet through Line interfaces respectively. Use a bidirectional test method to test Ethernet throughput between RAX700 A and RAX700 B. RAX700 A is the local device for performing the ETH-Test throughput test operation and RAX700 B is the remote device.

Configure parameters as below:

- MEP ID of RAX700 A: 1
- MEP ID of RAX700 B: 2
- MD level: 2
- SVLAN ID: 100
- CVLAN ID: 200
- CoS priority: 3
- Destination test bandwidth: 100 Mbit/s
- Duration time: 60s
- Other parameters: default values

Figure 8-4 Configuring ETH-Test throughput test



Configuration steps

Step 1 Configure RAX700 A and RAX700 B respectively. Set RAX700 A and RAX700 B to different MEPs in a service instance. In addition, RAX700 A and RAX700 B can discover each other.

For detailed configurations, see section 8.8.2 Example for configuring CFM. Note that the ETH-Test supports MEP in Down direction only.

Step 2 Enable RAX700 A ETH-Test test operation and configure basic information.

```
RAX700A(config)#sla y1731-throughput enable
RAX700A(config)#sla y1731-throughput 1 local-mep 1 remote-mep 2 level 2
svlan 100 cvlan 200 cos 3
RAX700A(config)#sla y1731-throughput 1 two-way object 100 packet-size
1024 pattern null duration 60
```

Step 3 Enable RAX700 B ETH-Test test operation.

```
RAX700B(config)#sla y1731-throughput enable
```

Step 4 Schedule RAX700 A ETH-Test test operation.

```
RAX700A(config)#sla schedule y1731-throughput 1
```

Step 5 Save configurations.

- Save configurations of RAX700 A.

```
RAX700A#write
```

- Save configurations of RAX700 B.

```
RAX700B#write
```

Checking results

Use the **show sla y1731-throughput** *oper-id* **configuration** command on RAX700 A to show configurations on the ETH-Test test operation.

```
RAX700A(config)#show sla y1731-throughput 1 configuration
Operation <1>:
   Remote mac-address:           0000.0000.0000
   Local MEP ID:               1
   Remote MEP ID:              2
   MD Level:                  2
   Service Vlan ID:             100
   Customer Vlan ID:            200
   CoS:                     3
   CFI:                     1
   Bothway Config:              1
   Object Band-width:           100
   Packet Length:              1024
   Packet Pattern:             null
   Test Duration:              60
   Schedule Status:            completed
```

Use the **show sla y1731-throughput** *oper-id* **result** command to show throughput test results.

```
RAX700A(config)#show sla y1731-throughput 1 result
------------------------------------------------------------------------
Operation <1>:
   Test Starttime:   0  days, 00:13:11:46
   Test Endtime:   0  days, 00:14:11:46
   Statistic Starttime:   0  days, 00:13:07:30
   Statistic Endtime:   0  days, 00:14:17:30
Operation <1>: Success
------------------------------------------------------------------------
   Statistic of Test:   Local Dev   Remote Dev
------------------------------------------------------------------------
   SendUsrPStatics:        0        0
   SendUsrBStatics:        0        0
   RecvUsrPStatics:        0        0
   RecvUsrBStatics:        0        0
   SendTestPStatics:        0        0
   SendTestBStatics:        0        0
   RecvTestPStatics:        0        0
   RecvTestBStatics:        0        0
   ReceiveSeqErrStatics:      0        0
```

```
    ReceiveCrcErrStatic:        0         0
    ReceivePrbsErrStatics:       0         0
    L2R throughput(bps):            0
R2L throughput(bps):           0
```

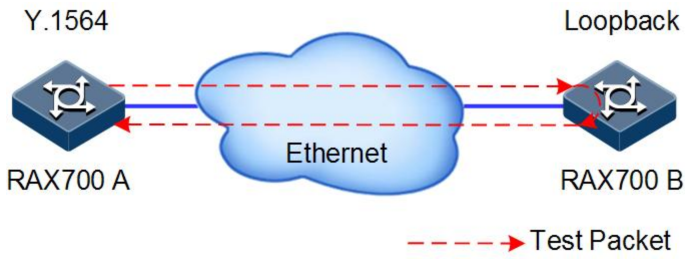
8.8.5 Example for configuring RCSAM

Networking requirements

As shown in Figure 8-5, configure the test type of RCSAM, create the test service, and configure properties of the test packet on RAX700 A to enable configuration test and performance test on RAX700 A. The MAC address of RAX700 B is 000E.5E11.1234. Configure loopback on RAX700 B to return test traffic to RAX700 A for analysis. And then configure parameters as below:

- UNI of RAX700 A: UNI 1
- Test packet: Layer 2 Ethernet packet
- Outer VLAN ID: 20
- CoS value: 1
- Inner VLNA ID: 21

Figure 8-5 Configuring RCSAM



Configuration steps

Configure RAX700 A. By default, RAX700 B is enabled loopback based on SVLAN.

Step 1 Configure the test type of RCSAM.

```
Raisecom#hostname RAX700A
RAX700A#config
RAX700A(config)#rcsam cir step 10 50 100
RAX700A(config)#rcsam step-time 5
RAX700A(config)#rcsam configuration-test enable
RAX700A(config)#rcsam performance-test duration 1
RAX700A(config)#rcsam performance-test enable
```

Step 2 Create RCSAM service 1 and configure properties of the test packet. You can configure multiple test services as required by just repeating the following configuration steps.

```
RAX700A(config)#rcsam service 1 l2-eth
RAX700A(config-rcsamservice)#name data
RAX700A(config-rcsamservice)#dmac 000e.5e11.1234
RAX700A(config-rcsamservice)#svlan 20 cos 1
RAX700A(config-rcsamservice)#cvlan 21
RAX700A(config-rcsamservice)#frame-size fix 128
RAX700A(config-rcsamservice)#uni uni 1
RAX700A(config-rcsamservice)#cir 100000 cbs 64 eir 10000 ebs 64
RAX700A(config-rcsamservice)#service enable
RAX700A(config-rcsamservice)#exit
```

Step 3 Enable RCSAM.

```
RAX700A(config)#rcsam test start
```

Checking results

Use the **show rcsam configuration global** command to show RCSAM global configurations.

```
RAX700A#show rcsam configuration global
Source MAC Address                  :0080.4804.ab56(read-only)

Global Setup--
Test Mode                          :Round-Trip
Service Configuration Test            :enable
Service Configuration Test Duration(sec.) :15
Service Performance Test             :enable
Service Performance Test Duration(minute) :1

Ramp--
Step Time(sec.)    :5
Step Num.         Step Values
1                10(%CIR)
2                50(%CIR)
3                100(%CIR)
4                --(%CIR)
5                CIR+EIR
6                Traffic policing

Numbers of service tested      : 1
```

Use the **show rcsam result detail** command to show RCSAM results.

```
RAX700A#show rcsam result detail
Cofiguration Test Status: complete
Configuration Test Result: pass
Duration(sec.): 30
```

```
Service 1: Data
Test   Result   Avg.IR   FLR(%)          FD(ms)              FDV(ms)
               (Mbit/s)           Min   mean   max     min   mean  max
----------------------------------------------------------------------
CIR
Step 1   pass     15     0.001    0.001  0.002   0.003    0.001  0.002
0.003
Step 2   pass     20     0.001    0.001  0.002   0.003    0.001  0.002
0.003
Step 3   pass     25     0.001    0.001  0.002   0.003    0.001  0.002
0.003
Step 4   pass     30     0.001    0.001  0.002   0.003    0.001  0.002
0.003
EIR     pass     50     0.001    0.001  0.002   0.003    0.001  0.002
0.003
Tra-pol   pass    60     0.001    0.001  0.002   0.003    0.001  0.002
0.003

Service 2: Video
Test   Result   Avg.IR   FLR(%)          FD(ms)              FDV(ms)
               (Mbit/s)           Min   mean   max     min   mean  max
----------------------------------------------------------------------
CIR
Step 1  pass     15     0.001    0.001  0.002   0.003    0.001  0.002
0.003
Step 2  pass     20     0.001    0.001  0.002   0.003    0.001  0.002
0.003
Step 3  pass     25     0.001    0.001  0.002   0.003    0.001  0.002
0.003
Step 4  pass     30     0.001    0.001  0.002   0.003    0.001  0.002
0.003
Tra-pol  fail     60     0.001    0.001  0.002   0.003    0.001  0.002
0.003

Performance Test Status: Complete
Performance Test Result: fail
Duration(H:M:S): 2:00:00

Test    Result   Avg.IR   FLR(%)       FD(ms)             FDV(ms)
               (Mbit/s)         | Min   mean   max   |  min   mean  max
---------------------------------------------------------------------
service1  pass     15     0.001    0.001  0.002   0.003    0.001  0.002
0.003
service2  pass     20     0.001    0.001  0.002   0.003    0.001  0.002
0.003
```

9 Security

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

- Configuring ACL
- Configuring RADIUS
- Configuring TACACS+
- Configuring storm control
- Maintenance
- Configuration examples

9.1 Configuring ACL

9.1.1 Preparing for configurations

Scenario

To filter packets, device needs to be configured with ACL to identify packets to be filtered. Devices cannot allow/disallow related packets to pass based on pre-configured policies unless they identify specified packets.

ACLs are grouped in to the following types:

- IP ACL/IPv6 ACL: make classification rules based on properties of packets, such as source/destination IP address carried by the IP header of packets or used TCP/UDP port ID.
- MAC ACL: make classification rules based on Layer 2 information, such as source MAC address, destination MAC address, or Layer 2 protocol type carried by the Layer 2 frame header of packets.
- MAP ACL: compared with IP ACL and MAC ACL, MAP ACL can define more protocols and more detailed protocol fields. In addition, it can be used to match any byte in first 64 packets of a Layer 2 data frame based on user's definition.
- MAC-IPv4 ACL: specify the classification rule according to the attribute information, such as, source/destination MAC address carried by the Layer 2 frame head of the packet, source/destination IP address carried by the IP head of the packet, and TCP/UDP port ID.

Based on real scenarios, ACL can be applied based on the whole device, interface, or VLAN.

Prerequisite

N/A

9.1.2 Configuring IP ACL

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip-access-list** *acl-id* { **deny** | **permit** } { *protocol-id* | **icmp** | **igmp** | **ip** } { *source-ip-address mask* | **any** } { *destination-ip-address mask* | **any** } Raisecom(config)#**ip-access-list** *acl-id* { **deny** | **permit** } { **tcp** | **udp** } { *source-ip-address mask* | **any** } [*source-protocol-port*] { *destination-ip-address mask* | **any** } [*destination-protocol-port*]	Create IP ACL and define the matching rule.

9.1.3 Configuring IPv6 ACL

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6-access-list** *acl-id* { **deny** | **permit** } { *next-header-value* | **icmpv6** | **ipv6** } [**traffic-class** *class-id*] [**flow-label** *label-id*] { *source-ipv6-address/mask* | **any** } { *destination-ipv6-address/mask* | **any** }	Configure the binding protocol type as ICMPv6 or IPv6; or enter the protocol type of IPv6 ACL.
3	Raisecom(config)#**ipv6-access-list** *acl-id* { **deny** | **permit** } { **tcp** | **udp** } [**traffic-class** *class-id*] [**flow-label** *label-id*] { *source-ipv6-address/mask* | **any** } [*source-protocol-port*] { *destination-ipv6-address/mask* | **any** } [*destination-protocol-port*]	Configure the binding protocol type as TCP/UDP IPv6 ACL.

9.1.4 Configuring MAC ACL

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mac-access-list** *acl-id* { **deny** | **permit** } [*protocol* | **arp** | **ip** | **rarp** | **any**] { *source-mac-address mask* | **any** } { *destination-mac-address mask* | **any** }	Create MAC ACL and define the matching rule.

9.1.5 Configuring MAP ACL

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**access-list-map** *acl-id* { **deny** | **permit** }	Create the MACP ACL and enter ACLMAP configuration mode.
3	Raisecom(config-aclmap)#**match mac** { **destination** | **source** } *mac-address mask*	(Optional) define the matching rule of source or destination MAC address. By default, the MAC address is not matched.
4	Raisecom(config-aclmap)#**match cos** *cos-value*	(Optional) define the matching rule of CoS value. By default, the CoS value is not matched.
5	Raisecom(config-aclmap)#**match ethertype** *ethertype*	(Optional) define the matching rule of Ethernet frame type. By default, the Ethernet frame type is not matched.
6	Raisecom(config-aclmap)#**match** { **arp** | **eapol** | **flowcontrol** | **ip** | **loopback** | **pppoe** | **pppoedisc** | **slowprotocol** | **x25** | **x75** }	(Optional) define the matching rule of upper protocol carried by Layer 2 packet header.
7	Raisecom(config-aclmap)#**match ip** { **destination-address** | **source-address** } *ip-address* [*mask*]	(Optional) define the matching rule of source or destination IP address. By default, the IP address is not matched.
8	Raisecom(config-aclmap)#**match ip dscp** { *dscp-value* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41**| **af42** |**af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7**| **default** | **ef** }	(Optional) define the matching rule of IP DSCP value. By default, the IP DSCP value is not matched.
9	Raisecom(config-aclmap)#**match ip protocol** { *protocol-id* | **ahp** | **esp** | **gre** | **icmp** | **igmp** | **igrp** |**ipinip** | **ospf** | **pcp** | **pim** | **tcp** | **udp** }	(Optional) define the matching rule of IP protocol value. By default, the IP protocol value is not matched.
10	Raisecom(config-aclmap)#**match ip tcp** { **destination-port** | **source-port** } { *port-id* | **bgp** | **domain** | **echo** | **exec** | **finger** | **ftp** | **ftp-data** | **gopher** | **hostname** | **ident** | **irc** | **klogin** | **kshell** | **login** | **lpd** | **nntp** | **pim-auto-rp** | **pop2** | **pop3** | **smtp** | **sunrpc** | **syslog** | **tacacs** | **talk** | **telnet** | **time** | **uucp** | **whois** | **www** }	(Optional) define the matching rule of TCP port ID. By default, the TCP port ID is not matched.
11	Raisecom(config-aclmap)#**match ip udp** { **destination-port** | **source-port** } { *port-id* | **biff** | **bootpc** | **bootps** | **domain** | **echo** | **mobile-ip** | **netbios-dgm** | **netbios-ns** | **netbios-ss** | **ntp** | **pim-auto-rp** | **rip** | **snmp** | **snmptrap** | **sunrpc** | **syslog** | **tacacs** | **talk** | **tftp** | **time** | **who** }	(Optional) define the matching rule of UDP port ID. By default, the UDP port ID is not matched.

Step	Command	Description
12	Raisecom(config-aclmap)#**match** { **cvlan** | **svlan** } *vlan-id*	Define the matching rule based on VLAN IDs of packets.
13	Raisecom(config-aclmap)#**match exp** *exp*	(Optional) define the matching rule of CoS in PW.
14	Raisecom(config-aclmap)#**match label** *label-id*	(Optional) define the matching rule of label in MPLS network.
15	Raisecom(config-aclmap)#**match user-define** *rule-string rule-mask offset*	(Optional) define the matching rule of customized fields. Use the rule mask and the offset parameters to extract 23–64 bytes from the first 64 bytes of a data frame and then use the customized rule to filter matched data frame for process. For example, to filter all TCP packets, you can set the rule, rule mask, and offset to 06, FF and 27 respectively. In this case, the rule mask cooperates with offset to extract TCP ID from received data frames and then use the rule to filer all TCP packers. **Note** The rule must even number of hexadecimal digits. The offset includes the 802.1q VLAN Tag field, even the received packet is an untagged one.

9.1.6 Configuring MAC-IPv4 ACL

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mac-ipv4-access-list** *acl-id* { **deny** | **permit** } [**source-mac** *source-mac-address source-mac-mask*] [**destination-mac** *destination-mac-address destination-mac-mask* [**vlan** *vlan-id*]] [**cos** *cos-value*] [**source-address** *source-ip-address source-ip-address-mask*] [**destination-address** *destination-ip-address destination-ip-address-mask*] [**dscp** *dscp-value*] [**tos** *tos-value*]	Configure MAC-IPv4 ACL and define the matching rule.

Step	Command	Description
3	Raisecom(config)#**mac-ipv4-access-list** *acl-id* { **deny** | **permit** } [**source-mac** *source-mac-address source-mac-mask*] [**destination-mac** *destination-mac-address destination-mac-mask* [**vlan** *vlan-id*]] [**cos** *cos-value*] { **tcp** | **udp** } [**source-address** *source-ip-address source-ip-address-mask* [**source-port** *source-port-number*]] [**destination-address** *destination-ip-address destination-ip-address-mask* [**destination-port** *destination-port-number*]] [**dscp** *dscp-value*] [**tos** *tos-value*]	Configure binding the MAC-IPv4 ACL whose protocol type is TCP or UDP.

9.1.7 Applying ACL to device

Note

ACL cannot take effect on the RAX711-L unless it is added to the filter. Multiple ACL matching rules can be added to the filter to form multiple filtering rules. When you configure a flow-based filter, the sequence to add ACL rules decides their priorities. The later an ACL rule is added, the higher the priority is. If ACL rules are exclusive, the ACL rule with the highest priority takes effect. Therefore, you must arrange their sequence reasonably to filter packets properly.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**filter** { **ip-access-list** | **ipv6-access-list** | **mac-access-list** | **access-list-map** | **mac-ipv4-access-list** } { *acl-id* | **all** } [**statistics**]	Configure filtering based on device. If the **statistics** parameter is configured, statistics will be taken according to the filtering rule.
	Raisecom(config)#**filter** { **access-list-map** | **ip-access-list** | **ipv6-access-list** | **mac-access-list** | **mac-ipv4-access-list** } { **all** | *acl-id* } **ingress** { *interface-type interface-list* | **port-channel** *port-channel-number*} [**statistics**]	Configure filtering based on interface. If the **statistics** parameter is configured, statistics will be taken according to the filtering rule.
	Raisecom(config)#**filter**{ **mac-access-list** | **access-list-map** } { *acl-id* | **all** } **vlan** *vlan-id* [**double-tagging inner**][**statistics**]	Configure filtering based on VLAN. If the **statistics** parameter is configured, statistics will be taken according to the filtering rule.
3	Raisecom(config)#**filter enable**	Enable the filter to make the filtering rule take effect. After the filter is enabled, not only previously configured filtering rules take effect, but also the filtering rules configured later take effect immediately. By default, the filter is disabled.

9.1.8 Checking configurations

No.	Command	Description
1	Raisecom#**show ip-access-list** [*acl-id*]	Show IP ACL configurations.
2	Raisecom#**show ipv6-access-list** [*acl-id*]	Show IPv6 ACL configurations.
3	Raisecom#**show mac-access-list** [*acl-id*]	Show MAC ACL configurations.
4	Raisecom#**show access-list-map** [*acl-id*]	Show MAP ACL configurations.
5	Raisecom#**show mac-ipv4-access-list** [*acl-id*]	Show MAC-IPv4 ACL configurations
6	Raisecom#**show filter** [**access-list-map** | **ip-access-list** | **ipv6-access-list** | **mac-access-list** | **mac-ipv4-access-list**] { **all** | *acl-list* }	Show global filter configurations.
7	Raisecom#**show filter** { **access-list-map** | **ip-access-list** | **ipv6-access-list** | **mac-access-list** | **mac-ipv4-access-list** } { **all** | *acl-list* } **ingress** { *interface-type interface-list* }	Show filter configurations based on interface.
8	Raisecom#**show filter** { **access-list-map** | **mac-access-list** } { **all** | *acl-list* } **vlan** *vlan-id* [**double-tagging inner**]	Show filter configurations based on VLAN.

9.2 Configuring RADIUS

9.2.1 Preparing for configurations

Scenario

To control users accessing the device network, you can deploy the RADIUS server at the network to authenticate and account users. The RAX711-L can be used as a proxy of the RADIUS server to authenticate users based on results returned by the RADIUS server.

Prerequisite

N/A

9.2.2 Configuring RADIUS authentication

Step	Command	Description
1	Raisecom#**radius**[**backup**] { *ip-address* | *ipv6-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.

Step	Command	Description
2	Raisecom#**radius-key** *string*	Configure the shared key for RADIUS authentication.
3	Raisecom#**user login** { **local-user** | **radius-user** | **local-radius** | **radius-local** [**server-no-response**] }	Configure the authentication mode for login when RADIUS authentication is applied.
4	Raisecom#**enable login** { **local-user** | **radius-user** | **local-radius** | **radius-local** [**server-no-response**] }	Configure the authentication mode for entering privileged EXEC mode when RADIUS authentication is applied.

9.2.3 Configuring RADIUS accounting

Step	Command	Description
1	Raisecom#**aaa accounting login enable**	Enable RADIUS accounting. By default, RADIUS accounting is disabled.
2	Raisecom#**radius** [**backup**] **accounting-server** { *ip-address* | *ipv6-address* } *ip-address* [*account-port*]	Specify the IP address and port ID of the RADIUS accounting server. By default, the UDP port ID is set to 1813. The **backup** parameter is used to specify a backup RADIUS accounting server.
3	Raisecom#**radius accounting-server key** *string*	Configure the shared key used for communicating with the RADIUS accounting server. The shared key must be identical to the one configured on the RADIUS accounting server. Otherwise, accounting operation fails. By default, the shared key is empty.
4	Raisecom#**aaa accounting fail** { **online** | **offline** }	Configure the processing policy for accounting failure. By default, the processing policy is set to **online**. In indicates that users are allowed to log in if accounting operation fails.
5	Raisecom#**aaa accounting update** *period*	Configure the interval for sending accounting update packets. If the interval is set to 0, it indicates that no accounting update packet is sent. By default, the interval for sending accounting update packets is set to 0. **Note** With the accounting begin packet, accounting update packet, and accounting end packet, the RADIUS server can record the access time and operations of each user.

9.2.4 Checking configurations

No.	Command	Description
1	Raisecom(config)#**show radius-server**	Show RADIUS server configurations.

9.3 Configuring TACACS+

9.3.1 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. Compared with RADIUS, TACACS+ is more secure and reliable. The RAX711-L can be used as a Proxy of the TACACS+ server to authenticate users based on results returned by the TACACS+ server.

