RAISECOM

www.raisecom.com

ISCOM21xx
Configuration Guide
(Rel_09)

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 supported by the ISCOM21xx, and related configurations, including basic principles and configuration procedure of Ethernet, route, reliability, OAM, security, and QoS, and related configuration examples.

The appendix lists terms, acronyms, and abbreviations involved in this document.

By reading this document, you can master principles and configurations of the ISCOM21xx, and how to network with the ISCOM21xx.

Versions

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

Product name	Hardware version	Software version
ISCOM2110EA-MA	B	ROS_4.14
ISCOM2118EA-MA	B	ROS_4.14
ISCOM2126E-MA	C	ROS_4.14
ISCOM2126EA-MA	C	ROS_4.14
ISCOM2126S-MA	E	ROS_4.14
ISCOM2128EA-MA	B	ROS_4.14
ISCOM2150-MA	B	ROS_4.14
ISCOM2110EA-MA-PWR	A	ROS_4.14
ISCOM2110A-MA-PWR	A	ROS_4.14
ISCOM2118EA-MA-PWR	C	ROS_4.14
ISCOM2126EA-MA-PWR	C	ROS_4.14
ISCOM2126E-MA-PWR	B	ROS_4.14
ISCOM2128EA-MA-PWR	A	ROS_4.14

Conventions

Symbol conventions

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

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

Convention	Description
[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 09 (2016-09-30)

Ninth commercial release

- Added port security MAC commands.
- Deleted SLA.
- Deleted cluster management.

Issue 08 (2015-12-31)

Eighth commercial release

- Deleted the related commands about IP routing.

Issue 07 (2015-07-22)

Seventh commercial release

- Added the following IPv6 configurations:
  - IPv6 address commands
  - Telnet commands
  - Routing commands
  - SNMP commands
  - DHCP Client commands
  - IPv6 ND commands
  - IPv6 Source Guard commands
  - IPv6 uploading/downloading
  - IPv6 ACL commands
  - RA Snooping commands
  - SNTP commands

- Added DHCP Relay commands.
- Added the feature of enabling interface+VLAN Snooping.
- Added the feature of static binding to change packet CoS.

Issue 06 (2015-04-30)

Sixth commercial release

- Fixed known bugs.

Issue 05 (2014-09-30)

Fifth commercial release

- Upgraded the hardware version of the ISCOM2118EA-MA to B.

Issue 04 (2013-12-31)

Fourth commercial release

- Added configurations of dual system software and dual configuration files.
- Modified company address and postal code.

Issue 03 (2013-09-30)

Third commercial release

- Upgraded the hardware version of the ISCOM2118EA-MA-PWR to C.
- Added a new model ISCOM2126E-MA.
- Added a new model ISCOM2150-MA.

Issue 02 (2013-08-15)

Second commercial release

- Upgraded the hardware version of the ISCOM2128EA-MA to B.
- Upgraded the hardware version of the ISCOM2126EA-MA-PWR to C.

Issue 01 (2013-02-01)

Initial commercial release

Contents

Figures

Tables

1 Basic configurations

This chapter describes basic principles and configuration procedures of the ISCOM21xx and provides related configuration examples, including the following sections:

- Accessing device
- CLI
- Managing users
- Managing files
- Configuring time management
- Configuring interface management
- Configuring basic information
- Task scheduling
- Watchdog
- Load and upgrade

1.1 Accessing device

1.1.1 Introduction

The ISCOM21xx can be configured and managed in Command Line Interface (CLI) mode or NView NNM mode.

The ISCOM21xx CLI mode has a variety of configuration modes:

- Console mode: it must be used in configuration for the first time. The ISCOM21xx supports the Console interface of the RJ45 type or USB type.
- Telnet mode: log in through the Console mode, open Telnet service on the ISCOM21xx, configure the IP address of the Layer 3 interface, configure the user name and password, and then conduct remote Telnet configuration.
- SSHv2 mode: before accessing the ISCOM21xx through SSHv2, you need to log in to the ISCOM21xx and start the SSHv2 service through the Console interface.

When configuring the ISCOM21xx in network management mode, you must first configure the IP address of the Layer 3 interface in CLI, and then configure the ISCOM21xx through the NView NNM system.

Note

Configuration steps in this document are in CLI mode.

1.1.2 Accessing through Console interface

The Console interface is an interface which is commonly used for a network device to be connected to a PC with terminal emulation program. You can use this interface to configure and manage the local device. This management method can communicate directly without a network, so it is called out-of-band management. You can also perform configuration and management on the ISCOM21xx through the Console interface when the network fails.

In the following two conditions, you can log in to the ISCOM21xx and configure it through the Console interface only:

- The ISCOM21xx is powered on to start for the first time.
- You cannot access the ISCOM21xx through Telnet.

Note

When logging in to the ISCOM21xx through the Console interface, use the CBL-RS232-DB9F/RJ45-2m/RoHS cable delivered with the ISCOM21xx. If you need to make the Console cable, see *ISCOM21xx Hardware Description*.

If you wish to access the ISCOM21xx on a PC through the Console interface, connect the Console interface on the ISCOM21xx to the RS-232 serial interface on the PC, as shown in Figure 1-1; then run the terminal emulation program such as Windows XP Hyper Terminal program on the PC to configure communication parameters as shown in Figure 1-2, and then log in to the ISCOM21xx.

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

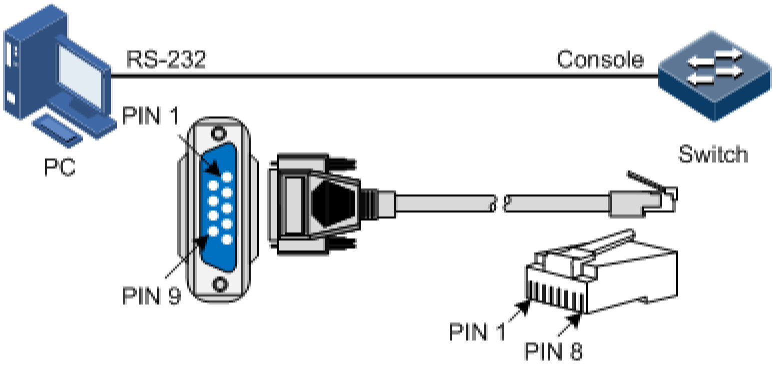
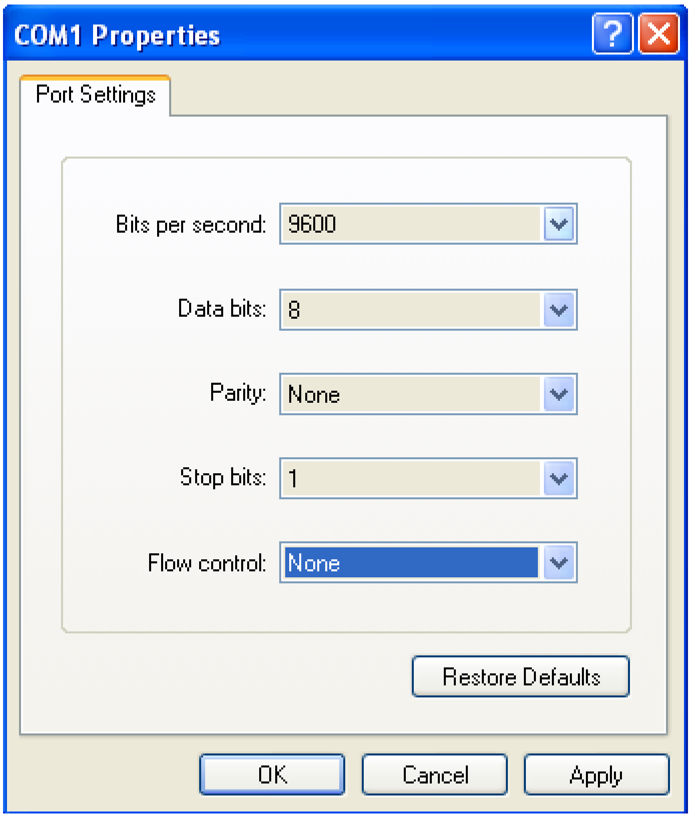


Figure 1-2 Configuring communication parameters in Hyper Terminal



Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

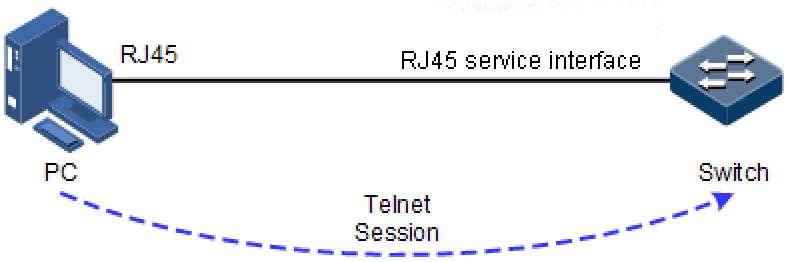
1.1.3 Accessing through Telnet

Use a PC to log in to the ISCOM21xx remotely through Telnet, log in to an ISCOM21xx from the PC at first, and then Telnet other ISCOM21xx devices on the network. Thus, you do not need to connect a PC to each ISCOM21xx.

Telnet services provided by the ISCOM21xx are as below.

- Telnet Server: run the Telnet client program on a PC to log in to the ISCOM21xx, and conduct configuration and management. As shown in Figure 1-3, the ISCOM21xx is providing Telnet Server service in this case.

Figure 1-3 Networking with device as Telnet server



Before accessing the ISCOM21xx through Telnet, you need to log in to the ISCOM21xx through the Console interface and start the Telnet service. Configure the ISCOM21xx as below.

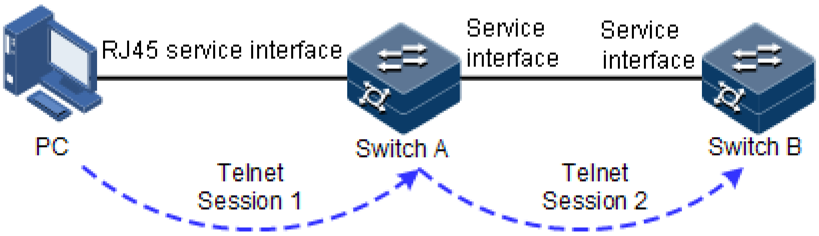
Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface ip if-number`	Enter Layer 3 interface configuration mode.

3	`Raisecom(config-ip)#ip address ip-address [ ip-mask ] [ vlan-id ]`
	`Raisecom(config-ip)#quit`
		Configure the IP address for the ISCOM21xx and bind the VLAN of specified ID. The interface on which the Telnet service is started belongs to this VLAN.

4	`Raisecom(config)#telnet-server link-local-address { enable | disable }`	(Optional) enable/disable the local link to be used for the Telnet session.
5	`Raisecom(config)#telnet-server accept port-list { all | port-list }`	(Optional) configure the interfaces that support Telnet.
6	`Raisecom(config)#telnet-server close terminal-telnet session-number`	(Optional) disconnect the specified Telnet session.
7	`Raisecom(config)#telnet-server max-session session-number`	(Optional) configure the maximum number of Telnet sessions supported by the ISCOM21xx.

- Telnet Client: after you connect a PC to the ISCOM21xx through the terminal emulation program or Telnet client program, telnet another device through the ISCOM21xx, and configure/manage it. As shown in Figure 1-4, Switch A not only acts as the Telnet server but also provides Telnet client service.

Figure 1-4 Networking with device as Telnet client



Configure the Telnet client as below.

Step	Command	Description
1	`Raisecom#telnet ip-address [ port port-id ]`	Log in to another device through Telnet.
2	`Raisecom(config)#telnet ipv6-address [ scope-id ] [ port ]`	Log in to another device through Telnet with an IPv6 address.

1.1.4 Accessing through SSHv2

Telnet is lack of security authentication and it transports packets by Transmission Control Protocol (TCP) which exists with big potential security hazard. Telnet service may cause hostile attacks, such as Deny of Service (DoS), host IP deceiving, and routing deceiving.

The traditional Telnet and File Transfer Protocol (FTP) transmit password and data in plaintext, which cannot satisfy users' security demands. SSHv2 is a network security protocol, which can effectively prevent the disclosure of information in remote management through data encryption, and provide greater security for remote login and other network services in network environment.

SSHv2 allows data to be exchanged through TCP and it builds up a secure channel over TCP. Besides, SSHv2 supports other service interfaces besides standard port 22, avoiding illegal attacks from the network.

Before accessing the ISCOM21xx through SSHv2, you must log in to the ISCOM21xx through the Console interface and start the SSHv2 service.

Default configurations of accessing through SSHv2 are as below.

Function	Default value
SSHv2 Server status	Disable
Local SSHv2 key pair length	512 bits
SSHv2 authentication method	password
SSHv2 authentication timeout	600s
Allowable failure times for SSHv2 authentication	20
SSHv2 snooping port number	22
SSHv2 session status	Enable

Configure SSHv2 service for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`generate ssh-key`** `[` *`length`* `]`	Generate local SSHv2 key pair and designate its length.
3	`Raisecom(config)#`**`ssh2 server`**	(Optional) start the SSHv2 server. Use the **no ssh2 server** command to shut down the SSHv2 server.
4	`Raisecom(config)#`**`ssh2 server authentication`** `{` **`password`** `|` **`rsa-key`** `}`	(Optional) configure SSHv2 authentication mode.
5	`Raisecom(config)#`**`ssh2 server authentication public-key`**	(Optional) type the public key of clients to the ISCOM21xx in rsa-key authentication mode.

Step	Command	Description
6	Raisecom(config)#**ssh2 server authentication-timeout** *period*	(Optional) configure SSHv2 authentication timeout. The ISCOM21xx refuses to authenticate the client and then closes the connection when client authentication times exceed the upper limit.
7	Raisecom(config)#**ssh2 server authentication-retries** *times*	(Optional) configure the allowable failure times for SSHv2 authentication. The ISCOM21xx refuses to authenticate and then closes the connection when client authentication failure numbers exceeds the upper limit.
8	Raisecom(config)#**ssh2 server port** *port-id*	(Optional) configure SSHv2 snooping port number. **Note** When you configure SSHv2 snooping port number, the input parameter cannot take effect until SSHv2 is restarted.
9	Raisecom(config)#**ssh2 server session** *session-list* **enable**	(Optional) enable SSHv2 sessions on the ISCOM21xx.

1.1.5 Checking configurations

Use the following commands to check the configuration results.

No.	Command	Description
1	Raisecom#**show telnet-server**	Show configurations of the Telnet server.
2	Raisecom#**show ssh2 public-key** [**authentication** | **rsa**]	Show the public key used for SSHv2 authentication on the ISCOM21xx and client.
3	Raisecom#**show ssh2** { **server** | **session** }	Show information about the SSHv2 server or sessions.

1.2 CLI

1.2.1 Introduction

The CLI is a medium for you to communicate with the ISCOM21xx. You can configure, monitor, and manage the ISCOM21xx through the CLI.

You can log in to the ISCOM21xx through a terminal or a PC that runs terminal emulation program. Enter commands at the system prompt.

The CLI supports the following features:

- Configure the ISCOM21xx locally through the Console interface.
- Configure the ISCOM21xx 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 the 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 ISCOM21xx.
- Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.
- The ISCOM21xx supports multiple intelligent analysis methods, such as fuzzy match and context association.

1.2.2 Levels

The ISCOM21xx uses hierarchy protection methods to divide command line into 16 levels from low to high.

- 0–4: visitor. Users can execute the **ping**, **clear**, **history** commands, and so on.
- 5–10: monitor. Users can execute the **show** command and so on.
- 11–14: operator. Users can execute commands for different services like Virtual Local Area Network (VLAN), Internet Protocol (IP), and so on.
- 15: administrator. Users can execute basic command for operating the system.

1.2.3 Modes

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

Establish a connection with the ISCOM21xx. If the ISCOM21xx is in default configurations, it will enter user EXEC mode, and the screen will display:

```
Raisecom>
```

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

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

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

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

Note

- The CLI prompts that Raisecom is a default host name. You can modify it by executing the **hostname** *string* command in privileged EXEC mode.
- Commands executed in global configuration mode can also be executed in other modes. The functions vary with command modes.
- You can use the **exit** or **quit** command to return to upper command mode. However, in privileged EXEC mode, you need to execute the **disable** command to return to user EXEC mode.
- You can use the **end** command to return to privileged EXEC mode from any modes but user EXEC mode and privileged EXEC mode.

The ISCOM21xx supports the following command line modes.

Mode	Enter method	Description
User EXEC	Log in to the ISCOM21xx, and input correct username and password	`Raisecom>`
Privileged EXEC	In user EXEC mode, input the **enable** command and correct password.	`Raisecom#`
Global configuration	In privileged EXEC mode, input the **config terminal** command.	`Raisecom(config)#`
Physical layer interface configuration	In global configuration mode, input the **interface port** *port-id* command.	`Raisecom(config-port)#`
Layer 3 interface configuration	In global configuration mode, input the **interface ip** *if-number* command.	`Raisecom(config-ip)#`
VLAN configuration	In global configuration mode, input the **vlan** *vlan-id* command.	`Raisecom(config-vlan)#`
Traffic classification configuration	In global configuration mode, input the **class-map** *class-map-name* command.	`Raisecom(config-cmap)#`
Traffic policy configuration	In global configuration mode, input the **policy-map** *policy-map-name* command.	`Raisecom(config-pmap)#`
Traffic policy configuration binding with traffic classification	In traffic policy configuration mode, input the **class-map** *class-map-name* command.	`Raisecom(config-pmap-c)#`
Access control list configuration	In global configuration mode, input the **access-list-map** *acl-number* { **deny** | **permit** } command.	`Raisecom(config-aclmap)#`
Service instance configuration	In global configuration mode, input the **service** *cisid* **level** *level* command.	`Raisecom(config-service)#`

Mode	Enter method	Description
MST region configuration	In global configuration mode, input the **spanning-tree region-configuration** command.	`Raisecom(config-region)#`
Profile configuration	In global configuration mode, input the **igmp filter profile** *profile-number* command.	`Raisecom(config-igmp-profile)#`

1.2.4 Shortcut keys

The ISCOM21xx supports the following command line shortcut keys:

Shortcut key	Description
Up Arrow (↑)	Show the previous command if there is any command entered earlier; the display has no change if the current command is the earliest one in history records.
Down Arrow (↓)	Show the next command if there is any newer command. The display does not change if the current command is the newest one in history records.
Left Arrow (←)	Move the cursor leftward by one character. The display does not change if the cursor is already at the beginning of the command.
Right Arrow (→)	Move the cursor rightward by one character. The display does not change if the cursor is already at the end of the command.
Backspace	Delete the character before the cursor. The display does not change if the cursor is already at the beginning of the command.
Tab	Press **Tab** after entering a complete keyword, and the cursor will automatically appear a space to the end. Press **Tab** again, and the system will show the follow-up entering keywords. Press **Tab** after entering an incomplete keyword, and the system automatically executes partial helps: • When only one keyword matches the entered incomplete keyword, the system takes the complete keyword to replace the entered incomplete keyword and leaves one space between the cursor and end of the keyword. • When no keyword or multiple keywords match the entered incomplete keyword, the system displays the prefix, and you can press **Tab** to check words circularly. In this case, there is no space from the cursor to the end of the keyword. Press **Space bar** to enter the next word. • If you enter an incorrect keyword, pressing **Tab** will move the cursor to the next line and the system will prompt an error. In this case, the entered keyword does not change.
Ctrl+A	Move the cursor to the beginning of the command line.

Shortcut key	Description
Ctrl+C	The ongoing command will be interrupted, such as **ping**, and **traceroute**.
Ctrl+D or **Delete**	Delete the character at the cursor.
Ctrl+E	Move the cursor to the end of the command line.
Ctrl+G	Delete all characters in the row.
Ctrl+K	Delete all characters from the cursor to the end of the command line.
Ctrl+L	Clear screen information.
Ctrl+N	Return to the previous mode.
Ctrl+X	Delete all characters before the cursor (except cursor location).
Ctrl+Z	Return to privileged EXEC mode from the current mode (excluding user EXEC mode).
Space or **Y**	Scroll down one screen.
Enter	Scroll down one line.

1.2.5 Acquiring help

Complete help

You can acquire complete help under following three conditions:

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

```
Raisecom>?
```

The command output is displayed as below.

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

- After you enter a keyword, press **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 command output is displayed as below.

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

- After you enter a keyword, press **Space** and enter a question mark (?), the value range and descriptions are displayed if the question mark (?) matches a parameter.

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

The command output is displayed as below.

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

Incomplete help

You can acquire incomplete help under following three conditions:

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

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

The command output is displayed as below.

```
class-map         Set class map
clear            Clear screen
cluster          Cluster configuration mode
cluster-autoactive  Cluster autoactive function
console-cli       Console CLI
cpu              Configure cpu parameters
create           Create static VLAN
```

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

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

The command output is displayed as below.

```
link-admin-status    link administrator status
link-state-tracking  Link state tracking
```

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

Error message

The ISCOM21xx prints out the following error messages according to the error type when you input incorrect commands.

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

Note

If there is error message mentioned above, use the CLI help message to solve the problem.

1.2.6 Display information

Display features

The CLI provides the following display features:

- The help information and prompt messages displayed at the CLI are in English.

- When messages are displayed at more than one screen, you can suspend displaying them with one of the following operations, as listed in Table 1-1.

Table 1-1 Shortcut keys for display features

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

Filtering displayed information

The ISCOM21xx provides a series of commands which begin with **show** to show configuration, running status, or diagnostic message of the device. You can add filtering rules to remove unwanted information.

The **show** 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.

Page-break

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

By default, page-break is enabled.

Configure page-break for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`terminal page-break enable`**	Enable page-break.

1.2.7 Command history

The historical commands can be automatically saved at the CLI. You can use the up arrow (↑) or down arrow (↓) to schedule a historical command. By default, the last 20 historical commands are saved. You can configure the number of commands to be saved at the CLI.

Configure command history for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom>`**`terminal history`** *`number`*	(Optional) configure the number of system stored historical command.

Step	Command	Description
2	Raisecom>**terminal time-out** *period*	(Optional) configure the Console terminal timeout period.
3	Raisecom>**enable**	Enter privileged EXEC mode.
4	Raisecom#**history**	Show historical input commands.
5	Raisecom#**show terminal**	Show terminal configurations.

1.2.8 Restoring default value of commands

The default value of command line can be restored by **no** form or **enable | disable** form.

To restore the default value of a command, use the **no**/**enable** | **disable** form of the command.

- **no** form of a command: be provided in front of a command and used to restore the default value. It is used to disable a feature, delete a configuration, or perform an operation that is opposite to the command. Therefore, the command with a **no** form is also called a reverse command.
- **enable** | **disable** form of a command: be provided behind a command or in the middle of a command. The **enable** parameter is used to enable some feature or function while the **disable** parameter is used to disable some feature or function.

For example:

- In physical layer configuration mode, the **description** *text* command is used to modify descriptions about an interface while the **no description** command is used to delete descriptions about the interface.
- Use the **shutdown** command in physical layer interface mode to disable an interface; use the **no shutdown** command to enable an interface.
- Use the **terminal page-break enable** command in global configuration mode to enable page-break; use the **terminal page-break disable** command to disable page-break.

Note

Most configuration commands have default values, which often are restored by the **no** form.

1.3 Managing users

1.3.1 Introduction

When you start the ISCOM21xx for the first time, connect the PC through the Console interface to the ISCOM21xx, input the initial user name and password in HyperTerminal to log in and configure the ISCOM21xx.