Prerequisite

N/A

9.3.2 Configuring TACACS+ authentication

Step	Command	Description
1	Raisecom#**tacacs-server** [**backup**] *ip-address*	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 key** *string*	Configure the shared key for TACACS+ authentication.
3	Raisecom#**tacacs** [**backup**] **accounting-server** *ip-address*	Specify the IP address and port ID of the TACACS+ accounting server. The **backup** parameter is used to specify a backup TACACS+ accounting server.
4	Raisecom#**user login** { **local-user** | **tacacs-user** | **local-tacacs** | **tacacs-local** [**server-no-response**] }	Configure the authentication mode for login when TACACS+ authentication is applied.
5	Raisecom#**enable login** { **local-user** | **tacacs-user** | **local-tacacs** | **tacacs-local** [**server-no-response**] }	Configure the authentication mode for entering privileged EXEC mode when TACACS+ authentication is applied.

9.3.3 Checking configurations

No.	Command	Description
1	`Raisecom(config)#`**`show tacacs-server`**	Show TACACS+ server configurations.

9.4 Configuring storm control

9.4.1 Preparing for configurations

Scenario

Configuring storm control on Layer 2 devices can prevent broadcast storm from occurring when broadcast packets increase sharply in the network. Therefore, this helps ensure that the unicast packets can be properly forwarded.

Broadcast traffic may exist in following forms, so you need to limit the bandwidth for them on Layer 2 devices.

- Unknown unicast traffic: the unicast traffic whose destination MAC address is not in MAC address table. It is broadcasted by Layer 2 devices.
- Multicast traffic: the traffic whose destination MAC address is a multicast MAC address. Generally, it is broadcasted by Layer 2 devices.
- Broadcast traffic: the traffic whose destination MAC address is a broadcast MAC address. It is broadcasted by Layer 2 devices.

Prerequisite

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

9.4.2 Configuring storm control

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**storm-control** { **broadcast** | **dlf** | **multicast** } { **enable** | **disable** } *interface-type interface-list*	Enable storm control on broadcast traffic, multicast traffic, and unknown unicast traffic. By default, storm control is enabled on broadcast traffic while is disabled on multicast traffic and unknown unicast traffic.
3	Raisecom(config)#**storm-control** { **broadcast** | **multicast** | **dlf** | **all** } **pps** *value* [*interface-type interface-list*]	Configure the threshold. By default, the storm control threshold is set to 1024 pps.

9.4.3 Enabling DLF packet forwarding

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#dlf-forwarding enable`	Enable DLF packet forwarding. By default, DLF packet forwarding is enabled.

9.4.4 Checking configurations

No.	Command	Description
1	`Raisecom(config)#show storm-control`	Show storm control configurations.
2	`Raisecom#show dlf-forwarding`	Show DLF packet forwarding status.

9.5 Maintenance

Command	Description
`Raisecom(config)#clear filter statistics`	Clear filter statistics.

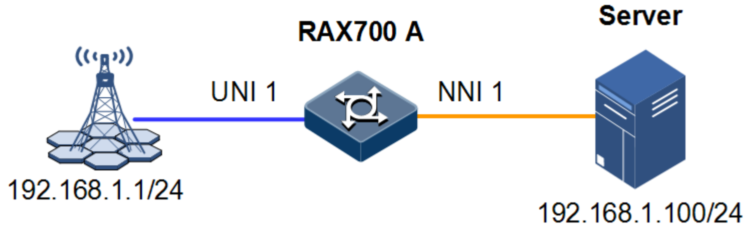
9.6 Configuration examples

9.6.1 Example for configuring ACL

Networking requirements

As shown in Figure 9-1, to control users accessing the server, you can deploy ACL on RAX700 A to disallow 192.168.1.1 to access 192.168.1.100.

Figure 9-1 Configuring ACL



Configuration steps

Step 1 Configure IP ACL.

```
Raisecom#config
Raisecom(config)#ip-access-list 1 deny ip 192.168.1.1 255.255.255.0
192.168.1.100 255.255.255.0
```

Step 2 Apply ACL to UNI 1 of RAX700 A.

```
Raisecom(config)#filter ip-access-list 1 ingress uni 1
Raisecom(config)#filter enable
```

Step 3 Save configurations.

```
Raisecom#write
```

Checking results

Use the **show ip-access-list** command to show IP ACL configurations.

```
Raisecom#show ip-access-list
Src Ip: Source Ip Address
Src Ip Mask: Source Ip Address Mask
Dest Ip: Destination Ip Address
Dest Ip Mask: Destination Ip Address Mask
List  Access  Protocol Ref. Src Ip    Src Ip Mask:Port     Dest Ip
Dst Ip Mask:Port
-------------------------------------------------------------------------
-------------------------------
1    deny    IP      1   192.168.1.1   255.255.225.0:0   192.168.1.100
255.255.255.0:0
```

Use the **show filter** command to show filter configurations.

```
Raisecom#show filter
Rule filter: Enable
Filter list(In accordance with the priority from low to high):
ACL-Index  IPort   EPort  VLAN   VLANType Hardware Valid   StatHw  Pkts
-------------------------------------------------------------------------
IP   1    uni1  --      --      --      Yes     Yes     No      --
```

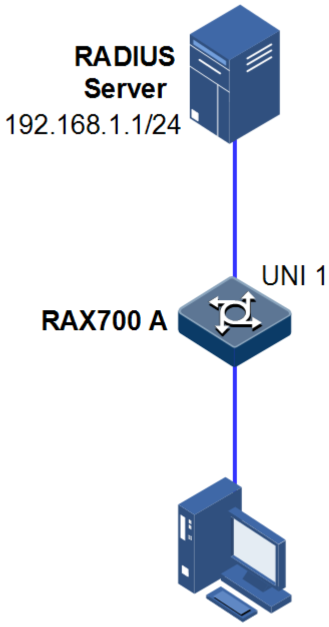
9.6.2 Example for configuring RADIUS

Networking requirements

As shown in Figure 9-2, to control users accessing RAX700 A, you need to deploy RADIUS authentication and accounting features on RAX700 A to authenticate users logging in to RAX700 A and record their operations.

Set the interval for sending accounting update packet to 2min. Set the processing policy for accounting failure to **offline**.

Figure 9-2 Configuring RADIUS



Configuration steps

Step 1 Authenticate login users through RADIUS.

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

Step 2 Account login users through RADIUS.

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

Step 3 Save configurations.

```
Raisecom#write
```

Checking results

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

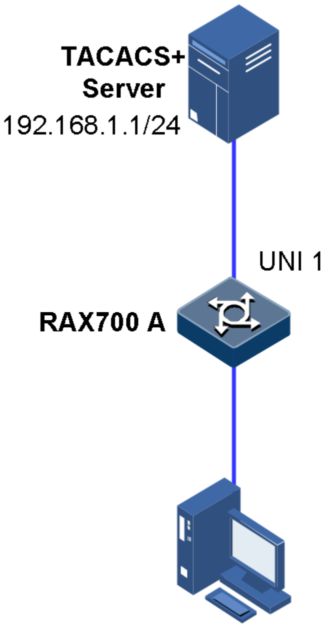
```
Raisecom#show radius-server
Authentication server IP:      192.168.1.1 port:1812
Backup authentication server IP:0.0.0.0 port:1812
Authentication server key:     raisecom
Accounting server IP:          192.168.1.1 port:1813
Backup accounting server IP:    0.0.0.0 port:1813
Accounting server key:         raisecom
Accounting login:             enable
Update interval:              120
Accounting fail policy:        offline
```

9.6.3 Example for configuring TACACS+

Networking requirements

As shown in Figure 9-3, to control users accessing RAX700 A, you need to deploy TACACS+ authentication on RAX700 A to authenticate users logging in to RAX700 A.

Figure 9-3 Configuring TACACS+



Configuration steps

Step 1 Authenticate login users through TACACS+.

```
Raisecom#tacacs-server 192.168.1.1
Raisecom#tacacs-server key raisecom
Raisecom#user login tacacs-user
```

Step 2 Save configurations.

```
Raisecom#write
```

Checking results

Use the **show tacacs-server** command to show TACACS+ configurations.

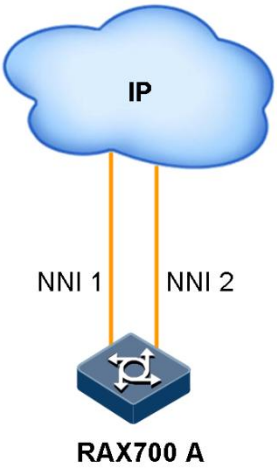
```
Raisecom#show tacacs-server
Server Address:      192.168.1.1
Backup Server Address:          --
Sever Shared Key:    raisecom
Accounting server Address:      --
Backup Accounting server Address: --
Total Packet Sent:   0
Total Packet Recv:   0
Num of Error Packets: 0
```

9.6.4 Example for configuring storm control

Networking requirements

As shown in Figure 9-4, to control the influence of the broadcast storm on RAX700 A, you need to deploy storm control on RAX700 A to control broadcast and unknown unicast packets. The storm control threshold is set to 2000 pps.

Figure 9-4 Configuring storm control



Configuration steps

Step 1 Configure storm control on RAX700 A.

```
Raisecom#config
Raisecom(config)#storm-control broadcast enable nni 1-2
Raisecom(config)#storm-control dlf enable nni 1-2
Raisecom(config)#storm-control pps 2000
```

Step 2 Save configurations.

```
Raisecom#write
```

Checking results

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

```
Raisecom#show storm-control
Threshold: 2000 pps
Interface      Broadcast      Multicast      Unicast
-----------------------------------------------------------
nni1           Enable         Disable        Enable
nni2           Enable         Disable        Enable
uni1           Enable         Disable        Disable
uni2           Enable         Disable        Disable
......
```

10 QoS

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

- Configuring priority trust and priority mapping
- Configuring priority mapping in MPLS network
- Configuring traffic classification and traffic policy
- Configuring queue scheduling
- Configuring congestion avoidance and queue shaping
- Configuring rate limiting based on interface, Tunnel, and PW
- Configure hierarchical rate limiting
- Maintenance
- Configuration examples

10.1 Configuring priority trust and priority mapping

10.1.1 Preparing for conifgurations

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 configuring interface-based DSCP priority remarking. After priority trust is configured, the RAX711-L 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 the device will perform queue scheduling on these packets based on local priorities.

In general, for IP packets, you need to configure the mapping between ToS priority/DSCP priority and local priority. For VLAN packets, you need to configure the mapping between CoS priority and local priority.

Prerequisite

Ensure the related interfaces Up.

10.1.2 Configuring priority trust

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos enable**	Enable global QoS. By default, the global QoS is enabled.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#**mls qos trust** { **cos** | **dscp** }	Configure the priority trusted by an interface. By default, the interface trusts the CoS priority.

10.1.3 Configuring DSCP priority remarking

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos enable**	Enable global QoS. By default, the global QoS is enabled.
3	Raisecom(config)#**mls qos mapping dscp-mutation** *profile-id*	Create the DSCP remarking profile and enter dscp-mutation configuration mode.
4	Raisecom(dscp-mutation)#**dscp** *dscp-value* **to new-dscp** *dscp-value* Raisecom(dscp-mutation)#**exit**	Remark the DSCP priority of specified packets and return to global configuration mode.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
6	Raisecom(config-port)#**mls qos dscp-mutation** *profile-id*	Apply the DSCP remarking profile to an interface.

10.1.4 Configuring mapping from DSCP priority to local priority

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos enable**	Enable global QoS. By default, the global QoS is enabled.
3	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.

Step	Command	Description
4	Raisecom(dscp-to-pri)#**dscp** *dscp-value* **to local-priority** *localpri-value* [**color** { **green** | **red** | **yellow** }] Raisecom(dscp-to-pri)#**exit**	Configure mapping from DSCP priority to local priority (color) and return to global configuration mode.
5	Raisecom(config)#**mls qos dscp-to-local-priority** *profile-id*	Apply the DSCP-to-local priority (color) mapping profile in global configuration mode.
6	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
7	Raisecom(config-port)#**mls qos dscp-to-local-priority** *profile-id*	Apply the DSCP-to-local priority (color) mapping profile to an interface.

10.1.5 Configuring mapping from CoS priority to local priority

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos enable**	Enable global QoS. By default, the global QoS is enabled.
3	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.
4	Raisecom(cos-to-pri)#**cos** *cos-value* **to local-priority** *localpri-value* [**color** { **green** | **red** | **yellow** }] Raisecom(dscp-to-pri)#**exit**	Configure mapping from CoS priority to local priority (color) and return to global configuration mode.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
6	Raisecom(config-port)#**mls qos cos-to-local-priority** *profile-id*	Apply the CoS-to-local priority (color) mapping profile to an interface.

10.1.6 Configuing mapping from CoS DEI priority to local priority

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos enable**	Enable global QoS. By default, the global QoS is enabled.
3	Raisecom(config)#**mls qos mapping cos-dei-to-local-priority** *profile-id*	Create the CoS DEI-to-local priority (color) mapping profile and enter cos-dei-to-pri configuration mode.

Step	Command	Description
4	Raisecom(cos-to-pri)#**cos** *cos-value* **dei** *dei-value* **to local-priority** *localpri-value* [**color** { **green** | **red** | **yellow** }] Raisecom(cos-to-pri)#**exit**	Configure mapping from the CoS DEI priority to local priority (color) and return to global configuration mode.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
	Raisecom(config-port)#**mls qos cos-dei-to-local-priority** *profile-id*	Apply the CoS DEI-to-local priority (color) mapping profile to an interface.

10.1.7 Configuring mapping from local priority to CoS priority

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos enable**	Enable global QoS. By default, the global QoS is enabled.
3	Raisecom(config)#**mls qos mapping cos-remark** *profile-id*	Create the local-to-CoS mapping profile and enter cos-remark configuration mode.
4	Raisecom(cos-remark)#**local-priority** *localpri-value* **to cos** *cos-value* Raisecom(cos-remark)#**exit**	Configure the local-to-CoS priority mapping profile and return to global configuration mode.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
6	Raisecom(config-port)#**mls qos cos-remark** profile-id	Apply the local-to-CoS mapping profile in physical layer interface configuration mode.
7	Raisecom(config-port)#**mls qos cos-remark** *profile-id*	Apply the local-to-CoS mapping profile to an interface.

10.1.8 Configuring mapping from local priority to CoS DEI priority

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos enable**	Enable global QoS. By default, the global QoS is enabled.
3	Raisecom(config)#**mls qos mapping cos–dei-remark** *profile-id*	Create the local-to-CoS DEI mapping profile and enter cos-remark configuration mode.
4	Raisecom(cos-remark)#**local-priority** *priority* **to cos** *cos-value* **dei** *dei-value* Raisecom(cos-remark)#**exit**	Configure mapping from local priority to CoS DEI priority and return to global configuration mode.

Step	Command	Description
5	Raisecom(config)#**mls qos cos-dei-remark** *profile-id*	Apply the local-to-CoS DEI mapping profile in global configuration mode.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
6	Raisecom(config-port)#**mls qos cos-dei-remark** *profile-id*	Apply the local-to-CoS DEI mapping profile in physical layer interface configuration mode.
7	Raisecom(config-port)#**mls qos cos-dei-remark** *profile-id*	Apply the local-to-CoS DEI mapping profile to an interface.

10.1.9 Checking configurations

No.	Command	Description
1	Raisecom#**show mls qos** [*interface-type interface-list*]	Show global QoS configurations or QoS configurations on an interface.
2	Raisecom#**show mls qos cos-to-local-priority** *interface-type interface-list*	Show information about the CoS-to-local priority (color) mapping profile on an interface.
3	Raisecom#**show mls qos cos-dei-to-local-priority** *interface-type interface-list*	Show information about the CoS DEI-to-local priority (color) mapping profile on an interface.
4	Raisecom#**show mls qos dscp-to-local-priority** *interface-type interface-list*	Show information about the DSCP-to-local priority (color) mapping profile on an interface.
5	Raisecom#**show mls qos mapping cos-to-local-priority** [*profile-id*]	Show mapping from CoS priority to local priority (color).
6	Raisecom#**show mls qos mapping cos-dei-to-local-priority** [*profile-id*]	Show mapping from CoS DEI priority to local priority (color).
7	Raisecom#**show mls qos mapping dscp-to-local-priority** [*profile-id*]	Show mapping from DSCP priority to local priority (color).
8	Raisecom#**show mls qos mapping local-priority**	Show information about the local-to-queue mapping table.
9	Raisecom#**show mls qos dscp-mutation** *interface-type interface-number*	Show information about the DSCP remarking profile on an interface.
10	Raisecom#**show mls qos mapping dscp-mutation** [*profile-id*]	Show information about all/specified DSCP remarking profiles.
11	Raisecom#**show mls qos mapping cos-remark** [*profile-id*]	Show information about local-to-CoS mapping profiles.
12	Raisecom#**show mls qos mapping cos-dei-remark** [*profile-id*]	Show information about the CoS DEI remarking profile.

No.	Command	Description
13	Raisecom#**show mls qos cos-remark** *interface-type interface-number*	Show information about the local-to-CoS mapping profile on an interface.
14	Raisecom#**show mls qos cos-dei-remark** *interface-type interface-number*	Show information about the local-to-CoS DEI mapping profile on an interface.

10.2 Configuring priority mapping in MPLS network

10.2.1 Preparing for configurations

Scenario

The MPLS-TP QoS technology is used to ensure the instantaneity and integrity of services when the MPLS-TP network is overloaded or congested. In addition, it is used to ensure the whole MPLS-TP network to run efficiently.

On the RAX711-L, MPLS-TP QoS is mainly used to configure the EXP priorities of MPLS-TP packets or local priorities and then it performs QoS management (such as traffic classification, queue scheduling, and traffic policy) on MPLS-TP packets through basic QoS.

Prerequisite

- Connect the interface, configure its physical parameters, and make it Up at the physical layer.
- Complete basic network configurations of MPLS-TP.

10.2.2 Configuring priority mapping on Ingress node

When service packets of the user network enter the MPLS network through the Ingress node, you need to map priorities of packets to realize QoS management on them.

Configuring mapping between DSCP priority and local priority on ingress interface

For details, see section10.1.4 Configuring mapping from DSCP priority to local priority.

Configuring mapping between CoS priority and local priority on ingress interface

For details, see section 10.1.5 Configuring mapping from CoS priority to local priority.

Configuring EXP priority of MPLS packets on egress interface

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

Step	Command	Description
2	Raisecom(config)#**mls qos vc-id** *vc-id* **peer** *ip-address* **exp generation-mode { fixed | mapping }**	Set the EXP priority generation mode of the specified VC to **fixed** or **mapping**. By default, the EXP priority generation mode of all VCs is set to **mapping**.
3	Raisecom(config)#**mls qos vc-id** *vc-id* **peer** *ip-address* **exp** *exp* **[fixed]**	(Optional) configure the EXP priority of the specified VC. By default, the EXP priority of all VCs is set to 0.
4	Raisecom(config)#**mls qos mapping local-priority** *local-priority* **to { tunnel | vc } exp** *exp*	(Optional) map local priorities to EXP priorities of Tunnels or VCs.

10.2.3 Configuring priority mapping on Transit node

Configuring mapping between EXP priority and local priority (color)

On the Transit node, configure the mapping between EXP priorities of VCs and local priorities and between EXP priorities of VCs and color.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos mapping { tunnel | vc } exp** *exp* **to local-priority** *local-priority*	(Optional) map EXP priorities of Tunnels/VCs to local priorities.
3	Raisecom(config)#**mls qos mapping { tunnel | vc } exp** *exp* **to color { green | red | yellow }**	Map EXP priorities of Tunnels/VCs to the packet color. By default, all packets are mapped to green.

Configuring mapping between local priority and EXP priority

On the Transit node, configure the mapping between local priorities and EXP priorities of Tunnels/VCs.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos mapping local-priority** *local-priority* **to { tunnel | vc } exp** *exp*	(Optional) map the local priorities to EXP priorities of Tunnels/VCs.

10.2.4 Configuring priority mapping on Egress node

Configuring local priorities and color of packets on ingress interface

On the Egress node, double labels of the PLS packet are encapsulated to re-establish the service packet. By default, the EXP priority of the Tunnel label does not override the one of the VC label. Therefore, for the mapping from the EXP priority to the local priority, it is based on the EXP priority of the VC.

On the Egress node, configure the mapping between EXP priorities and local priorities and between EXP priorities and color.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos vc-id** *vc-id* **peer** *ip-address* **local-priority generation-mode** { **fixed** | **mapping** | **not-change** }	Set the local priority generation mode of the specified VC to **fixed** or **mapping**. By default, the local priority generation mode of all VCs is set to **mapping**.
3	Raisecom(config)#**mls qos vc-id** *vc-id* **peer** *ip-address* **local-priority** *local-priority* [**fixed**]	(Optional) configure the local priority of the specified VC.
4	Raisecom(config)#**mls qos mapping vc exp** *exp* **to local-priority** *local-priority*	(Optional) map EXP priorities of VCs to local priorities.
5	Raisecom(config)#**mls qos mapping vc exp** *exp* **to color** { **green** | **red** | **yellow** }	Map EXP priorities of VCs to the packet color. By default, all packets are mapped to green.

Configuring mapping between local priority and CoS priority on egress interface

For details, see section 10.1.7 Configuring mapping from local priority to CoS priority.

10.2.5 Checking configurations

No.	Command	Description
1	Raisecom#**show mls qos mapping** { **tunnel** | **vc** } **exp to color**	Show mapping between EXP priorities of Tunnels/VCs and packet color.
2	Raisecom#**show mls qos mapping** { **tunnel** | **vc** } **exp to local-priority**	Show mapping between EXP priorities of Tunnels/VCs and local priorities.
3	Raisecom#**show mls qos mapping local-priority to** { **tunnel** | **vc** } **exp**	Show mapping between local priorities and EXP priorities of Tunnels/VCs.

10.3 Configuring traffic classification and traffic policy

10.3.1 Preparing for configurations

Scenario

Traffic classification is the basis of QoS. For packets from upstream devices, you can classify them according to their priorities or 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

To perform traffic classification based on the priority of packets, you need to configure priority trust.