Note

By default, both the user name and password are raisecom

If there is not any privilege restriction, any remote user can log in to the ISCOM21xx through Telnet or access network by building Point to Point Protocol (PPP) connection when the Simple Network Management Protocol (SNMP) interface or other service interface of the ISCOM21xx are configured with IP address. This is unsafe to the ISCOM21xx and network. Thus, creating user for the ISCOM21xx and configuring password and privilege help manage the login users and ensures network and device security.

1.3.2 Configuring user management

Configure user management for the ISCOM21xx of as below.

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 login user privilege. The initial user privilege is 15, which is the highest privilege.
3	`Raisecom#`**`user`** *`user-name`* `{` **`allow-exec`** `|` **`disallow-exec`** `}` *`first-keyword`* `[` *`second-keyword`* `]`	Configure the priority rule for login user to perform the command line. ● The **allow-exec** parameter allows you to perform commands higher than the current priority. ● The **disallow-exec** parameter allows you to perform commands lower than the current priority only.
4	`Raisecom#`**`enable`** `[` *`privilege`* `]`	Configure the user right.

1.3.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show user`** `[` **`detail`** `]`	Show information about login users

1.4 Managing files

1.4.1 Managing BootROM files

The BootROM file is used to boot the ISCOM21xx and finish device initialization. You can upgrade the BootROM file through File Transfer Protocol (FTP) FTP or Trivial File Transfer Protocol (TFTP). By default, the name of the BootROM file is bootrom or bootromfull.

After being powered on, the ISCOM21xx runs the BootROM file. When the system prompts "Press space into Bootrom menu", press **Space** to enter the Bootrom menu.

```
begin...
ram size: 64M DDR  testing...done
File System Version:1.0

Init flash ...Done

Bootstrap_3.1.5.ISCOM2110EA-MA.1.20111012, Raisecom Compiled Oct 12 2011,
12:46:56
Base Ethernet MAC address: 00:0e:5e:13:d2:66

Press space into Bootstrap menu...
 4
```

In Boot mode, you can do the following operations.

Operation	Description
?	List all executable operations.
b	Quick execution for system bootrom software.
D	Choose the system software to be loaded upon device startup.
E	Format the memory of the ISCOM21xx.
h	List all executable operations.
N	Configure Medium Access Control (MAC) address.
R	Reboot the ISCOM21xx.
T	Download the system startup software through TFTP and replace it.
u	Download the system startup file through the XMODEM.
V	Show device BootROM version.

1.4.2 Managing system files

System files are the files needed for system operation (such as system software and configuration file). These files are usually saved in the memory. The ISCOM21xx manages them by a file system to facilitate user managing the memory. The file system can create, delete, and modify the file and directory.

In addition, the ISCOM21xx supports dual-system. There are 2 sets of system software saved at the memory. These 2 sets of system software are independent. When the ISCOM21xx fails to work due to upgrade failure in one set of system software, you can use the other set to boot the ISCOM21xx.

Manage system files for the ISCOM21xx as below.

All the following steps are optional and in any sequence.

Step	Command	Description
1	Raisecom#**download bootstrap** { **ftp** *ip-address user-name password file-name* | **tftp** *ip-address file-name* }	(Optional) download the BootROM file through FTP or TFTP.
2	Raisecom#**download system-boot** { **ftp** *ip-address user-name password file-name* | **tftp** *ip-address file-name* }	(Optional) download the system software through FTP or TFTP.
3	Raisecom#**upload system-boot** { **ftp** [*ip-address user-name password file-name*] | **tftp** [*ip-address file-name*] }	(Optional) upload the system software through FTP or TFTP.
4	Raisecom#**download backup-system ftp** *ip-address user-name password file-name* Raisecom#**download backup-system tftp** *ip-address file-name*	(Optional) download the backup system software through FTP or TFTP.
5	Raisecom#**upload backup-system ftp** *ip-address user-name password file-name* Raisecom#**upload backup-system tftp** *ip-address file-name*	(Optional) upload the backup system software through FTP or TFTP.
6	Raisecom#**erase** [*file-name*]	(Optional) delete files saved in the memory.

Manage system files based on IPv6 for the ISCOM21xx as below.

All the following steps are optional and in any sequence.

Step	Command	Description
1	Raisecom#**download bootstrap ftp6** *ipv6-address user-name password file-name*	(Optional) download the BootROM file based on IPv6 through FTP.
2	Raisecom#**download system-boot ftp6** *ipv6-address user-name password file-name*	(Optional) download the system software based on IPv6 through FTP.
3	Raisecom#**upload system-boot ftp6** *ipv6-address user-name password file-name*	(Optional) upload the system software based on IPv6 through FTP.
4	Raisecom#**download backup-system ftp6** *ipv6-address user-name password file-name*	(Optional) download the backup system software based on IPv6 through FTP.
5	Raisecom#**download backup-system ftp6** *ipv6-address user-name password file-name*	(Optional) upload the backup system software based on IPv6 through FTP.
6	Raisecom#**erase** [*file-name*]	(Optional) delete files saved in the memory.

1.4.3 Managing configuration files

Configuration files are loaded after starting the system; different files are used in different scenarios to achieve different service functions. After starting the system, you can configure the ISCOM21xx and save the configuration files. New configurations will take effect in next boot.

The configuration file has a suffix ".cfg", and can be opened by the text book program in Windows system. The contents are in the following format:

- Be saved as Mode+Command format.
- Just keep the non-default parameters to save space (see the command reference manual for default values of configuration parameters).
- Use the command mode for basic frame to organize commands. Put parameters of one mode together to form a section, and the sections are separated by the exclamation mark (!).

The ISCOM21xx starts initialization by reading configuration files from the memory after being powered on. Thus, the configurations in configuration files are called the default configurations. If there is no configuration file in the memory, the ISCOM21xx uses the default parameters for initialization.

The configuration that is currently used by the ISCOM21xx is called the running configuration.

You can modify the running configuration of ISCOM21xx through CLI. The running configuration can be used as initial configuration upon next power-on. You must use the **write** command to save running configurations in the memory and form a configuration file.

Manage configuration files for the ISCOM21xx as below.

All the following steps are optional and in any sequence.

Step	Command	Description
1	Raisecom#**download startup-config** { **ftp** [*ip-address user-name password file-name*] [**reservedevcfg**] | **tftp** [*ip-address file-name*] [**reservedevcfg**] }	(Optional) download the startup configuration file through FTP or TFTP.
2	Raisecom#**erase** [*file-name*]	(Optional) delete files saved in the memory.
3	Raisecom#**upload startup-config** { **ftp** [*ip-address user-name password file-name*] | **tftp** [*ip-address file-name*] }	(Optional) upload the startup configuration file through FTP or TFTP.
4	Raisecom#**write**	(Optional) save the running configuration file into the memory.

Manage configuration files based on IPv6 for the ISCOM21xx as below.

All the following steps are optional and in any sequence.

Step	Command	Description
1	`Raisecom#download startup-config ftp6 ipv6-address user-name password file-name`	(Optional) download the startup configuration file based on IPv6 through FTP.
2	`Raisecom#erase [ file-name ]`	(Optional) delete files saved in the memory.
3	`Raisecom#upload startup-config ftp6 ipv6-address user-name password file-name`	(Optional) upload the startup configuration file based on IPv6 through FTP.
4	`Raisecom#write`	(Optional) save the running configuration file into the memory.

1.4.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show startup-config [ file-name ]`	Show configurations loaded upon device startup.
2	`Raisecom#show running-config [ interface port [ port-id ] ]`	Show the running configurations.

1.5 Configuring time management

1.5.1 Configuring time and time zone

To coordinate the ISCOM21xx to work well with other devices, you must configure system time and the local time zone accurately.

The ISCOM21xx supports 3 system time modes, which are time stamp mode, auxiliary time mode, and default mode from high to low according to timing unit accuracy. You need to select the most suitable system time mode manually in accordance with actual application environment.

Default configurations of time and time zone are as below.

Function	Default value
System time	2000-01-01 08:00:00.000
System clock mode	Default
System local time zone	UTC+8
Time zone offset	+08:00

Function	Default value
DST status	Disable

Configure time and time zone for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**clock set** *hour minute second year month day*	Configure system time.
2	Raisecom#**clock timezone** { **+** | **-** } *hour minute timezone-name*	Configure system belonged time zone.
3	Raisecom#**clock mode** { **auxiliary** | **default** | **timestamp** }	Configure system clock mode.

1.5.2 Configuring DST

Daylight Saving Time (DST) is a kind of artificially stipulated local time system for saving energy. At present, there are nearly 110 countries operating DST every summer around the world, but different countries have different stipulations for DST. Thus, you should consider the local conditions when configuring DST.

Configure DST for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**clock summer-time enable**	Enable DST. Use the **clock summer-time disable** command to disable this function.
2	Raisecom#**clock summer-time recurring** { *week* | **last** } { **fri** | **mon** | **sat** | **sun** | **thu** | **tue** | **wed** } *month hour minute* { *week* | **last** } { **fri** | **mon** | **sat** |**sun** | **thu** | **tue** | **wed** } *month hour minute offset-mm*	Configure calculation period for system DST.

Note

- When you configure system time manually where the local 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; namely, configure time offset to 60 minutes. The period from 2 a.m. to 3 a.m. on the second Sunday, April each year does not exist. Manually configuring time during this period will fail.
- The summer time in southern hemisphere is opposite to northern hemisphere, which is from September to April of next year. If you configure the start time later than the ending time, the system will suppose that it is in the Southern Hemisphere. Namely, the summer time is the start time this year to the ending time of next year.

1.5.3 Configuring NTP

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

The purpose of NTP is to synchronize all clocks in a network quickly and then the ISCOM21xx can provide different applications over a unified time. Meanwhile, NTP can ensure very high accuracy, with accuracy of 10ms around.

The ISCOM21xx in support of NTP cannot only accept synchronization from other clock source, but also synchronize other devices as a clock source.

The ISCOM21xx adopts multiple NTP working modes for time synchronization:

- 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 active equity sends a clock synchronization message to the passive equity. The passive equity works in passive mode automatically after receiving the message and sends the answering message back. By exchanging messages, the two equities build up the symmetric peer mode. The active and passive equities in this mode can synchronize each other.

Default configurations of NTP are as below.

Function	Default value
Whether the ISCOM21xx is NTP master clock	No
Global NTP server	Inexistent
Global NTP equity	Inexistent
Reference clock source	0.0.0.0

Configure NTP for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`ntp server`** *`ip-address`* `[` **`version`** `[` **`v1`** `|` **`v2`** `|` **`v3`** `] ]`	(Optional) configure NTP server address for the client working in server/client mode.
3	`Raisecom(config)#`**`ntp peer`** *`ip-address`* `[` **`version`** `[` **`v1`** `|` **`v2`** `|` **`v3`** `] ]`	(Optional) configure NTP equity address for the ISCOM21xx working in symmetric peer mode.

Step	Command	Description
4	Raisecom(config)#**ntp refclock-master** [*ip-address*] [*stratum*]	Configure clock of the ISCOM21xx as NTP reference clock source for the ISCOM21xx.

Note

If the ISCOM21xx is configured as the NTP reference clock source, it cannot be configured as the NTP server or NTP symmetric peer; vice versa.

1.5.4 Configuring SNTP

Simple Network Time Protocol (SNTP) is used to synchronize the system time of the ISCOM21xx with the time of the SNTP device on the network. The time synchronized by SNTP protocol is Greenwich Mean Time (GMT), which can be translated into the local time according to system configurations of time zone.

Default configurations of SNTP are as below.

Function	Default value
IP address of the SNTP server	Inexistent

Configure SNTP for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sntp server** *ip-address*	(Optional) configure the IP address of the SNTP server for the client device working in server/client mode.
	Raisecom(config)#**sntp server ipv6** *ipv6-address*	

Note

After you configure the IP address of the SNTP server, the ISCOM21xx will try to obtain clock information from the SNTP server every 3s. The maximum timeout for clock information is 10s.

1.5.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show clock** [**summer-time-recurring**]	Show configurations of the system time, time zone, and DST.

No.	Command	Description
2	`Raisecom#show sntp`	Show SNTP configurations.
3	`Raisecom#show ntp status`	Show NTP configurations.
4	`Raisecom#show ntp associations [ detail ]`	Show NTP connection information.
5	`Raisecom(config)#show sntp6`	Show SNTP IPv6 status.

1.6 Configuring interface management

1.6.1 Default configurations of interfaces

Default configurations of physical layer interface are as below.

Function	Default value
Maximum forwarding frame length of interface	9712 bytes
Duplex mode of interface	Auto-negotiation
Interface rate	Auto-negotiation
Interface flow control status	Disable
Optical/Electrical mode of the Combo interface	Automatic
Flow control of the Combo interface	Disable
Time interval of interface dynamic statistics	2s
Interface status	Enable

1.6.2 Configuring basic attributes of interfaces

The interconnected devices cannot communicate normally if their interface attributes (such as MTU, duplex mode, and rate) are inconsistent, and then you have to adjust the interface attribute to make the devices at both ends match each other.

Configure basic attributes of interface of the ISCOM21xx.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface port` *port-id*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#flowcontrol { off | on }`	Enable/Disable flow control over 802.3x packets on the interface.

Step	Command	Description
4	`Raisecom(config-port)#`**`duplex`** `{` **`full`** `|` **`half`** `}`	Configure the duplex mode of the interface.
5	`Raisecom(config-port)#`**`speed`** `{` **`auto`** `|` **`10`** `|` **`100`** `|` **`1000`** `}`	Configure the interface rate. For optical interfaces, the interface rate depends on specifications of the optical module.
6	`Raisecom(config-port)#`**`mdi`** `{` **`across`** `|` **`auto`** `|` **`normal`** `}`	Configure the crossover mode of line order on the electrical interface.

1.6.3 Configuring flow control on interfaces

IEEE 802.3x is a flow control method for full duplex on the Ethernet data layer. When the client sends request to the server, it will send the PAUSE frame to the server if there is system or network jam. Then, it delays data transmission from the server to the client.

Configure flow control on interfaces for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#`**`flowcontrol`** `{` **`off`** `|` **`on`** `}`	Enable/Disable flow control over 802.3x packet on the interface.

1.6.4 Configuring Combo interface

The Combo interface on the ISCOM21xx supports both optical modules and electrical modules, so transmission media can be optical fiber or cables according to interface media type supported by the peer device. If both two kinds of transmission media for connection are used, service transmission can only use one of them at the same time.

The Combo interface selects transmission medium in two modes: mandatory and automatic. If the configuration mode is automatic and two kinds of transmission medium of optical fiber and cable connections are normal, the interface will automatically choose one of them as an effective transmission line as well as automatically select the other for service transmission when the current one fails.

In auto-selection mode, after the Combo optical interface and Combo electrical interface are configured respectively, the device automatically use the optical/electrical interface if needed, without configuring them every time upon use.

Configure the Combo interface for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface port port-id`	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#media-priority { fiber | copper }`	Configure optical/electrical priorities of the Combo interface. The optical/electrical priority selection function can make the ISCOM21xx select the optical interface or electrical interface in prior when inserting optical interface or electrical interface at the same time.
4	`Raisecom(config-port)#description medium-type { fiber | copper } word`	Configure optical/electrical description of the Combo interface.
5	`Raisecom(config-port)#speed medium-type { fiber | copper } { auto | 10 | 100 | 1000 }`	Configure the optical/electrical transmission rate of the Combo interface. The interface rate also depends on specifications of the selected module.
6	`Raisecom(config-port)#duplex medium-type copper { full | half }`	Configure electrical duplex mode of the Combo interface.
7	`Raisecom(config-port)#mdi medium-type copper { auto | normal | across }`	Configure the Combo interface as electrical interface MDI mode.
8	`Raisecom(config-port)#flowcontrol medium-type { fiber | copper } { on | off }`	Configure optical/electrical flow control on the Combo interface.

1.6.5 Configuring interface rate statistics

Configure interface rate statistics for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface port port-id`	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#sfp detect-mode { auto-detect | force-100base-x | force-1000base-x }`	Configure SFP interface detection mode. Non-SFP interfaces cannot be configured to detection mode.

1.6.6 Configuring interface statistics

Configure interface statistics for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#dynamic statistics time period`	Configure the period for interface dynamic statistics. By default, it is 2s.
3	`Raisecom(config)#clear interface port port-id statistics`	Clear interface statistics saved on the ISCOM21xx.

1.6.7 Enabling/Disabling interface

Enable/Disable an interface for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface port port-id`	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#shutdown`	Disable the current interface. Use the **no shutdown** command to re-enable the disabled interface.

1.6.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show interface port [ port-id ]`	Show interface status.
2	`Raisecom#show interface port port-id statistics dynamic [ detail ]`	Show interface statistics.
3	`Raisecom#show interface port [ port-id ] flowcontrol`	Show flow control on the interface.
4	`Raisecom#show system mtu`	Show system MTU.
5	`Raisecom#show combo description port [ port-id ]`	Show information about the Combo interface.
6	`Raisecom#show combo configuration port [ port-id ]`	Show configurations of the Combo interface.
7	`Raisecom#show sfp detect-mode port [ port-id ]`	Show detection mode of the SFP interface.

1.7 Configuring basic information

Configure basic information for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**hostname** *name*	(Optional) configure device name. By default, the device name is Raisecom. The system supports changing device name to make users distinguish different devices on the network. Device name become effective immediately, which can be seen in terminal prompt.
2	Raisecom#**language** { **chinese** | **english** }	(Optional) configure language mode. By default, the language is English. The system supports displaying help and prompt information in both English and Chinese.
3	Raisecom#**write**	Save configuration. Save configurations to the ISCOM21xx after configuration, and the new saved configurations will overwrite the original configurations. Without saving, the new configurations will lose after rebooting, and the ISCOM21xx will continue working with the original configuration. ⚠ **Caution** Use the **erase** *file-name* command to delete the configuration file. This operation cannot be rolled back, so use this command with care.
4	Raisecom#**reboot** [**now**]	(Optional) configure reboot options. When the ISCOM21xx fails, reboot it to try to solve the problem according to actual condition.
5	Raisecom#**erase** [*file-name*]	(Optional) delete files saved in the memory.

1.8 Task scheduling

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

The ISCOM21xx supports realizing task scheduling by combining the program list to command lines. You just need to specify the start time of the task, period, and end time in the program list, and then bind the program list to command lines to realize the periodic execution of command lines.

Configure task scheduling for the ISCOM21xx as below.

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`** *`period hour`*`:`*`minute`*`:`*`second`* `] }`	Create a schedule list, and configure it.
3	`Raisecom(config)#`*`command-string`* **`schedule-list`** *`list-number`*	Bind the command line which needs periodic execution and supports schedule list to the schedule list.
4	`Raisecom#`**`show schedule-list`** `[` *`list-number`* `]`	Show configurations of the schedule list.

1.9 Watchdog

External electromagnetic field interferes with the working of single chip microcomputer, and causes program fleet and dead circulation so that the system cannot work normally. Considering the real-time monitoring of the running state of single chip microcomputer, a program is specially used to monitor the running status of switch hardware, which is commonly known as the Watchdog.

The ISCOM21xx will be rebooted when it fails due to task suspension or dead circulation, and without kicking the dog within a kicking dog period.

The Watchdog function can prevent the system program from dead circulation due to uncertain fault, thus improving stability of the system.

Configure Watchdog for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`watchdog enable`**	Enable Watchdog.
2	`Raisecom#`**`show watchdog`**	Show Watchdog status.

1.10 Load and upgrade

1.10.1 Introduction

Load

Traditionally, configuration files are loaded through the serial interface, which takes a long time due to low rate and unavailable remote loading. FTP and TFTP loading modes can solve those problems and make operation more convenient.

The ISCOM21xx supports TFTP auto-loading mode.

TFTP auto-loading means that you can obtain the configuration files from a server and then configure the ISCOM21xx. Auto-loading allows configuration files to contain loading related commands for multiple configurations loading to meet file auto-loading requirements in complex network environment.

The ISCOM21xx provides several methods to confirm configuration file name in the TFTP server, such as manually inputting, obtaining through DHCP, and using default name of the configuration file. Besides, you can assign certain naming conventions for configuration files, and then the ISCOM21xx confirms the name according to naming conventions and its attributes (such as device type, MAC address, and software version).

Upgrade

The ISCOM21xx needs to be upgraded if you wish to add new features, optimize functions or solve current software version bugs.

The ISCOM21xx supports the following two upgrade modes:

- Upgrade through BootROM
- Upgrade through CLI

1.10.2 Configuring TFTP auto-loading mode

You need to build a TFTP environment before configuring TFTP auto-loading mode to interconnect the ISCOM21xx with the TFTP server.

Note

- When you perform configuration auto-loading, the priority of the IP address configured by the command is higher than the one obtained through DHCP.
- When you perform configuration auto-loading, the priorities of modes for obtaining configuration file names are: file name confirmed by naming convention > file name configured by command > file name obtained through DHCP Client.

Configure TFTP auto-loading for the ISCOM21xx as below.

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. By default, this address is not configured.

Step	Command	Description
3	`Raisecom(config)#`**`service config filename rule`** `[` *`rule-number`* `]`	Configure naming convention rule for file names. By default, there is no naming convention, and the system uses the default file name startup_config.conf.
4	`Raisecom(config)#`**`service config filename`** *`file-name`*	Specify the name of the configuration file to be loaded.
5	`Raisecom(config)#`**`service config version`** `{` **`system-boot`** `|` **`bootstrap`** `|` **`startup-config`** `}` *`version`*	(Optional) configure file version No.
6	`Raisecom(config)#`**`service config overwrite enable`**	(Optional) enable overwriting local configuration file.
7	`Raisecom(config)#`**`service config`**	Enable configuration auto-loading.
8	`Raisecom(config)#`**`service config trap enable`**	Enable Trap function.

1.10.3 Specifying system software to be loaded

The ISCOM21xx supports dual system software. You can specify the system software to be loaded upon next startup.

Specify system software to be loaded for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`multisystem select`** `{` **`0`** `|` **`1`** `}`	Specify the system software to be loaded upon next startup.

1.10.4 Specifying configuration file to be loaded

The ISCOM21xx supports dual configuration files. You can specify the configuration file to be loaded upon next startup.

Specify the configuration file to be loaded for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`startup-config select`** `{` **`0`** `|` **`1`** `}`	Specify the configuration file to be loaded upon next startup.

1.10.5 Upgrading system software through BootROM

You need to upgrade system software through BootROM in the following conditions:

- The device is started for the first time.
- A system file is damaged.
- The card is started improperly.

Before upgrading system software through BootROM, you should build a FTP environment, and use the PC as the FTP server and the ISCOM21xx as the client. Basic requirements are as below.

- The ISCOM21xx is connected to the FTP server through the service interface.
- Configure the FTP server. Ensure that the server is available.
- Configure the IP address of the TFTP server; keep it in the same network segment with IP address of the ISCOM21xx.

Upgrade system software through BootROM for the ISCOM21xx as below.

Step	Operation

1	Log in to the ISCOM21xx through the serial interface as the administrator and enter Privileged EXEC mode, reboot the ISCOM21xx by the **reboot** command.
	`Raisecom#reboot`
	`Please input 'yes' to confirm:yes`
	`Rebooting ...`

2	Click **Space** key to enter interface of **raisecom** when the display shows "Press space into Bootstrap menu...", then input "?" to display command list:
	`[Raisecom]:?`
	`?                 - List all available commands`
	` h                 - List all available commands`
	` V                 - Show bootstrap version`
	` b                 - Boot an executable image`
	` E                 - Format both DOS file systems`
	` T                 - Download system program`
	` u                 - XMODEM download system boot image`
	` N                 - set ethernet address`
	` R                 - Reboot`
	Caution
	The input letters are case sensitive.