10.3.2 Creating and configuring traffic classification

Steps 4–9 are coordinate. You can select one as required.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos enable**	Enable global QoS. By default, the global QoS is enabled.
3	Raisecom(config)#**class-map** *class-map-name* { **match-all** | **match-any** }	Create traffic classification and enter traffic classification configuration mode.
4	Raisecom(config-cmap)#**match** { **access-list-map** | **ip-access-list** | **ipv6-access-list** | **mac-access-list** | **mac-ipv4-access-list** } *acl-number*	(Optional) configure traffic classification based on ACL rules. For configurations on ACL see section 9.1 Configuring ACL.
5	Raisecom(config-cmap)#**match cos** *cos-value*	(Optional) configure traffic classification based on CoS priority of VLAN packets.
6	Raisecom(config-cmap)#**match ip dscp** *dscp-value*	(Optional) configure traffic classification based on DSCP priority of IP packets.
7	Raisecom(config-cmap)#**match vlan** *vlan-id* [**double-tagging inner**]	(Optional) configure traffic classification based on VLAN ID of VLAN packets/inner VLAN ID of QinQ packets.
8	Raisecom(config-cmap)#**match inner-vlan** *vlan-id* **outer-vlan** *vlan-id*	(Optional) configure traffic classification based on the inner/outer VLAN ID of QinQ packets.
9	Raisecom(config-cmap)#**match class-map** *class-map-name*	(Optional) configure traffic classification based on the above traffic classification rules. The *class-map-name* parameter is the name of other created traffic classification.

10.3.3 Creating and configuring traffic policing profile

To perform traffic policing on packets, you need to configure traffic policing profile and then apply this profile to traffic classification bound to traffic policy. Therefore, you can perform related QoS policies on users/services.

On the traffic policing profile, you can configure rate limiting rules or perform relate operations on specified packets based on the color.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos policer-profile** *policer-name* [**aggregate** | **class** | **single**]	Create the traffic policing profile and enter traffic policing profile configuration mode.
3	Raisecom(traffic-policer)#**cir** *cir* **cbs** *cbs* [[**eir** *eir*] **ebs** *ebs* [**coupling**] | **pir** *pir* **pbs** *pbs*]	(Optional) configure rate limiting parameters on the traffic policing profile. You can select the working mode of the traffic policing profile as required. If you specify any optional parameter, the RAX711-L works in single traffic policing profile mode, where only red and green packets are supported. Otherwise, the RAX711-L works in dual traffic policing profile mode, where red, yellow, and green packets are supported.
4	Raisecom(traffic-policer)#**color-mode** { **aware** | **blind** }	(Optional) configure the color-mode of the traffic policing profile. By default, the traffic policing profile works in **blind** mode.
5	Raisecom(traffic-policer)#**recolor** { **green-recolor** { **red** | **yellow** } | **red-recolor** { **green** | **yellow** } | **yellow-recolor** { **green** | **red** } }	(Optional) configure re-coloring.
6	Raisecom(traffic-policer)#**drop-color** { **red** [**yellow**] | **yellow** }	(Optional) discard packets with specified color.
7	Raisecom(traffic-policer)#**set-cos** { **green** *cos-value* [**red** *cos-value* | **yellow** *cos-value* [**red** *cos-value*]] | **red** *cos-value* | **yellow** *cos-value* [**red** *cos-value*] }	(Optional) configure the mapping between packet color and CoS priority.
8	Raisecom(traffic-policer)#**set-dscp** { **green** *dscp-value* [**red** *dscp-value* | **yellow** *dscp-value* [**red** *dscp-value*]] | **red** *dscp-value* | **yellow** *dscp-value* [**red** *dscp-value*] }	(Optional) configure the mapping between packet color and DSCP priority.
9	Raisecom(traffic-policer)#**set-pri** { **green** *local-value* [**red** *local-value* | **yellow** *local-value* [**red** *local-value*]] | **red** *local-value* | **yellow** *local-value* [**red** *local-value*] }	(Optional) configure the mapping between packet color and local priority.

10.3.4 Creating and configuring traffic policy

Steps 6–12 are coordinate. You can select one as required.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**policy enable**	Enable traffic policy. By default, traffic policy is disabled.
3	Raisecom(config)#**policy-map** *policy-map-name*	Create a traffic policy and enter traffic policy configuration mode.
4	Raisecom(config-pmap)#**description** *string*	(Optional) configure descriptions about the traffic policy.
5	Raisecom(config-pmap)#**class-map** *class-map-name*	Bind the traffic classification to the traffic policy. Perform traffic policy on packets that match the traffic classification. **Note** To bind traffic classification to a traffic policy, you should create and configure traffic classification in advance. In addition, the created traffic classification must be based on at least one kind of rules. Otherwise, the binding operation fails.
6	Raisecom(config-pmap-c)#**police** *policer-name*	(Optional) apply the configured traffic policing profile under the traffic classification and limit the rate of traffic based on the rule configured in the traffic policing profile. For details about the traffic policing profile, see section 10.3.3 Creating and configuring traffic policing profile.
7	Raisecom(config-pmap-c)**add outer-vlan** *vlan-id*	(Optional) add the outer VLAN under the traffic classification.
8	Raisecom(config-pmap-c)#**redirect-to** *interface-type interface-number*	(Optional) configure redirection rules under traffic classification to forward matched packets from the specified interface.
9	Raisecom(config-pmap-c)#**set** { **cos** *cos-value* | **local-priority** *priority-value* | **inner-vlan** *inner-vlan-id* | **ip dscp** *ip-dscp-value* | **ip precedence** *ip-precedence-value* | **vlan** *vlan-id* }	(Optional) configure remarking rules under traffic classification to modify the CoS priority, local priority, inner VLAN ID, DSCP priority, and ToS priority of matched packets.
10	Raisecom(config-pmap-c)#**statistics enable**	(Optional) enable taking statistics of packets matched with the traffic classification. • If the rate limiting rules defined in the traffic policing profile is applied under the traffic classification, traffic statistics refer to counting green packets passed in the rate limiting rules. • If the traffic policing profile applied under the traffic classification does not define the rate limiting rules while defines other rules instead, traffic statistics refer to counting packets matching the traffic classification.

Step	Command	Description
11	Raisecom(config-pmap-c)#**hierarchy-police** *policer-name*	(Optional) bind hierarchical rate limiting rules under different traffic classification to control the total speed of packets in these traffic classifications.
12	Raisecom(config-pmap-c)#**copy-to-mirror**	Configure the mirroring feature of traffic to mirror matched packets to the monitor port.
13	Raisecom(config-pmap-c)#**exit**	Return to traffic policy configuration mode.
	Raisecom(config-pmap)#**exit**	Return to global configuration mode.
	Raisecom(config)#**service-policy** *policy-map-name* **ingress** *interface-type interface-number*	Apply the configured traffic policy to the ingress interface.

10.3.5 Creating and configuring hierarchical traffic policy

At present, the RAX711-L supports the hierarchical traffic policy based on:

- VLAN and VLAN+CoS
- Port and Port+VLAN

Creating and configuring hierarchical traffic policy based on VLAN and VLAN+CoS

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**cos-policy-map** *policy-map-name*	Create the traffic policy based on CoS and enter traffic policy configuration mode.
3	Raisecom(config-cos-pmap)#**car cir** *cir* **cbs** *cbs* **eir** *eir* **ebs** *ebs* [**coupling**] **cos** *cos-value*	Configure rate limiting parameters under the CoS-based traffic policy.
4	Raisecom(config-cos-pmap)#**hierarchy-car cir** *cir* **cbs** *cbs*	Configure hierarchical rate limiting rules for the CoS-based traffic policy.
5	Raisecom(config-cos-pmap)#**exit**	Return to global configuration mode.
6	Raisecom(config)#**service-policy** *policy-map-name* **ingress** *interface-type interface-number* **cos-policy** *vlan-id*	Apply the CoS-based traffic policy to the ingress direction of the specified VLAN on the interface.

Creating and configuring hierarchical traffic policy based on Port and Port+VLAN

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

Step	Command	Description
2	Raisecom(config)#**vlan-policy-map** *policy-map-name*	Create the traffic policy based on VLAN and enter traffic policy configuration mode.
3	Raisecom(config-vlan-pmap)#**car cir** *cir* **cbs** *cbs* **eir** *eir* **ebs** *ebs* [**coupling**] **vlan** *vlan-id*	Configure rate limiting parameters under the VLAN-based traffic policy.
4	Raisecom(config-vlan-pmap)#**hierarchy-car cir** *cir* **cbs** *cbs*	Configure hierarchical rate limiting rules for the VLAN-based traffic policy.
5	Raisecom(config-vlan-pmap)#**exit**	Return to global configuration mode.
6	Raisecom(config)#**service-policy** *policy-map-name* **ingress** *interface-type interface-number* **vlan-policy**	Apply the VLAN-based hierarchical traffic policy to the ingress interface.

10.3.6 Checking configurations

No.	Command	Description
1	Raisecom(config)#**show class-map** [*class-map-name*]	Show configurations on specified traffic classification rules.
2	Raisecom(config)#**show policy-map** [*policy-map-name* | **class** *class-map-name* | *interface-type interface-number*]	Show configurations on specified traffic policy.
3	Raisecom#**show mls qos policer-profile** [*policer-name*]	Show configurations on rate limiting rules or traffic policing profiles in QoS.
4	Raisecom#**show service-policy** *interface-type interface-list* [**cos-policy** *vlan-id* | **vlan-policy**]	Show information about the applied traffic policy.
5	Raisecom#**show service-policy statistics** [*interface-type interface-list*] [**cos-policy** *vlan-id* | **vlan-policy**]	Show statistics about applied policies.
6	Raisecom#**show mls qos** *interface-type interface-number* **policers**	Show configurations on rate limiting rules in QoS.
7	Raisecom#**show cos-policy-map** [*policy-map-name*]	Show information about the CoS-based traffic policy.
8	Raisecom#**show vlan-policy-map** [*policy-map-name*]	Show information about the VLAN-based traffic policy.

10.4 Configuring queue scheduling

10.4.1 Preparing for configurations

Scenario

When congestion occurs, you need to balance delay and jitter of packets, making packets of core services, such as video and voice services, processed first while packets of non-core services of the same priority, such as email, processed in a fair manner. Therefore, services of different priorities are processed according to the weights. This can be realized by configuring queue scheduling. The selection of scheduling algorithm depends on service types and users' requirements.

After queue scheduling, you can configure the mapping between local priority and CoS priority of packets. Therefore, packets enter downstream devices by carrying the specified CoS priority.

Prerequisite

To configure local priority and queue scheduling, you need to configure priority trust.

10.4.2 Configuring queue scheduling

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)#`**`mls qos queue scheduler sp`**	Set the scheduling mode to SP.

10.4.3 Configuring WRR/SP+WRR queue scheduling

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)#`**`mls qos queue scheduler wrr`**	Set the scheduling mode to WRR.
4	`Raisecom(config-port)#`**`mls qos queue wrr`** *`weight1 weight2 weight3 weight4 weight5 weight6 weight7 weight8`*	Set the scheduling mode to WRR and configure the weight for all queues. When the priority of some queue is set to 0, perform SP scheduling on the queue.

10.4.4 Configuring DRR/SP+DRR queue scheduling

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)#**mls qos queue scheduler drr**	Set the scheduling mode to DRR.
4	Raisecom(config-port)#**mls qos queue drr** *weight1 weight2 weight3 weight4 weight5 weight6 weight7 weight8*	Set the scheduling mode to DRR and configure priorities for all queues. When the priority of some queue is set to 0, perform SP scheduling on the queue.

10.4.5 Checking configurations

No.	Command	Description
1	Raisecom(config)#**show mls qos queue** [**shapping** | **wredprofile**] *interface-type interface-list*	Show queue scheduling configurations.
2	Raisecom#**show mls qos queue drop-pkts statistics** *interface-type interface-list*	Show statistics about lost packets of a queue on an interface.

10.5 Configuring congestion avoidance and queue shaping

10.5.1 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 RAX711-L 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 traffic shaping on the egress interface of upstream devices to shape upstream traffic.

Prerequisite

N/A

10.5.2 Configuring queue-based WRED

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos wred enable**	Enable WRED. By default, WRED is disabled.
3	Raisecom(config)#**mls qos wred profile** *profile-id*	Create the WRED profile and enter WRED profile configuration mode.
4	Raisecom(wred)#**wred** [**color** { **green** | **red** | **yellow** }] **start-drop-threshold** *start-drop* **end-drop-threshold** *end-drop* **max-drop-probability** *max-drop* Raisecom(wred)#**exit**	Configure the WRED profile and return to global configuration mode.
5	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
6	Raisecom(config-port)#**mls qos queue** *queue-id* **wredprofile** *wredprofile-num*	Apply the WRED profile to specified queues on an interface.
7	Raisecom(config-port)#**mls qos queue** *queue-id* **max-buffer** *length*	Configure the queue size on an interface.

10.5.3 Configuring queue shaping

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)#**mls qos queue** *queue-id* **shaping** *minband maxband*	(Optional) configure queue-based bandwidth guarantee without setting the EBS on an interface.
4	Raisecom(config-port)#**mls qos queue** *queue-id* **shaping cir** *minband* [**cbs** *minburst*] **eir** *maxband* [**ebs** *maxburst*]	(Optional) configure queue-based bandwidth guarantee with setting the EBS on an interface.

10.5.4 Checking configurations

No.	Command	Description
1	Raisecom#**show mls qos wred profile** [*profile-id*]	Show WRED profile configurations.
2	Raisecom#**show mls qos queue wredprofile** *interface-type interface-number*	Show WRED profile information on an interface.
3	Raisecom(config)#**show mls qos queue shaping** *interface-type interface-number*	Show queue shaping configurations on an interface.
4	Raisecom#**show mls qos queue max-buffer** *interface-type interface-number*	Show queue size configurations on an interface.

10.6 Configuring rate limiting based on interface, Tunnel, and PW

10.6.1 Preparing for configurations

Scenario

To avoid/remit network congestion, you can configure Level 3 rate limiting based on the interface, Tunnel, and PW. Rate limiting is used to make packets transmitted at a relative average speed by controlling the burst traffic on an interface, Tunnel, and PW.

Prerequisite

- To configure VLAN-based rate limiting, you need to create related VLANs.
- To configure Tunnel-based rate limiting, you need to create the static LSP and relate it to the Tunnel interface.
- To configure PW-based rate limiting, you need to create the static LSP.

10.6.2 Configuring interface-based rate limiting

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**rate-limit** *interface-type interface-list* { **both** | **egress** | **ingress** } *rate-value* [*burst-value*]	Configure interface-based rate limiting rules.

10.6.3 Configuring VLAN-based rate limiting

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**rate-limit vlan** *vlan-id rate-value burst-value* [**statistics**]	(Optional) configure VLAN-based rate limiting rules.

10.6.4 Configuring rate limiting based on interface+VLAN

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**rate-limit vlan** *vlan-id interface-type interface-list* { **both** | **egress** | **ingress** } **cir** *minband* **cbs** *minburst* [**eir** *maxband* **ebs** *maxburst*] [**statistics**]	Configure rate limiting rules based on interface+VLAN.

10.6.5 Configuring rate limiting based on interface+VLAN+CoS

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**rate-limit vlan** *vlan-id* **cos** *cos-value interface-type interface-list* **ingress cir** *cir* **cbs** *cbs* [**eir** *eir* **ebs** *ebs*] [**statistics**]	Configure rate limiting rules based on interface+VLAN+CoS.

10.6.6 Configuring rate limiting based on interface+VLAN+DSCP

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**rate-limit vlan** *vlan-id* **dscp** *dscp-value interface-type interface-list* **ingress cir** *cir* **cbs** *cbs* [**eir** *eir* **ebs** *ebs*] [**statistics**]	Configure rate limiting rules based on interface+VLAN+DSCP.

10.6.7 Configuring Tunnel-based rate limiting

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface tunnel** *tunnel-number*	Enter Tunnel interface configuration mode.
3	Raisecom(config-tunnelif)#**bandwidth cir** *cir* **pir** *pir*	Configure Tunnel-based rate limiting.

10.6.8 Configuring PW-based rate limiting

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)#**mpls static-l2vc** [**cvlan** *vlan-id* | **vlan** *vlan-id*] **destination** *ip-address* **raw vc-id** *vc-id* **vc-label** *vc-label* [**tunnel-policy** *policy-name* | **tunnel-interface** *tunnel-number*] [**priority** *priority*] [**no-control-word**] [**mtu** *mtu*] [**tpid** { **0x8100** | **0x9100** | **0x88a8** }] **bandwidth cir** *cir* **pri** *pri*	Create a PW and configure PW-based rate limiting. The PW is based on the RAW encapsulation mode and has identical incoming label value and outgoing label value.

Step	Command	Description
	Raisecom(config-port)#**mpls static-l2vc** { **cvlan** *vlan-id* | **vlan** *vlan-id* } **destination** *ip-address* **tagged vc-id** *vc-id* **vc-label** *vc-label* [**tunnel-policy** *policy-name* | **tunnel-interface** *tunnel-number*] [**priority** *priority*] [**no-control-word**] [**mtu** *mtu*] [**tpid** { **0x8100** | **0x9100** | **0x88a8** }] [**svlan** *vlan-id*] **bandwidth cir** *cir* **pri** *pri*	Create a PW and configure PW-based rate limiting. The PW is based on the Tagged encapsulation mode and has identical incoming label value and outgoing label value.
	Raisecom(config-port)#**mpls static-l2vc** [**cvlan** *vlan-id* | **vlan** *vlan-id*] **destination** *ip-address* **raw vc-id** *vc-id* **in-label** *in-label* **out-label** *out-label* [**tunnel-policy** *policy-name* | **tunnel-interface** *tunnel-number*] [**priority** *priority*] [**no-control-word**] [**mtu** *mtu*] [**tpid** { **0x8100** | **0x9100** | **0x88a8** }] **bandwidth cir** *cir* **pri** *pri*	Create a PW and configure PW-based rate limiting. The PW is based on the RAW encapsulation mode and has different incoming label value and outgoing label value.
	Raisecom(config-port)#**mpls static-l2vc** { **cvlan** *vlan-id* | **vlan** *vlan-id* } **destination** *ip-address* **tagged vc-id** *vc-id* **in-label** *in-label* **out-label** *out-label* [**tunnel-policy** *policy-name* | **tunnel-interface** *tunnel-number*] [**priority** *priority*] [**no-control-word**] [**mtu** *mtu*] [**tpid** { **0x8100** | **0x9100** | **0x88a8** }] [**svlan** *vlan-id*] **bandwidth cir** *cir* **pri** *pri*	Create a PW and configure PW-based rate limiting. The PW is based on the Tagged encapsulation mode and has different incoming label value and outgoing label value.

10.6.9 Checking configurations

No.	Command	Description
1	Raisecom#**show rate-limit** { *interface-type interface-list* | **port-channel** *port-channel-list* | **port-list** }	Show interface-based rate limiting configurations.
2	Raisecom#**show rate-limit vlan** [*vlan-id*]	Show VLAN-based rate limiting configurations.
3	Raisecom#**show rate-limit vlan-port** [**vlan** *vlan-id interface-type interface-list* { **both** | **egress** | **ingress** }] [**statistics**]	Show rate limiting configurations based on the interface+VLAN.
4	Raisecom#**show rate-limit vlan-cos-port** [**vlan** *vlan-id* **cos** *cos-value interface-type interface-list* **ingress**] [**statistics**]	Show rate limiting configurations based on interface+VLAN+CoS.
5	Raisecom#**show rate-limit vlan-dscp-port** [**vlan** *vlan-id* **dscp** *dscp-value interface-type interface-list* **ingress**] [**statistics**]	Show rate limiting configurations based on interface+VLAN+DSCP.

10.7 Configure hierarchical rate limiting

10.7.1 Preparing for configurations

Scenario

To ensure special services can transmit according to requirements when the network is blocked, you can configure the hierarchical rate limiting. Configure rate limiting profile and hierarchical bandwidth profile matching the packets with profiles to ensure normal transmission of the special services.

10.7.2 Configuring bandwidth guarantee

Configure bandwidth guarantee for the RAX700 as below.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**bandwidth enable**	Enter bandwidth guarantee.
3	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-port)#**bandwidth color-aware enable**	Configure color identification of the packets in the ingress direction of the interface.
4	Raisecom(config-port)#**bandwidth dei enable**	Configure color identification of the packets in the egress direction of the interface.

10.7.3 Configuring bandwidth profile

Configure bandwidth profile for the RAX700 as below.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**bandwidth enable**	Enter bandwidth guarantee.
3	Raisecom(config)#**bandwidth-profile** *index* **cir** *cir* **cbs** *cbs* [**color-aware**] Raisecom(config)#**bandwidth-profile** *index* **cir** *cir* **cbs** *cbs* **eir** *eir* **ebs** *ebs* [**color-aware** [**coupling**]]	Create bandwidth guarantee profile, and configure transmitting bandwidth rate.
4	Raisecom(config)#**bandwidth-profile** *bwp-index* **description** *string*	Configure description of bandwidth guarantee profile.
5	Raisecom(config)#**bandwidth ingress** { **client** *client-number* | **line** *line-number* | **port-channel** *port-channel-number* } *bwp-index* Raisecom(config)# **bandwidth egress** { **client** *client-number* | **line** *line-number* } *bwp-index*	Bind the bandwidth guarantee profile and interface.