Step	Operation

3	Input "T" to download system boot file through TFTP. The system displays the following information.
	`[Raisecom]:T`
	`dev name:et`
	`unit num:1`
	`file name: system_boot.Z ROS_4.14.1781.ISCOM2110EA-MA.167.20120813`
	`local ip: 192.168.1.1 192.168.18.250`
	`server ip: 192.168.1.2 192.168.18.16`
	`user:wrs  1`
	`password:wrs 123456`
	`Loading...   Done`
	`Saving file to flash...`
	Caution
	Ensure the input file name here is correct, the file name should not be longer than 80 characters.

4	Input "b" to quick execute bootstrap file. The ISCOM21xx will reboot and load the downloaded system boot file.

1.10.6 Upgrading system software through CLI

Before upgrading system software through CLI, you should build a FTP environment, and use a PC as the FTP server and the ISCOM21xx as the client. Basic requirements are as below.

- The ISCOM21xx is connected to the FTP/TFTP server.
- Configure the FTP/TFTP server. Ensure that the FTP/TFTP server is available.
- Configure the IP address of the FTP/TFTP server to ensure that ISCOM21xx can access the server.

Upgrade system software through CLI for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**download system-boot** { **ftp** [*ip-address user-name password file-name*] | **tftp** [*ip-address file-name*] }	Download system software through FTP/TFTP.
2	Raisecom#**write**	Write the configuration file into the memory.
3	Raisecom#**reboot** [**now**]	Reboot the ISCOM21xx, and it will automatically load the downloaded system software.

1.10.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show service config`	Show auto-loading information.
2	`Raisecom#show service config filename rule rule-number`	Show naming convention for configuration files.
3	`Raisecom#show version`	Show system version.

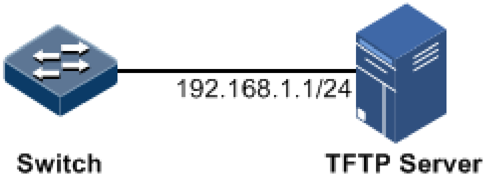
1.10.8 Exampe for configuring TFTP auto-loading

Networking requirements

As shown in Figure 1-5, connect the TFTP server with the switch, and configure auto-loading on the switch to make the switch automatically load configuration file from the TFTP server. Wherein, the IP address of the TFTP server is 192.168.1.1, the subnet mask is 255.255.255.0, and the naming convention for configuration file name meets the following conditions:

- The device model is included in the name of the configuration file.
- The complete MAC address is included in the name of the configuration file.
- First 2 digits of software version are included in the name of the configuration file.
- No extension rules are supported.

Figure 1-5 Auto-loading networking



Configuration steps

Step 1 Configure the IP address of the TFTP server.

```
Raisecom#config
Raisecom(config)#service config tftp-server 192.168.1.1
```

Step 2 Configure naming convention rules.

```
Raisecom(config)#service config filename rule 81650
```

Step 3 Configure the file name.

```
Raisecom(config)#service config filename ABC
```

Step 4 Enable overwriting the local configuration file.

```
Raisecom(config)#service config overwrite enable
```

Step 5 Enable configuring auto-loading.

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

Checking results

Use the **show service config** command to show auto-loading configurations.

```
Raisecom#show service config
  Auto upgrade :                    enable
  Config server IP address:           192.168.1.1
  Config filename rule:               81650
  Config file name:                   ABC
  System boot file version:           1107290
  Bootstrap flie version :            :48:050
  Startup-config file version:         0000000
  Overwrite local configuration file:  enable
  Send Completion trap:                disable
  Current File Type:                 none
  Operation states:                  done
  Result:                            none
```

2 Ethernet

This chapter describes basic principles and configuration procedures of Ethernet, and provides related configuration examples, including the following sections:

- MAC address table
- VLAN
- QinQ
- VLAN mapping
- Interface protection
- Port mirroring
- Layer 2 protocol transparent transmission

2.1 MAC address table

2.1.1 Introduction

The MAC address table records mappings between MAC addresses and interfaces. It is the basis for an Ethernet device to forward packets. When the Ethernet device forwards packets on Layer 2, it searches for the forwarding interface according to the MAC address table, implements fast forwarding of packets, and reduces broadcast traffic.

The MAC address table contains the following information:

- Destination MAC address
- Destination MAC address related interface ID
- Interface belonged VLAN ID
- Flag bits

The ISCOM21xx supports showing MAC address information by device, interface, or VLAN.

Modes for forwarding MAC addresses

When forwarding packets, based on the information about MAC addresses, the ISCOM21xx adopts the following modes:

- Unicast: when a MAC address entry, related to the destination MAC address of a packet, is listed in the MAC address table, the ISCOM21xx will directly forward the packet to the receiving interface through the egress interface of the MAC address entry. If the entry is not listed, the ISCOM21xx broadcasts the packet to other devices.
- Multicast: when the ISCOM21xx receives a packet of which the destination MAC address is a multicast address, and multicast is enabled, the ISCOM21xx sends the packet to the specified Report interface. If an entry corresponding to the destination address of the packet is listed in the MAC address table, the ISCOM21xx sends the packet from the egress interface of the entry. If the corresponding entry is not listed, the ISCOM21xx broadcasts the packet to other interfaces except the receiving interface.
- Broadcast: when the ISCOM21xx receives a packet with an all-F destination address, or its MAC address is not listed in the MAC address table, the ISCOM21xx forwards the packet to all interfaces except the receiving interface.

Classification of MAC addresses

The MAC address table contains static address entries and dynamic address entries.

- Static MAC address entry: also called permanent address, added and removed by the user manually, not aged with time. For a network with small changes of devices, manually adding static address entries can reduce the network broadcast traffic, improve the security of the interface, and prevent entries from losing after the system is reset.
- Dynamic MAC address entry: added through MAC address learning. The entries are aged according to the configured aging time, and will be lost after the system is reset.

The ISCOM21xx supports up to 32K dynamic MAC addresses, and each interface supports 1024 static MAC addresses.

Aging time of MAC addresses

There is limit on the capacity of the MAC address table on the ISCOM21xx. To maximize the use of the MAC address table, the ISCOM21xx uses the aging mechanism to update the MAC address table. For example, when the ISCOM21xx creates a dynamic entry, it starts the aging timer. If it does not receive packets from the MAC address in the entry during the aging time, the ISCOM21xx will delete the entry.

The ISCOM21xx supports automatic aging of MAC addresses. The aging time ranges from 10s to 1000000s and can be 0. The value 0 indicates no aging.

Note

The aging mechanism takes effect on dynamic MAC addresses only.

Policies of forwarding MAC addresses

The MAC address table has two forwarding policies:

When receiving packets on an interface, the ISCOM21xx searches the MAC address table for the interface related to the destination MAC address of packets.

- If search is successful, it forwards packets on the related interface, records the source MAC addresses of packets, interface ID of ingress packets, and VLAN ID in the MAC address table. If packets from other interfaces are sent to the MAC address, the ISCOM21xx can send them to the related interface.

- If search fails, it broadcasts packets to all interfaces except the source interface, and records the source MAC address in the MAC address table.

MAC address limit

MAC address limit is to limit the number of MAC addresses, avoid extending the searching time of forwarding entry caused by too large MAC address table and degrading the forwarding performance of the Ethernet switch, and it is effective to manage the MAC address table.

MAC address limit improves the speed of forwarding packets.

2.1.2 Preparing for configurations

Scenario

Configure the static MAC address table in the following situations:

- The static MAC address can be configured for a fixed server, special persons (manager, financial staff, and so on), fixed and important hosts to ensure that all data flow forwarding to these MAC addresses are forwarded from static MAC address related interface in priority.
- For the interface with fixed static MAC address, you can disable MAC address learning to avoid other hosts visiting LAN data from the interface.
- Configure the aging time of dynamic MAC addresses to avoid saving excessive MAC address entries in the MAC address table and running out of MAC address table resources, and to achieve aging of dynamic MAC addresses.

Prerequisite

N/A

2.1.3 Default configurations of MAC address table

Default configurations of the MAC address table are as below.

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

2.1.4 Configuring static MAC address

Configure static MAC address as below.

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

Step	Command	Description
2	Raisecom(config)#**mac-address-table static unicast** *mac-address* **vlan** *vlan-id* **port** *port-id*	Configure static unicast MAC addresses.
	Raisecom(config)#**mac-address-table static multicast** *mac-address* **vlan** *vlan-id* **port-list** *port-list*	Configure static multicast MAC addresses.
3	Raisecom(config)#**mac-address-table blackhole** { **destination** | **source** } *mac-address* **vlan** *vlan-id*	Configure blackhole MAC addresses.

Note

- The MAC address of the source device, multicast MAC address, FFFF.FFFF.FFFF, and 0000.0000.0000 cannot be configured as static unicast MAC address.
- The maximum number of static unicast MAC addresses supported by the ISCOM21xx is 1024.

2.1.5 Configuring multicast filtering mode for MAC address table

Configure multicast filtering mode for the MAC address table for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mac-address-table multicast filter-mode** { **filter-all** [**include-reserved-multicast**] | **forward-all** | **filter-vlan** *vlan-list* }	Configure multicast filtering mode of MAC address table.

2.1.6 Configuring MAC address learning

Configure MAC address learning for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mac-address-table learning** { **enable** | **disable** } { **port-list** { **all** | *port-list* } | **vlanlist** *vlan-id* }	Enable/Disable MAC address learning.

2.1.7 Configuring MAC address limit

Configuring interface-based MAC address limit

Configure the interface-based MAC address limit for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface`** *`interface-type interface-number`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#`**`mac-address-table threshold`** *`threshold-value`*	Configure interface-based MAC address limit.

2.1.8 Configuring aging time of MAC addresses

Configure the aging time of MAC addresses for ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`mac-address-table aging-time`** `{` **`0`** `|` *`period`* `}`	Configure the aging time of MAC addresses. The aging time ranges from 10s to 1000000s, and can be 0 which indicates no aging.

2.1.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show mac-address-table static`** `[` **`port`** *`port-id`* `|` **`vlan`** *`vlan-id`* `]`	Show static unicast MAC addresses.
2	`Raisecom#`**`show mac-address-table multicast`** `[` **`vlan`** *`vlan-id`* `]` `[` **`count`** `]`	Show all Layer 2 multicast addresses and the current multicast MAC address number.
3	`Raisecom#`**`show mac-address-table l2-address`** `[` **`count`** `]` `[` **`vlan`** *`vlan-id`* `|` **`port`** *`port-id`* `]`	Show all Layer 2 unicast MAC addresses and the current unicast MAC address number.
4	`Raisecom#`**`show mac-address-table threshold`** `[` **`port-list`** *`port-list`* `]`	Show dynamic MAC address limit.
5	`Raisecom#`**`show mac aging-time`**	Show the aging time of dynamic MAC addresses.

2.1.10 Maintenance

Maintain the ISCOM21xx as below.

Command	Description
`Raisecom(config)#clear mac-address-table { all | blackhole | dynamic | static } [ vlan vlan-id ]`	Clear MAC address.
`Raisecom#search mac-address mac-address`	Search MAC address.

2.1.11 Example for configuring MAC address table

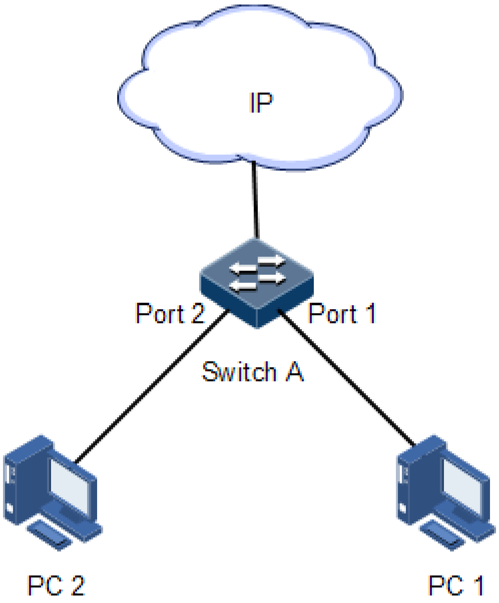
Networking requirements

Configure static unicast MAC address for Port 2 on Switch A, and configure the aging time for dynamic MAC addresses (it takes effect only after dynamic MAC address learning is enabled).

As shown in Figure 2-1, configure Switch A as below:

- Create VLAN 10, and activate it.
- Configure a static unicast MAC address 0001.0203.0105 on Port 2, and configure its VLAN to VLAN 10.
- Configure the aging time to 500s.

Figure 2-1 MAC networking



Configuration steps

Step 1 Create VLAN 10 and active it, and add Port 2 into VLAN 10.

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

Step 2 Configure a static unicast MAC address on Port 2, and configure its VLAN to VLAN 10.

```
Raisecom(config)#mac-address-table static unicast 0001.0203.0405 vlan 10
port 2
```

Step 3 Configure the aging time to 500s.

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

Checking results

Use the **show mac-address-table l2-address port** *port-id* command to show configurations of MAC addresses.

```
Raisecom#show mac-address-table l2-address port 2
Aging time: 500 seconds
Mac Address       Port        Vlan    Flags
-------------------------------------------------------
0001.0203.0405      2         10      Static
```

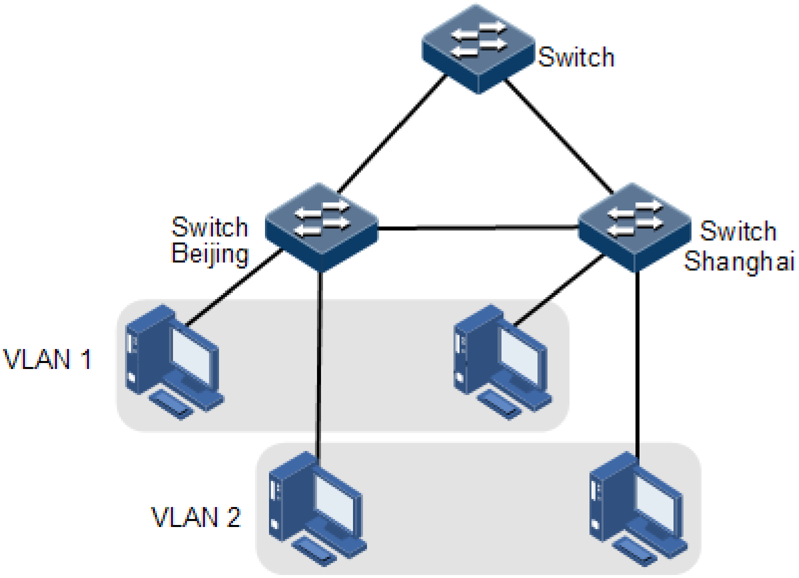
2.2 VLAN

2.2.1 Introduction

Overview

Virtual Local Area Network (VLAN) is a protocol to solve Ethernet broadcast and security problems. It is a Layer 2 isolation technique that partitions a LAN to different broadcast domains logically rather than physically, and then the different broadcast domains can work as virtual groups without influence on each other. VLAN has the same features as LAN, but members in one VLAN can access one another without physical restriction.

Figure 2-2 Partitioning VLANs



VLAN technique can partition a physical LAN into different broadcast domains logically. Hosts without intercommunication requirements can be isolated by VLAN, so VLAN partitioning improves network security, and reduces broadcast flow and broadcast storm.

The ISCOM21xx supports interface-based VLAN partitioning.

The ISCOM21xx complies with IEEE 802.1Q standard VLAN and supports 4094 concurrent VLANs.

Interface mode and packet processing

The interface modes of the ISCOM21xx include Access mode and Trunk mode. Table 2-1 lists interfaces types and modes for processing packets.

Table 2-1 Interface mode and packet processing

Interface type	Processing ingress packets		Processing egress packets
	Untag packets	**Tag packets**	
Access	Add Access VLAN Tag to the packet.	• If the VLAN ID is equal to the Access VLAN ID, receive the packet. • If the VLAN ID is not equal to the Access VLAN ID, discard the packet.	• If the VLAN ID is equal to the Access VLAN ID, remove Tag and transmit the packet. • If the VLAN ID of the packet is not included the VLAN ID list allowed to pass by the interface, discard the packet.
Trunk	Add Native VLAN Tag to the packet.	• If the packet VLAN ID is included in the VLAN ID list allowed to pass by the interface, receive the packet. • If the packet VLAN ID is not included in the VLAN ID list allowed to pass by the interface, discard the packet.	• If the VLAN ID is equal to the Native VLAN ID, remove Tag and transmit the packet. • If the VLAN ID is not equal to the Native VLAN ID, and the interface allows the packet to pass, transmit the packet with Tag.

Note

- By default, the default VLAN on the ISCOM21xx is VLAN 1.
- By default, the Access VLAN of the Access interface is VLAN 1, and the Native VLAN of the Trunk interface is VLAN 1.
- By default, VLAN 1 is in the list permitted by all interfaces. Use the **switchport access egress-allowed vlan** { { **all** | *vlan-list* } [**confirm**] | { **add** | **remove** } *vlan-list* } command to modify the VLAN list allowed to pass by the Access interface. Use the **switchport trunk allowed vlan** { { **all** | *vlan-list* } [**confirm**] | { **add** | **remove** } *vlan-list* } command to modify the VLAN list allowed to pass by the Trunk interface.

2.2.2 Preparing for configurations

Scenario

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

- One kind is that in a small LAN several VLANs are created on a device, the hosts that connect to the device are divided by VLAN. 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. Generally, the interface to connect host is in Access mode.
- The other kind is that in bigger LAN or enterprise network multiple devices connect to multiple hosts and the devices are cascaded, and data packets carry VLAN Tag for forwarding. The interfaces in the same VLAN on multiple devices can communicate, but the interfaces in different VLANs cannot communicate. This mode is used in enterprise that has many employees and needs a large number of hosts, in the same department but different position, the hosts in one department can access one another, so users have to partition VLANs on multiple devices. Layer 3 devices like router are required if users want to communicate among different VLAN. The cascaded interfaces among devices are configured in Trunk mode.

When configuring the IP address for VLAN, you can associate a Layer 3 interface for it. Each Layer 3 interface corresponds to one IP address and one VLAN.

Prerequisite

N/A

2.2.3 Default configurations of VLAN

Default configurations of VLAN are as below.

Function	Default value
Create VLAN	VLAN 1
Active status of static VLAN	Suspend
Interface mode	Access
Access VLAN of the Access interface	VLAN 1

Function	Default value
Native VLAN of the Trunk interface	VLAN 1
Allowed VLAN in Trunk mode	All VLANs
Allowed Untag VLAN in Trunk mode	VLAN 1

2.2.4 Configuring VLAN attributes

Configure VLAN attributes for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`create vlan`** *`vlan-list`* `{` **`active`** `|` **`suspend`** `}`	Create VLAN. The command can also be used to create VLANs in batches.
3	`Raisecom(config)#`**`vlan`** `v`*`lan-id`*	Enter VLAN configuration mode.
4	`Raisecom(config-vlan)#`**`name`** *`vlan-name`*	(Optional) configure VLAN name.
5	`Raisecom(config-vlan)#`**`state`** `{` **`active`** `|` **`suspend`** `}`	Configure VLAN in active or suspend status.

Note

- The VLAN created by the **vlan** *vlan-id* command is in suspend status, you need to use the **state active** command to activate VLAN if they want to make it effective in system.
- By default, there is VLAN 1, the default VLAN (VLAN 1). All interfaces in Access mode belong to the default VLAN. VLAN 1 cannot be created and deleted.
- By default, the default VLAN (VLAN 1) is called Default; cluster VLAN Other VLAN is named as "VLAN + 4-digit VLAN ID". For example, VLAN 10 is named VLAN 0010 by default, and VLAN 4094 is named as "VLAN 4094" by default.
- All configurations of VLAN are not effective until the VLAN is activated. When VLAN status is Suspend, you can configure the VLAN, such as delete/add interface, configure VLAN name, and so on. The system will keep the configurations, once the VLAN is activated, the configurations will take effect in the system.

2.2.5 Configuring interface mode

Configure interface mode for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**switchport mode** { **access** | **trunk** }	Configure the interface to Access or Trunk mode.

2.2.6 Configuring VLAN on Access interface

Configure VLAN on the Access interface for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**switchport mode access** Raisecom(config-port)#**switchport access vlan** *vlan-id*	Configure interface in Access mode and add Access interface into VLAN.
4	Raisecom(config-port)#**switchport access egress-allowed vlan** { { **all** | *vlan-list* } [**confirm**] | { **add** | **remove** } *vlan-list* }	(Optional) configure Access interface permitted VLAN.

Note

- The interface allows Access VLAN packets to pass regardless of configuration for VLAN permitted by the Access interface. the forwarded packets do not carry VLAN Tag.
- When configuring the Access VLAN, the system creates and activates a VLAN automatically if you have not created and activated a VLAN in advance.
- If you delete or suspend the Access VLAN manually, the system will automatically configure the interface Access VLAN as the default VLAN.
- If the configured Access VLAN is not default VLAN and there is no default VLAN in the allowed VLAN list of the Access interface, the interface does not allow default VLAN packets to pass.
- The allowed VLAN list of the Access interface is only effective to static VLANs, and ineffective to dynamic VLAN, and so on.

2.2.7 Configuring VLAN on Trunk interface

Configure VLAN on Trunk interface for the ISCOM21xx as below.

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

Step	Command	Description
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**switchport mode trunk**	Configure interface in Trunk mode.
4	Raisecom(config-port)#**switchport trunk native vlan** { **tagged** | **untagged** }	Configure the interface Native VLAN.
5	Raisecom(config-port)#**switchport trunk allowed vlan** { { **all** | *vlan-list* } [**confirm**] | { **add** | **remove** } *vlan-list* }	(Optional) configure VLANs allowed to pass by the Trunk interface.
6	Raisecom(config-port)#**switchport trunk untagged vlan** { { **all** | *vlan-list* } [**confirm**] | { **add** | **remove** } *vlan-list* }	(Optional) configure Untag VLANs allowed to pass by the Trunk interface.
7	Raisecom(config-port)#**switchport reject-frame untagged**	(Optional) configure the Trunk interface to prohibit Untag packets from passing.

Note

- The interface allows Native VLAN packets to pass regardless of configuration in the VLAN list and Untagged VLAN list allowed by the Trunk interface and, the forwarded packets do not carry VLAN Tag.
- The system will create and activate the VLAN if no VLAN is created and activated in advance when configuring the Native VLAN.
- The system configures the interface Trunk Native VLAN as the default VLAN if you have deleted or blocked Native VLAN manually.
- The interface allows incoming and outgoing VLAN packet allowed by the Trunk interface. If the VLAN is Trunk Untagged VLAN, the VLAN Tag is removed from the packets at the egress interface; otherwise the packets are not modified.
- If the configured Native VLAN is not default VLAN, and there is no default VLAN in Trunk interface allowed VLAN list, the interface will not allow default VLAN packets to pass.
- When configuring Trunk Untagged VLAN list, the system automatically adds all Untagged VLAN into the VLAN allowed by the Trunk interface.
- The VLAN list and Untagged VLAN list allowed by the Trunk interface are only effective to static VLAN, and ineffective for dynamic VLAN, and so on.

2.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show vlan** [*vlan-list* | **static** | **dynamic**]	Show VLAN configuration.
2	Raisecom#**show interface port** [*port-id*] **switchport**	Show interface VLAN configuration.

No.	Command	Description
3	`Raisecom#show switchport reject-frame untagged`	Show the status of disallowing Untagged packets to pass.

2.3 QinQ

2.3.1 Introduction

QinQ (also known as Stacked VLAN or Double VLAN) technique is an extension for 802.1Q defined in IEEE 802.1ad standard.