Step	Configuration	Description
7	Raisecom(config)#**bandwidth ingress** { **client** *client-number* | **line** *line-number* | **port-channel** *port-channel-number* } **vlan** *vlan-id bwp-index*	(Optional) bind the bandwidth guarantee with interface and VLAN.
	Raisecom(config)#**bandwidth egress** { **client** *client-number* | **line** *line-number* } **vlan** *vlan-id bwp-index*	
9	Raisecom(config)#**bandwidth ingress** { **client** *client-number* | **line** *line-number* | **port-channel** *port-channel-number* } **vlan** *vlan-id* **coslist** *coslist bwp-index*	(Optional) bind the bandwidth guarantee with interface, VLAN, and CoS.
	Raisecom(config)#**bandwidth egress** { **client** *client-number* | **line** *line-number* } **vlan** *vlan-id* **coslist** *coslist bwp-index*	

10.7.4 Configuring hierarchical bandwidth profile

Configure hierarchical bandwidth profile for the RAX700 as below.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**hierarchy-cos bandwidth-profile** *hc-bwp-index*	Create CoS-based hierarchical bandwidth guarantee profile.
	Raisecom(config)#**hierarchy-vlan bandwidth-profile** *hv-bwp-index*	Create VLAN-based hierarchical bandwidth guarantee profile.
4	Raisecom(config-hcos/hvlan)#**description** *string*	Configure description of hierarchical bandwidth guarantee profile.
5	Raisecom(config-hcos)#**bandwidth coslist** *coslist index*	Bind the hierarchical bandwidth guarantee profile and the CoS.
	Raisecom(config- hvlan)#**bandwidth vlanlist** *vlanlist index*	Configure hierarchical bandwidth guarantee profile and VLAN.
	Raisecom(config-hcos/hvlan)#**bandwidth-profile** *index* **cir** *cir* **cbs** *cbs* [**color-aware**]	Configure hierarchical bandwidth garantee profile transmission rate.
	Raisecom(config-hcos/hvlan)#**bandwidth-profile** *index* **cir** *cir* **cbs** *cbs* **eir** *eir* **ebs** *ebs* [**color-aware** [**coupling**]]	
	Raisecom(config-hcos)#**exit** Raisecom(config)#**bandwidth ingress** { **client** *client-number* | **line** *line-number* | **port-channel** *port-channel-number* } **vlan** *vlan-id bwp-index* **hierarchy-cos** *hc-bwp-index*	Bind the CoS-based hierarchical bandwidth guarantee profile with interface, VLAN, and bandwidth guarantee profile.
	Raisecom(config-hvlan)#**exit** Raisecom(config)#**bandwidth ingress** { **client** *client-number* | **line** *line-number* | **port-channel** *port-channel-number* } *bwp-index* **hierarchy-vlan** *hv-bwp-index*	Bind the VLAN-based hierarchical bandwidth guarantee profile with interface and bandwidth guarantee profile.

10.7.5 Checking configurations

Use the following command to check configuration results.

No.	Configuration	Description
1	Raisecom#**show bandwidth** { **client** *client-number* | **line** *line-number* | **port-channel** *port-channel-number* }	Show the interface-based bandwidth guarantee profile.
2	Raisecom#**show bandwidth-profile** [*index*]	Show bandwidth guarantee profile configuration.
3	Raisecom#**show bandwidth-status** { **client** *client-number* | **line** *line-number* }	Show identification and tab of the packets on the bandwidth guarantee interface.
4	Raisecom#**show bandwidth** { **client** *client-number* | **line** *line-number* | **port-channel** *port-channel-number* } **vlan** [*vlan-id*]	Show the interface-based and VLAN-based bandwidth guarantee.
5	Raisecom#**show** { **hierarchy-cos-bandwidth** | **hierarchy-vlan-bandwidth** } **profile** [*index*]	Show CoS-based or VLAN-based bandwidth guarantee profile.

10.8 Maintenance

10.8.1 Maintaining QoS features

Command	Description
Raisecom(config)#**clear service-policy statistics**	Clear QoS packet statistics.
Raisecom(config)#**clear service-policy statistics** *interface-type interface-list*	Clear QoS packet statistics on an interface.
Raisecom(config)#**clear service-policy statistics ingress** *interface-type interface-list* [**class-map** *class-map-name*]	Clear traffic statistics in a specified traffic classification direction.
Raisecom(config)#**clear rate-limit statistics vlan** [*vlan-id*]	Clear VLAN-based rate limiting packet loss statistics.
Raisecom(config)#**clear rate-limit statistics vlan-port** [**vlan** *vlan-id interface-type interface-list* { **both** | **egress** | **ingress** }]	Clear rate limiting packet loss statistics based on interface+VLAN.
Raisecom(config)#**clear rate-limit statistics vlan-cos-port vlan** *vlan-id* **cos** *cos-value interface-type interface-list* **ingress**	Clear rate limiting packet loss statistics based on interface+VLAN+CoS.
Raisecom(config)#**clear rate-limit statistics vlan-dscp-port** [**vlan** *vlan-id* **dscp** *dscp-value interface-type interface-list* **ingress**]	Clear rate limiting packet loss statistics based on interface+VLAN+DSCP.

10.8.2 Configuring performance statistics

Configure performance states for the RAX700 as below.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)# **performance statistics file enable**	Enable the Flash data file being written in the device performance statistics.
	Raisecom(config)#**performance statistics** { *interface-type interface-number* | **management-port** } [**file**] **enable**	Enable Flash data file being written in the interface performance statistics.
3	Raisecom(config)#**performance statistics** { **longinterval** | **shortinterval** } **buckets** *buckets*	Configure the period data block of the performance statistics.
4	Raisecom(config-port)#**performance statistics file** { **longinterval** | **shortinterval** } **interface period** *period*	Configure the period of Flash data file being written in the performance statistics.

10.8.3 Checking configurations

Use the following command to check the configuration results.

No.	Configuration	Description
1	Raisecom#**show performance statistics**	Show global performance statistics.
2	Raisecom#**show performance statistics interface** { *interface-type interface-number* | **management-port** } { **current** | **history** }	Show the historical or present performance statistics.
3	Raisecom#**show performance statistics file**	Show performance statistics file.

10.9 Configuration examples

10.9.1 Example for configuring rate limiting based on traffic policy

Networking requirements

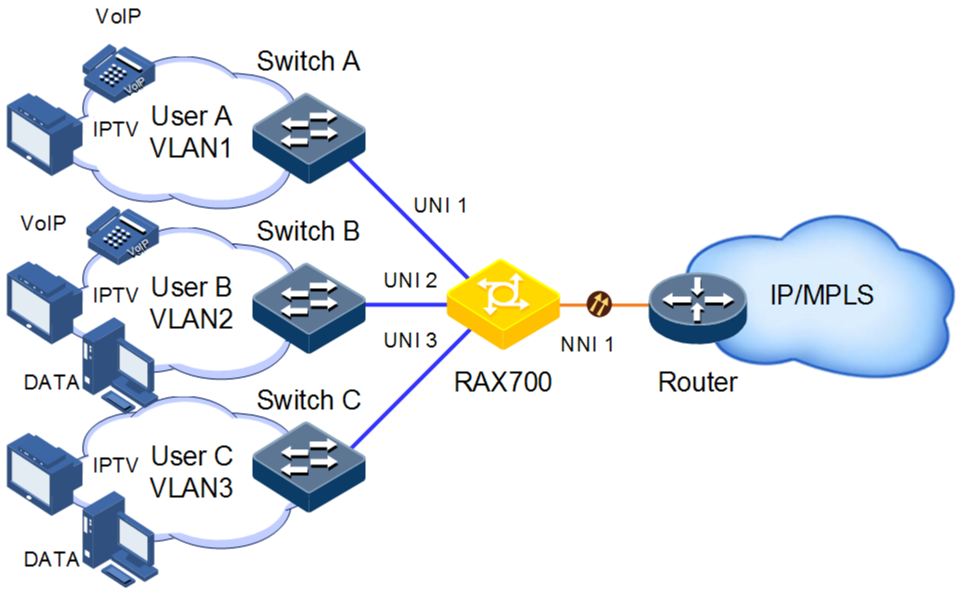
As shown in Figure 10-1, User A, User B, and User C are respectively within VLAN 1, VLAN 2, and VLAN 3. And they are respectively connected to the RAX711-L through Switch A, Switch B, and Switch C.

User A transmits voice and video services; User B transmits voice, video, and data services; User C transmits video and data services.

According to users' requirements, make following rules:

- For User A, provide 25 Mbit/s bandwidth; set the burst traffic to 100 kbit/s and discard the redundant traffic.
- For User B, provide 35 Mbit/s bandwidth; set the burst traffic to 100 kbit/s and discard the redundant traffic.
- For User C, provide 30 Mbit/s bandwidth; set the burst traffic to 100 kbit/s and discard the redundant traffic.

Figure 10-1 Configuring rate limiting based on traffic policy



Configuration steps

Step 1 Create and configure traffic classifications. Classify packets from different users based on the VLAN IDs.

```
Raisecom#config
Raisecom(config)#mls qos enable
Raisecom(config)#class-map usera match-any
Raisecom(config-cmap)#match vlan 1
Raisecom(config-cmap)#exit
Raisecom(config)#class-map userb match-any
Raisecom(config-cmap)#match vlan 2
Raisecom(config-cmap)#exit
Raisecom(config)#class-map userc match-any
Raisecom(config-cmap)#match vlan 3
Raisecom(config-cmap)#exit
```

Step 2 Create traffic policing profiles and configure rate limiting rules.

```
Raisecom(config)#mls qos policer-profile usera single
Raisecom(traffic-policer)#cir 25000 cbs 100
Raisecom(traffic-policer)#drop-color red
```

```
Raisecom(traffic-policer)#exit
Raisecom(config)#mls qos policer-profile userb single
Raisecom(traffic-policer)#cir 35000 cbs 100
Raisecom(traffic-policer)#drop-color red
Raisecom(traffic-policer)#exit
Raisecom(config)#mls qos policer-profile userc single
Raisecom(traffic-policer)#cir 30000 cbs 100
Raisecom(traffic-policer)#drop-color red
Raisecom(traffic-policer)#exit
```

Step 3 Create and configure traffic policies.

```
Raisecom(config)#policy-map usera
Raisecom(config-pmap)#class-map usera
Raisecom(config-pmap-c)#hierarchy-police usera
Raisecom(config-pmap-c)#exit
Raisecom(config-pmap)#exit
Raisecom(config)#service-policy usera ingress uni 1
Raisecom(config)#policy-map userb
Raisecom(config-pmap)#class-map userb
Raisecom(config-pmap-c)#hierarchy-police userb
Raisecom(config-pmap-c)#exit
Raisecom(config-pmap)#exit
Raisecom(config)#service-policy userb ingress uni 2
Raisecom(config)#policy-map userc
Raisecom(config-pmap)#class-map userc
Raisecom(config-pmap-c)#hierarchy-police userc
Raisecom(config-pmap-c)#exit
Raisecom(config-pmap)#exit
Raisecom(config)#service-policy userc ingress uni 3
Raisecom(config)#policy enable
```

Step 4 Save configurations.

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

Checking results

Use the **show class-map** command to show traffic classification configurations.

```
Raisecom#show class-map usera
Class Map match-any usera (id 0)
    Match vlan 1
Raisecom#show class-map userb
Class Map match-any userb (id 1)
    Match vlan 2
Raisecom#show class-map userc
```

```
Class Map match-any userc (id 2)
    Match vlan 3
```

Use the **show mls qos policer** command to show rate limiting rule configurations.

```
Raisecom#show mls qos uni 1 policers
port: uni1
policymap name: usera
policer type: Single, name: usera
cir: 25000 kbps, cbs: 100 kB,
Raisecom(config)#show mls qos uni 2 policers
port: uni2
policymap name: userb
policer type: Single, name: userb
cir: 35000 kbps, cbs: 100 kB,
Raisecom(config)#show mls qos  uni 3 policers
port: uni3
policymap name: userc
policer type: Single, name: userc
cir: 30000 kbps, cbs: 100 kB,
```

Use the **show policy-map** command to show traffic policy configurations.

```
Raisecom(config)#show policy-map usera
  Policy Map usera
    Class-map usera
        hierarchy-policer usera
Raisecom(config)#show policy-map userb
  Policy Map userb
    Class-map userb
        hierarchy-policer userb
Raisecom(config)#show policy-map userc
  Policy Map userc
    Class-map userc
        hierarchy-policer userc
```

10.9.2 Example for configuring queue scheduling and congestion avoidance

Networking requirements

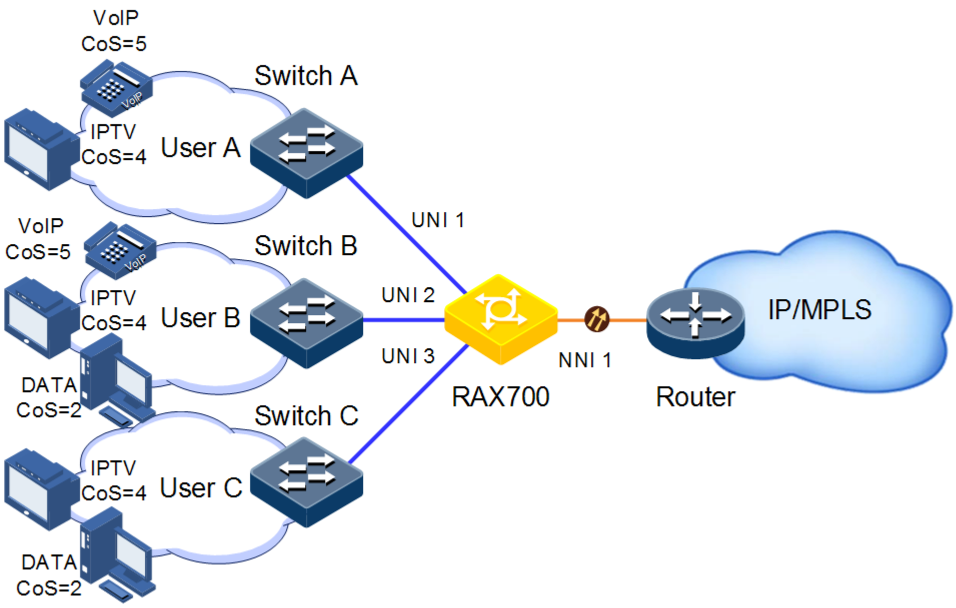
As shown in Figure 10-2, User A transmits voice and video services; User B transmits voice, video, and data services; User C transmits video and data services.

CoS priorities for voice, video and data services are configured with 5, 4, and 2 respectively. And these three CoS priorities are mapped to local priorities 6, 5, and 2 respectively.

Make following rules based on service types.

- Perform SP scheduling on voice service to ensure that the traffic is first transmitted.
- Perform WRR scheduling on video service and set the weight to 50.
- Perform WRR scheduling on data service and set the weight to 20. In addition, you need to set the drop threshold to 50 to avoid network congestion caused by too large burst traffic.

Figure 10-2 Configuring queue scheduling



Configuration steps

Step 1 Create the WRED profile.

```
Raisecom#config
Raisecom(config)#mls qos wred enable
Raisecom(config)#mls qos wred profile 1
Raisecom(wred)#wred start-drop-threshold 50 end-drop-threshold 90 max-drop-probability 60
Raisecom(wred)#exit
```

Step 2 Configure the priority trust and congestion avoidance on interfaces.

```
Raisecom#config
Raisecom(config)#mls qos enable
Raisecom(config)#interface uni 1
Raisecom(config-port)#mls qos trust cos
Raisecom(config-port)#mls qos queue 6 wredprofile 1
Raisecom(config-port)#mls qos queue 5 wredprofile 1
Raisecom(config-port)#mls qos queue 2 wredprofile 1
Raisecom(config-port)#exit
Raisecom(config)#interface uni 2
Raisecom(config-port)#mls qos trust cos
```

```
Raisecom(config-port)#mls qos queue 6 wredprofile 1
Raisecom(config-port)#mls qos queue 5 wredprofile 1
Raisecom(config-port)#mls qos queue 2 wredprofile 1
Raisecom(config-port)#exit
Raisecom(config)#interface uni 3
Raisecom(config-port)#mls qos trust cos
Raisecom(config-port)#mls qos queue 6 wredprofile 1
Raisecom(config-port)#mls qos queue 5 wredprofile 1
Raisecom(config-port)#mls qos queue 2 wredprofile 1
Raisecom(config-port)#exit
```

Step 3 Configure the mapping between the CoS priority and local priority.

```
Raisecom(config)#mls qos mapping cos-to-local-priority 1
Raisecom(cos-to-pri)#cos 5 to local-priority 6
Raisecom(cos-to-pri)#cos 4 to local-priority 5
Raisecom(cos-to-pri)#cos 2 to local-priority 2
Raisecom(cos-to-pri)#exit
Raisecom(config)#interface uni 1
Raisecom(config-port)#mls qos cos-to-local-priority 1
Raisecom(config-port)#interface uni 2
Raisecom(config-port)#mls qos cos-to-local-priority 1
Raisecom(config-port)#interface uni 3
Raisecom(config-port)#mls qos cos-to-local-priority 1
Raisecom(config-port)#exit
```

Step 4 Configure SP+WRR queue scheduling.

```
Raisecom(config)#interface uni 1
Raisecom(config-port)#mls qos queue scheduler wrr
Raisecom(config-port)#mls qos queue wrr 1 1 20 1 1 50 0 0
Raisecom(config)#exit
Raisecom(config)#interface uni 2
Raisecom(config-port)#mls qos queue scheduler wrr
Raisecom(config-port)#mls qos queue wrr 1 1 20 1 1 50 0 0
Raisecom(config)#interface uni 3
Raisecom(config-port)#mls qos queue scheduler wrr
Raisecom(config-port)#mls qos queue wrr 1 1 20 1 1 50 0 0
```

Step 5 Save configurations.

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

Checking results

Use the **show mls qos mapping cos-to-local-priority** command to show mapping configurations on specified priorities.

```
Raisecom(config)#show mls qos mapping cos-to-local-priority
G:GREEN
Y:Yellow
R:RED
cos-to-localpriority(color)
Index Description   CoS:      0     1     2     3     4     5     6     7
--------------------------------------------------------------------
1  localpri(color) :0(G)   1(G)   2(G)   3(G)   5(G)   6(G)   6(G)   7(G)
```

Use the **show mls qos queue** command to show queue scheduling configurations.

```
Raisecom#show mls qos queue uni 1
uni1
Queue    Weight(WRR)
-------------------------
  1      1
  2      1
  3      20
  4      1
  5      1
  6      50
  7      0
  8      0
Queue    Weight(DRR)
-------------------------
  1      1
  2      1
  3      1
  4      1
  5      1
  6      1
  7      1
  8      1
```

Use the **show mls qos wred profile** command to show WRED profile configurations.

```
Raisecom#show mls qos wred profile
GSDT:Green Start Drop Threshold
GEDT:Green End Drop Threshold
GDP:Green Drop Probability
YSDT:Yellow Start Drop Threshold
YEDT:Yellow End Drop Threshold
YDP:Yellow Drop Probability
RSDT:Red Start Drop Threshold
```

```
REDT:Red End Drop Threshold
RDP:Red Drop Probability
Index Description     GSDT     GEDT     GDP      YSDT     YEDT     YDP
RSDT      REDT      RDP
--------------------------------------------------------------------
1                   50       90       60       50       90       60       50
90        60
```

10.9.3 Example for configuring interface-based rate limiting

Networking requirements

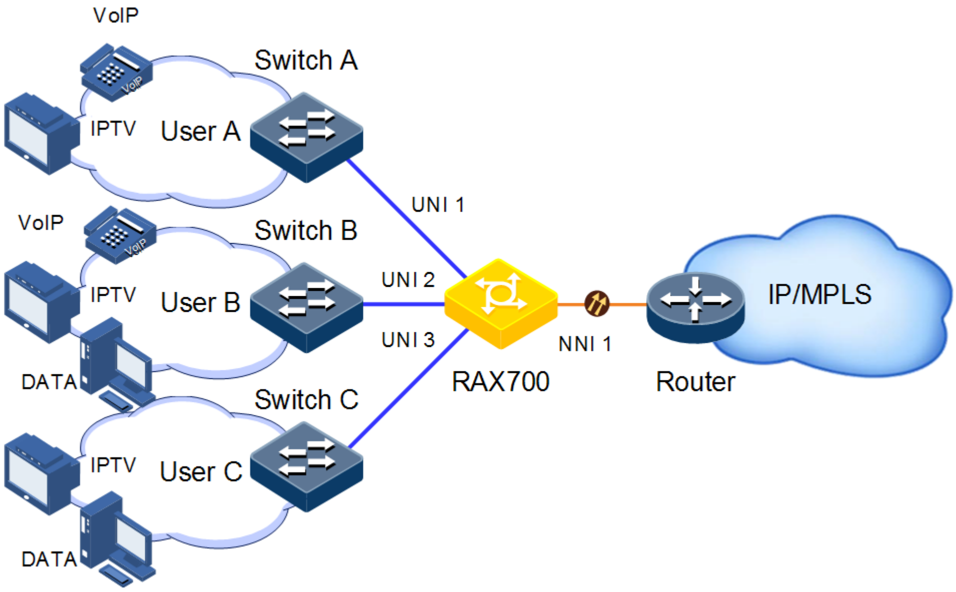
As shown in Figure 10-3, User A, User B, and User C are connected to the RAX711-L through Switch A, Switch B, and Switch C.

User A transmits voice and video services; User B transmits voice, video, and data services; User C transmits video and data services.

According to users' requirements, make following rules:

- For User A, provide 25 Mbit/s bandwidth; set the burst traffic to 100 kbit/s and discard the redundant traffic.
- For User B, provide 35 Mbit/s bandwidth; set the burst traffic to 100 kbit/s and discard the redundant traffic.
- For User C, provide 30 Mbit/s bandwidth; set the burst traffic to 100 kbit/s and discard the redundant traffic.

Figure 10-3 Configuring interface-based rate limiting



Configuration steps

Step 1 Configure interface-based rate limiting.

```
Raisecom#config
Raisecom(config)#rate-limit uni 1 ingress 25000 100
Raisecom(config)#rate-limit uni 2 ingress 35000 100
Raisecom(config)#rate-limit uni 3 ingress 30000 100
```

Step 2 Save configurations.