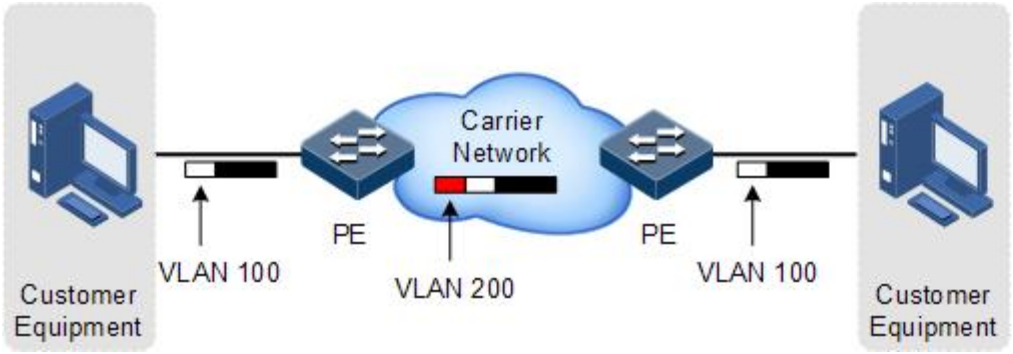
Basic QinQ is a simple Layer 2 VPN tunnel technique, which encapsulate outer VLAN Tag for user private network packet at the carrier access end, then the packet takes double VLAN Tag to transmit through backbone network (public network) of carrier. In public network, packet just be transmitted in accordance with outer VLAN Tag (namely the public network VLAN Tag), the user private network VLAN Tag is transmitted as data in packets.

This technique can save public network VLAN ID resource. You can mark out private network VLAN ID to avoid conflict with public network VLAN ID.

Basic QinQ

Figure 2-3 shows typical networking with basic QinQ, with the ISCOM21xx as the Provider Edge (PE).

Figure 2-3 Typical networking with basic QinQ



The packet transmitted to the PE from user device, and the VLAN ID of packet Tag is 100. The packet will be added with outer Tag with VLAN 200 when passing the user side interface on the PE device and then enter the PE network.

The VLAN 200 packet is transmitted to the PE on the other end of the carrier, and then the other Switch will remove the outer Tag VLAN 200 and send it to the user device. So the packet returns to the status that it carries VLAN 100 Tag only.

Selective QinQ

Selective QinQ is an enhancement to basic QinQ, which classifies flows by user data features, then encapsulates different types of flows with different outer VLAN Tags. This technique is implemented by combination of the interface and VLAN. Selective QinQ can perform different actions on different VLAN Tags received by one interface and add different outer VLAN IDs for different inner VLAN IDs. According to configured mapping rules for inner and outer Tags, you can encapsulate different outer Tags for different inner Tag packets.

Selective QinQ makes structure of the carrier network more flexible. You can classify different terminal users on the access device interface by VLAN Tag and then add different outer Tags for services of different types of users. On the public network, you can configure QoS policy according to outer Tag and configure data transmission priority flexibly to make different types of users receive corresponding services.

2.3.2 Preparing for configurations

Scenario

With application of basic QinQ, you can add outer VLAN Tag to plan Private VLAN ID freely to make the user data at both ends of carrier network transparently transmitted without conflicting with the VLAN ID in Service Provider (SP) network.

Prerequisite

- Connect the interface and configure its physical parameters to make it Up.
- Create VLANs.

2.3.3 Default configurations of QinQ

Default configurations of QinQ are as below.

Function	Default value
Outer Tag TPID	0x8100
Basic QinQ status	Disable

2.3.4 Configuring basic QinQ

Configure basic QinQ on the ingress interface as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`mls double-tagging tpid`** *`tpid`*	(Optional) configure TPID.
3	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
4	`Raisecom(config-port)#`**`switchport qinq dot1q-tunnel`**	Enable basic QinQ on the interface.

2.3.5 Configuring selective QinQ

Configure selective QinQ on the ingress interface as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`mls double-tagging tpid`** *`tpid`*	(Optional) configure TPID.
3	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
4	`Raisecom(config-port)#`**`switchport vlan-mapping`** *`vlan-list`* **`add-outer`** *`vlan-id`* [**`cos`** *`cos-value`*]	Configure selective QinQ rules on the interface.

2.3.6 Configuring egress interface to Trunk mode

Configure basic QinQ or selective QinQ on the network side interface as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#`**`switchport mode trunk`**	Configure interface trunk mode, allowing double Tag packet to pass.

2.3.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show switchport qinq`**	Show configurations of basic QinQ.
2	`Raisecom#`**`show interface port`** [*`port-id`*] **`vlan-mapping add-outer`**	Show configurations of selective QinQ.

2.3.8 Maintenance

Use the following commands to check configuration results.

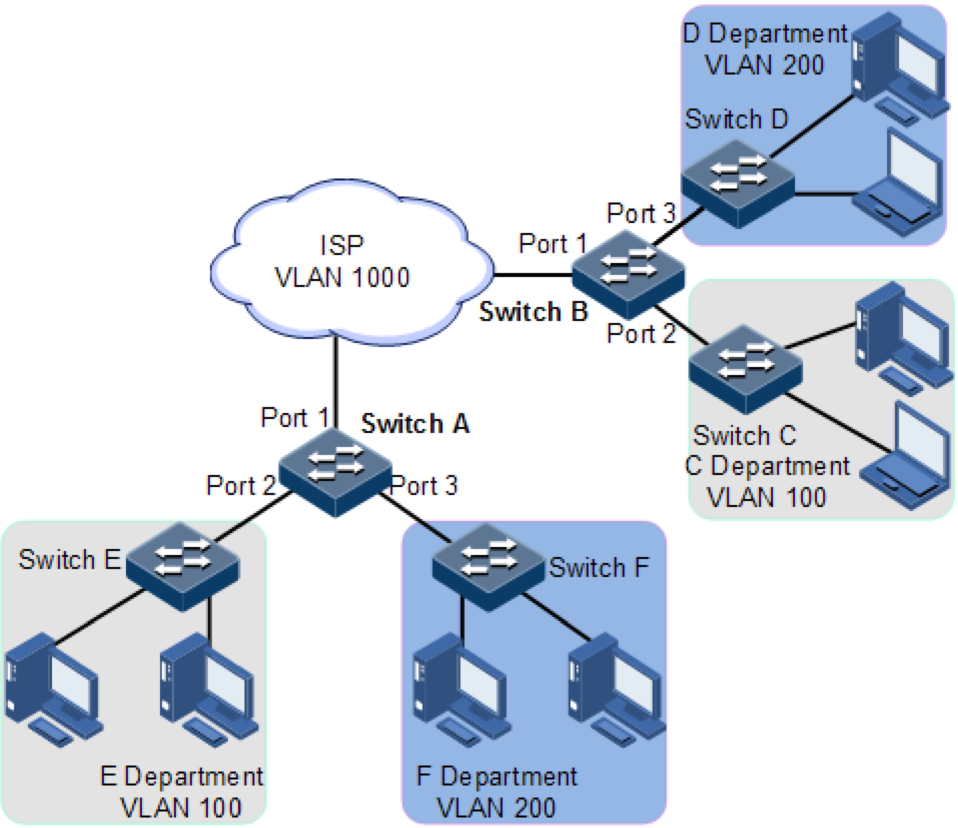
Command	Description
`Raisecom(config)#clear double-tagging-vlan statistics outer { vlan-id | any } inner { vlan-id | any }`	Clear statistics of double VLAN Tag packets.

2.3.9 Example for configuring basic QinQ

Networking requirements

As shown in Figure 2-4, Switch A and Switch B are connected to VLAN 100 and VLAN 200 respectively. Department C and department E need to communicate through the carrier network. Department D and Department F need to communicate, too. Thus, you need to configure the outer Tag to VLAN 1000. Configure Port 2 and Port 3 to dot1q-tunnel mode on Switch A and Switch B, and connect these two interfaces two different VLANs. Port 1 is the uplink port connected to the ISP, and it is configured to the Trunk mode to allow double Tag packets to pass. The carrier TPID is 9100.

Figure 2-4 Basic QinQ networking



Configuration steps

Step 1 Create VLAN 100, VLAN 200, and VLAN 1000 and activate them. TPID is 9100.

Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#mls double-tagging tpid 9100
SwitchA(config)#create vlan 100,200,1000 active
```

Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#mls double-tagging tpid 9100
SwitchB(config)#create vlan 100,200,1000 active
```

Step 2 Configure Port 2 and Port 3 to dot1q mode.

Configure Switch A.

```
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk native vlan 1000
SwitchA(config-port)#switchport qinq dot1q-tunnel
SwitchA(config-port)#exit
SwitchA(config)#interface port 3
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk native vlan 1000
SwitchA(config-port)#switchport qinq dot1q-tunnel
SwitchA(config-port)#exit
```

Configure Switch B.

```
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport trunk native vlan 1000
SwitchB(config-port)#switchport qinq dot1q-tunnel
SwitchB(config-port)#exit
SwitchB(config)#interface port 3
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport trunk native vlan 1000
SwitchB(config-port)#switchport qinq dot1q-tunnel
SwitchB(config-port)#exit
```

Step 3 Configure Port 1 to allow double Tag packets to pass.

Configure Switch A.

```
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk allowed vlan 1000 confirm
```

Configure Switch B.

```
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport trunk allowed vlan 1000 confirm
```

Checking results

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

Take Switch A for example.

```
SwitchA#show switchport qinq
Outer TPID: 0x9100
 Interface      QinQ Status
----------------------------
  1             --
  2          Dot1q-tunnel
  3          Dot1q-tunnel
     …
```

2.3.10 Example for configuring selective QinQ

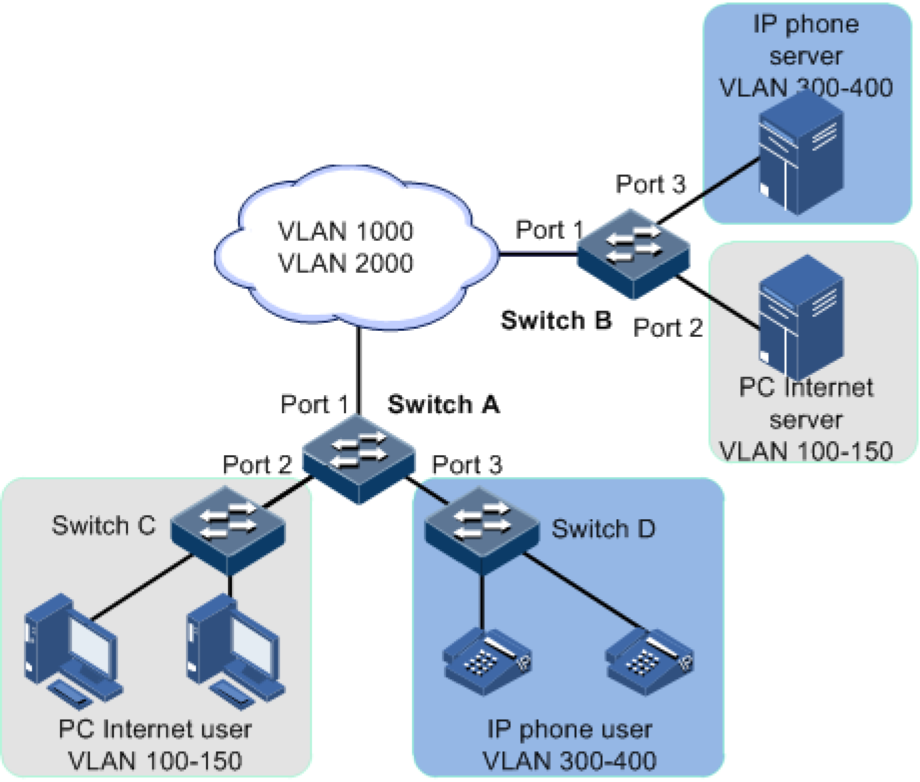
Networking requirements

As shown in Figure 2-5, the carrier network contains common PC Internet service and IP phone service. PC Internet service is assigned to VLAN 1000, and IP phone service is assigned to VLAN 2000.

Configure Switch A and Switch B as below to make client and server communicate through carrier network:

- Add outer Tag VLAN 1000 to the VLANs 100–150 assigned to PC Internet service.
- Add outer Tag 2000 for VLANs 300–400 for IP phone service.
- The carrier TPID is 9100.

Figure 2-5 Selective QinQ networking



Configuration steps

Step 1 Create and activate VLAN 100, VLAN 200, and VLAN 1000. The TPID is 9100.

Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#mls double-tagging tpid 9100
SwitchA(config)#create vlan 100-150,300-400,1000,2000 active
```

Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#mls double-tagging tpid 9100
SwitchB(config)#create vlan 100-150,300-400,1000,2000 active
```

Step 2 Configure Port 2 and Port 3 to dot1q mode.

Configure Switch A.

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

Configure Switch B.

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

Step 3 Configure Port 1 to allow double Tag packets to pass.

Configure Switch A.

```
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk allowed vlan 1000,2000 confirm
```

Configure Switch B.

```
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport trunk allowed vlan 1000,2000 confirm
```

Checking results

Use the **show interface port** *port-id* **vlan-mapping add-outer** command to show QinQ configurations.

Take Switch A for example.

```
SwitchA#show interface port 2 vlan-mapping add-outer
Based inner VLAN QinQ mapping rule:
Port Original Inner VLAN List      Add-outer VLAN Hw Status  Hw-ID
----------------------------------------------------------------------
2         100-150                      1000           Enable    1
SwitchA#show interface port 3 vlan-mapping add-outer
Based inner VLAN QinQ mapping rule:
Port Original Inner VLAN List      Add-outer VLAN Hw Status  Hw-ID
----------------------------------------------------------------------
3        300-400                    2000          Enable     2
```

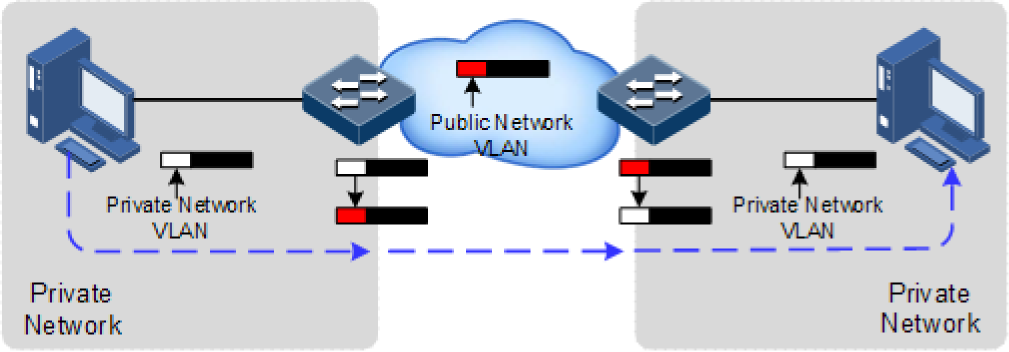
2.4 VLAN mapping

2.4.1 Introduction

VLAN Mapping is used to replace the private VLAN Tag of Ethernet packets with ISP's VLAN Tag, making packets transmitted according to ISP's VLAN forwarding rules. When packets are sent to the peer private network from the ISP network, the VLAN Tag is restored to the original private VLAN Tag according to the same VLAN forwarding rules. Therefore packets are correctly sent to the destination.

Figure 2-6 shows the principle of VLAN mapping.

Figure 2-6 Principle of VLAN mapping



After receiving a VLAN Tag contained in a user private network packet, the ISCOM21xx matches the packet according to configured VLAN mapping rules. If it matches successfully, it maps the packet according to configured VLAN mapping rules. The ISCOM21xx supports the following mapping modes:

- 1:1 VLAN mapping: the ISCOM21xx replaces the VLAN Tag carried by a packet from a specified VLAN to the new VLAN Tag.
- N:1 VLAN mapping: the ISCOM21xx replaces the different VLAN Tags carried by packets from two or more VLANs with the same VLAN Tag.

Different from QinQ, VLAN mapping does not encapsulate packets with multiple layers of VLAN Tags, but needs to modify VLAN Tag so that packets are transmitted according to the carrier's VLAN forwarding rules.

2.4.2 Preparing for configurations

Scenario

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

- A user service needs to be mapped to a carrier's VLAN ID.
- Multiple user services need to be mapped to a carrier's VLAN ID.

Prerequisite

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

2.4.3 Configuring 1:1 VLAN mapping

Configure 1:1 VLAN mapping for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#`**`switchport vlan-mapping`** `[` **`egress`** `|` **`ingress`** `]` *`cvlan-list`* **`translate`** *`vlan-id`*	Configure interface-based 1:1 VLAN mapping rules in the ingress or egress direction.

2.4.4 Configuring N:1 VLAN mapping

Configure N:1 VLAN mapping for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#`**`switchport vlan-mapping both n-to-1`** *`cvlan-list`* **`translate`** *`svlan-id`*	Configure rules of Tag-based N:1 VLAN mapping rules.
4	`Raisecom(config-port)#`**`switchport vlan-mapping both n-to-1`** *`cvlan-list`* **`translate dtag`** *`svlan-id cvlan-id`*	Configure rules of double-Tag-based N:1 VLAN mapping rules.
5	`Raisecom(config-port)#`**`switchport vlan-mapping both untag translate dtag`** *`svlan-id cvlan-id`*	Configure selective QinQ and double Tag rules on the interface.

2.4.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show interface port`** `[` *`port-id`* `]` **`vlan-mapping`** `{` **`egress`** `|` **`ingress`** `}` **`translate`**	Show configurations of 1:1 VLAN mapping.
2	`Raisecom#`**`show interface port`** `[` *`port-id`* `]` **`vlan-mapping both translate`**	Show configurations of N:1 VLAN mapping on the interface.
3	`Raisecom#`**`show interface port`** `[` *`port-id`* `]` **`vlan-mapping both untag`**	Show configurations of selective QinQ and double Tag rules on the interface.

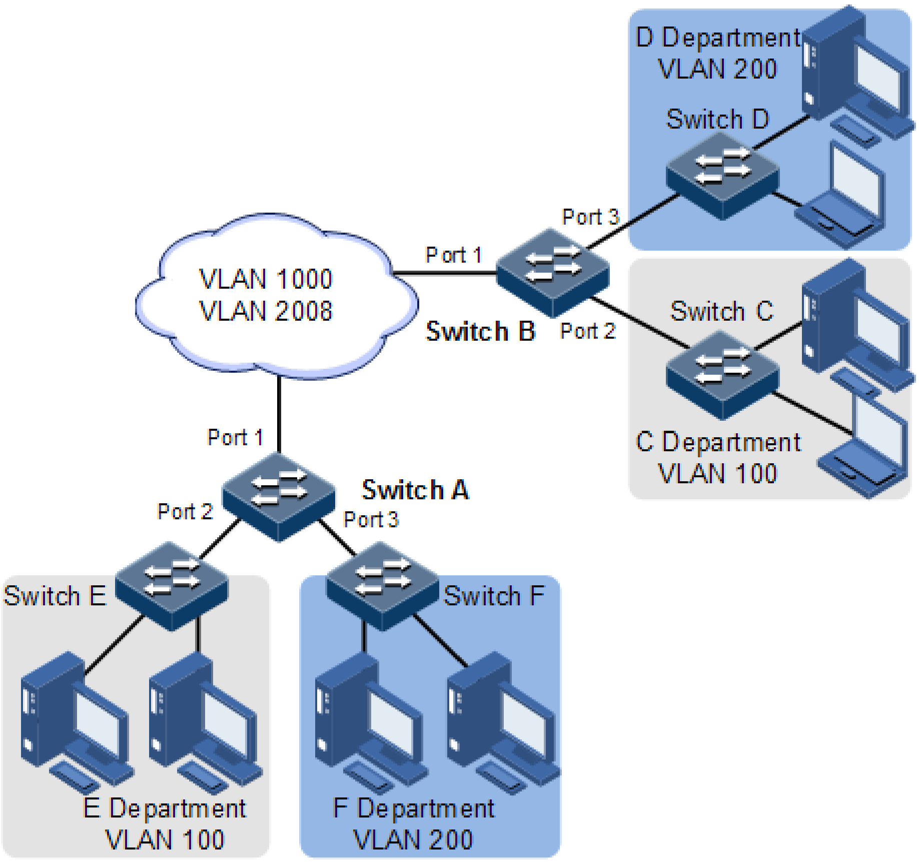
2.4.6 Example for configuring VLAN mapping

Networking requirements

As shown in Figure 2-7, Port 2 and Port 3 on Switch A are connected to Department E in VLAN 100 and Department F in VLAN 200, Port 2 and Port 3 on Switch B are connected to Department C in VLAN 100 and Department D in VLAN 200. The ISP assigns VLAN 1000 to transmit packets of Department E and Department C, and VLAN 2008 to transmit packets of Department F and Department D.

Configure 1:1 VLAN mapping on the Switch A and Switch B to implement normal communication between PC or terminal users and servers.

Figure 2-7 VLAN mapping networking



Configuration steps

Configurations of Switch A and Switch B are the same. Take Switch A for example.

Step 1 Create VLANs and activate them.

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

Step 2 Configure Port 1 to Trunk mode, allowing packets of VLAN 1000 and VLAN 2008 to pass.

```
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk allowed vlan 1000,2008 confirm
SwitchA(config-port)#exit
```

Step 3 Configure Port 2 to Trunk mode, allowing packets of VLAN 100 to pass. Enable VLAN mapping.

```
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk allowed vlan 100 confirm
SwitchA(config-port)#switchport vlan-mapping ingress 100 translate 1000
SwitchA(config-port)#switchport vlan-mapping egress 1000 translate 100
SwitchA(config-port)#exit
```

Step 4 Configure Port 3 to Trunk mode, allowing packets of VLAN 200 to pass. Enable VLAN mapping.

```
SwitchA(config)#interface port 3
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk allowed vlan 200 confirm
SwitchA(config-port)#switchport vlan-mapping ingress 200 translate 2008
SwitchA(config-port)#switchport vlan-mapping egress 2008 translate 200
```

Checking results

Use the **show interface port** *port-id* **vlan-mapping** { **ingress** | **egress** } **translate** command to show configurations of 1:1 VLAN mapping.

```
SwitchA#show interface port 2 vlan-mapping ingress translate
Direction: Ingress
          Original    Original    Outer-tag  New       Inner-tag New
Interface Inner VLANs Outer VLANs Mode       Outer-VID Mode      Inner-VID
Hw-ID
-------------------------------------------------------------------------
2         n/a            100       Translate   1000        --       --
```

2.5 Interface protection

2.5.1 Introduction

With interface protection, you can add an interface, which needs to be controlled, to an interface protection group, isolating Layer 2/Layer 3 data in the interface protection group. This can provide physical isolation between interfaces, enhance network security, and provide flexible networking scheme for users.

After being configured with interface protection, interfaces in an interface protection group cannot transmit packets to each other. Interfaces in and out of the interface protection group can communicate with each other. So do interfaces out of the interface protection group.

2.5.2 Preparing for configurations

Scenario

To isolate Layer 2 data from the interfaces in the same VLAN, like physical isolation, you need to configure interface protection.

Interface protection can implement mutual isolation of the interfaces in the same VLAN, enhance network security, and provide flexible networking solutions for you.

Prerequisite

N/A

2.5.3 Default configurations of interface protection

Default configurations for interface protection are as below.

Function	Default value
Interface protection status of each interface	Disable

2.5.4 Configuring interface protection

Configure interface protection for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#`**`switchport protect`**	Enable interface protection.

2.5.5 Checking configurations

Use the following commands to check configuration results.

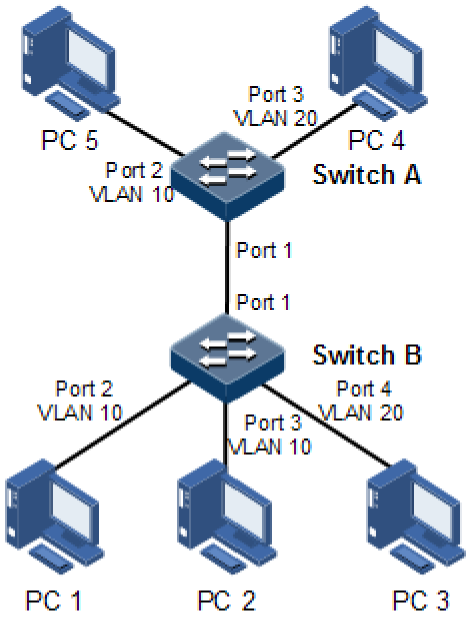
No.	Command	Description
1	`Raisecom#`**`show switchport protect`**	Show interface protection configuration.

2.5.6 Example for configuring interface protection

Networking requirements

As shown in Figure 2-7, PC 1, PC 2, and PC 5 belong to VLAN 10, and PC 3 and PC 4 belong to VLAN 20. The interfaces connecting two devices are in Trunk mode, but do not allow VLAN 20 packets to pass. As a result, PC 3 and PC 4 fail to communicate with each other. Enable interface protection on the interfaces of PC 1 and PC 2 which are connected to Switch B. As a result, PC 1 and PC 2 fail to communicate with each other, but they can communicate with PC 5 respectively.

Figure 2-8 Interface protection networking



Configuration steps

Step 1 Create VLAN 10 and VLAN 20 on both Switch A and Switch B, and activate them.

Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 10,20 active
```

Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#create vlan 10,20 active
```

Step 2 Add Port 2 and Port 3 on Switch B to VLAN 10 in Access mode, add Port 4 to VLAN 20 in Access mode, and configure Port 1 in Trunk mode to allow VLAN 10 packets to pass.

```
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode access
SwitchB(config-port)#switchport access vlan 10
SwitchB(config-port)#exit
SwitchB(config)#interface port 3
SwitchB(config-port)#switchport mode access
SwitchB(config-port)#switchport access vlan 10
SwitchB(config-port)#exit
SwitchB(config)#interface port 4
SwitchB(config-port)#switchport mode access
SwitchB(config-port)#switchport access vlan 20
SwitchB(config-port)#exit
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#switchport trunk allowed vlan 10 confirm
SwitchB(config-port)#exit
```

Step 3 Add Port 2 on Switch A to VLAN 10 in Access mode, add Port 3 to VLAN 20 in Trunk mode, and configure Port 1 in Trunk mode to allow VLAN 10 packets to pass.

```
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode access
SwitchA(config-port)#switchport access vlan 10
SwitchA(config-port)#exit
SwitchA(config)#interface port 3
SwitchA(config-port)#switchport mode access
SwitchA(config-port)#switchport access vlan 20
SwitchA(config-port)#exit
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#switchport trunk allowed vlan 10 confirm
```

Step 4 Enable interface protection on Port 2 and Port 3 on Switch B.

```
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport protect
SwitchB(config-port)#exit
SwitchB(config)#interface port 3
SwitchB(config-port)#switchport protect
```

Checking results

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

Take Switch B for example.

```
SwitchB#show vlan
VLAN Name       State   Status  Port       Untag-Port  Priority Create-Time
-----------------------------------------------------------------------------
1   Default     active  static  1-10       1-10        --       0:0:7
10   VLAN0010    active  static  1-3       2,3         --       0:1:1
20   VLAN0020    active  static  4        4            --       0:1:1
```

Use the **show interface port** *port-id* **switchport** command to show configurations of interface VLAN.

Take Switch B for example.

```
SwitchB#show interface port 2 switchport
Port:2
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: 1,10,20
Administrative Trunk Untagged VLANs: 1
Operational Trunk Untagged VLANs: 1
```

Use the **show switchport protect** command to show configurations of interface protection.

```
SwitchB#show switchport protect
Port     Protected State
--------------------------
   1      disable
   2      enable
   3      enable

   …
```

Check whether PC 1 can ping PC 5, PC 2 can ping PC 5, and PC 3 can ping PC 4 successfully. Check whether the VLAN allowed to pass on the Trunk interface is correct.

- If PC 1 can ping PC 5 successfully, VLAN 10 communicates properly.
- If PC 2 can ping PC 5 successfully, VLAN 10 communicates properly.
- If PC 3 fails ping PC 4, VLAN 20 fails to communicate.

By pinging PC 2 through PC 1, check whether interface protection is correctly configured.

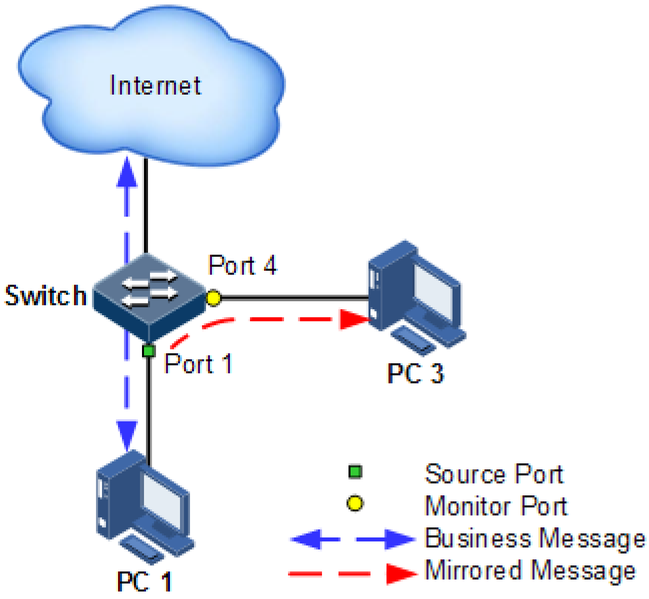
PC 1 fails to ping PC 3, so interface protection has taken effect.

2.6 Port mirroring

2.6.1 Introduction

Port mirroring refers to assigning some packets mirrored from the source interface to the destination interface, such as from the monitor port without affecting the normal packet forwarding. You can monitor sending and receiving status for packets on an interface through this function and analyze the relevant network conditions.

Figure 2-9 Principle of port mirroring



The basic principle of port mirroring is shown in Figure 2-9. PC 1 connects to the external network through Port 1; PC 3 is the monitor PC, connecting the external network through Port 4.

When monitoring packets from PC 1, you need to assign Port 1 to connect to PC 1 as the mirroring source port, enable port mirroring on the ingress port, and assign Port 4 as the monitor port to mirror packets to the destination port.

When service packets from PC 1 enter the switch, the switch will forward and copy them to monitor port (Port 4). The monitor device connected to the monitor port can receive and analyze these mirrored packets.

The ISCOM21xx supports data stream mirroring on the ingress port and egress port. The packets on the ingress/egress mirroring port will be copied to the monitor port after the switch is enabled with port mirroring. The monitor port and mirroring port cannot be the same one.

2.6.2 Preparing for configurations

Scenario

Port mirroring is used to monitor network data type and flow regularly by the network administrator.

Port mirroring copies the monitored flow to a monitor port or CPU to obtain the ingress/egress port failure or abnormal flow of data for analysis, discovers the root cause, and solves them timely.

Prerequisite

N/A

2.6.3 Default configurations of port mirroring

Default configurations of port mirroring are as below.

Function	Default value
Port mirroring status	Disable
Mirroring the source interface	N/A
Monitor port	Port 1

Note

The output of the monitor port is null when packets are mirrored to the CPU.

2.6.4 Configuring port mirroring on local port

Caution

- There can be multiple source mirroring ports but only one monitor port.
- The ingress/egress mirroring port packet will be copied to the monitor port after port mirroring takes effect. The monitor port cannot be configured to the mirroring port again.

Configure port mirroring on the local port for the ISCOM21xx as below.

Step	Configure	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`mirror monitor-port`** *`port-id`*	Configure mirroring packets to CPU or specified monitor port.
3	`Raisecom(config)#`**`mirror source-port-list`** `{` **`both`** *`port-list`* `|` **`egress`** *`port-list`* `|` **`ingress`** *`port-list`* `[` **`egress`** *`port-list`* `] }`	Configure the mirror source port of port mirroring, and designate the mirroring rule for port mirroring.
4	`Raisecom(config)#`**`mirror enable`**	Enable port mirroring.

2.6.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show mirror`	Show configurations of port mirroring.

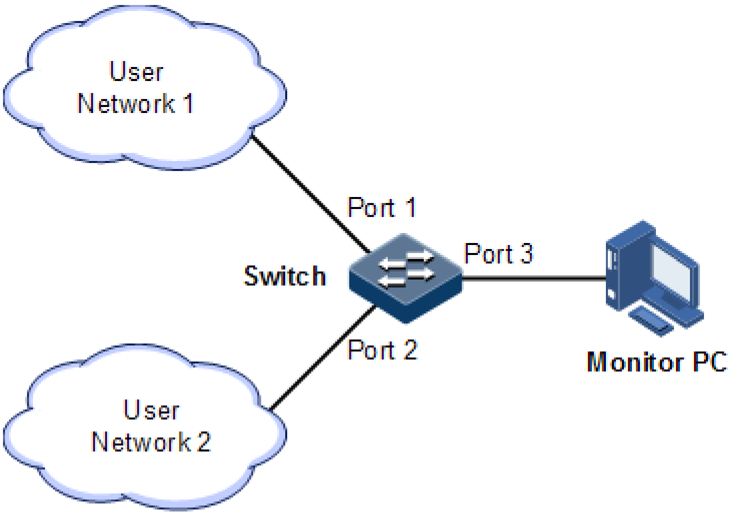
2.6.6 Example for configuring port mirroring

Networking requirements

As shown in Figure 2-10, the network administrator wishes to monitor user network 1 through the monitor device, to catch the fault or abnormal data flow for analyzing and discovering problem, and then to solve it.

The ISCOM21xx is disabled with storm control and automatic packets sending. User network 1 accesses the ISCOM21xx through Port 2, user network 2 accesses the ISCOM21xx through Port 1, and the data monitor device is connected to Port 3.

Figure 2-10 Port mirroring networking



Configuration steps

Enable port mirroring on the switch.

```
Raisecom#config
Raisecom(config)#mirror monitor-port 3
Raisecom(config)#mirror source-port-list both 1
Raisecom(config)#mirror enable
```

Checking results

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

```
Raisecom#show mirror
Mirror: Enable
Monitor port: 3
Non-mirror port: Not block
-----------the both mirror rule-----------
Mirrored ports: 1
Divider: 0
MAC address: 0000.0000.0000
-----------the both mirror rule-----------
Mirrored ports: --
Divider: 0
MAC address: 0000.0000.0000
```

2.7 Layer 2 protocol transparent transmission

2.7.1 Introduction

Transparent transmission is one of the main Ethernet device functions, and usually the edge network devices of carrier conduct Layer 2 protocol packet transparent transmission. Transparent transmission is enabled on the interface that connects edge network devices of carrier and user network. The interface is in Access mode, connecting to Trunk interface on user device. The layer 2 protocol packet of the user network is send from transparent transmission interface, encapsulated by the edge network device (ingress end of packets), and then send to the carrier network. The packet is transmitted through the carrier network to reach the edge device (egress end of packet) at the other end or carrier network. The edged device decapsulates outer layer 2 protocol packet and transparent transmits it to the user network.

The transparent transmission function includes packet encapsulation and decapsulation function, the basic implementing principle as below.

- Packet encapsulation: at the packet ingress end, the ISCOM21xx modifies the destination MAC address from user network layer 2 protocol packets to special multicast MAC address (it is 010E.5E00.0003 by default). On the carrier network, the modified packet is forwarded as data in user VLAN.
- Packet decapsulation: at the packet egress end, the ISCOM21xx senses packet with special multicast MAC address (it is 010E.5E00.0003 by default), reverts the destination MAC address to DMAC of Layer 2 protocol packets, then sends the packet to assigned user network.

Layer 2 protocol transparent transmission can be enabled at the same time with QinQ or enabled independently. In actual networking, after modifying the MAC address of protocol packets, you need to add an outer Tag to packets to send them through the carrier network.

The ISCOM21xx supports transparent transmission of BPDU packet, DOT1X packet, LACP packet, CDP packet, PVST packet, PAGP packet, STP packet, UDLD packet, and VTP packet.

2.7.2 Preparing for configurations

Scenario

This function enables layer 2 protocol packets of one user network to traverse the carrier network to make one user networks in different regions uniformly running the same Layer 2 protocol. You can configure rate limiting on transparent transmission packets to prevent packet loss.

Prerequisite

Connect the interface and configure its physical parameters to make it Up.

2.7.3 Default configurations of Layer 2 protocol transparent transmission

Default configurations of Layer 2 protocol transparent transmission are as below.

Function	Default value
Layer 2 protocol transparent transmission status	Disable
Egress interface and belonged VLAN of Layer 2 protocol packet	N/A
TAG CoS value of transparent transmission packet	5
Destination MAC address of transparent transmission packet	010E.5E00.0003
Discarding threshold and disabling threshold of transparent transmission packet	N/A

2.7.4 Configuring transparent transmission parameters

Configure transparent transmission parameter for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`relay destination-address`** *`mac-address`*	(Optional) configure destination MAC for transparent transmission packets. The default value is 010E.5E00.0003.
3	`Raisecom(config)#`**`relay cos`** *`cos-value`*	(Optional) configure CoS value for transparent transmission packets.
4	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode or LAG configuration mode.
5	`Raisecom(config-port)#`**`relay port`** *`port-id`*	Configure specified egress interface for transparent transmission packets.

Step	Command	Description
6	`Raisecom(config-port)#relay vlan vlan-id`	Configure specified VLAN for transparent transmission packets. This configuration enables packets to be forwarded according to the specified VLAN instead of the ingress interface.
7	`Raisecom(config-port)#relay { all | cdp | dot1x | lacp | pagp | pvst | stp | udld | vtp }`	Configure the type of transparent transmission packets on the interface.

2.7.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show relay [ port-list port-list ]`	Show configurations and status of transparent transmission.
2	`Raisecom#show relay statistics [ port-list port-list ]`	Show statistics of transparent transmission packets.

2.7.6 Maintenance

Maintain the ISCOM21xx as below.

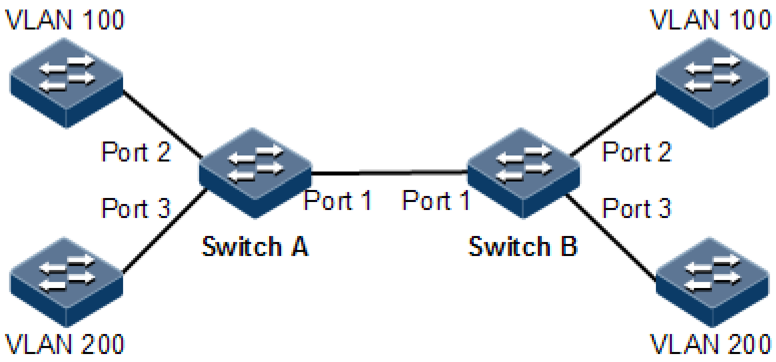
Commands	Description
`Raisecom(config)#clear relay statistics [ port-list port-list ]`	Clear statistics of transparent transmission packets.
`Raisecom(config-port)#no relay shutdown`	Enable the interface again.

2.7.7 Example for configuring Layer 2 protocol transparent transmission

Networking requirements

As shown in Figure 2-11, Switch A and Switch B are connected to two user networks VLAN 100 and VLAN 200 respectively. You need to configure Layer 2 protocol transparent transmission on Switch A and Switch B to make the same user network in different regions run STP entirely.

Figure 2-11 Layer 2 protocol transparent transmission networking



Configuration steps

Step 1 Create VLANs 100 and 200, and activate them.

Configure Switch A.

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

Configure Switch B.

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

Step 2 Configure the switching mode of Port 2 to Access mode, configure the Access VLAN to 100, and enable STP transparent transmission.

Configure Switch A.

```
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode access
SwitchA(config-port)#switchport access vlan 100
SwitchA(config-port)#relay stp
SwitchA(config-port)#relay port 1
SwitchA(config-port)#exit
```

Configure Switch B.

```
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode access
SwitchB(config-port)#switchport access vlan 100
SwitchB(config-port)#relay stp
SwitchB(config-port)#relay port 1
SwitchB(config-port)#exit
```

Step 3 Configure the switching mode of Port 3 to Access mode, configure the Access VLAN to 200, and enable STP transparent transmission.

Configure Switch A.

```
SwitchA(config)#interface port 3
SwitchA(config-port)#switchport mode access
SwitchA(config-port)#switchport access vlan 200
SwitchA(config-port)#relay stp
SwitchA(config-port)#relay port 1
SwitchA(config-port)#exit
```

Configure Switch B.

```
SwitchB(config)#interface port 3
SwitchB(config-port)#switchport mode access
SwitchB(config-port)#switchport access vlan 200
SwitchB(config-port)#relay stp
SwitchB(config-port)#relay port 1
SwitchB(config-port)#exit
```

Step 4 Configure Port 1 to Trunk mode.

Configure Switch A.

```
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport mode trunk
```

Configure Switch B.

```
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
```

Checking results

Use the **show relay** command to show configurations of Layer 2 protocol transparent transmission.

Take Switch A for example.

```
SwitchA#show relay port-list 1-3
COS for Encapsulated Packets: 5
Destination MAC Address for Encapsulated Packets: 010E.5E00.0003
Port    vlan  Egress-Port  Protocol     Drop-Threshold  Shutdown-Threshold
-------------------------------------------------------------------------
1(up)    --   --           stp            --               --
                              dot1x          --               --
                              lacp           --               --
                              cdp         --               --
                               vtp         --               --
                               pvst        --
                               udld             ---              ---
                              pagp             ---
2(up)   --        1       stp(enable)     --             --
                               dot1x          --               --
                               lacp           --               --
                               cdp         --               --
                               vtp         --               --
                               pvst        --
                               udld             ---              ---
                              pagp             ---
3(up)   --        1        stp(enable)    --             --
                              dot1x          --               --
                               lacp           --               --
                               cdp         --               --
                               vtp         --               --
                               pvst        --
```

3 IP services

This chapter describes basic principles and configuration procedures of IP services, and provides related configuration examples, including the following sections:

- ARP
- Layer 3 interface
- Default gateway
- DHCP Client
- DHCP Relay
- DHCP Snooping
- DHCP Options

3.1 ARP

3.1.1 Introduction

In TCP/IP network environment, each host is assigned with a 32-bit IP address that is a logical address used to identify hosts between networks. To transmit packets in physical link, you must know the physical address of the destination host, which requires mapping the IP address to the physical address. In Ethernet environment, the physical address is a 48-bit MAC address. The system has to transfer the 32-bit IP address of the destination host to the 48-bit Ethernet address for transmitting packets to the destination host correctly. Then Address Resolution Protocol (ARP) is applied to resolve IP address to MAC address and configure mapping between IP address and MAC address.

ARP address table includes the following two types:

- Static entry: bind IP address and MAC address to avoid ARP dynamic learning cheating.
  - Static ARP address entry needs to be added/deleted manually.
  - No aging to static ARP address.
- Dynamic entry: MAC address automatically learned through ARP.
  - This dynamic entry is automatically generated by switch. You can adjust partial parameters of it manually.
  - The dynamic ARP address entry will be aged after the aging time if not used.

The ISCOM21xx supports the following two modes of dynamically learning ARP address entries:

- Learn-all: in this mode, the ISCOM21xx learns both ARP request packets and response packets. When device A sends its ARP request, it writes mapping between its IP address and physical address in ARP request packets. When device B receives ARP request packets from device A, it learns the mapping in its address table. In this way, device B will no longer send ARP request when sending packets to device A.
- Learn-reply-only mode: in this mode, the ISCOM21xx learns ARP response packets only. For ARP request packets from other devices, it responds with ARP response packets only rather than learning ARP address mapping entry. In this way, network load is heavier but some network attacks based on ARP request packets can be prevented.

3.1.2 Preparing for configurations

Scenario

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

Generally, the ARP address table is dynamically maintained by the ISCOM21xx. The ISCOM21xx searches for the mapping between the IP address and MAC address automatically according to ARP. You just need to configure the ISCOM21xx manually for preventing ARP dynamic learning from cheating and adding static ARP address entries.

Prerequisite

N/A

3.1.3 Default configurations of ARP

Default configurations of ARP are as below.

Function	Default value
Static ARP entry	N/A
Dynamic ARP entry learning mode	Learn-reply-only

3.1.4 Configuring static ARP entries

⚠ Caution

- The IP address in static ARP entry must belong to the IP network segment of Layer 3 interface on the switch.
- The static ARP entry needs to be added and deleted manually.

Configure static ARP entries for the ISCOM21xx as below.

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

Step	Command	Description
2	`Raisecom(config)#`**`arp`** *`ip-address mac-address`*	Configure static ARP entry.

3.1.5 Configuring aging time of dynamic ARP entries

Configure the aging time of dynamic ARP entries for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`arp aging-time`** *`period`*	(Optional) configure dynamic ARP entry learning mode. The value 0 indicates no aging.

3.1.6 Configuring dynamic ARP entry learning mode

Configure dynamic ARP entry learning mode for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`arp mode`** `{` **`learn-all`** `|` **`learn-reply-only`** `}`	(Optional) configure dynamic ARP entry learning mode.

3.1.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show arp`**	Show information about ARP address table.
2	`Raisecom#`**`show arp`** *`ip-address`*	Show ARP table information related to specified IP address.
3	`Raisecom#`**`show arp ip`** *`if-number`*	Show ARP table information related to Layer 3 interface.
4	`Raisecom#`**`show arp static`**	Show ARP statistics.

3.1.8 Maintenance

Maintain the ISCOM21xx as below.

Command	Description
`Raisecom(config)#clear arp`	Clear all entries in the ARP address table.

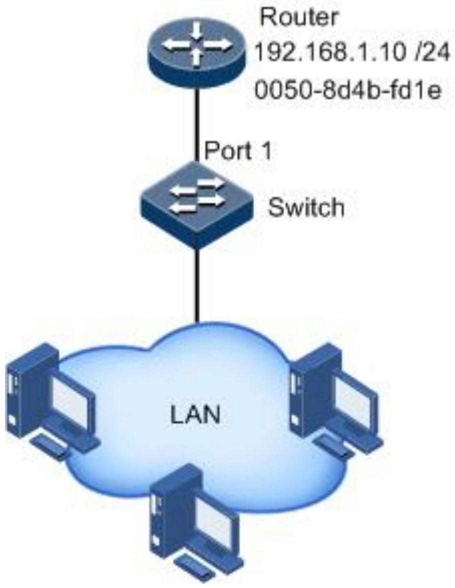
3.1.9 Configuring ARP

Networking requirements

As shown in Figure 3-1, the ISCOM21xx connects to the host, and connects to the upstream router by Port 1. For the Router, the IP address is 192.168.1.10/24, the subnet mask is 255.255.255.0, and the MAC address is 0050-8d4b-fd1e.

To improve communication security between the Switch and Router, configure related static ARP entry on the ISCOM21xx.

Figure 3-1 ARP networking



Configuration steps

Step 1 Create an ARP static entry.