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

Checking results

Use the **show rate-limit port-list** command to show interface-based rate limiting configurations.

```
Raisecom#show rate-limit port-list
I-Rate:  Ingress Rate
I-Burst: Ingress Burst
E-Rate:  Egress Rate
E-Burst: Egress Burst

Port    I-Rate(kbps)  I-Burst(kB)  E-Rate(kbps)  E-Burst(kB)
----------------------------------------------------------------
N1       1000000          512       1000000          512
N2       1000000          512       1000000          512
U1       25000            100       1000000          512
U2       35000            100       1000000          512
U3       30000            100       1000000          512
U4       1000000          512       1000000          512
```

11 Multicast

This chapter describes basic principle and configuration of multicast and provides related configuration examples, including the following sections:

- Overview
- IGMP basis
- Configuring IGMP Snooping
- Configuring IGMP filtering
- Configuration examples

11.1 Overview

With the continuous development of Internet, more and more various interactive data, voice, and video emerge on the network. On the other hand, the emerging e-commerce, online meetings, online auctions, video on demand, remote learning, and other services also rise gradually. These services come up with higher requirements for network bandwidth, information security, and paid feature. Traditional unicast and broadcast cannot meet these requirements well, while multicast has met them timely.

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

Comparison among unicast, broadcast, and multicast

Multicast is a kind of packets transmission method which is parallel with unicast and broadcast.

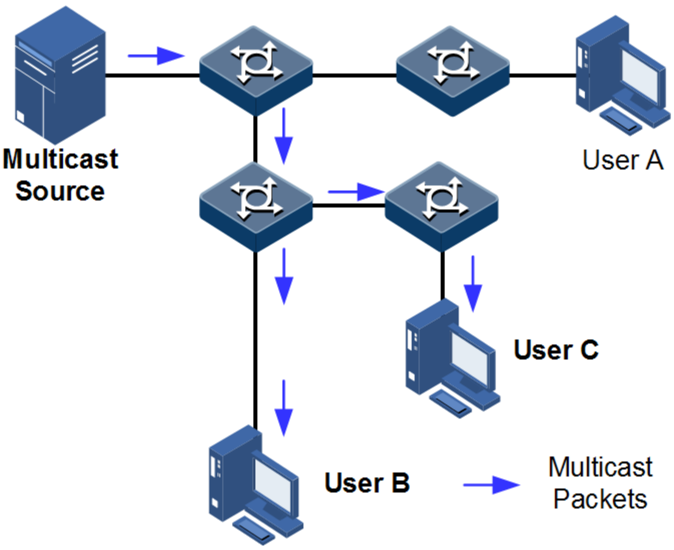
- Unicast: the system establishes a data transmission path for each user who needs the information, and sends separate copy information about them. Through unicast, the amount of information transmitted over the network is proportional to the number of users, so when the number of users becomes huge, there will be more identical information on the network. In this case, bandwidth will become an important bottleneck, and unicast will not be conducive to large-scale information transmission.
- Broadcast: the system sends information to all users regardless of whether they need or not, so any user will receive it. Through broadcast, the information source delivers information to all users in the network segment, which fails to guarantee information

security and paid service. In addition, when the number of users who require this kind of information decreases, the utilization of network resources will be very low, and the bandwidth will be wasted seriously.

- Multicast: when some users in the network need specific information, the sender only sends one piece of information, then the transmitted information can be reproduced and distributed in fork junction as far as possible.

As shown in Figure 11-1, assume that User B and User C need information, you can use multicast transmission to combine User B and User C to a receiver set, then the information source just needs to send one piece of information. Each switch on the network will establish their multicast forwarding table according to IGMP packets, and finally transmits the information to the actual receiver User B and User C.

Figure 11-1 Multicast transmission networking



In summary, the unicast is for a network with sparse users and broadcast is for a network with dense users. When the number of users in the network is uncertain, unicast and broadcast will present low efficiency. When the number of users are doubled and redoubled, the multicast mode does not need to increase backbone bandwidth, but sends information to the user in need. These advantages of multicast make itself become a hotspot in study of the current network technology.

Advantages and application of multicast

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

- Improve efficiency: reduce network traffic, relieve server and CPU load.
- Optimize performance: reduce redundant traffic and guarantee information security.
- Support distributed applications: solve the problem of point-point data transmission.

The multicast technology is used in the following aspects:

- Multimedia and streaming media, such as, network television, network radio, and real-time video/audio conferencing
- Training, cooperative operations communications, such as: distance education, telemedicine
- Data warehousing, financial applications (stock)

- Any other "point-to-multipoint" applications

Basic concepts in multicast

- Multicast group

A multicast group refers to the recipient set using the same IP multicast address identification. Any user host (or other receiving device) will become a member of the group after joining the multicast group. They can identify and receive multicast data with the destination address as IP multicast address.

- Multicast group members

Each host joining a multicast group will become a member of the multicast group. Multicast group members are dynamic, and hosts can join or leave multicast group at any time. Group members may be widely distributed in any part of the network.

- Multicast source

A multicast source refers to a server which regards multicast group address as the destination address to send IP packet. A multicast source can send data to multiple multicast groups; multiple multicast sources can send to a multicast group.

- Multicast router

A multicast router is a router that supports Layer 3 multicast. The multicast router can achieve multicast routing and guide multicast packet forwarding, and provide multicast group member management to distal network segment connecting with users.

- Router interface

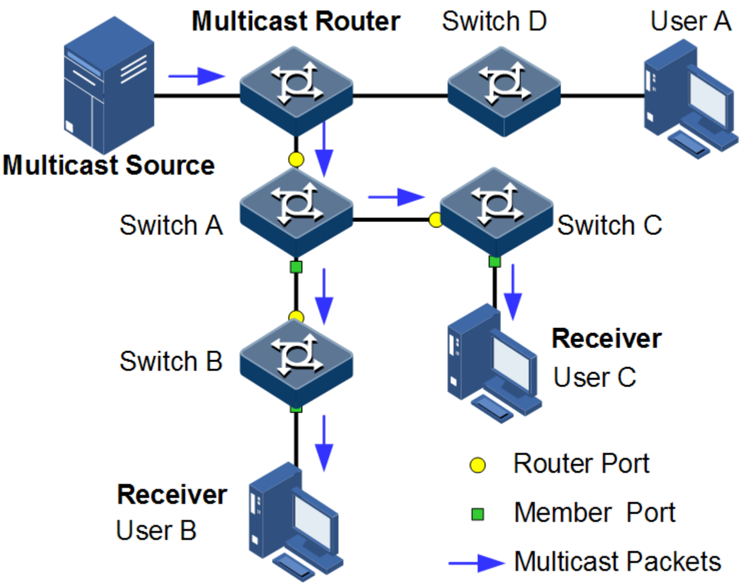
A router interface refers to the interface toward multicast router between a multicast router and a host. The RAX700 receives multicast packets from this interface.

- Member interface

Known as the receiving interface, a member interface is the interface towards the host between multicast router and the host. The RAX700 sends multicast packets from this interface.

Figure 11-2shows basic concepts in multicast.

Figure 11-2 Basic concepts in multicast



Multicast address

To make multicast source and multicast group members communicate across the Internet, you need to provide network layer multicast address and link layer multicast address, namely, the IP multicast address and multicast MAC address.

- IP multicast address

Internet Assigned Numbers Authority (IANA) assigns Class D address space to IPv4 multicast; the IPv4 multicast address ranges from 224.0.0.0 to 239.255.255.255.

- Multicast MAC address

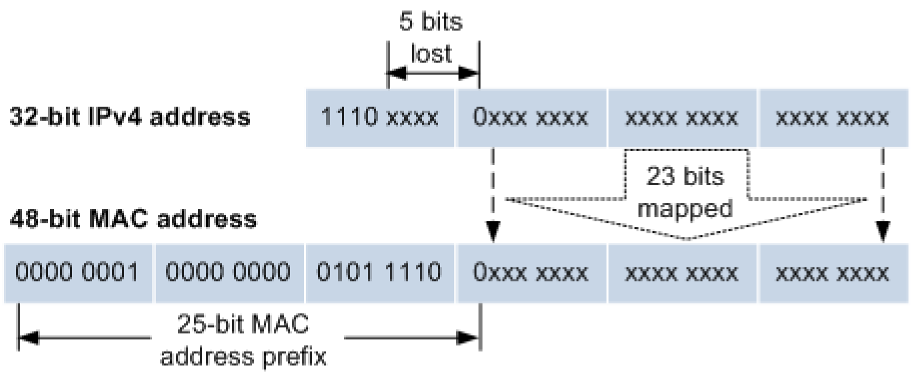
When the Ethernet transmits unicast IP packets, it uses the MAC address of the receiver as the destination MAC address. However, when multicast packets are transmitted, the destination is no longer a specific receiver, but a group with an uncertain number of members, so the Ethernet needs to use the multicast MAC address.

The multicast MAC address identifies receivers of the same multicast group on the link layer.

According to IANA, high bit 24 of the multicast MAC address are 0x01005E, bit 25 is fixed to 0, and the low bit 23 corresponds to low bit 23 of the IPv4 multicast address.

Figure11-3 shows mapping between the IPv4 multicast address and MAC address

Figure 11-3 Mapping between IPv4 multicast address and multicast MAC address



The first 4 bits of IP multicast address are 1110, indicating multicast identification. In the last 28 bits, only 23 bits are mapped to the multicast MAC address, and the missing of 5 bits makes 32 IP multicast addresses mapped to the same multicast MAC address. Therefore, in Layer 2, the RAX700 may receive extra data besides IPv4 multicast group, and these extra multicast data needs to be filtered by the upper layer on the RAX700.

11.2 IGMP basis

11.2.1 Introduction

The concepts related to IGMP basic functions are as below.

- Multicast router interface

The router interface can be learnt dynamically (learnt through IGMP query packets, on the condition that the multicast routing protocol is enabled on multicast routers) on Layer 2 multicast switch, or set manually to forward downstream multicast report and leave packets to the router interface.

The router interface learnt dynamically has an aging time, while the router interface configured manually will not be aged.

- Aging time

The configured aging time takes effect on both multicast forwarding entries and the router interface.

On Layer 2 switch running multicast function, each router interface learnt dynamically starts a timer, of which the expiration time is the aging time of IGMP Snooping. The router interface will be deleted if no IGMP Query packets are received in the aging time. The timer of the router interface will be updated when an IGMP Query packet is received.

Each multicast forwarding entry starts a timer, namely, the aging time of a multicast member. The expiration time is IGMP Snooping aging time. The multicast member will be deleted if no IGMP Report packets are received in the aging time. Update timeout for multicast forwarding entry when receiving IGMP Report packets. The timer of the multicast forwarding entry will be updated when an IGMP Report packet is received.

- Immediate leaving

On Layer 2 switch running multicast function, the system will not delete the corresponding multicast forwarding entry immediately, but wait until the entry is aged after sending Leave packets. Enable this function to delete the corresponding multicast forwarding entry quickly when there are a large number of downstream users and adding or leaving is more frequently required.

Note

Only IGMPv2/v3 version supports immediate leaving.

IGMP ring network forwarding:

- On Layer 2 switch running multicast function, IGMP ring network forwarding can be enabled on any type of interfaces.
- Enabling IGMP ring network forwarding can implement multicast backup protection on the ring network, make multicast services more stable, and prevent link failure from causing multicast service failure.
- IGMP ring network forwarding can be applied to the Ethernet ring, STP/RSTP/MSTP ring, and G.8032 ring, etc.

11.2.2 Configuring preparatons

Scenario

Basic functions of Layer 2 multicast provide Layer 2 multicast common features, which must be used on the RAX700 enabled with IGMP Snooping or IGMP MVR

Reprequisite

Before configuring multicast basis, finish the following issues.

- Create VLAN.
- Access the corresponding interface to VLAN.

11.2.3 Configuring basic IGMP functions

Configure basic IGMP functions for the RAX700 as below.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**igmp mrouter vlan** *vlan-id interface-type interface-number*	(Optional) configure multicast route interface.
3	Raisecom(config)#**igmp immediate-leave** *interface-type interface-number* **vlan** *vlan-list*	(Optional) configure immediate leaving on the interface+VLAN. By default, it is disabled.
4	Raisecom(config)#**igmp timeout** { *period* | **infinite** }	(Optional) configure the aging time of multicast forwarding entries. The aging time configured takes effect on all dynamically learnt router interfaces and multicast forwarding entries. By default, it is 300s.

Step	Configuration	Description
5	Raisecom(config)#**igmp ring** *interface-type interface-number-list*	(Optional) enable IGMP ring network forwarding on the interface. By default, it is disabled.
6	Raisecom(config)#**mac-address-table static multicast** *mac-address* **vlan** *vlan-id interface-type interface-number-list*	(Optional) configure the interface to join static multicast group. An interface is added to the multicast group through the IGMP Report packet send by a host. You can also manually add it to a multicast group.

11.2.4 Checking configurations

Use the following command to check the configuration results.

No.	Configuration	Description
1	Raisecom#**show igmp mrouter**	Show configurations of the multicast route interface.
2	Raisecom#**show igmp immediate-leave** [*interface-type interface-number*]	Show configuration of immediate leaving on Layer 2 multicast.
3	Raisecom#**show igmp statistics** [*interface-type interface-number*]	Show Layer 2 multicast statistics.

11.2.5 Maintenance

Maintain the IGMP features as below.

Configuration	Description
Raisecom(config)#**clear igmp statistics** [*interface-type interface-number*]	Clear Layer 2 multicast statistics of the IGMP.
Raisecom(config)#**no igmp member** *interface-type interface-number*	Delete transmission entries of the specified multicast.

11.3 IGMP Snooping

11.3.1 Introduction

IGMP Snooping is a multicast constraining mechanism running on Layer 2 devices, used for managing and controlling multicast groups, and implementing Layer 2 multicast.

IGMP Snooping allows the RAX700 to monitor IGMP session between the host and multicast router. When monitoring a group of IGMP Report from host, the RAX700 will add host-related interface to the forwarding entry of this group. Similarly, when a forwarding entry reaches the aging time, the RAX700 will delete host-related interface from forwarding entry.

IGMP Snooping forwards multicast data through Layer 2 multicast forwarding entry. When receiving multicast data, the RAX700 will forward them directly according to the corresponding receiving interface of the multicast forwarding entry, instead of flooding them to all interfaces, to save bandwidth of the RAX700 effectively.

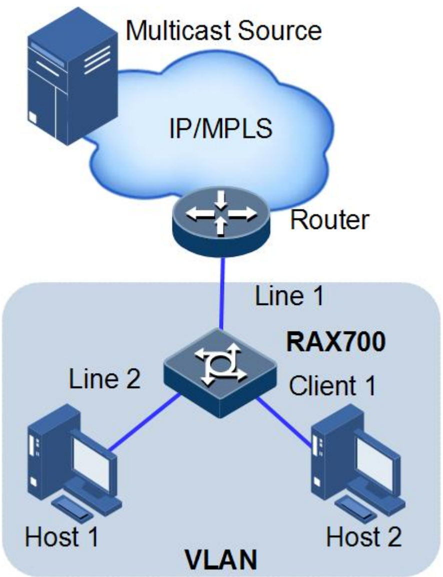
IGMP Snooping establishes a Layer 2 multicast forwarding table, of which entries can be learnt dynamically or configured manually.

11.3.2 Preparing for configurations

Scenario

As shown in Figure 11-4, multiple hosts belonging to a VLAN receive data from the multicast source. Enable IGMP Snooping on the Switch that connects the multicast router and hosts. By listening IGMP packets transmitted between the multicast router and hosts, creating and maintaining the multicast forwarding table, you can implement Layer 2 multicast.

Figure 11-4 Application scenario of IGMP Snooping



Prerequisite

Before configuring IGMP Snooping, finish the following issues.

- Disable multicast VLAN copy on the RAX700.
- Create a VLAN, and add related interfaces to the VLAN.

11.3.3 Configuring IGMP Snooping

Configure IGMP Snooping for the RAX700 as below.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**igmp snooping**	Enable global IGMP Snooping.
3	Raisecom(config)#**igmp snooping vlan** *vlan-list*	Enable VLAN IGMP Snooping.
4	Raisecom(config)#**mac-address-table static multicast** *mac-address* **vlan** *vlan-id* { *interface-type interface-list* | **port-channel** *port-channel-list* }	(Optional) configure the static multicast forwarding table. An interface is added to the multicast group through the IGMP Report packet send by a host. You can also manually add it to a multicast group.

11.3.4 Checking configurations

Use the following command to check the configuration results.

No.	Configuration	Description
1	Raisecom#**show igmp snooping vlan** *vlan-list*	Show configurations of IGMP Snooping.
2	Raisecom#**show igmp snooping member** [*interface-type interface-number* | **vlan** *vlan-id*]	Show information about multicast group members of IGMP Snooping.

11.4 Configuring IGMP filtering

11.4.1 Introduction

To control user access, you can set IGMP filtering. IGMP filtering contains the range of accessible multicast groups passing filtering rules and the maximum number of groups.

- IGMP filtering rules

To ensure information security, the administrator needs to limit the multicast users, such as what multicast data are allowed to receive and what are not.

Configure IGMP Profile filtering rules to control the interface. One IGMP Profile can be set one or more multicast group access control restrictions and access the multicast group according to the restriction rules (**permit** and **deny**). If a rejected IGMP Profile filter profile is applied to the interface, the interface will discard the IGMP report packet from this group directly once receiving it and does not allow receiving this group of multicast data.

IGMP filtering rules can be configured on an interface or VLAN.

IGMP Profile only applies to dynamic multicast groups, but not static ones.

- Limit to the maximum number of multicast groups

The maximum allowed adding number of multicast groups and the maximum group limitation rule can be set on an interface or interface+VLAN.

The maximum group limitation rule sets the actions for reaching the maximum number of multicast group users added, which can be no longer allowing user adding groups, or covering the original adding group.

Note

IGMP filtering is usually used with IGMP Snooping.

11.4.2 Preparing for configurations

Scenario

Different users in the same multicast group receive different multicast requirements and permissions, and allow configuring filtering rules on the switch which connects multicast router and user host to restrict multicast users.

The maximum number of multicast groups allowed for users to join can be set.

IGMP filtering is used in cooperation with IGMP Snooping or IGMP MVR.

Prerequisite

Before configuring IGMP filtering, finish the following issues.

- Create a VLAN.
- Add related interfaces to the VLAN.

11.4.3 Enabling global IGMP filtering

Configure global IGMP filtering for the RAX700 as below.

Step	Configuration	Description
1	`Raisecom#`**`config`**	Enter global configuration mode
2	`Raisecom(config)#`**`igmp filter`**	Enable global IGMP filtering. By default, it is disabled.

11.4.4 Configuring IGMP filtering profile

IGMP filtering rules can be used on an interface or on the interface+VLAN.

Configure the IGMP filter profile for the RAX700 as below.

Step	Configuration	Description
1	`Raisecom#`**`config`**	Enter global configuration mode
2	`Raisecom(config)#`**`igmp filter profile`** *`profile-number`*	Create IGMP Profile and enter Profile configuration mode.

Step	Configuration	Description
3	Raisecom(config-igmp-profile)#**permit** | **deny**	Configure IGMP Profile action.
4	Raisecom(config-igmp-profile)#**range** *range-id start-ip-address* [*end-ip-address*]	Configure to control IP multicast address access and range.
5	Raisecom(config-igmp-profile)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode or LAG configuration mode.
6	Raisecom(config-port)#**igmp filter profile** *profile-number* [**vlan** *vlan-list*]	Configure IGMP Profile filter profile to physical interface or interface+VLAN.
	Raisecom(config-aggregator)#**igmp filter profile** *profile-number* [**vlan** *vlan-list*]	Configure IGMP Profile filter profile to LAG interface or interface+VLAN.

Note

Perform the command of **igmp filter profile** *profile-number* in interface configuration mode to make the created IGMP Profile apply to the specified interface. One IGMP Profile can be applied to multiple interfaces, but each interface can have only one IGMP Profile.

11.4.5 Configuring maximum number of multicast groups

Users can add the maximum number of multicast groups applied to interface or interface+VLAN.

Configure maximum number of multicast groups for the RAX700 as below.

Step	Configuration	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode or LAG configuration mode.
3	Raisecom(config-port)#**igmp filter max-groups** *group-number* [**vlan** *vlan-list*]	Configure the maximum number of multicast groups to physical interface or interface+VLAN. By default, physical interface and interface+VLAN both have not the maximum number of multicast groups.
	Raisecom(config-aggregator)#**igmp filter max-groups** *group-number* [**vlan** *vlan-list*]	Configure the maximum number of multicast groups to LAG interface or interface+VLAN. By default, LAG interface and interface+VLAN both have not the maximum number of multicast groups.

Step	Configuration	Description
4	Raisecom(config-port)#**igmp filter max-groups action** { **drop** | **replace** } [**vlan** *vlan-list*]	(Optional) configure the action to take when the number of physical interfaces or interface+VLANs exceeds the maximum number of multicast groups. By default, it is drop.
	Raisecom(config-aggregator)#**igmp filter max-groups action** { **drop** | **replace** } [**vlan** *vlan-list*]	(Optional) configure the action to take when the number of LAG interfaces or interface+VLANs exceeds the maximum number of multicast groups. By default, it is drop.

11.4.6 Checking configurations

Use the following command to check the configuration results.

No.	Configuration	Description
1	Raisecom#**show igmp filter** [**interface** | *interface-type interface-number* [**vlan** *vlan-id*]]	Show configuration of IGMP filtering.
2	Raisecom#**show igmp filter profile** [*profile-number*]	Show IGMP Profile.