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

Checking results

Use the **show arp** command to show configurations of the ARP address table.

```
Raisecom#show arp
```

```
ARP table aging-time: 1200 seconds(default: 1200s)
ARP mode: Learn reply only
Ip Address       Mac Address        Type   Interface ip
---------------------------------------------------------
192.168.1.10     0050.8d4b.fd1e     static     --
192.168.100.1    000F.E212.5CA0     dynamic   1

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

3.2 Layer 3 interface

3.2.1 Introduction

The Layer 3 interface refers to the IP interface, and it is the virtual interface based on VLAN. Configuring Layer 3 interface is generally used for network management or routing link connection of multiple devices. Associating a Layer 3 interface to VLAN requires configuring IP address; each Layer 3 interface will correspond to an IP address and associate with at least one VLAN.

If only one IP address is configured on Layer 3 interface of the ISCOM21xx, only part of hosts can communicate with external networks through the ISCOM21xx. To enable all hosts to communicate with external networks, configure the secondary IP address of the interface. To enable hosts in two network segments to interconnect with each other, configure the ISCOM21xx as the gateway for all hosts.

3.2.2 Preparing for configurations

Scenario

You can connect a Layer 3 interface for VLAN when configuring its IP address. Each Layer 3 interface will correspond to an IP address and connects to a VLAN.

Prerequisite

Configure the VLAN associated with the interface and activate it.

3.2.3 Configuring IPv4 address of Layer 3 interface

Configure the IPv4 address of the Layer 3 interface for the ISCOM21xx 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)#`**`description`** *`string`*	Configure description of the Layer 3 interface.

Step	Command	Description
4	Raisecom(config-ip)#**ip address** *ip-address* [*ip-mask*] [*vlan-list*]	Configure the IP address of the Layer 3 interface, and associate the Layer 3 interface with a VLAN.
5	Raisecom(config-ip)#**ip vlan** *vlan-list*	(Optional) configure the mapping between the Layer 3 interface and VLAN.

Note

- Configure the VLAN associated with the Layer 3 interface, and the VLAN must be activated. Use the **state** { **active** \| **suspend** } command to activate and then configure the suspended VLAN. When you configure the mapping between a Layer 3 interface and a VLAN which does not exist or is deactivated, the configuration can be successful but does not take effect.
- Up to 15 IP interfaces can be configured, and their IDs range from 0 to 14.

3.2.4 Configuring IPv6 address of Layer 3 interface

Configure the IPv6 address of the Layer 3 interface for the ISCOM21xx 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 address** *ipv6-address/prefix-length* [**eui-64**] [*vlan-list*]	Configure the IPv6 address of the Layer 3 interface, and associate the Layer 3 interface with a VLAN.
	Raisecom(config-ip)#**ipv6 address link-local** [*vlan-list*]	

3.2.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show interface ip**	Show IP address configuration of the Layer 3 interface.
2	Raisecom#**show interface ipv6**	Show IPv6 address configuration of the Layer 3 interface.
3	Raisecom#**show interface ip description**	Show mapping between Layer 3 interface and VLAN.
4	Raisecom#**show interface ip statistics**	Show management VLAN configurations.

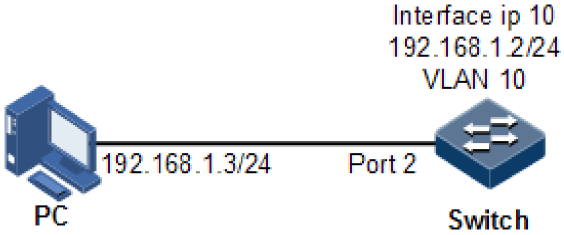
No.	Command	Description
5	`Raisecom#show ipv6 neighbor`	Show neighbors of the ISCOM21xx.

3.2.6 Example for configuring Layer 3 interface to interconnect with host

Networking requirements

As shown in Figure 3-2, configure the Layer 3 interface to the switch so that the PC and the ISCOM21xx can Ping through each other.

Figure 3-2 Layer 3 interface networking



Configuration steps

Step 1 Create a VLAN and add the interface into the VLAN.

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

Step 2 Configure Layer 3 interface on the ISCOM21xx, and configure the IP address, and associate the IP address with the VLAN.

```
Raisecom(config)#interface ip 10
Raisecom(config-ip)#ip address 192.168.1.2 255.255.255.0 10
```

Checking results

Use the **show vlan** command to show mapping between the physical interface and VLAN.

```
Raisecom#show vlan 10
VLAN Name       State   Status  Port      Untag-Port  Priority Create-Time
-----------------------------------------------------------------------------
```

```
10  VLAN0010  active  static  2         2         --      1:16:49
```

Use the **show interface ip** command to show configurations of the Layer 3 interface, and the mapping between the Layer 3 interface and VLAN.

```
Raisecom#show interface ip
Index    Ip Address      NetMask         Vid            Status   Mtu
-------------------------------------------------------------------------
0       192.168.27.63   255.255.255.0   1               active   1500
10      192.168.1.2     255.255.255.0   10              active   1500
```

Use the **ping** command to check whether the ISCOM21xx and PC can ping each other.

```
Raisecom#ping 192.168.1.3
Type CTRL+C to abort
Sending 5, 8-byte ICMP Echos to 192.168.1.3, timeout is 3 seconds:
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms
Reply from 192.168.1.3: time<1ms

---- PING Statistics----
5 packets transmitted, 5 packets received,
Success rate is 100 percent(5/5),
round-trip (ms)  min/avg/max = 0/0/0.
```

3.3 Default gateway

3.3.1 Introduction

When the packet to be forwarded is not configured with a route, you can configure the default gateway to enable a device to send the packet to the default gateway. The IP address of the default gateway should be in the same network segment with the local IP address of the device.

3.3.2 Preparing for configurations

Scenario

When the packet to be forwarded is not configured with a route, you can configure the default gateway to enable a device to send the packet to the default gateway.

Prerequisite

Configure the IP address of the switch in advance; otherwise, configuring the default gateway will fail.

3.3.3 Configuring default gateway

Note

The IP address of the default gateway should be in the same network segment of any local IP interface.

Configure the default gateway for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip default-gateway** *ip-address*	Configure the IP address of the default gateway.
3	Raisecom(config)#**ipv6 default-gateway** *ipv6-address*	Configure the default IPv6 gateway.

3.3.4 Checking configurations

Use the following command to check configuration result.

No.	Command	Description
1	Raisecom#**show ip route**	Show information about the routing table.

3.4 DHCP Client

3.4.1 Introduction

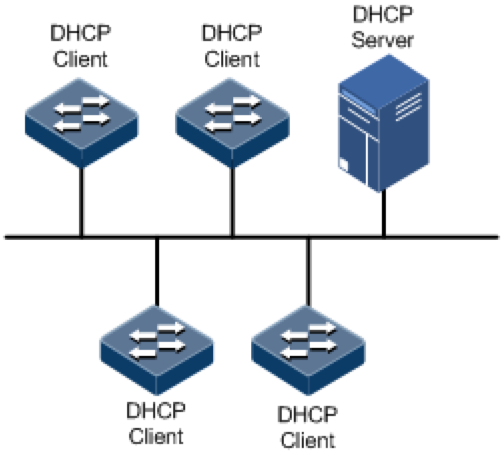
Dynamic Host Configuration Protocol (DHCP) refers to assign IP address configurations dynamically for users in TCP/IP network. It is based on BOOTP (Bootstrap Protocol) protocol, and automatically adds the specified available network address, network address re-use, and other extended configuration options over BOOTP protocol.

With the enlargement of network scale and development of network complexity, the number of PCs on a network usually exceeds the maximum number of distributable IP addresses. Meanwhile, the widely use of laptops and wireless networks lead to frequent change of PC positions and also related IP addresses must be updated frequently. As a result, network configurations become more and more complex. DHCP is developed to solve these problems.

DHCP adopts client/server communication mode. A client applies for configurations (including the IP address, subnet mask, and default gateway) to the server, and the server replies to the client with the IP address and other related configurations to implement dynamic configurations of IP addresses, and so on.

Typical applications of DHCP usually include a set of DHCP server and multiple clients (for example PC or Notebook), as shown in Figure 3-3.

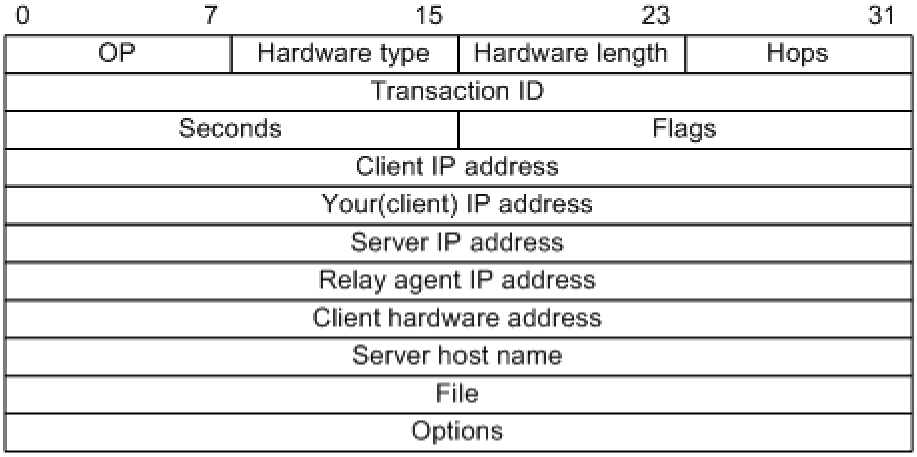
Figure 3-3 DHCP typical networking



DHCP technology ensures rational allocation, avoid waste, and improve the utilization rate of IP addresses on the entire network.

Figure 3-4 shows the structure of a DHCP packet. The DHCP packet is encapsulated in a UDP data packet.

Figure 3-4 Structure of a DHCP packet



0 7	15	23	31
OP	Hardware type	Hardware length	Hops
Transaction ID			
Seconds		Flags	
Client IP address			
Your(client) IP address			
Server IP address			
Relay agent IP address			
Client hardware address			
Server host name			
File			
Options			

Table 3-1 describes fields of DHCP packets.

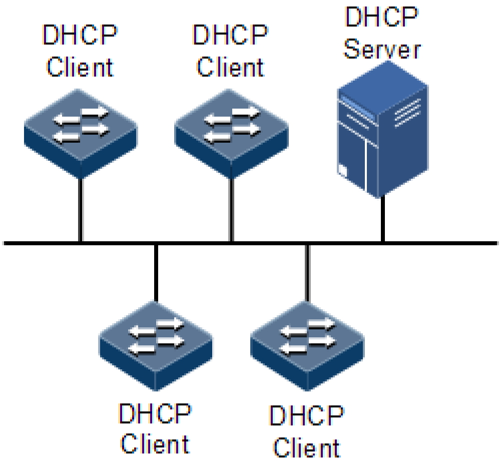
Table 3-1 Fields of DHCP packets

Field	Length	Description
OP	1	Packet type • 1: a request packet • 2: a reply packet

Field	Length	Description
Hardware type	1	Hardware address type of a DHCP client.
Hardware length	1	Hardware address size of a DHCP client.
Hops	1	Number of DHCP hops passed by the DHCP packet. It increases by 1 every time when the DHCP request packet passes a DHCP hop.
Transaction ID	4	The client chooses a number at random when starting a request, used to mark process of address request.
Seconds	2	Passing time for the DHCP client after starting DHCP request. It is unused now, fixed as 0.
Flags	2	Bit 1 is the broadcast reply flag, used to mark whether the DHCP server replies packets in unicast or broadcast mode. • 0: unicast • 1: broadcast Other bits are reserved.
Client IP address	4	DHCP client IP address, only filled when the client is in bound, updated or re-bind status, used to reply ARP request.
Your (client) IP address	4	IP address of the client distributed by the DHCP server
Server IP address	4	IP address of the DHCP server
Relay agent IP address	4	IP address of the first DHCP hop after the DHCP client sends request packets.
Client hardware address	16	Hardware address of the DHCP client
Server host name	64	Name of the DHCP server
File	128	Name of the startup configuration file of the DHCP client and path assigned by the DHCP server
Options	Modifiable	A modifiable option field, including packet type, available leased period, Domain Name System (DNS) server IP address, Windows Internet Name Server (WINS) IP address, and so on.

The ISCOM21xx can be used as a DHCP client to obtain the IP address from the DHCP server for future management, as shown in Figure 3-5.

Figure 3-5 DHCP client networking



3.4.2 Preparing for configurations

Scenario

As a DHCP client, the ISCOM21xx obtains its IP address from the DHCP server.

The IP address assigned by the DHCP client is limited with a certain lease period when adopting dynamic assignment of IP addresses. The DHCP server will take back the IP address when it is expired. The DHCP client has to renew the IP address for continuous use. The DHCP client can release the IP address if it does not want to use the IP address before expiration.

We recommend configuring the number of DHCP relay devices smaller than 4 if the DHCP client needs to obtain IP address from the DHCP server through multiple DHCP relay devices.

Prerequisite

- Create a VLAN and add Layer 3 interface to it.
- Disable both DHCP Snooping and DHCP Relay.

3.4.3 Default configurations of DHCP Client

Default configurations of DHCP Client are as below.

Function	Default value
hostname	raisecom
class-id	raisecom-ROS
client-id	raisecom-SYSMAC-IF0

3.4.4 Applying for IP address through DHCP

Apply for IP address through DHCP for the ISCOM21xx 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)#**ip address dhcp** *vlan-list* [**server-ip** *ip-address*]	Apply for the IP address through DHCP.

Note

If the ISCOM21xx obtains IP address from the DHCP server through DHCP previously, it will restart the application process for IP address if you use the **ip address dhcp** command to modify the IP address of the DHCP server.

3.4.5 (Optional) configuring DHCPv4 Client

Configure DHCPv4 Client for the ISCOM21xx 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 dhcp client** { **class-id** *class-id* | **client-id** *client-id* | **hostname** *hostname* }	Configure information about the DHCPv4 client, including type ID, client ID, and host name.

3.4.6 (Optional) renewing or releasing IP address

Renew or release the IP address for the ISCOM21xx 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)#**ip dhcp client renew**	Renew the IP address. If the ISCOM21xx has obtained the IP address through DHCP, it will automatically renew the IP address upon the IP address expires.
4	Raisecom(config-ip)#**no ip address dhcp**	Release the IP address.

3.4.7 Checking configurations

Use the following commands to check configuration results.

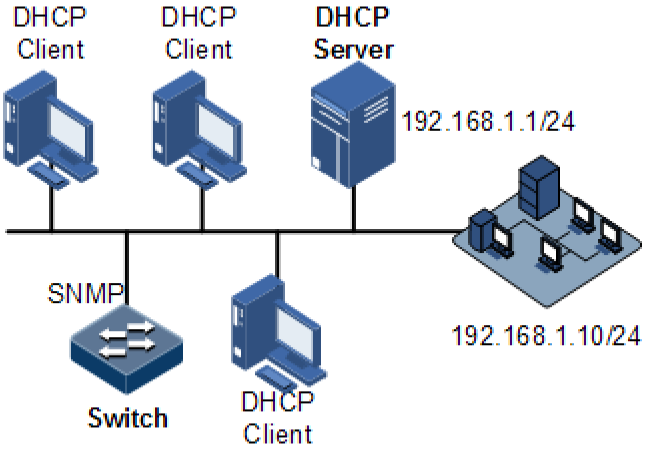
No.	Command	Description
1	`Raisecom#show ip dhcp client`	Show configurations of DHCP Client.
2	`Raisecom#show ipv6 dhcp client`	Show configurations of DHCPv6 Client.

3.4.8 Example for configuring DHCP Client

Networking requirements

As shown in Figure 3-6, the Switch is used as the DHCP client, and the host name is raisecom. The DHCP server should assign IP address to the SNMP interface of the Switch and make NMS platform manage the Switch.

Figure 3-6 Configuring DHCP Client



Configuration steps

Step 1 Configure DHCP client information.

```
Raisecom#config
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip dhcp client hostname raisecom
```

Step 2 Configure applying for IP address through DHCP.

```
Raisecom(config-ip)#ip address dhcp 1 server-ip 192.168.1.1
```

Checking results

Use the **show ip dhcp client** command to show configurations of DHCP Client.

```
Raisecom#show ip dhcp client
  Hostname:                 raisecom
  Class-ID:                 raisecomFTTH-ROS_4.14.1727
  Client-ID:                raisecomFTTH-000e5e123456-IF0
  DHCP Client is requesting for a lease.
```

3.5 DHCP Relay

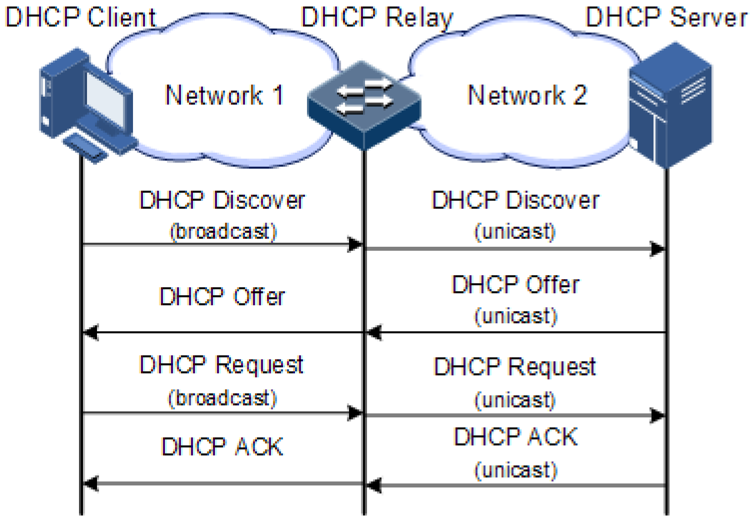
3.5.1 Introduction

At the beginning, DHCP requires the DHCP server and clients to be in the same network segment, instead of different network segments. As a result, a DHCP server is configured for all network segments for dynamic host configuration, which is not economic.

DHCP Relay is introduced to solve this problem. It can provide relay service between DHCP clients and DHCP server that are in different network segments. It relays packets across network segments to the DHCP server or clients.

Figure 3-7 shows the principle of DHCP Relay.

Figure 3-7 Principle of DHCP Relay



Step 1 The DHCP client sends a request packet to the DHCP server.

Step 2 After receiving the packet, the DHCP relay device process the packet in a certain way, and then sends it to the DHCP server on the specified network segment.

Step 3 The DHCP server sends acknowledgement packet to the DHCP client through the DHCP relay device according to the information contained in the request packet. In this way, the configuration of the DHCP client is dynamically configured.

3.5.2 Preparing for configurations

Scenario

When DHCP Client and DHCP Server are not in the same network segment, you can use DHCP Relay function to make DHCP Client and DHCP Server in different network segments carry relay service, and relay DHCP protocol packets across network segment to destination DHCP server, so that DHCP Client in different network segments can share the same DHCP Server.

Prerequisite

DHCP Relay is exclusive to DHCP Client, or DHCP Snooping. Namely, you cannot configure DHCP Relay on the device configured with DHCP Client, or DHCP Snooping.

3.5.3 Default configurations of DHCP Relay

Default configurations of DHCP Relay are as below.

Function	Default value
Global DHCP Relay	Disable
Interface DHCP Relay	Enable
DHCP Relay supporting Option 82	Disable
Policy for DHCP Relay to process Option 82 request packets	Replace
Interface DHCP Relay trust	Untrust

3.5.4 Configuring global DHCP Relay

Configure global DHCP Relay for the ISCOM21xx as below.

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

3.5.5 Configuring interface DHCP Relay

Configure interface DHCP Relay for the ISCOM21xx 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.

Step	Command	Description
3	Raisecom(config-ip)#**ip dhcp relay**	Enable DHCP Relay on the IP interface.

3.5.6 Configuring destination IP address for forwarding packets

Configure the destination IP address for forwarding packets for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp relay ip-list** { **all** | *ip-interface-list* } **target-ip** *ip-address*	Configuring the destination IP address for DHCP Relay on the IP interface.
3	Raisecom(config)#**ip dhcp relay vlan-list** *vlan-list*	Enable DHCP Relay based on VLAN. Use the **no ip dhcp relay vlan-list** command to disable DHCP Relay.
4	Raisecom(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
5	Raisecom(config-ip)#**ip dhcp realy target-ip** *ip-address*	Configure the destination IP address for Layer 3 interface to forward packets.

3.5.7 Configuring pseudo Layer 3 Relay

Configure the destination IP address for forwarding packets for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp relay**	Enable global DHCP Relay.
3	Raisecom(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
4	Raisecom(config-ip)#**ip dhcp relay**	Enable interface DHCP Relay.
5	Raisecom(config-ip)#**ip dhcp relay target-ip** *ip-address* Raisecom(config-ip)#**exit**	Configure the destination IP address of DHCP Relay.
6	Raisecom(config)#**ip dhcp relay relay-ip** *ip-address*	Configure the pseudo Layer 3 IP address.

Note

- After receiving the Discover packet sent from the DHCP client, the DHCP relay pads the manually configured Relay IP address to the Discover packet, and then forwards the Discover packet to the DHCP server.
- After receiving the Discover packet sent from the DHCP client, the DHCP relay pads the manually configured Relay IP address to the Discover packet, and then forwards the Discover packet to the DHCP server.

3.5.8 (Optional) configuring DHCP Relay to support Option 82

Configure DHCP Relay to support Option 82 for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip dhcp relay information option**	Configure DHCP Relay to support Option 82.
3	Raisecom(config)#**ip dhcp relay information policy** { **drop** | **keep** | **replace** }	Configure the policy for DHCP Relay to process Option 82 request packets.
4	Raisecom(config)#**ip dhcp relay information trusted port-list** *port-list*	Configure global Option 82 trusted interface list.
	Raisecom(config)#**interface port** *port-id* Raisecom(config-port)**ip dhcp relay information trusted**	Configure the specified interface to the Option 82 trusted interface.
5	Raisecom(config-port)#**ip dhcp relay information option vlan-list** *vlan-list*	Enable DHCP Relay Option 82 based on VLAN.

3.5.9 Configuring DHCP Relay binding table

Configure the DHCP Relay binding table for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**ip dhcp relay binding maximum** *maximum* Raisecom#**exit**	Configure the maximum number of DHCP Relay binding entries.
4	Raisecom(config)#**ip dhcp relay binding delete** *ip-address*	Delete DHCP Relay binding entries.

3.5.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show ip dhcp relay [ information | statistics ]`	Show configurations or statistics of DHCP Relay.
2	`Raisecom#show ip dhcp relay binding`	Show information about the DHCP Relay binding table, number of current binding entries, and maximum number of binding entries.

3.6 DHCP Snooping

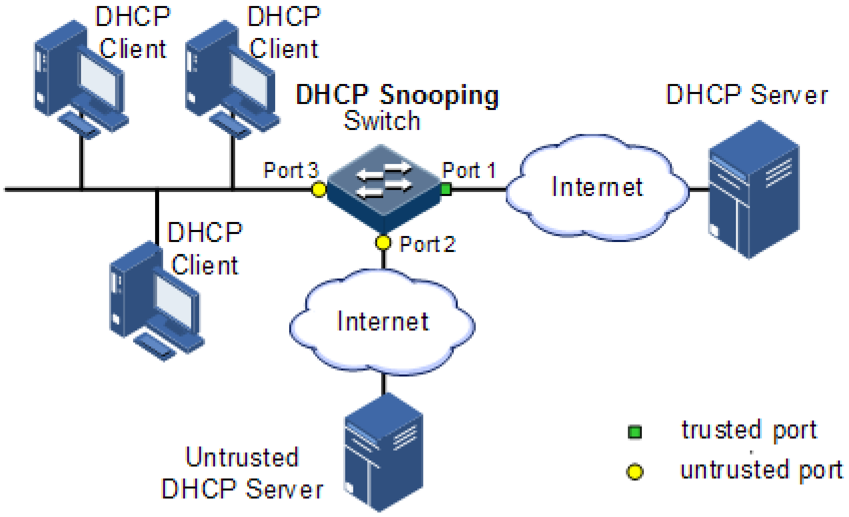
3.6.1 Introduction

DHCP Snooping is a security feature of DHCP with the following functions:

- Make the DHCP client obtain the IP address from a legal DHCP server.

If a false DHCP server exists on the network, the DHCP client may obtain incorrect IP address and network configuration parameters and cannot communicate normally. As shown in Figure 3-8, to make DHCP client obtain the IP address from ta legal DHCP server, the DHCP Snooping security system allows you to configure an interface as the trusted interface or untrusted interface: the trusted interface forwards DHCP packets normally while the untrusted interface discards the reply packets from the DHCP server.

Figure 3-8 DHCP Snooping networking



- Record mapping between DHCP client IP address and MAC address.

DHCP Snooping records entries through monitor request and reply packets received by the trusted interface, including client MAC address, obtained IP address, DHCP client-connected interface and VLAN of the interface, and so on. The following features can be implemented by using the information:

- ARP detection: judge legality of a user that sends ARP packet and avoid ARP attack from illegal users.
- IP Source Guard: filter packets forwarded by interfaces by dynamically getting DHCP Snooping entries to avoid illegal packets to pass the interface.
- VLAN mapping: modify mapped VLAN of packets sent to users to original VLAN by searching IP address, MAC address, and original VLAN information in DHCP Snooping entry corresponding to the mapped VLAN.

The Option field in DHCP packet records position information of DHCP clients. The Administrator can use this Option filed to locate DHCP clients and control client security and accounting.

If the ISCOM21xx configures DHCP Snooping to support Option function:

- When the ISCOM21xx receives a DHCP request packet, it processes packets according to Option field included or not and filling mode as well as processing policy configured by user, then forwards the processed packet to DHCP server.
- When the ISCOM21xx receives a DHCP reply packet, it deletes the field and forward to DHCP client if the packet does not contain Option field; it then forwards packets directly if the packet does not contain Option field.

3.6.2 Preparing for configurations

Scenario

DHCP Snooping is a security feature of DHCP, used to make DHCP client obtain its IP address from a legal DHCP server and record mapping between IP address and MAC address of a DHCP client.

The Option field of a DHCP packet records location of a DHCP client. The administrator can locate a DHCP client through the Option field and control client security and accounting. The device configured with DHCP Snooping and Option can perform related process according to Option field status in the packet.

Prerequisite

DHCP Snooping is exclusive to DHCP Client, or DHCP Replay. Namely, you cannot configure DHCP Relay on the device configured with DHCP Client, or DHCP Snooping.

3.6.3 Default configurations of DHCP Snooping

Default configurations of DHCP Snooping are as below.

Function	Default value
Global DHCP Snooping status	Disable
Interface DHCP Snooping status	Enable
Interface trust/untrust status	Untrust
DHCP Snooping in support of Option 82	Disable

3.6.4 Configuring DHCP Snooping

Generally, ensure that the ISCOM21xx interface connected to DHCP server is in trust state, while the interface connected to user is in distrust state.

Enabled with DHCP Snooping, if the ISCOM21xx is not configured with DHCP Snooping supporting DHCP Option, it will do nothing to Option fields for packets. For packets without Option fields, the ISCOM21xx still does not do insertion operation.

By default, DHCP Snooping of all interfaces is enabled, but only when global DHCP Snooping is enabled, interface DHCP Snooping can take effect.

Configure DHCP Snooping for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`ip dhcp snooping`**	Enable global DHCP Snooping. By default, global IPv4-based DHCP Snooping is not configured.
3	`Raisecom(config)#`**`ip dhcp snooping port-list`** `{` **`all`** `|` *`port-list`* `}`	(Optional) enable interface DHCP Snooping. By default, it is enabled.
4	`Raisecom(config)#`**`ip dhcp snooping port`** *`port-id`* **`vlan-list`** *`vlan-list`*	(Optional) configure DHCP Snooping based on VLAN.
5	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.

6	`Raisecom(config-port)#`**`ip dhcp snooping trust`**
	`Raisecom(config-port)#`**`exit`**
		Configure trust interface of DHCP Snooping.
		By default, the ISCOM21xx does not trust DHCP packets received on the interface.

7	`Raisecom(config)#`**`ip dhcp snooping information option`**	(Optional) configure DHCP Snooping to support Option 82 function.

3.6.5 Configuring DHCPv6 Snooping

Configure DHCPv6 Snooping for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`ipv6 dhcp snooping`**	Enable global IPv6-based DHCP Snooping.

Step	Command	Description
3	`Raisecom(config)#ipv6 dhcp snooping port-list { all | port-list }`	(Optional) enable interface IPv6-based DHCP Snooping.
4	`Raisecom(config)#ipv6 dhcp snooping port port vlan-list vlan-list`	(Optional) configure DHCP Snooping based on interface+VLAN.
5	`Raisecom(config)#interface port port-list`	Enter physical layer interface configuration mode.
6	`Raisecom(config-port)#ipv6 dhcp snooping trust`	Configure the IPv6-based trusted interface.

7	`Raisecom(config-port)#ipv6 dhcp snooping interface-id { ascii ascii-string | hex hex-data | ipv6-address ipv6-address }`
	`Raisecom(config-port)#exit`
		(Optional) configure interface-id on the interface.

8	`Raisecom(config)#ipv6 dhcp snooping remote-id option`	(Optional) configure DHCP Snooping to support Option 82 function.

3.6.6 Checking configurations

Use the following commands to check configuration results.

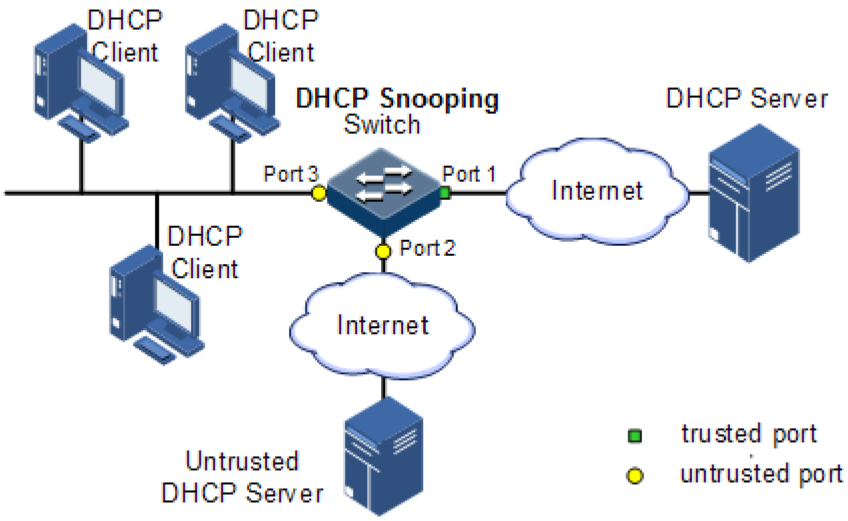
Step	Command	Description
1	`Raisecom#show ip dhcp snooping`	Show configurations of IPv4 DHCP Snooping.
2	`Raisecom#show ip dhcp snooping binding`	Show configurations of the IPv4 DHCP Snooping binding table.
3	`Raisecom#show ipv6 dhcp snooping`	Show configurations of IPv6 DHCP Snooping.
4	`Raisecom#show ipv6 dhcp snooping binding`	Show configurations of the IPv6 DHCP Snooping binding table.

3.6.7 Example for configuring DHCP Snooping

Networking requirements

As shown in Figure 3-9, the Switch is used as the DHCP Snooping device. The network requires DHCP clients to obtain the IP address from a legal DHCP server and support Option 82 field to facilitate client management; you can configure circuit ID sub-option on Port 3 as raisecom, and remote ID sub-option as user01.

Figure 3-9 Configuring DHCP Snooping



Configuration steps

Step 1 Configure global DHCP Snooping.

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

Step 2 Configure the trusted interface.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#ip dhcp snooping trust
Raisecom(config-port)#quit
```

Step 3 Configure DHCP Snooping to support Option 82 field and configure the Option 82 field.

```
Raisecom(config)#ip dhcp snooping information option
Raisecom(config)#ip dhcp information option remote-id string user01
Raisecom(config)#interface port 3
Raisecom(config-port)#ip dhcp information option circuit-id raisecom
```

Checking results

Use the **show ip dhcp snooping option** command to show configurations of DHCP Snooping.

```
Raisecom#show ip dhcp information option
DHCP Option Config Information
```

```
Attach-string:   raisecom
Remote-ID Mode:  string
Remote-ID String:  user01
Port:  3    Circuit ID:  raisecom
```

3.7 DHCP Options

3.7.1 Introduction

DHCP transmits control information and network configuration parameters through Option fields in packets to implement dynamic distribution of addresses to provide abundant network configurations for clients. DHCP has 255 kinds of Options, with the final option as Option 255. Table 3-2 lists frequently used DHCP Options.

Table 3-2 Common DHCP Options

Options	Description
3	Router option, to assign gateway for DHCP clients
6	DNS server option, to assign DNS server address distributed by DHCP clients
18	DHCP client flag option, to assign interface information for DHCP clients
51	IP address lease option
53	DHCP packet type, to mark type for DHCP packets
55	Request parameter list option. Client uses this optical to indicate network configuration parameters need to obtain from server. The content of this option is values corresponding to client requested parameters.
60	Vendor ID option. The client and DHCP server can distinguish the vendor of the client by this option. The DHCP server can assign IP addresses in a specified range to clients.
61	DHCP client flag option, to assign device information for DHCP clients
66	TFTP server name, to assign domain name for TFTP server distributed by DHCP clients
67	Startup file name, to assign startup file name distributed by DHCP clients
82	DHCP client flag option, user-defined, mainly used to mark position of DHCP clients
150	TFTP server address, to assign TFTP server address distributed by DHCP clients
184	DHCP reserved option, at present Option184 is used to carry information required by voice calling. Through Option184 it can distribute IP address for DHCP client with voice function and meanwhile provide voice calling related information.
255	Complete option

Options 18, 61, and 82 in DHCP Option are relay agent information options in DHCP packets. When a request packet sent by the DHCP client arrives at the DHCP server with traversing a DHCP relay or DHCP Snooping, the DHCP relay or DHCP Snooping device adds Option fields into the request packet.

Options 18, 61, and 82 implement the recording of DHCP client information on the DHCP server. By using them with other software, the device can implement functions such as limiting on the assignment of IP addresses and accounting. For example, when you use them with IP Source Guard, the device can defend IP address+MAC address spoofing.

Option 82 can include up to 255 sub-options. If Option 82 is defined, at least one sub-option must be defined. The ISCOM21xx supports the following two sub-options:

- Sub-Option 1 (Circuit ID): it contains interface ID, interface VLAN, and the additional information about DHCP client request packet.
- Sub-Option 2 (Remote ID): it contains interface MAC address (DHCP Relay), or bridge MAC address (DHCP snooping device) of the ISCOM21xx, or user-defined string of DHCP client request packets.

3.7.2 Preparing for configurations

Scenario

Options 18, 61, and 82 in DHCP Option are relay information options in DHCP packets. When request packets from DHCP clients reach the DHCP server, DHCP Relay or DHCP Snooping added Option field into request packets if request packets pass the DHCP relay device or DHCP snooping device is required.

Options 18, 61, and 82 implement record DHCP client information on the DHCP server. By cooperating with other software, it can implement functions such as limit on IP address distribution and accounting.

Prerequisite

N/A

3.7.3 Default configurations of DHCP Option

Default configurations of DHCP Option are as below.

Function	Default value
attach-string in global configuration mode	N/A
remote-id in global configuration mode	switch-mac
circuit-id in interface configuration mode	N/A

3.7.4 Configuring DHCP Option field

Configure DHCP Option field for the ISCOM21xx as below.

All the following steps are optional and in any sequence.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`ip dhcp information option attach-string`** *`attach-string`*	(Optional) configure attached string for Option 82 field.

3	`Raisecom(config)#`**`interface port`** *`port-id`*
	`Raisecom(config-port)#`**`ip dhcp information option circuit-id`** *`circuit-id`*
		(Optional) configure circuit ID sub-option information for Option 82 field on the interface.

4	`Raisecom(config-port)#`**`exit`**
	`Raisecom(config)#`**`ip dhcp information option remote-id`** `{` **`client-mac`** `|` **`client-mac-string`** `|` **`hostname`** `|` **`switch-mac`** `|` **`switch-mac-string`** `|` **`string`** *`string`* `}`
		(Optional) configure remote ID sub-option information for Option 82 field.

3.7.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show ip dhcp information option`**	Show configurations of DHCP Option fields.

4 PoE

This chapter describes basic principles and configuration procedures of PoE, and provides related configuration examples, including the following sections:

- Introduction
- Configuring PoE
- Example for configuring PoE switch power supply

Note

Descriptions and configurations in this chapter are supported by PoE switches among the ISCOM21xx family, rather than non-PoE switches.

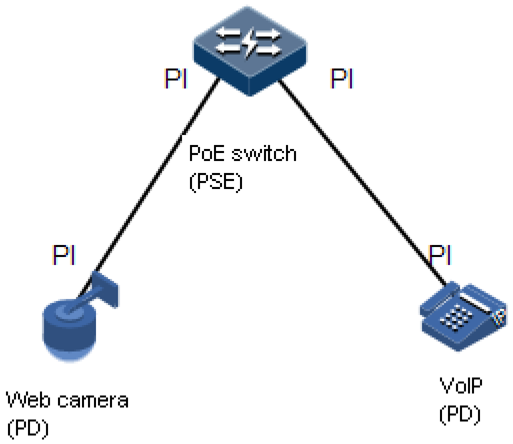
4.1 Introduction

4.1.1 PoE principle

Power over Ethernet (PoE) means that the Power Sourcing Equipment (PSE) both supplies power and transmits data to the remote Power Device (PD) through the Ethernet cable and Ethernet electrical interface.

Figure 4-1 shows PoE networking.

Figure 4-1 PoE networking



4.1.2 PoE modules

The PoE system is composed of the following modules:

- PSE: composed of the power module and PSE functional module. The PSE can detect PDs, obtain PD power information, supply power remotely, monitor power supply, and power off devices.
- PD: supplied with power by the PSE. There are standard PDs and non-standard PDs. Standard PDs must comply with IEEE 802.3af, such as IP phone and web camera.
- Power Interface (PI): the interface between the PSE/PD and the Ethernet cable, namely, RJ45 interface

4.1.3 PoE advantages

PoE has the following advantages:

- Reliability: a centralized PSE supplies power with convenient backup, uniform management of power modules, and high security.
- Easy connection: the network terminal does not need an external power; instead, it needs only an Ethernet cable connected to the PoE interface.
- Standardization: PoE complies with IEEE 802.3at and uses globally uniform power interface.
- Wide applications: applicable to IP phones, wireless Access Point (AP), portable device charger, credit card reader, web camera, and data collection system.

4.1.4 PoE concepts

- Maximum output power of interface power supply

It is the maximum output power output by the interface to the connected PD.

- Priority of interface power supply

There are three levels of priorities for power supply: critical, high, and low. Firstly, power on the interface connected PD with critical priority, then the PD with high priority, and finally the PD with low priority.

- Switch overtemperature protection

When the current temperature exceeds the overtemperature threshold, overtemperature alarms occur and the system sends Trap to the Network Management System (NMS).

- Global Trap

When the current temperature exceeds the overtemperature threshold, the PSE power utilization ratio exceeds the threshold, or the status of PoE interface power supply changes, the ISCOm21xx sends Trap to the NMS.

- PSE power utilization ratio threshold

When the PSE power utilization ratio exceeds the threshold for the first time, the system sends Trap.

4.2 Configuring PoE

4.2.1 Preparing for configurations

Scenario

When the remotely connected PE is inconvenient to draw power, it needs to draw power from the Ethernet electrical interface, to concurrently transmit power and data.

Prerequisite

N/A

4.2.2 Default configurations of PoE

Default configurations of PoE are as below.

Function	Default value
Power supply interface PoE status	Enable
Non-standard PD identification	Disable
Maximum output power of interface power supply	30000 mW
Power supply management mode	Auto
Power supply priority	Low
Switch overtemperature protection status	Enable
Power supply global Trap switch status	Enable
PSE power utilization threshold	99%

4.2.3 Enabling interface PoE

Enable interface PoE for the ISCOM21xx as below:

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#`**`poe enable`**	Enable interface PoE.

4.2.4 Configuring power supply management mode

Note

For standard PDs, automatic power supply mode is recommended.

Configure power supply management mode for the ISCOM21xx as below:

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**poe power-management** { **auto** | **manual** }	Configure power supply management mode.

4.2.5 Configuring maximum output power of interface power supply

Configure maximum output power of interface power supply for the ISCOM21xx as below:

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**poe max-power** *max-power-value*	Configure maximum output power of interface power supply.

4.2.6 Configuring priority of interface power supply

Configure priority of interface power supply for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**poe priority** { **critical** | **high** | **low** }	Configure priority of interface power supply.

4.2.7 Configuring PSE power utilization ratio threshold

Configure the PSE power utilization ratio threshold for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#poe pse power-thredshold percent`	Configure the PSE power utilization ratio threshold.

4.2.8 Enabling non-standard PD identification

Note

To use a non-standard PD, confirm its power consumption, voltage, and current in advance to properly configure the maximum output power on the PSE and to avoid damaging the PD due to over high power.

Enable non-standard PD identification for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#poe legacy enable`	Enable non-standard PD identification.

4.2.9 Enabling forcible power supply on interface

Caution

When supplying power for a remote PD by the ISCOM21xx, use a standard PD, pre-standard PD, or Cisco-primate standard PD. To use other non-standard PD, confirm its power consumption, voltage, and current in advance to properly configure the maximum output power on the PSE and to avoid damaging the PD due to over high power.

Enable forcible power supply on interfaces for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface port port-id`	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#poe force-power`	Enable forcible PoE power supply on the interface.

4.2.10 Enabling overtemperature protection

Enable overtemperature protection for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**poe temperature-protection enable**	Enable overtemperature protection.

4.2.11 Enabling global Trap

Enable global Trap for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**poe pse trap enable**	Enable global Trap function.

4.2.12 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show poe port-list** *port-list* [**detail**]	Show power supply status on specified interfaces.
2	Raisecom#**show poe pse** [**detail**]	Show PSE configurations and realtime operating information.

4.3 Example for configuring PoE switch power supply

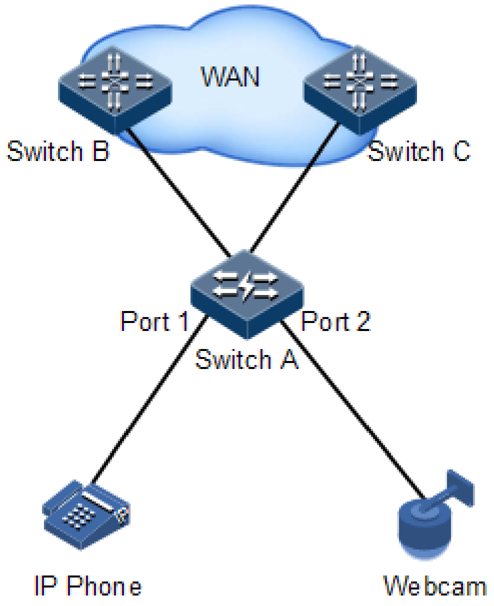
Networking requirements

As shown in Figure 4-2, Switch A is connected to the upper layer WAN through Switch B and Switch C. It is used to supply power to an IP phone and a web camera. It is required to supply power to the web camera in precedence when it runs in full load.

Configure parameters according to user requirements as below:

- Configure the maximum output power of Port 1 and Port 2 to 30000 mW.
- Enable overtemperature protection on the switch.
- Enable Trap function for power supply on the switch.
- Configure the priorities of Port 2 and Port 1 to high and low respectively.

Figure 4-2 PoE switch power supply networking



Configuration steps

Step 1 Enable PoE on Port 1 and Port 2.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)#poe enable
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#poe enable
Raisecom(config-port)#exit
```

Step 2 Configure the maximum output power of Port 1 and Port 2 to 30000 mW.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#poe max-power 30000
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#poe max-power 30000
Raisecom(config-port)#exit
```

Step 3 Enable overtemperature protection.

```
Raisecom(config)#poe temperature-protection enable
```

Step 4 Enable global Trap.

```
Raisecom(config)#poe pse trap enable
```

Step 5 Configure priorities of Port 2 and Port 1 to high and low respectively.

```
Raisecom(config)#interface port 2
Raisecom(config-port)#poe priority high
Raisecom(config-port)#exit
Raisecom(config)#interface port 1
Raisecom(config-port)#poe priority low
```

Checking results

Use the **show poe port-list 1,2 detail** command to show PoE configurations on Port 1 and Port 2.

```
Raisecom#show poe port-list 1,2 detail
Port: 1
-------------------------------------------------
POE administrator status: Enable
POE operation status: Enable
Power detection status:Searching
POE Power Pairs mode:Signal
PD power classification:Class0
POE power Priority:Low
POE power max:30000 (mW)
POE power output:0 (mW)
POE power average:0 (mW)
POE power peak:0 (mW)
POE current output:0 (mA)
POE voltage output:0 (V)
Port: 2
-------------------------------------------------
POE administrator status: Enable
POE operation status: Enable
Power detection status:Searching
POE Power Pairs mode:Signal
PD power classification:Class0
POE power Priority:High
POE power max:30000 (mW)
POE power output:0 (mW)
POE power average:0 (mW)
POE power peak:0 (mW)
POE current output:0 (mA)
POE voltage output:0 (V)
```

5 QoS

This chapter describes basic principles and configuration procedures of QoS and provides related configuration examples, including the following sections:

- Introduction
- Configuring basic QoS
- Configuring traffic classification and traffic policy
- Configuring priority mapping
- Configuring congestion management
- Configuring rate limiting
- Configuring examples

5.1 Introduction

Users bring forward different service quality demands for network applications, then the network should distribute and schedule resources for different network applications according to user demands. Quality of Service (QoS) can ensure service in real time and integrity when network is overloaded or congested and guarantee that the whole network runs efficiently.

QoS is composed of a group of flow management technologies:

- Service model
- Priority trust
- Traffic classification
- Traffic policy
- Priority mapping
- Congestion management

5.1.1 Service model

QoS technical service models:

- Best-effort Service
- Differentiated Services (DiffServ)

Best-effort

Best-effort service is the most basic and simplest service model on the Internet (IPv4 standard) based on storing and forwarding mechanism. In Best-effort service model, the application can send a number of packets at any time without being allowed in advance and notifying the network. For Best-effort service, the network will send packets as possible as it can, but cannot guarantee the delay and reliability.

Best-effort is the default Internet service model now, applying to most network applications, such as FTP and E-mail, which is implemented by First In First Out (FIFO) queue.

DiffServ

DiffServ model is a multi-service model, which can satisfy different QoS requirements.

DiffServ model does not need to maintain state for each flow. It provides differentiated services according to the QoS classification of each packet. Many different methods can be used for classifying QoS packets, such as IP packet priority (IP precedence), the packet source address or destination address.

Generally, DiffServ is used to provide end-to-end QoS services for a number of important applications, which is implemented through the following techniques:

- Committed Access Rate (CAR): CAR refers to classifying the packets according to the pre-set packets matching rules, such as IP packets priority, the packet source address or destination address. The system continues to send the packets if the flow complies with the rules of token bucket; otherwise, it discards the packets or remarks IP precedence, DSCP, EXP, and so on. CAR can not only control the flows, but also mark and remark the packets.
- Queuing technology: the queuing technologies of SP, WRR, SP+WRR cache and schedule the congestion packets to implement congestion management.

5.1.2 Priority trust

Priority trust means that the ISCOM21xx uses priority of packets for classification and performs QoS management.