11.5 Configuration examples

11.5.1 Example for applying multicast on ring network

Networking requirements

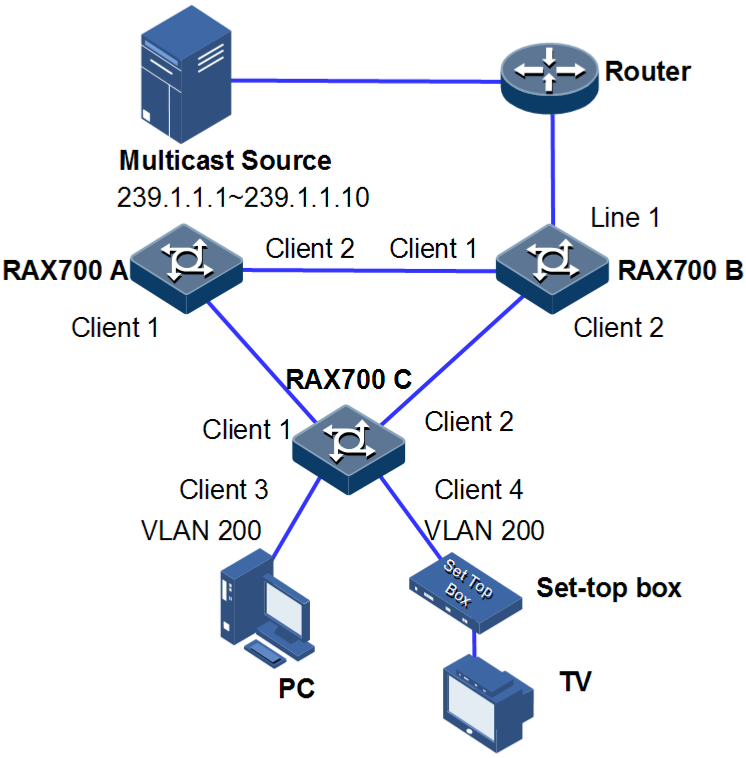
Configure IGMP ring forwarding on single Ethernet ring to make multicast service more stable and prevent multicast service from being disrupted by link failure.

As shown in Figure 11-5, Client 1 and Client 2 on RAX700 A, Client 2 and Client 3 on RAX700 B, Client 2 and Client 4 on RAX700 C form a physical ring. Multicast traffic is input from Client 1 on RAX700 B. The user demands multicast stream through Client 5 and Client 6 on RAX700 C. By doing this, whichever links fail in the RAX700, it will not affect user's on-demand multicast stream.

When using single Ethernet ring to provide multicast services, you can adopt IGMP Snooping to receive the multicast stream.

The following example shows that STP provides ring network detection and IGMP Snooping provides multicast function.

Figure 11-5 Ring network multicast networking



Configuration steps

Step 1 Enable STP function, create a VLAN, and add interfaces into the VLAN.

Configure RAX700 A.

```
RAX700A#config
RAX700A(config)#spanning-tree enable
RAX700A(config)#spanning-tree mode stp
RAX700A(config)#interface client 1
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#switchport trunk native vlan 200
RAX700A(config)#exit
RAX700A(config-port)#interface client 2
RAX700A(config-port)#switchport mode trunk
RAX700A(config-port)#switchport trunk native vlan 200
```

Configure RAX700 B.

```
RAX700B#config
RAX700B(config)#spanning-tree enable
RAX700B(config)#spanning-tree mode stp
RAX700B(config)#interface client 1
RAX700B(config-port)switchport mode trunk
```

```
RAX700B(config-port)#switchport trunk native vlan 200
RAX700B(config-port)#exit
RAX700B(config)#interface client 2
RAX700B(config-port)#switchport mode trunk
RAX700B(config-port)#switchport trunk native vlan 200
```

Configure RAX700 C.

```
RAX700C#config
RAX700C(config)#spanning-tree enable
RAX700C(config)#spanning-tree mode stp
RAX700C(config)#interface client 1
RAX700C(config-port)#switchport mode trunk
RAX700C(config-port)#switchport trunk native vlan 200
RAX700C(config-port)#exit
RAX700C(config)#interface client 2
RAX700C(config-port)#switchport mode trunk
RAX700C(config-port)#switchport trunk native vlan 200
```

Step 2 Enable IGMP Snooping and IGMP ring network forwarding on the interface.

Configure RAX700 A.

```
RAX700A(config)#igmp ring client 1-2
RAX700A(config)#igmp snooping
RAX700A(config)#igmp snooping vlan 200
```

Configure RAX700 B.

```
RAX700B(config)#igmp ring client 1-2
RAX700B(config)#igmp snooping
RAX700B(config)#igmp snooping vlan 200
```

Configure RAX700 C.

```
RAX700C(config)#igmp ring client 1-2
RAX700C(config)#igmp snooping
RAX700C(config)#igmp snooping vlan 200
```

Checking results

Disconnect any link in the ring, and check whether the multicast flow can be received normally.

11.5.2 Example for applying IGMP filtering on interface

Networking requirements

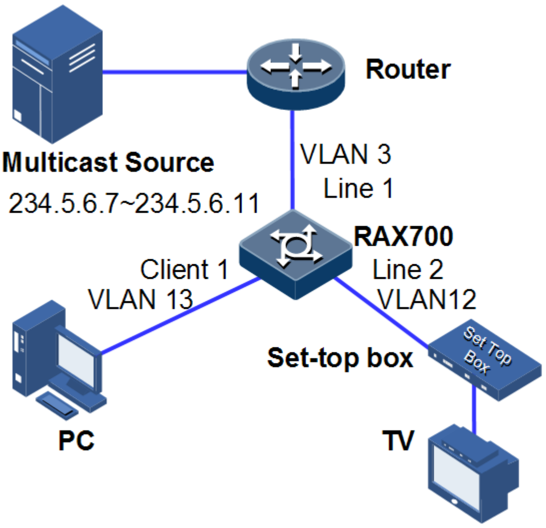
Enable IGMP filtering on the switch. Add filtering rules on the interface to filter multicast users.

As shown Figure 11-6

- Create an IGMP filtering rule Profile 1, set the action to pass for the multicast group ranging from 234.5.6.7 to 234.5.6.10.
- Apply filtering IGMP filtering rule Client 1 on Port 2, allow the STB to join the 234.5.6.7 multicast group, forbid it to join the 234.5.6.11 multicast group.
- Apply no filtering rule on Client 2, and allow PCs to join the 234.5.6.11 multicast group.

Configure the maximum number of multicast groups on Client 1. After the STB is added to the 234.5.6.7 multicast group, add it to the 234.5.6.8 multicast group while it quits the 234.5.6.7 multicast group.

Figure 11-6 Applying IGMP filtering on interface



Configuration steps

Step 1 Create VLANs, and add interfaces into VLANs.

```
Raisecom#config
Raisecom(config)#creat vlan 3,12,13 active
Raisecom(config)#interface client 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk native vlan 3
Raisecom(config-port)#switchport trunk untagged vlan 12,13
Raisecom(config-port)#exit
Raisecom(config)#interface client 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk native vlan 12
Raisecom(config-port)#switchport trunk untagged vlan 3
```

```
Raisecom(config-port)#exit
Raisecom(config)#interface client 3
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk native vlan 13
Raisecom(config-port)#switchport trunk untagged vlan 3
Raisecom(config-port)#exit
```

Step 2 Configure IGMP Snooping.

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

Step 3 Configure IGMP filtering profile.

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

Step 4 Configure the STB to apply the IGMP filter profile.

```
Raisecom(config)#igmp filter
Raisecom(config)#interface client 2
Raisecom(config-port)#igmp filter profile 1
```

Step 5 Configure the maximum number of multicast groups on the STB interface.

```
Raisecom(config-port)#igmp filter max-groups 1
Raisecom(config-port)#igmp filter max-groups action replace
```

Checking results

Use the following command to show configurations of IGMP filtering on the interface.

```
Raisecom#show igmp filter client 2
igmp profile:  1
max group:      1
current group:  0
action:       replace
```

12 System management and maintenance

This chapter describes principles and configuration procedures of system management and maintenance, as well as related configuration examples, including following sections:

- Managing files
- Load and upgrade
- Configuring system log
- Configuring alarm management
- Configuring CPU protection
- Configuring CPU monitoring
- Configuring RMON
- Configuring optical module DDM
- Configuring Loopback
- Configuring extended OAM
- Configuring LLDP
- Configuring fault detection
- Maintenance
- Configuration examples

12.1 Managing files

12.1.1 Managing BootROM file

The BootROM file is used to boot the RAX711-L and finish device initialization. You can upgrade BootROM file through FTP or Trivial File Transfer Protocol (TFTP). By default, BootROM file is named as bootrom or bootromfull.

After powering on the RAX711-L, run the BootROM files at first, press **Space** to enter BootROM menu when the prompt "Press space into Bootrom menu…" appears:

```
Raisecom Boot Loader Bootrom version 1.1.0
Raisecom Technology CO..LTD. .Compiled Mar 18 2013 17:33:50
Base ethernet Mac address: 00:0e:5e:02:03:04
Press Space to Enter Bootrom menu......
 1
 [Raisecom]:
```

You can perform the following operations in the menu below.

Operation	Description
?	List all executable operations.
h	List all executable operations.
b	Quick execution for system bootstrap software.
i	Modify the IP address of the RAX711-L in BootROM mode.
m	Upgrade the firmware version (such as CPLD mirroring) of the RAX711-L.
r	Reboot the RAX711-L.
S	List all system startup software name and related information and specify system startup software name loaded at the time of startup.
u	Upgrade the system software through the serial port or network interface.
ub	Upgrade the BootROM software.

12.1.2 Managing system files

System files are the files needed for system operation (like system startup software and configuration file). These files are usually saved in the memory, the RAX711-L manages them by a file system to facilitate user managing the memory. The file system can create, delete, and modifies the file and directory.

In addition, the RAX711-L supports 2 sets of system startup software. When one set of software fails, you can manually switch to the other to reduce influences caused by service crashes.

Step	Command	Description
1	Raisecom#**multi-system overwrite version***index*	Specify the ID of the system boot software downloaded by the device.
2	Raisecom#**download** { **bootstrap** | **system-boot** | **fpga** } { **ftp** | **sftp** } { *ip-address* | *ipv6-address* } *user-name password file-name*}	Download the system bootstrap software via FTP or TFTP.
	Raisecom#**download** { **bootstrap** | **system-boot** | **fpga** } **tftp** { *ip-address* | *ipv6-address* } *file-name*	
3	Raisecom#**multi-system upload version** *index*	Specify the ID of the system boot software uploaded by the device.
4	Raisecom#**upload** { **logging-file**| **startup-config** | **command-log** | **running-config** | **bootstrap** } { **ftp** | **sftp** } { *ip-address* | *ipv6-address* } *user-name password file-name*]	Upload the system boot software via FTP or TFTP.
	Raisecom#**upload** { **logging-file** | **system-boot** | **command-log** | **running-config** | **bootstrap** } **tftp** { *ip-address* | *ipv6-address* } *file-name*	.

Step	Command	Description
5	Raisecom#**config** [**terminal**] Raisecom(config)#**auto-write enable**	Enable auto-write.

12.1.3 Managing configuration files

The configuration file is the configuration items to be loaded when the RAX711-L is booted this time or next time.

Configuration file has an affix ".cfg", and these files can be open by text book program in Windows system. The contents in the following format:

- Saved as Mode+Command format;
- Just reserve the non-defaulted parameters to save space (see command reference for default values of configuration parameters);
- Take the command mode for basic frame to organize commands, put commands of one mode together to form a section, the sections are separated by "!".

The RAX711-L starts initialization by reading configuration files from memory after powering on. Thus, the configuration in configuration files are called as initialization configuration, if there is no configuration files in memory, the device take the default parameters for initialization.

The device running configuration is called current configuration.

You can modify device current configuration through CLI. The current configuration can be used as initial configuration when next time power on, you must use the **write** command to save current configuration into memory and form configuration file.

Step	Command	Description
1	Raisecom#**download startup-config** { **ftp** | **sftp** } { *ip-address* | *ipv6-address* } *user-name password file-name* Raisecom#**download startup-config tftp** { *ip-address* | *ipv6-address* } *file-name*	Download system startup configuration files through FTP, TFTP, or SFTP.
2	Raisecom#**erase** [*file-name*]	Delete the files from memory.
3	Raisecom#**upload startup-config** { **ftp** | **sftp** } { *ip-address* | *ipv6-address* } *user-name password file-name* Raisecom#**upload startup-config tftp** { *ip-address* | *ipv6-address* } *file-name*	Upload system startup configuration files through FTP, TFTP or SFTP.
4	Raisecom#**write**	Write the configured files into memory.

12.1.4 Checking configurations

No.	Command	Description
1	Raisecom#**show multi-system**	Show the system boot software information of the RAX711-L.

No.	Command	Description
2	Raisecom#**show startup-config**	Show configurations loaded when the RAX711-L is being booted.
3	Raisecom#**show running-config**	Show the current configurations of the RAX711-L.

12.2 Load and upgrade

12.2.1 Configuring TFTP auto-loading mode

Before configuring the TFTP auto-loading mode, you need to build a TFTP environment and have the RAX711-L interconnect with the TFTP server.

Note

- When performing auto-loading, the IP address configured through CLI has a higher priority than the one obtained through DHCP Client.
- When performing auto-loading, the priorities of configuration file names obtained from server are arranged in a descending order as below: the file name confirmed by the naming rule > file name configured through CLI > file name obtained through DHCP Client.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**service config tftp-server** *ip-address*	Configure the IP address of the TFTP server.
3	Raisecom(config)#**service config filename rule** [*rule-number*]	Set the naming rule for file name. By default, there is no denomination rule, system uses default file name as **startup_config.conf**.
4	Raisecom(config)#**service config filename** *filename*	Specify the configuration file name to be uploaded.
5	Raisecom(config)#**service config overwrite enable**	Enable local configuration file overwriting. Use the **service config overwrite disable** command to disable local configuration file overwriting.
6	Raisecom(config)#**service config trap enable**	(Optional) enable the Trap module used for update configuration files automatically.
7	Raisecom(config)#**service config version** { **bootstrap** | **startup-config** | **system-boot** } *version*	(Optional) configure the version ID of the system Bootrom file, system startup configuration file, and system startup file.
8	Raisecom(config)#**service config**	Enable auto-loading.

12.2.2 Upgrading system software through BootROM

In the below cases, you need to upgrade system software through BootROM:

- The RAX711-L is booted for the first time.

- The system files are damaged.
- The card cannot be booted properly.

Before upgrading the system software through BootROM, you should build a TFTP environment, taking a PC as the TFTP server and the RAX711-L as the client. Basic requirements are as below.

- The RAX711-L is connected to the TFTP server through SNMP interface.
- Configure the TFTP server and ensure the TFTP server is available.
- Configure the IP address of TFTP server and make the IP address in the same network segment with IP addresses configured by the **T** command.

<table>
<tr><th>Step</th><th>Operation</th></tr>
<tr><td>1</td><td>Log in to the RAX711-L through serial port as the administrator and enter privileged EXEC mode and then use the reboot command to reboot the RAX711-L.
<pre>
Raisecom#reboot
Please input 'yes' to confirm:yes
Rebooting ...
booting...
Raisecom Boot Loader Bootrom version 1.1.0
Raisecom Technology CO..LTD. .Compiled Mar 18 2013 17:33:50
Base ethernet Mac address: 00:0e:5e:02:03:04
Press Space to Enter Bootrom menu......
 2
</pre></td></tr>
<tr><td>2</td><td>Press Space to enter the raisecom interface when "Press space into Bootstrap menu..." appears on the screen, then input "?" to display the command list:
<pre>
[Raisecom]:?
?   print this list
h   print this list
b   boot system
i   modify network manage port ip address
m   update microcode
r   reboot system
S   select system to boot
u   update system
ub   update bootrom
</pre>
Caution
The input letters are case sensitive.</td></tr>
</table>

<table>
<tr><th>Step</th><th>Operation</th></tr>
<tr><td>3</td><td>

Input "u" to download the system boot file through FTP and replace the original one, the display information is shown as below:

```
[Raisecom]: u
Index   Name                                  Size
----------------------------------------------------------
1*      system_1.1.1.20130411             10420581
2       system_1.1.1.20130411             10420581
Current selected version is 1
Please select a version to overwrite: 2
choose mode for updating core file.
            -----------------------------------
            -     1.  |    serial        -
            -----------------------------------
            -     2.  |    network       -
            -----------------------------------
please input mode choose...
2
config network infor ...
            host ip address:192.168.4.100
                   usr:  wrs
                   passwd:  wrs
                 filename:  RAX711-L-4GCenms-b.z
   starting connect host,please waiting...
   Do you want to update image file?<Y/N>y
   start update core , please wait some minutes...
   success.
```

Caution

Ensure the input file name here is correct. In addition, the file name should not be longer than 80 characters.

</td></tr>
<tr><td>4</td><td>

Enter "S" and correctly select the system boot file to be loaded when the RAX711-L is booted next time. The "*" character indicates the default system startup file loaded currently.

```
[Raisecom]: S
Index   Name                                  Size
----------------------------------------------------------
1*      system_1.1.1.20130411             10420581
2       system_1.1.1.20130411             10420581
Current selected version is 1
Please select a version to start: 2
saving...  done
```

</td></tr>
<tr><td>5</td><td>Enter "b" to execute the bootstrap file quickly. The RAX711-L will be rebooted and upload the downloaded system boot file.</td></tr>
</table>

12.2.3 Upgrading system software through FTP/TFTP

Before upgrading the system software through FTP/TFTP, you should build a FTP/TFTP environment, taking a PC as the TFTP server and the RAX711-L as the client. Basic requirements are as below.

- The RAX711-L is connected to the TFTP server through UNI/NNI.
- Configure the FTP/TFTP server and ensure the FTP/TFTP server is available.
- Configure the IP address of TFTP server.

Step	Command	Description
1	Raisecom#**multi-system overwrite version** *version*	Specify the ID of the system boot software downloaded by the device. By default, the downloaded system boot software ID is set to 1.
2	Raisecom#**download system-boot** { **ftp** [*ip-address username password filename local-filename*] | **tftp** [*ip-address filename local-filename*] } [**reservedevcfg**]	Download the system boot software via FTP or TFTP.
3	Raisecom#**multi-system boot version** *version*	Specify the ID of the system boot software uploaded by the device. By default, the uploaded system boot software ID is set to 1.
4	Raisecom#**write**	Write the configured files into the memory.
5	Raisecom#**reboot** [**now**]	Reboot the RAX711-L and the device will automatically upload the downloaded system boot software.

12.2.4 Checking configurations

No.	Command	Description
1	Raisecom#**show multi-system**	Show the system boot software information of the current device.
2	Raisecom#**show service config**	Show automatically-configured loading information.
3	Raisecom#**show service config filename rule** [*rule-number*]	Show the naming rule of the configuration file.
4	Raisecom#**show version**	Show the system version.

12.3 Configuring system log

12.3.1 Preparing for configurations

Scenario

The RAX711-L generates critical information, debugging information, or error information of the system to system logs and outputs the system logs to log files or transmits them to the host, Console interface, or monitor for viewing and locating faults.

Prerequisite

N/A

12.3.2 Configuring basic information about system log

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**logging on**	(Optional) Enable system log. By default, system log is enabled.
3	Raisecom(config)#**logging time-stamp** { **debug** | **log** } { **datetime** | **none** | **uptime** }	(Optional) configure the timestamp of system log. The optional parameter **debug** is used to assign debug-level (7) system log timestamp. By default, this system log does not have timestamp The optional parameter **log** is used to assign levels 0–6 system log timestamp. By default, these system logs adopt **date-time** as timestamp.
4	Raisecom(config)#**logging rate-limit** *rate*	(Optional) configure the transport rate of system log. By default, no transport rate is configured.
5	Raisecom(config)#**logging buginf** [**high** | **low** | **none** | **normal**]	(Optional) send Level 7 (debugging) debugging log.
6	Raisecom(config)#**logging buffered size** *size*	(Optional) configure the log buffer size. By default, the log buffer size is set to 4KB.
7	Raisecom(config)#**logging discriminator** *discriminator-number* { **facility** | **mnemonics** | **msg-body** } { **drops** *key* | **includes** *key* | **none** }	(Optional) configure the log discriminator.
8	Raisecom(config)#**logging 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** }	(Optional) configure the facility field in the log to be sent to the log host. By default, the facility field value is set to local7.

Step	Command	Description
9	Raisecom(config)#**logging sequence-number**	(Optional) enable the sequence number field of the log.

12.3.3 Configuring system log output destination

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**logging console** [*log-level* | **alerts** | **critical** | **debugging** | **discriminator** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**]	(Optional) output system logs to the Console interface.
3	Raisecom(config)#**logging host** *ip-address* [*log-level* | **alerts** | **critical** | **debugging** | **discriminator** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**]	(Optional) output system logs to the log host.
4	Raisecom(config)#**logging monitor**[*log-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**]	(Optional) output system logs to the monitor.
5	Raisecom(config)#**logging file** [**discriminator** *discriminateor-number*]	(Optional) output system logs to the Flash of the RAX711-L.
6	Raisecom(config)#**logging buffered** [*log-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**]	(Optional) output system logs to the log buffer.
7	Raisecom(config)#**logging history**	(Optional) output system logs to the log history table.
8	Raisecom(config)#**logging history size** *size*	Configure the log history table size. By default, the log history table size is set to 1.
9	Raisecom(config)#**logging trap** [*log-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**]	(Optional) translate logs output to the log history table to Traps. By default, warning Logs output to the log history table is translated to Traps.

12.3.4 Checking configurations

No.	Command	Description
1	Raisecom#**show logging**	Show system log configurations.
2	Raisecom#**show logging file**	Show contents of the system log file.
3	Raisecom#**show logging buffer**	Show contents of the log buffer.

No.	Command	Description
4	Raisecom#**show logging discriminator [facility module]**	Show information about the log discriminator.
5	Raisecom#**show logging history**	Show contents of the log history table.

12.4 Configuring alarm management

12.4.1 Preparing for configurations

Scenario

When the RAX711-L fails, the alarm management module will collect the fault information and output the alarm in a log. The alarm information includes the time when the alarm is generated, the name and descriptions of the alarm. It helps you quickly locate the fault.

If Trap is configured on the RAX711-L, when the operating environment of the device is abnormal, the RAX711-L supports saving to the hardware monitoring alarm table, sending Trap to the NView NNM system, and outputting to the system log. It notifies users to process the fault and prevent the fault from occurring.

With alarm management, you can directly perform following operations on the RAX711-L: alarm inhibition, alarm auto-report, alarm monitoring, alarm inverse, alarm delay, alarm storage mode, alarm clearing, and alarm viewing.

Prerequisite

After hardware monitoring is configured on the RAX711-L,

- When alarms are output in Syslog form, alarms are generated to the system log. When needing to send alarms to the log host, you need to configure the IP address of the log host on the RAX711-L.
- When needing to send alarms to the NView NNM system in a Trap form, you need to configure the IP address of the NView NNM system on the RAX711-L.

12.4.2 Configuring basic functions of alarm management

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**alarm inhibit enable**	(Optional) enable alarm inhibition. By default, alarm inhibition is enabled.
3	Raisecom(config)#**alarm auto-report** { *module_name* [*group_name*] | *interface-type interface-number* [*module_name* [*group_name*]] } **enable**	(Optional) enable alarm auto-report. By default, alarm auto-report is enabled.

Step	Command	Description
4	Raisecom(config)#**alarm monitor**{ *module_name* [*group_name*] | *interface-type interface-number* [*module_name* [*group_name*]] } **enable**	(Optional) enable alarm monitoring. By default, alarm monitoring is enabled.
5	Raisecom(config)#**alarm inverse** *interface-type interface-number* { **none** | **auto** | **manual** }	(Optional) configure the alarm inverse mode. By default, the alarm inverse mode is set to **none** (non-inverse).
6	Raisecom(config)#**alarm active delay** *second*	(Optional) configure the time for delaying an alarm to be generated. By default, alarm delay is set to 0s.
7	Raisecom(config)#**alarm active storage-mode** { **loop** | **stop** }	(Optional) configure the alarm storage mode. By default, the alarm storage mode is set to **stop**.
8	Raisecom(config)#**alarm clear index** *index*	(Optional) clear specified current alarms.
	Raisecom(config)#**alarm clear** *module_name* [*group_name*]	(Optional) clear specified current alarms on the specified alarm module.
	Raisecom(config)#**alarm clear** *interface-type interface-number* [*module_name* [*group_name*]]	(Optional) clear specified current alarms of the specified alarm source (interface).
9	Raisecom(config)#**alarm syslog enable**	(Optional) enable alarm Syslog. By default, alarm Syslog is enabled.
10	Raisecom(config)#**exit** Raisecom#**show alarm active** [*module_name* | **severity** *severity*]	(Optional) show current alarms.
	Raisecom#**show alarm cleared** [*module_name* | **severity** *severity*]	(Optional) show historical alarms.

12.4.3 Configuring hardware monitoring alarm output

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**hw_monitor syslog enable**	(Optional) enable global hardware monitoring alarm Syslog output. By default, global hardware monitoring alarm Syslog output is disabled.
3	Raisecom(config)#**snmp-server trap hw_monitor enable**	(Optional) enable global hardware monitoring alarm Trap. By default, global hardware monitoring alarm Trap is enabled.
4	Raisecom(config)#**hw_monitor power-supply** { **notifies** | **syslog** }	(Optional) enable power supply dying-gasp alarm output and configure the power supply dying-gasp alarm output mode. By default, power supply dying-gasp alarm Syslog output and power supply dying-gasp alarm Trap output are enabled.

Step	Command	Description
5	Raisecom(config)#**hw_monitor temperature** { **high** *high-value* | **low** *low-value* | **notifies** | **syslog** }	(Optional) enable temperature alarm output and configure the temperature alarm output mode/temperature alarm threshold. The high-temperature threshold (*high-value*) must be greater than the low-temperature threshold (*low-value*). By default, temperature alarm Syslog output and temperature alarm Trap output are enabled. The high-temperature threshold is set to 75 ℃ and the low-temperature threshold is set to -10 ℃.
6	Raisecom(config)#**hw_monitor voltage** { **notifies** | **syslog** | **high** *high-value* | **low** *low-value* }	(Optional) enable voltage alarm output and configure the voltage alarm output mode/voltage alarm threshold. By default, voltage alarm Syslog output and voltage alarm Trap output are enabled. **Note** The RAX711-L monitors 3.3 V master chip voltage only.
7	Raisecom(config)#**hw_monitor port** { **link-down** | **link-fault** } { **notifies** | **syslog** } *interface-type interface-list*	(Optional) enable interface status alarm output and configure the voltage alarm output mode. By default, only interface **link-down** alarm Syslog output and interface **link-down** alarm Trap output are enabled.
8	Raisecom(config)#**clear hw_monitor**	(Optional) clear alarms manually. **Note** • This command can be used to clear all alarms from the current alarm table. In addition an alarm, whose type is all-alarm, is generated in the historical alarm table. • If global Trap is enabled, this all-alarm alarm will be output in a Trap form. If global Syslog is enabled, this all-alarm alarm will be output in a Syslog form.

Note

- Alarms cannot be generated into Syslog unless global hardware monitoring alarm Syslog output is enabled and Syslog output of monitored alarm events is enabled.
- Trap cannot be sent unless global hardware monitoring alarm Trap output is enabled and Trap output of monitored alarm events is enabled.

12.4.4 Configuring Layer 3 dying-gasp and link-fault alarms

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**power-down trap enable**	Enable Layer 3 dying-gasp alarm. By default, Layer 3 dying-gasp alarm is enabled.

Step	Command	Description
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#**snmp trap link-fault enable**	Enable Layer 3 link-fault alarm on the uplink Line interface. By default, Layer 3 link-fault alarm is enabled.

12.4.5 Checking configurations

No.	Command	Description
1	Raisecom#**show alarm management** [*module_name*]	Show current alarm parameters. Alarm parameters displayed by this command include alarm inhibition, alarm inverse mode, alarm delay, alarm storage mode, alarm buffer size, and alarm log size.
2	Raisecom#**show alarm management statistics**	Show alarm management module statistics.
3	Raisecom#**show hw_monitor**	Show global hardware monitoring alarm configurations. Hardware monitoring information displayed by this command includes global alarm Syslog output, global Trap, power supply dying-gasp alarms, temperature alarms, and voltage alarms.
4	Raisecom#**show hw_monitor** *interface-type interface-list*	Show interface status alarms.
5	Raisecom#**show hw_monitor currrent**	Show current hardware monitoring alarms.
6	Raisecom#**show hw_monitor history**	Show historical hardware monitoring alarms.
7	Raisecom#**show hw_monitor environment** [**power** | **temperature** | **voltage**]	Show current power supply, temperature, and voltage alarms and current environment information.
8	Raisecom#**show power-down**	Show Layer 3 dying-gasp alarm status.
9	Raisecom#**show alarm active** [*module_name* | **severity** *severity*]	Show the current alarm table.
10	Raisecom#**show alarm cleared** [*module_name* | **severity** *severity*]	Show cleared alarms.

12.5 Configuring CPU protection

12.5.1 Preparing for configurations

Scenario

Because the network environment of the RAX711-L is complex, the RAX711-L may be attacked by rogue packets. It consumes a great number of CPU resources to process these packets. This will reduce device performance. What worse, it may cause system crash. To prevent the RAX711-L from attack, you can limit the number of received packets on an interface to protect the CPU.

Prerequisite

N/A

12.5.2 Configuring CPU protection

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**flood-protect car global** { **kbps** | **pps** } **cir** *cir* **cbs** *cbs*	Configure global rate limiting on packets sent to the CPU.

12.5.3 Checking configurations

No.	Command	Description
1	Raisecom#**show flood-protect**	Show configurations of CPU protection.

12.6 Configuring CPU monitoring

12.6.1 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 RAX711-L, that is, the IP address of the NView NNM system.

12.6.2 Viewing CPU monitoring information

Step	Command	Description
1	Raisecom#**show cpu-utilization** [**dynamic** | **history** { **10min** | **1min** | **2hour** | **5sec** }]	Show CPU utilization rate.
2	Raisecom#**show process** [**dead** | **sorted** { **normal-priority** | **process-name** } | *taskname*]	Show task status.
3	Raisecom#**show process cpu** [**sorted** [**10min** | **1min** | **5sec** | **invoked**]]	Show CPU utilization rate of all tasks.

12.6.3 Configuring CPU monitoring alarm

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server traps enable cpu-threshold**	Enable CPU threshold Trap. By default, CPU threshold Trap is disabled.
3	Raisecom(config)#**cpu rising-threshold** *rising-threshold-value* [**falling-threshold** *falling-threshold-value*] [**interval** *interval-value*]	(Optional) configure the upper CPU threshold and lower CPU threshold. The upper CPU threshold must be greater than the lower CPU threshold. By default, the upper CPU threshold is set to 100% and the lower CPU threshold is set to 1%. The sampling interval is set to 60s. After CPU threshold Trap is enabled, in the sampling interval, when the CPU utilization rate is higher than the upper CPU threshold or is smaller than the lower CPU threshold, a Trap is sent automatically.

12.6.4 Checking configruations

No.	Command	Description
1	Raisecom#**show cpu-utilization** [**dynamic**]	Show CPU utilization rate and related configurations.

12.7 Configuring RMON

12.7.1 Preparing for configurations

Scenario

RMON helps monitor and count network traffics.

Compared with SNMP, RMON is a more high-efficient monitoring method. After you specifying the alarm threshold, the RAX711-L actively sends alarms when the threshold is exceeded without gaining the variable information. This helps reduce the traffic of management and managed devices and facilitates managing the network.

Prerequisite

The route between the RAX711-L and the NView NNM system is reachable.

12.7.2 Configuring RMON statistics

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

12.7.3 Configuring RMON historical statistics

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

12.7.4 Configuring RMON alarm group

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

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

12.7.5 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 parameters related to the RMON event group.

12.7.6 Checking configurations

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

12.8 Configuring optical module DDM

12.8.1 Preparing for configurations

Scenario

Optical module DDM provides a method for monitoring SFP performance parameters. By analyzing monitored data provided by the optical module, the administrator can predict the SFP module lifetime, isolate system faults, as well as verify the compatibility of the optical module.

Prerequisite

N/A

12.8.2 Enabling optical module DDM

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**transceiver ddm enable**	Enable optical module DDM. By default, optical module DDM is disabled.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#**transceiver check-password enable**	Enable optical module password-check on an interface. By default, optical module password-check is enabled.

12.8.3 Enabling optical module parameter anomaly Trap

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server trap transceiver enable**	Enable optical module parameter anomaly Trap. By default, optical module parameter anomaly Trap is disabled.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#**transceiver trap enable**	Enable optical module DDM Trap on an interface. By default, optical module DDM Trap is enabled.

12.8.4 Checking configurations

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

12.9 Configuring Loopback

12.9.1 Preparing for configurations

Scenario

The network maintenance engineers can detect and analyze interface and network faults through interface loopback.

Ingress packets and egress packets are defined as below:

- Ingress packets: test packets received by an interface
- Egress packets: test packets return to the peer device through an interface

Prerequisite

When the current interface is in Forwarding status, packets entering the interface can be properly forwarded or transmitted to the CPU.

12.9.2 Configuring parameters of interface loopback rules

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)#**loopback** { **dmac** | **smac** } *mac-address*	Configure the parameter for enabling the loopback rule based on the destination/source MAC address. The parameter is set to the destination/source MAC address.
4	Raisecom(config-port)#**loopback** { **cvlan** | **svlan** } *vlan-id*	Configure the parameter for enabling the loopback rule based on the CVLAN ID/SVLAN ID. The parameter is set to the CVLAN ID/SVLAN ID.
5	Raisecom(config-port)#**loopback** { **dip** | **sip** } *ip-address*	Configure the parameter for enabling the loopback rule based on the DIP/SIP. The parameter is set to the DIP/SIP.

Note

- The first 3 bytes of the destination MAC address cannot be set to 0x0180C2.
- The source MAC address cannot be a multicast/broadcast MAC address.

12.9.3 Configuring source/destination MAC address translation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**loopback localmac** *mac-address*	(Optional) configure the local MAC address. By default, the local MAC address is the one of the current device.

Step	Command	Description
3	Raisecom(config)#**loopback unicast-smac { localmac | swap }**	(Optional) configure the source MAC address translation rule of unicast loopback packets. By default, the source MAC address of the unicast loopback packets is changed to the local MAC address.
4	Raisecom(config)#**loopback dmac-swap enable**	Enable destination MAC address translation of multicast and broadcast packet.

Note

- Unicast source MAC address translation: for unicast packets, which enter the interface and meet loopback rules and parameters, you can perform source MAC address translation. Their source MAC address is changed to the local MAC address of the current device or other destination MAC addresses.
- Multicast/Broadcast destination MAC address translation: for multicast and broadcast packets, which enter the interface and meet loopback rules and parameters, you can perform destination MAC address translation as required. You can configure changing their destination MAC address to the local MAC address of the current device.

12.9.4 Configuring destination IP address translation

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**loopback localip** *ip-address*	(Optional) configure the local IP address. By default, the local IP address is set to 127.0.0.1. **Note** The source IP address of all loopback egress packets is changed to the local IP address.
3	Raisecom(config)#**loopback dip-swap enable**	Enable destination IP address translation of multicast IP packets. By default, destination IP address translation is enabled.

Note

- Multicast destination IP address translation: for multicast IP packets, which enter the interface and meet loopback rules, you can perform destination IP address translation as required. After multicast destination IP address translation is enabled, the destination IP address is changed to the source IP address of the ingress packets. The source IP address of loopback egress packets is changed to the source IP address (local IP address) of the current device.
- Broadcast destination IP address translation: the destination IP address of loopback egress packets is always changed to the source IP address of ingress packets.

12.9.5 Enabling loopback by selecting loopback rule

Caution

- Loopback may influence normal services. Be careful to perform it.
- After loop detection, disable loopback immediately. Otherwise, normal services fail.

<table>
<tr><th>Step</th><th>Command</th><th>Description</th></tr>
<tr><td>1</td><td>Raisecom#config</td><td>Enter global configuration mode.</td></tr>
<tr><td>2</td><td>Raisecom(config)#interface interface-type interface-number</td><td>Enter physical layer interface configuration mode.</td></tr>
<tr><td>3</td><td>Raisecom(config-port)#loopback mode { cvlan | cvlan-ccos | dip | dmac | dvlan | ether-type | exfo-l2 | exfo-l3 | inner-loopback | rc-l2 | rc-l3 | rc-mpls | sip | sip-dip | smac | svlan | svlan-scos | svlan-scos-cvlan-ccos | tcp-dport | tcp-sport | udp-dport | udp-sport } [timeout time-out-second]</td><td>Configure the rule for enabling interface loopback.
By default, loopback is performed on all packets. The timeout is set to 0, which indicates that the interface is always in loopback status.</td></tr>
<tr><td>4</td><td>Raisecom(config-port)#loopback ether-type ether-type</td><td>Configure the Ethernet type of the loopback packets.</td></tr>
<tr><td>5</td><td>Raisecom(config-port)#loopback lsp-label lsp-label</td><td>Configure the LSP label of the loopback services.</td></tr>
<tr><td>6</td><td>Raisecom(config-port)#loopback pw-label lsp-label</td><td>Configure the PW label of the loopback services.</td></tr>
<tr><td>7</td><td>Raisecom(config-port)#loopback { tcp-dport | tcp-sport } port-number</td><td>Configure the interface ID of the TCP for the loopback services.</td></tr>
<tr><td>8</td><td>Raisecom(config-port)#loopback { udp-dport | udp-sport } port-number</td><td>Configure the interface ID of the loopback services.</td></tr>
<tr><td>9</td><td>Raisecom(config-port)#loopback [timeout timeout-minute]</td><td>Enable interface loopback.
By default, it is disabled.</td></tr>
</table>

12.9.6 Configuring loopback packets statistics

Configure loopback packets statistics for the RAX700 as below.

<table>
<tr><th>Step</th><th>Configuration</th><th>Description</th></tr>
<tr><td>1</td><td>Raisecom#config</td><td>Enter global configuration mode.</td></tr>
<tr><td>2</td><td>Raisecom(config)#interface interface-type interface-number</td><td>Enter physical interface configuration mode.</td></tr>
<tr><td>3</td><td>Raisecom(config-port)#loopback mode { cvlan | cvlan-ccos | dip | dmac | dvlan | ether-type | exfo-l2 | exfo-l3 | inner-loopback | rc-l2 | rc-l3 | rc-mpls | sip | sip-dip | smac | svlan | svlan-scos svlan-scos-cvlan-ccos | tcp-dport | tcp-sport | udp-dport | udp-sport } statistic { enable | disable }</td><td>Enable loopback packets statistics.</td></tr>
</table>

12.9.7 Checking configurations

No.	Command	Description
1	Raisecom#**show interface** *interface-type interface-list* **loopback**	Show interface loopback configurations.

12.10 Configuring extended OAM

12.10.1 Preparing for configurations

Scenario

Extended OAM is mainly used to establish connection between local and remote devices to manage remote devices.

Prerequisite

N/A

12.10.2 Establishing OAM links

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)#**oam** { **active** | **passive** }	Configure the OAM working mode. By default, the OAM working mode is set to passive.
4	Raisecom(config-port)#**oam enable**	Enable OAM on an interface.

12.10.3 Checking configurations

No.	Command	Description
1	Raisecom#**show extended-oam status** *interface-type interface-list*	Show extended OAM link status.
2	Raisecom#**show extended-oam statistics** *interface-type interface-number*	Show extended OAM frame statistics.

12.11 Configuring LLDP

12.11.1 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 RAX711-L. Therefore, the RAX711-L can notify its information to the neighbours mutually, and store neighbour information to facilitate the NView NNM system querying information.

Prerequisite

N/A

12.11.2 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, global LLDP is disabled.

12.11.3 Enabling LLDP on 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.
3	Raisecom(config-port)#**lldp enable**	Enable LLDP on the interface. By default, LLDP is enabled on the interface.
4	Raisecom(config-port)#**lldp dest-address** *mac-address*	Specify the destination MAC address of packets sent by the interface.

12.11.4 Configuring basic functions of LLDP

Caution

- We recommend configuring the LLDP delivery period in advance. The delivery period and delivery delay are interact on each other. The delivery delay must be smaller than or equal to 0.25 delivery period. Otherwise, configuration fails.
- The LLDP delivery delay should be smaller than the aging time. The aging time = aging coefficient × delivery period.

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

12.11.5 Configuring LLDP Trap

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

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server lldp-trap enable**	Enable LLDP Trap.
3	Raisecom(config)#**lldp trap-interval** *second*	(Optional) configure the LLDP Trap period timer . By default, the LLDP Trap period timer is set to 5s.

Note

After enabled with LLDP Trap, the RAX711-L will send Traps after detecting aged neighbours, newly-added neighbours, and changed neighbour information.

12.11.6 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.

12.12 Configuring fault detection

12.12.1 Configuring task scheduling

When you need to use some commands to perform periodical maintenance on the RAX711-L, you can configure task scheduling. The RAX711-L supports achieving task scheduling through the schedule list and CLI. You can use commands to perform periodical operation just by specifying the begin time, period, and end time of a specified task in the schedule list and bind the schedule list to the CLI.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**schedule-list** *list-number* **start** { **date-time** *month-day-year hour*:*minute*:*second* [**every** { **day** | **week** | *period hour*:*minute*:*second* }] **stop** month-day-year *hour*:*minute*:*second* | **up-time** *period hour*:*minute*:*second* [**every** *period hour*:*minute*:*second*] [**stop** *periodhour*:*minute*:*second*] }	Create and configure the schedule list.
3	Raisecom(config)#*command-string* **schedule-list** *list-number*	Bind the CLIs, which need to be performed periodically and support the schedule list, to the schedule list.
4	Raisecom#**show schedule-list**	Show schedule list configurations.

12.12.2 PING and Traceroute

PING

Step	Command	Description
1	Raisecom#**ping** *ip-address* [**count** *count*] [**size** *size*] [**waittime** *period*]	(Optional) use the **ping** command to test IPv4 network connectivity.

Step	Command	Description
2	Raisecom#**ping ipv6** *ipv6-address* [**count** *count*] [**size** *size*] [**waittime** *time*] [**interface ip** *if-number*]	(Optional) use the **ping** command to test IPv6 network connectivity.

Note

The RAX711-L cannot perform other operations in the process of Ping. It can perform other operations only when Ping is finished or Ping is broken off by pressing **Ctrl**+**C**.

Traceroute

Before using Traceroute, you should configure the IP address and default gateway of the RAX711-L.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface ip** *if-number*	Enter layer 3 interface configuration mode.
3	Raisecom(config-ip)#**ip address** *ip-address* [*ip-mask*] *vlan-id*	Configure the IP address of the interface.
	Raisecom(config-ip)#**ipv6 address** *ipv6-address/M* [**eui-64**] [*vlan-list*]	
4	Raisecom(config-ip)#**exit**	Exit Layer 3 interface configuration mode and enter global configuration mode.
5	Raisecom(config)#**exit**	Exit global configuration mode and enter privileged EXEC configuration mode.
6	Raisecom#**traceroute** { *ip-address* | **ipv6** *ipv6-address* } [**firstttl** *first-ttl*] [**maxttl** *max-ttl*] [**port** *port-number*] [**waittime** *period*] [**count** *times*]	(Optional) use the **traceroute** command to test the IPv4 network connectivity and view nodes passed by the packet.

12.13 Maintenance

Command	Description
Raisecom(config)#**clear lldp statistic** { *interface-type interface-number* | **port-channel** *port-channel-number*}	Clear LLDP statistics.
Raisecom(config)#**clear lldp remote-table** [interface-type interface-number]	Clear LLDP neighbour information.
Raisecom(config)#**clear rmon**	Clear all RMON configurations.

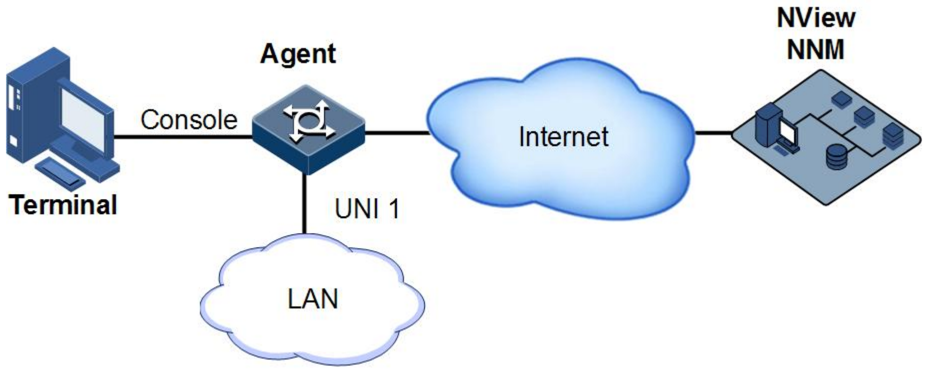
12.14 Configuration examples

12.14.1 Example for configuring RMON alarm group

Networking requirements

As shown in Figure 12-1, the RAX711-L is the Agent, which is connected to the terminal through the Console interface and is connected to the NView NNM system through the Internet. Enable RMON statistics on the RAX711-L to execute performance statistics on UNI 1. During a period, when the number of packets received by the interface exceeds the configured threshold, the RAX711-L records a log and sends a Trap to the NView NNM system.

Figure 12-1 Configuring RMON alarm group



Configuration steps

Step 1 Create event group 1. Event group 1 is used to record and send the log which contains the string High-ifOutErrors. The owner of the log is set to **system**.

```
Raisecom#config
Raisecom(config)#rmon event 1 log description High-ifOutErrors owner
system
```

Step 2 Create alarm group 10. Alarm group 10 is used to monitor the MIB variable (1.3.6.1.2.1.2.2.1.20.1) every 20 seconds. If the value of the variable is added by 15 or greater, a Trap is triggered. The owner of the Trap is also set to **system**.

```
Raisecom(config)#rmon alarm 10 1.3.6.1.2.1.2.2.1.20.1 interval 20 delta
rising-threshold 15 1 falling-threshold 0 owner system
```

Step 3 Save configurations.

```
Raisecom#write
```

Checking results

Use the **show rmon alarms** command to show RMON alarm group information.

```
Raisecom#show rmon alarms
Alarm 10 is active, owned by system
Monitors 1.3.6.1.2.1.2.2.1.20.1 every 20 seconds
Taking delta  samples, last value was 0
Rising threshold is 15, assigned to event 1
Falling threshold is 0, assigned to event 0
On startup enable rising and falling alarm
```

Use the **show rmon events** command to show RMON event group information.

```
Raisecom#show rmon events
Event 1 is active, owned by system
Event generated at 0:0:0
Send TRAP when event is fired.
```

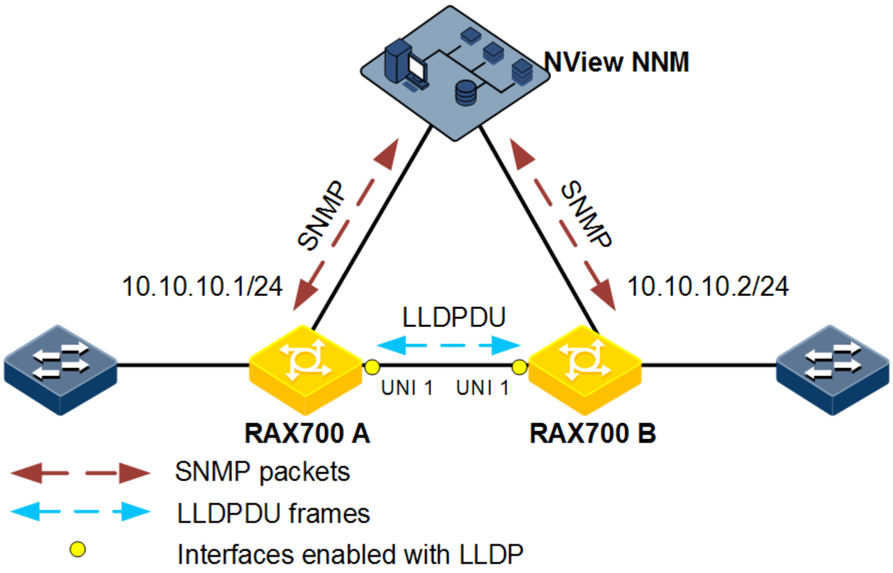
When an alarm event is triggered, you can view related records at the alarm management dialog box of the NView NNM system.

12.14.2 Example for configuring LLDP basic functions

Networking requirements

As shown in Figure 12-2, RAX700 A and RAX700 B are connected to the NView NNM system. Enable LLDP on links between RAX700 A and RAX700 B. And then you can query the Layer 2 link changes through the NView NNM system. If the neighbour is aged, added, or changed, RAX700 A and RAX700 B send LLDP alarm to the NView NNM system.

Figure 12-2 Configuring LLDP basic functions



Configuration steps

Step 1 Enable global LLDP and enable LLDP alarm.

- Configure RAX700 A.

```
Raisecom#hostname RAX700A
RAX700A#config
RAX700A(config)#lldp enable
RAX700A(config)#snmp-server lldp-trap enable
```

- Configure RAX700 B.

```
Raisecom#hostname RAX700B
RAX700B#config
RAX700B(config)#lldp enable
RAX700B(config)#snmp-server lldp-trap enable
```

Step 2 Configure management IP addresses.

- Configure RAX700 A.

```
RAX700A(config)#create vlan 1024 active
RAX700A(config)#interface uni 1
RAX700A(config-port)#lldp enable
RAX700A(config-port)#switchport access vlan 1024
RAX700A(config-port)#exit
RAX700A(config)#interface ip 1
RAX700A(config-ip)#ip address 10.10.10.1 1024
```

- Configure RAX700 B.

```
RAX700B(config)#create vlan 1024 active
RAX700B(config)#interface uni 1
RAX700A(config-port)#lldp enable
RAX700B(config-port)#switchport access vlan 1024
RAX700B(config)#interface ip 1
RAX700B(config-ip)#ip address 10.10.10.2 1024
```

Step 3 Configure LLDP properties.

- Configure RAX700 A.

```
RAX700A(config)#lldp message-transmission interval 60
RAX700A(config)#lldp message-transmission delay 9
RAX700A(config)#lldp trap-interval 10
```

- Configure RAX700 B.

```
RAX700A(config)#lldp message-transmission interval 60
RAX700A(config)#lldp message-transmission delay 9
RAX700A(config)#lldp trap-interval 10
```

Step 4 Save configurations.

- Save configurations of RAX700 A.

```
RAX700A#write
```

- Save configurations of RAX700 B.

```
RAX700B#write
```

Checking results

Use the **show lldp local config** command to show local configurations.

```
RAX700A#show lldp local config
System configuration:
-------------------------------------------------------------------------
LLDP enable status: enable  (default is disabled)
```

```
LLDP enable ports:1-3,7-9
LldpMsgTxInterval:60     (default is 30s)
LldpMsgTxHoldMultiplier:4      (default is 4)
LldpReinitDelay:2      (default is 2s)
LldpTxDelay:2      (default is 2s)
LldpNotificationInterval:5     (default is 5s)
LldpNotificationEnable:enable  (default is 0180.c200.000e)
--------------------------------------------------------------
nni1        :  destination-mac:0180.C200.000E
nni2        :  destination-mac:0180.C200.000E
uni1       :  destination-mac:0180.C200.000E
uni2       :  destination-mac:0180.C200.000E
uni3       :  destination-mac:0180.C200.000E
uni4       :  destination-mac:0180.C200.000E
port-channel1      :  destination-mac:0180.C200.000E
port-channel2      :  destination-mac:0180.C200.000E
port-channel3      :  destination-mac:0180.C200.000E
RAX700B#show lldp local config
System configuration:
--------------------------------------------------------------------------
LLDP enable status:enable  (default is disabled)
LLDP enable ports:1-3,7-9
LldpMsgTxInterval:60     (default is 30s)
LldpMsgTxHoldMultiplier:4      (default is 4)
LldpReinitDelay:2      (default is 2s)
LldpTxDelay:2      (default is 2s)
LldpNotificationInterval:5     (default is 5s)
LldpNotificationEnable:enable  (default is 0180.c200.000e)
--------------------------------------------------------------
nni1        :  destination-mac:0180.C200.000E
nni2        :  destination-mac:0180.C200.000E
uni1       :  destination-mac:0180.C200.000E
uni2       :  destination-mac:0180.C200.000E
uni3       :  destination-mac:0180.C200.000E
uni4       :  destination-mac:0180.C200.000E
port-channel1      :  destination-mac:0180.C200.000E
port-channel2      :  destination-mac:0180.C200.000E
port-channel3      :  destination-mac:0180.C200.000E
```

Use the **show lldp remote** command to show neighbour information.

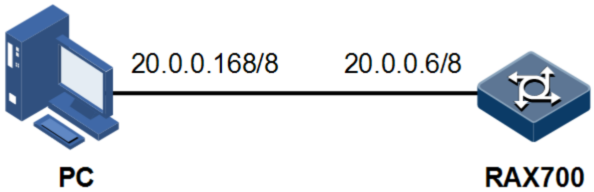
```
RAX700A#show lldp remote
Port  ChassisId         PortId       SysName   MgtAddress    ExpiredTime
--------------------------------------------------------------------------
uni 1000E.5E02.B010   uni1        RAX700B      10.10.10.2    106
RAX700B#show lldp remote
Port  ChassisId         PortId       SysName   MgtAddress    ExpiredTime
--------------------------------------------------------------------------
uni 1000E.5E12.F120   uni1       RAX700A     10.10.10.1      106
…
```

12.14.3 Example for outputting system logs to log host

Networking requirements

As shown in Figure 12-3, configure system log to output system logs of the RAX711-L to the log host, facilitating viewing them at any time.

Figure 12-3 Outputting system logs to log host



Configuration steps

Step 1 Configure the IP address of the RAX711-L.

```
Raisecom#config
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address 20.0.0.6 255.0.0.0 1
Raisecom(config-ip)#exit
```

Step 2 Output system logs to the log host.

```
Raisecom(config)#logging on
Raisecom(config)#logging time-stamp log datetime
Raisecom(config)#logging rate-limit 2
Raisecom(config)#logging host 20.0.0.168 warnings
```

Step 3 Save configurations.

```
Raisecom#write
```

Checking results

Use the **show logging** command to show system log configurations.

```
Raisecom#show logging
Syslog logging:          enable
Dropped Log messages:     0
Dropped debug messages:   0
```

```
Rate-limited:          2 messages per second
Logging config:        disable
Logging config level:    informational(6)
Squence number display:   disable
Log time stamp:        datetime
Debug time stamp:       none
Log buffer size:        4kB
Debug level:           low
Syslog history logging:   disable
Syslog history table size:1
Dest     Status   Level          LoggedMsgs  DroppedMsgs  Discriminator
------------------------------------------------------------------------
buffer   disable   informational(6)  0          0          0
console   enable   informational(6)  2          0          0
trap     disable  warnings(4)       0          0          0
file     disable  warnings(4)       0          0          0
monitor   disable  informational(6)  0          0          0
Log host information:
Max number of log server:    10
Current log server number:   1
```

View whether the log information is displayed on the terminal emulation Graphical User Interface (GUI) of the PC.

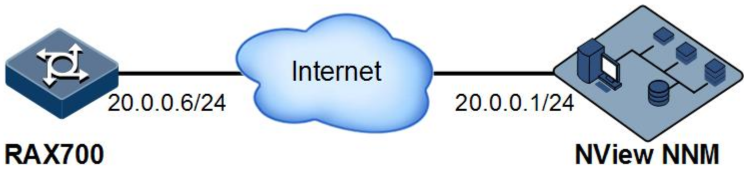
```
07-01-200811:31:28Local0.Debug20.0.0.6JAN 01 10:22:15 RAX711-L: CONFIG-7-
CONFIG:USER " raisecom "  Run " logging on "
07-01-200811:27:41Local0.Debug20.0.0.6JAN 01 10:18:30 RAX711-L: CONFIG-7-
CONFIG:USER " raisecom "  Run " ip address 20.0.0.6 255.0.0.0 1 "
07-01-200811:27:35Local0.Debug20.0.0.10JAN 01 10:18:24 RAX711-L: CONFIG-
7-CONFIG:USER " raisecom "  Run " ip address 20.0.0.6 255.0.0.1 1 "
07-01-200811:12:43Local0.Debug20.0.0.10JAN 01 10:03:41 RAX711-L: CONFIG-
7-CONFIG:USER " raisecom "  Run " logging host 20.0.0.168 local0 7 "
07-01-200811:12:37Local0.Debug20.0.0.10JAN 01 10:03:35 RAX711-L: CONFIG-
7-CONFIG:USER " raisecom "  Run " logging on"
```

12.14.4 Example for configuring hardware monitoring alarm output

Networking requirements

As shown in Figure 12-4, configure hardware monitoring to monitor the temperature of the RAX711-L. When the temperature value exceeds the threshold, an alarm is generated and is reported to the NView NNM system in a Trap form, notifying users to take related actions to prevent the fault.

Figure 12-4 Configuring hardware monitoring alarm output



Configuration steps

Step 1 Configure the IP address of the RAX711-L.

```
Raisecom#config
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address 20.0.0.6 255.255.255.0 1
Raisecom(config-ip)#exit
```

Step 2 Enable Trap.

```
Raisecom(config)#snmp-server enable traps
Raisecom(config)#snmp-server host 20.0.0.1 version 2c public
```

Step 3 Enable global hardware monitoring alarm Trap.

```
Raisecom(config)#snmp-server trap hw_monitor enable
```

Step 4 Configure temperature monitoring.

```
Raisecom(config)#hw_monitor temperature notifies
Raisecom(config)#hw_monitor temperature high 50
Raisecom(config)#hw_monitor temperature low 20
```

Step 5 Save configurations.

```
Raisecom#write
```

Checking results

Use the **show snmp config** command to show Trap configurations.

```
Raisecom#show snmp config
Contact information: support@Raisecom.com
Device location :   World China Raisecom
SNMP trap status:   enable
SNMP trap ip-binding: enable
SNMP engine ID:     800022B603000E5E156789
```

Use the **show snmp host** command to show Trap target host configurations.

```
Raisecom(config)#show snmp host
Index:        0
IP family:     IPv4
IP address:    20.0.0.1
Port:         162
User Name:     public
SNMP Version:   v2c
Security Level: noauthnopriv
TagList:      bridge config interface rmon snmp ospf
```

Use the **show hw_monitor** command to show hardware monitoring alarm configurations.

```
Raisecom#show hw_monitor
Traps alarm:                Enabled
Syslog alarm:               Disabled

Power Supply
   Notifies:               Enabled
   Syslog:                Enabled
Temperature
   High threshold(Celsius):   50
   Low  threshold(Celsius):   20
   Notifies:               Enabled
   Syslog:                Enabled
Voltage
   High threshold:          3460mV
   Low  threshold:          3150mV
   Notifies:               Enabled
   Syslog:                Enabled
```

13 Appendix

This chapter describe terms and abbreviations involved in this document.

- Terms
- Acronyms and abbreviations

13.1 Terms

C

Connectivity Fault Management (CFM)	CFM, defined by ITU-Y.1731 and IEEE802.1ag, is an end-to-end service-level Ethernet OAM technology. This function is used to actively diagnose faults for Ethernet Virtual Connection (EVC), provide cost-effective network maintenance solutions, and improve network maintenance.
Control word	The control word is a 4-byte TDM service data encapsulation packet header, used for circuit emulation services. The control word is mainly used to indicate a packet sequence number, link faults, shorter encapsulation packet, and encapsulation packet type.

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 of the IP packet is encapsulated with the 802.1Q frame header to form a VLAN frame structure.
Ethernet Linear Protection Switching (ELPS)	It is an APS protocol, based on ITU-T G.8031 standard, used to protect the Ethernet link. It is an end-to-end protection technology, including two line protection modes: linear 1:1 protection switching and linear 1+1 protection switching.

Ethernet Ring Protection Switching (ERPS)	It is an APS protocol based on ITU-T G.8032 standard, which is a link-layer protocol specially used for the Ethernet ring. In normal conditions, it can avoid broadcast storm caused by the data loop on the Ethernet ring. When the link or device on the Ethernet ring fails, services can be quickly switched to the backup line to enable services to be recovered in time.

F

Failover	Failover provides an interface linkage scheme, extending the range of link backup. Through monitoring upstream links and synchronizing downstream links, faults of the upstream device can be transferred quickly to the downstream device, and primary/backup switching is triggered. In this way, it avoids traffic loss because the downstream device does not sense faults of the upstream link.

J

Jitter Buffer	When packets are transmitted in the PSN, delay will be generated, which will influence the performance of emulation services. The Jitter Buffer can be used to reduce the influence caused by delay. Jitter Buffer is used to contain earlier- or later-received packets. Requirements are introduced to the distribution of Jitter Buffer capacity. If the capacity is too large, the buffer overflow can be prevented. However, longer delay will be generated. If the capacity is too small, it will cause buffer overflow. Therefore, you should set an appropriate value for the Jitter Buffer capacity.

L

Link Aggregation	With link aggregation, multiple physical Ethernet interfaces are combined to form a logical aggregation group. Multiple physical links in one aggregation group are taken as a logical link. Link aggregation helps share traffic among member interfaces in an aggregation group. In addition to effectively improving the reliability on links between devices, link aggregation can help gain greater bandwidth without upgrading hardware.

M

Mobile Backhaul	It is used to solve communication problems from BTS to BSC for 2G and from NodeB to RNC for 3G. In 2G times, mobile backhaul is realized through TDM microwave or SDH/PDH device since voice services play a primary role and there is no high requirement on the bandwidth. In 3G times, IP services are involved since lots of data services like HSPA and HSPA+ exist, and voice services tend to change to IP services, that is, IP RAN. To solve mobile backhaul problems of IP RAN, you need to establish a backhaul network, which can meet requirements on both data backhaul and voice transmission over IP (clock synchronization).

Q

QinQ	802.1Q in 802.1Q (QinQ), also called Stacked VLAN or Double VLAN, is extended from 802.1Q and defined by IEEE 802.1ad recommendation. This VLAN feature allows the equipment to add a VLAN tag to a tagged packet. The implementation of QinQ is to add a public VLAN tag to a packet with a private VLAN tag, making the packet encapsulated with two layers of VLAN tags. The packet is forwarded over the ISP's backbone network based on the public VLAN tag and the private VLAN tag is transmitted as the data part of the packet. In this way, the QinQ feature enables the transmission of the private VLANs to the peer end transparently. There are two QinQ types: basic QinQ and selective QinQ.

S

SyncE	A technology that adopts Ethernet link code stream to recover clocks, and provides high-precision frequency synchronization for the Ethernet similar to SDH clock synchronization. Different from the traditional network which just synchronizes data packets on the receiving node, the internal clock synchronization mechanism of the SyncE is real-time.

13.2 Acronyms and abbreviations

A

AC	Attachment Circuit
ACL	Access Control List
APS	Automatic Protection Switching
ASIC	Application Specific Integrated Circuit
ATM	Asynchronous Transfer Mode

B

BC	Boundary Clock

C

CAS	Channel Associated Signaling
CCS	Common Channel Signaling
CDMA2000	Code Division Multiple Access 2000
CE	Customer Edge
CES	Circuit Emulation Service
CESoPSN	Circuit Emulation Services over Packet Switch Network
CFM	Connectivity Fault Management
CoS	Class of Service
CR-LDP	Constraint-Routing Label Distribution Protocol

D

DoS	Deny of Service
DRR	Deficit Round Robin
DSCP	Differentiated Services Code Point
DUT	Device Under Test

E

EFM	Ethernet in the First Mile
ELPS	Ethernet Linear Protection Switching
ERPS	Ethernet Ring Protection Switching
EVC	Ethernet Virtual Connection

F

FEC	Forwarding Equivalence Class
FIB	Forwarding Information Base
FTP	File Transfer Protocol
FR	Frame Relay

G

GACH	Generic Associated Channel

GARP	Generic Attribute Registration Protocol
GPS	Global Positioning System
GSM	Global System for Mobile Communications
GVRP	GARP VLAN Registration Protocol

I

IANA	Internet Assigned Numbers Authority
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGMP Snooping	Internet Group Management Protocol Snooping
IP	Internet Protocol
ITU-T	International Telecommunications Union-Telecommunication Standardization Sector

L

LACP	Link Aggregation Control Protocol
LBM	LoopBack Message
LBR	LoopBack Reply
LDP	Label Distribution Protocol
LER	Label Edge Router
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
LOS	Loss of Signal
LTM	LinkTrace Message
LSR	Label Switching Router
LSA	Link Status Advertisement
LTR	LinkTrace Reply

M

MA	Maintenance Association
MAC	Medium Access Control
MAN	Metro Area Network

MD	Maintenance Domain
MEF	Metro Ethernet Forum
MEG	Maintenance Entity Group
MEP	Maintenance associations End Point
MIB	Management Information Base
MIP	Maintenance association Intermediate Point
MP-BGP	Multiprotocol Extensions for Border Gateway Protocol
MPLS	Multiprotocol Label Switching
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTU	Maximum Transfered Unit
MVR	Multicast VLAN Registration

N

NNM	Network Node Management

O

OAM	Operation, Administration, and Management
OC	Ordinary Clock
OOS	Out of Service

P

PC	Personal Computer
PE	Provider Edge
PPP	Point to Point Protocol
PSN	Packet Switched Network
PTP	Precision Time Protocol
PW	Pseudo Wire
PWE3	Pseudo Wire Emulation Edge-to-Edge

Q

QoS	Quality of Service

R

RADIUS	Remote Authentication Dial In User Service
RMON	Remote Network Monitoring
RMEP	Remote Maintenance association End Point
RNC	Radio Network Controller
RSTP	Rapid Spanning Tree Protocol
RSVP-TE	Resource Reservation Protocol Traffic Engineering
RTP	Real-time Transport Protocol

S

SAToP	Structure-Agnostic TDM over Packet
SES	Severely Errored Second
SFP	Small Form-factor Pluggables
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict-Priority
SSHv2	Secure Shell v2
STP	Spanning Tree Protocol

T

TACACS+	Terminal Access Controller Access Control System
TC	Transparent Clock
TCP	Transmission Control Protocol
TD-SCDMA	Time Division-Synchronous Code Division Multiple Access
TDM	Time Division Multiplex
TDMoP	Time Division Multiplex over Packet
TFTP	Trivial File Transfer Protocol
TLV	Type Length Value
ToS	Type of Service

V

VLAN	Virtual Local Area Network

VPN	Virtual Private Network

W

WAN	Wide Area Network
WCDMA	Wideband Code Division Multiple Access
WRR	Weight Round Robin

瑞斯康达科技发展股份有限公司
RAISECOM TECHNOLOGY CO.,LTD.
Address: 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