The ISCOM21xx supports packet priority trust based on interface, including:

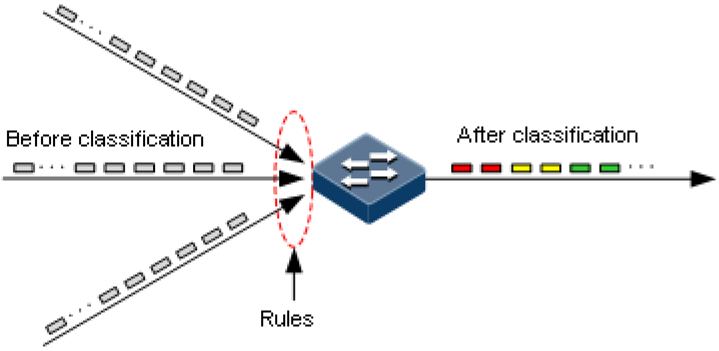
- Differentiated Services Code Point (DSCP) priority
- Class of Service (CoS) priority
- Interface priority

5.1.3 Traffic classification

Traffic classification refers to recognizing packets of certain types according to configured rules, conducting different QoS policies for packets matching with different rules. It is the prerequisite of differentiated services.

The ISCOM21xx supports traffic classification by IP priority, DSCP priority, and CoS priority over IP packets, as well as traffic classification by Access Control List (ACL) rule and VLAN ID. Figure 5-1 shows the principle of traffic classification.

Figure 5-1 Principle of traffic classification



IP priority and DSCP priority

Figure 5-2 shows the structure of the IP packet head. The head contains an 8-bit ToS field. Defined by RFC 1122, IP priority (IP Precedence) uses the highest 3 bits (0–3) with value range of 0–7; RFC2474 defines ToS field again, and applies the first 6 bits (0–5) to DSCP priority with value range 0–63, the last 2 bits (bit-6 and bit-7) are reserved. Figure 5-3 shows the structure of two priority types.

Figure 5-2 Structure of IP packet head

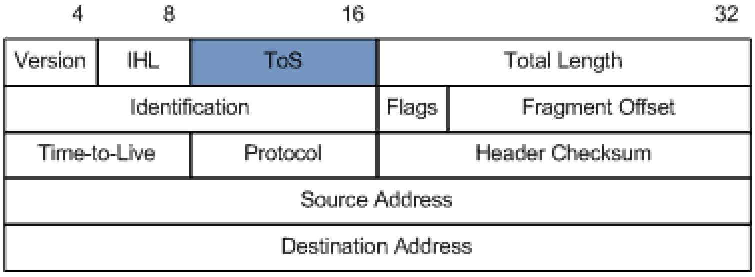
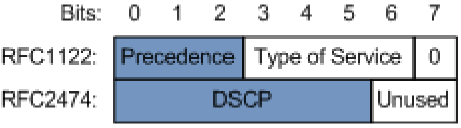


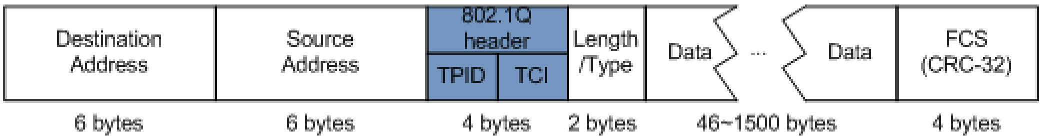
Figure 5-3 Structure of packets with IP priority and DSCP priority



CoS priority

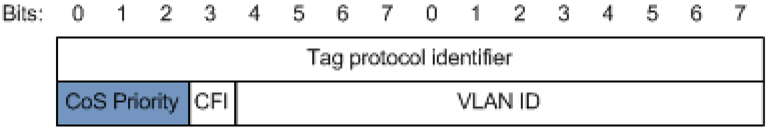
The format of Ethernet packets is modified to make VLAN packets based on IEEE 802.1Q. IEEE 802.1Q adds 4-Byte 802.1Q Tag between the source address field and protocol type field, as shown in Figure 5-4. The Tag includes a field of 2-Byte TPID (Tag Protocol Identifier, value being 0x8100) and a field of 2-Byte Tag Control Information (TCI).

Figure 5-4 Structure of VLAN packets



CoS priority is included in the first 3 bits of the TCI field, ranging from 0 to 7, as shown in Figure 5-5. It is used when QoS needs to be guaranteed on the Layer 2 network.

Figure 5-5 Structure of packets with CoS priority



5.1.4 Traffic policy

After classifying packets, the ISCOM21xx needs to take different actions for different packets. The binding of traffic classification and an action forms a traffic policy.

Rate limiting

Rate limiting refers to controlling network traffic, monitoring the rate of traffic entering the network, and discarding overflow part, so it controls ingress traffic in a reasonable range, thus protecting network resources and carrier interests.

The ISCOM21xx supports rate limiting based on traffic policy in the ingress direction on the interface.

The ISCOM21xx supports using token bucket for rate limiting, including single-token bucket and dual-token bucket.

Redirection

Redirection refers to redirecting packets to a specified interface, instead of forwarding packets according to the mapping between the original destination address and interface, thus implementing policy routing.

The ISCOM21xx supports redirecting packets to the specified interface for forwarding in the ingress direction of an interface.

Remarking

Remarking refers to configuring some priority fields in packets again and then classifying packets by user-defined standard. Besides, downstream nodes on the network can provide differentiated QoS service according to remarking information.

The ISCOM21xx supports remarking packets by the following priority fields:

- IP priority of IP packets
- DSCP priority
- CoS priority

Traffic statistics

Traffic statistics is used to gather statistics of data packets of a specified service flow, namely, the number of packets and Bytes matching traffic classification that pass the network or are discarded.

Traffic statistics is not a QoS control measure, but can be used in combination with other QoS actions to improve network supervision.

5.1.5 Priority mapping

Priority mapping refers when the ISCOM21xx receives packets, it sends them in queues with different local priorities in accordance with mapping from external priority to local priority, thus scheduling packets in the egress direction of packets.

The ISCOM21xx supports priority mapping based on DSCP priority or CoS priority.

Table 5-1 lists the default mapping among local priority, DSCP, and CoS.

Table 5-1 Default mapping among local priority, DSCP priority, and CoS priority

Local priority	0	1	2	3	4	5	6	7
DSCP	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
CoS	0	1	2	3	4	5	6	7

Local priority refers to a kind of packet priority with internal function assigned by the ISCOM21xx, namely, the priority corresponding to queue in QoS queue scheduling.

Local priority ranges from 0 to 7. Each interface of the ISCOM21xx supports 8 queues. Local priority and interface queue is in one-to-one mapping. The packet can be sent to the assigned queue according to the mapping between local priority and queue, as shown in Table 5-2.

Table 5-2 Mapping between local priority and queue

Local priority	0	1	2	3	4	5	6	7
Queue	1	2	3	4	5	6	7	8

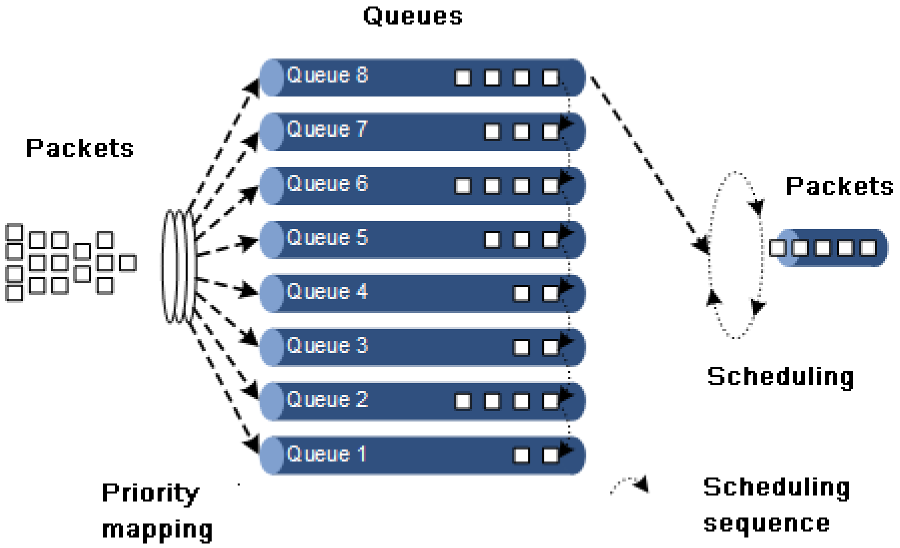
5.1.6 Congestion management

Queue scheduling is necessary when there is intermittent congestion on the network or delay sensitive services require higher QoS service than non-sensitive services.

Queue scheduling adopts different schedule algorithms to transmit packets in queues. The ISCOM21xx supports Strict Priority (SP), Weight Round Robin (WRR), and SP+WRR algorithm. Each algorithm solves specific network traffic problems, and has different influences on distribution, delay, and jitter of bandwidth resource.

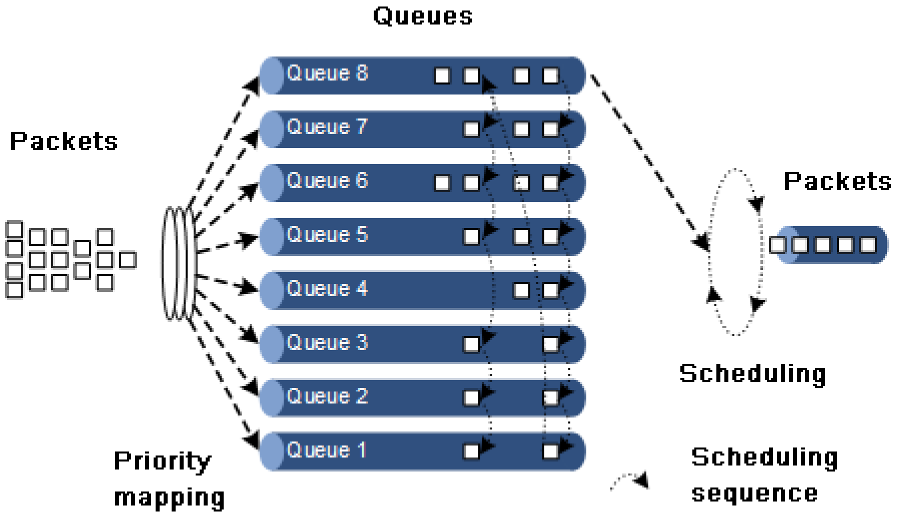
- SP: schedule packets strictly according to queue priority order. Queues with low priority cannot be scheduled until queues with higher priority finishes schedule, as shown in Figure 5-6.

Figure 5-6 SP scheduling



- WRR: on the basis of circular scheduling each queue according to queue priority, schedule packets in various queues according to weight of each queue, as shown in Figure 5-7.

Figure 5-7 WRR scheduling



- SP+WRR: dividing queues on interface into two groups, you can assign some queues perform SP schedule and other queues perform WRR schedule.

5.1.7 Rate limiting based on interface and VLAN

The ISCOM21xx supports rate limiting on both based on traffic policy and based on interface or VLAN ID. Similar to rate limiting based on traffic policy, the ISCOM21xx discards the exceeding traffic.

5.2 Configuring basic QoS

5.2.1 Preparing for configurations

Scenario

QoS enables the carrier to provide different service quality for different applications, and assign and schedule different network resources.

Prerequisite

N/A

5.2.2 Default configurations of basic QoS

Default configurations of basic QoS are as below.

Function	Default value
Global QoS status	Enable

5.2.3 Enabling global QoS

Enable global QoS for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`mls qos enable`**	Enable global QoS.

5.2.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show mls qos`**	Show global QoS status.

5.3 Configuring traffic classification and traffic policy

5.3.1 Preparing for configurations

Scenario

Traffic classification is the basis of QoS. You can classify packets from an upstream device by priorities or ACL rule.

A traffic classification rule will not take effect until it is bound to a traffic policy. Apply traffic policy according to current network loading conditions and period. Usually, the ISCOM21xx limits the rate of transmitting packets according to configured rate when packets enter the network, and remarks priority according to service feature of packets.

Prerequisite

Enable global QoS.

5.3.2 Default configurations of traffic classification and traffic policy

Default configurations of traffic classification and traffic policy are as below.

Function	Default value
Traffic policy statistics status	Disable

5.3.3 Creating traffic classification

Create traffic classification for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`class-map`** *`class-map-name`* `[` **`match-all`** `|` **`match-any`** `]`	Create traffic classification and enter traffic classification cmap configuration mode.
3	`Raisecom(config-cmap)#`**`description`** *`string`*	(Optional) describe traffic classification.

5.3.4 Configuring traffic classification rules

Configure traffic classification rules for the ISCOM21xx as below.

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

Step	Command	Description
2	Raisecom(config)#**class-map** *class-map-name* [**match-all** | **match-any**]	Create traffic classification and enter traffic classification cmap configuration mode.
3	Raisecom(config-cmap)#**match** { **access-list-map** | **ip-access-list** | **mac-access-list** } *acl-number*	(Optional) configure traffic classification over ACL rule. The ACL rule must be defined firstly and the type must be **permit**.
4	Raisecom(config-cmap)#**match class-map** *class-map-name*	(Optional) configure traffic classification over traffic classification rule. The pursuant traffic classification must be created and the matched type must be identical with the traffic classification type.
5	Raisecom(config-cmap)#**match ip dscp** *dscp-value*	(Optional) configure traffic classification over DSCP rules.
6	Raisecom(config-cmap)#**match ip precedence** *precedence-value*	(Optional) configure traffic classification over IP priority.
7	Raisecom(config-cmap)#**match vlan** *vlan-list* [**double-tagging inner**]	(Optional) configure traffic classification over VLAN ID rule of VLAN packets.

Note

- When the matched type of a traffic classification is **match-all**, the matched information may have conflict and the configuration may fail.
- Traffic classification rules must be created for traffic classification; namely, the **match** parameter must be configured.
- For traffic classification quoted by traffic policy, do not modify traffic classification rule; namely, do not modify the **match** parameter of traffic classification.

5.3.5 Creating token bucket and rate limiting rules

Create token bucket and rate limiting rules for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos** { **aggregate-policer** | **class-policer** | **single-policer** } *policer-name rate-value burst-value* [**exceed-action** { **drop** | **policed-dscp-transmit** *dscp-value*]	Create token bucket and configure rate limiting rules.

5.3.6 Creating traffic policy

Create traffic policy for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**policy-map** *policy-map-name*	Create traffic policy and enter traffic policy pmap configuration mode.
3	Raisecom(config-pmap)#**description** *string*	(Optional) configure traffic policy information.

5.3.7 Defining traffic policy mapping

Note

Define one or more defined traffic classifications to one traffic policy.

Define traffic policy mapping for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**policy-map** *policy-map-name*	Create traffic policy and enter traffic policy pmap configuration mode.
3	Raisecom(config-pmap)#**class-map** *class-map-name*	Bind traffic classification into traffic policy; only apply traffic policy to packets matching with traffic classification. **Note** At least one rule is necessary for traffic classification to bind traffic policy; otherwise the binding will fail.

5.3.8 Defining traffic policy operation

Note

Define different operations to different flows in policy.

Define a traffic policy operation for the ISCOM21xx as below.

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

Step	Command	Description
2	Raisecom(config)#**policy-map** *policy-map-name*	Create traffic policy and enter traffic policy pmap configuration mode.
3	Raisecom(config-pmap)#**class-map** *class-map-name*	Bind traffic classification with traffic policy; apply traffic policy to packets matching with traffic classification only. **Note** At least one rule is required for traffic classification to bind traffic policy, otherwise the binding will fail.
4	Raisecom(config-pmap-c)#**police** *policer-name*	(Optional) apply token bucket on traffic policy and take rate limiting and shaping. **Note** The token bucket needs to be created in advance and be configured with rate limiting and shaping rule; otherwise, the operation will fail.
5	Raisecom(config-pmap-c)#**redirect-to port** *port-id*	(Optional) configure redirecting rules under traffic classification, forwarding classified packets from assigned interface.
6	Raisecom(config-pmap-c)#**set** { **cos** *cos-value* | **ip precedence** *precedence-value* | **ip dscp** *ip-dscp-value* | **vlan** *vlan-id* }	(Optional) configure remarking rules under traffic classification, modify packet CoS priority, DSCP priority, IP priority, and VLAN ID.
7	Raisecom(config-pmap-c)#**copy-to-mirror**	(Optional) configure flow mirror to monitor interface.
8	Raisecom(config-pmap-c)#**statistics enable**	(Optional) configure flow statistic rule under traffic classification, statistic packets for matched traffic classification.

5.3.9 Applying traffic policy to interface

Apply traffic policy to the interface for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**service-policy** *policy-name* **ingress** *port-id*	Bind the configured traffic policy with the interface.

5.3.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show service-policy statistics** [**port** *port-id*]	Show traffic policy status and the statistics of the applied policy.
2	Raisecom#**show class-map** [*class-map-name*]	Show information about traffic classification.
3	Raisecom#**show policy-map** [*policy-map-name*]	Show traffic policy information.
4	Raisecom#**show policy-map** [*policy-map-name*] [**class** *class-map-name*]	Show information about traffic classification in traffic policy.
5	Raisecom#**show mls qos policer** [*policer-name*]	Show information about the assigned token bucket (rate limiting and shaping).
6	Raisecom#**show mls qos policer** [**aggregate-policer** | **class-policer** | **single-policer**]	Show information about the assigned type token bucket (rate limiting and shaping).
7	Raisecom#**show policy-map port** [*port-id*]	Show application information on about traffic policy the interface.
8	Raisecom#**show mls qos queue-rate** [**port-list** *port-list*]	Show rate limiting on the interface.

5.3.11 Maintenance

Command	Description
Raisecom(config)#**clear service-policy statistics** [**egress** *port-id* [**class-map** *class-map-name*] | **ingress** *port-id* [**class-map** *class-map-name*] | **port** *port-id*]	Clear statistics of QoS packets.

5.4 Configuring priority mapping

5.4.1 Preparing for configurations

Scenario

You can choose priority for trusted packets from upstream device, untrusted priority packets are processed by traffic classification and traffic policy. After configuring priority trust mode, the ISCOM21xx operates packets according to their priorities and provides related service.

To specify local priority for packets is the prerequisite for queue scheduling. For packets from the upstream device, you cannot only map the external priority carried by packets to different local priority, but also configure local priority for packets based on interface, then the ISCOM21xx will take queue scheduling according to local priority of packets. Generally speaking, IP packets need to configure mapping between IP priority/DSCP priority and local priority; while VLAN packets need to configure mapping between CoS priority and local priority.

Prerequisite

N/A

5.4.2 Default configurations of basic QoS

Default configurations of basic QoS are as below.

Function	Default value
Interface trust priority type	Trust CoS priority
Mapping between CoS and local priority	See Table 5-3.
Mapping between DSCP and local priority	See Table 5-4.
Interface priority	0

Table 5-3 Default mapping between CoS and local priority

CoS	0	1	2	3	4	5	6	7
Local	0	1	2	3	4	5	6	7

Table 5-4 Default mapping between DSCP and local priority

DSCP	0–7	8–15	16–23	24–31	32–39	40–47	48–55	56–63
Local	0	1	2	3	4	5	6	7

5.4.3 Configuring interface trust priority type

Configure interface trust priority type for the ISCOM21xx as below.

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

Step	Command	Description
3	`Raisecom(config-port)#mls qos port-priority priority`	Configure default priority on the interface.
4	`Raisecom(config-port)#mls qos trust { cos | dscp | port-priority }`	Configure priority type of interface trust.

5.4.4 Configuring mapping from CoS to local priority

Configure mapping from CoS to local priority for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#mls qos mapping cos cos-value to localpriority priority`	Create mapping from CoS to local priority.

5.4.5 Configuring mapping from DSCP to local priority

Configure mapping from DSCP to local priority for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#mls qos mapping dscp dscp-value to local-priority priority`	Create mapping from DSCP to local priority.

5.4.6 Configuring mapping from local priority to DSCP

Configure mapping from local priority to DSCP for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#policy-map policy-map-name`	Create traffic policy and enter traffic policy pmap configuration mode.
3	`Raisecom(config-pmap)#class-map class-map-name`	Bind traffic classification with traffic policy, and apply traffic policy to those packets that match traffic classification.

4	`Raisecom(config-pmap-c)#set local-priority priority`
	`Raisecom(config-pmap-c)#exit`
	`Raisecom(config-pmap)#exit`
		Configure local priority in pcmp-c mode, and return to global configuration mode.

Step	Command	Description
5	`Raisecom(config)#`**`mls qos mapping local-priority`** *`priority`* **`to dscp`** *`dscp-value`*	Create mapping from local priority to DSCP.

5.4.7 Configuring all-traffic modification on interface

Configure all-traffic modification on interface for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`mls qos mapping local-priority to dscp enable`**	Enable mapping from local priority to DSCP.
3	`Raisecom(config)#`**`mls qos non-modify port`** *`port-list`*	Configure the port list for disabling all-traffic modification.

5.4.8 Configuring specific-traffic modification

Configure specific-traffic modification for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`policy-map`** *`policy-map-name`*	Create traffic policy and enter traffic policy pmap configuration mode.
3	`Raisecom(config-pmap)#`**`class-map`** *`class-map-name`*	Bind traffic classification with traffic policy, and apply traffic policy to those packets that match traffic classification.
4	`Raisecom(config-pmap-c)#`**`modify enable`**	Enable specific-traffic modification.

5.4.9 Configuring CoS remarking

Configure CoS remarking for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#`**`switchport qinq dot1q-tunnel`**	(Optional) enable basic QinQ.

Step	Command	Description
4	Raisecom(config-port)#**switchport vlan-mapping** *vlan-id* **add-outer** *vlan-id*	(Optional) enable selective QinQ.
5	Raisecom(config-port)#**switchport vlan-mapping ingress** *vlan-id* **translate** *vlan-id*	(Optional) enable VLAN mapping.
6	Raisecom(config-port)#**exit**	Return to global configuration mode.
7	Raisecom(config)#**mls qos cos-remark enable**	Enable CoS remarking from local priority to CoS priority.

5.4.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show mls qos**	Show global QoS status.
2	Raisecom#**show mls qos port** [*port-id*]	Show interface QoS priority, and trust mode information.
3	Raisecom#**show mls qos mapping cos**	Show information about mapping from CoS to local priority.
4	Raisecom#**show mls qos mapping dscp**	Show information about mapping from DSCP to local priority.
5	Raisecom#**show mls qos mapping localpriority**	Show information about mapping from local priority to queue.
6	Raisecom#**show mls qos localpriority-to-dscp**	Show information about mapping from local priority to DSCP.

5.5 Configuring congestion management

5.5.1 Preparing for configurations

Scenario

When a network is congested, you need to balance delay and delay jitter of various packets. Packets of key services (such as video and voice) can be preferentially processed while packets of common services (such as E-mail) with identical priority can be fairly processed. Packets with different priorities can be processed according to its weight value. You can configure queue scheduling in this situation. Choose a schedule algorithm according to service condition and customer requirements.

Prerequisite

Enable global QoS.

5.5.2 Default configurations of congestion management

Default configurations of congestion management are as below.

Function	Default value
Queue scheduling mode	SP
Queue weight	WRR weight for scheduling 8 queues is 1.

5.5.3 Configuring SP queue scheduling

Configure SP queue scheduling for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos queue scheduler sp**	Configure interface queue scheduling mode as SP.

5.5.4 Configuring WRR or SP+WRR queue scheduling

Configure WRR or SP+WRR for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos queue scheduler wrr**	Configure interface queue scheduling mode as WRR.
3	Raisecom(config-port)#**mls qos queue wrr** *weigh1 weight2 weight3…weight8*	Configure weight for each queue. Conduct SP scheduling when the priority of a queue is 0.

5.5.5 Configuring queue transmission rate

Configure queue transmission rate for the ISCOM21xx as below.

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

Step	Command	Description
3	Raisecom(config-port)#**mls qos queue-rate** [**queue-list** *queue-list*] **min** *rate-limit* **max** *rate-limit*	Configure interface-based queue transmission rate.

5.5.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show mls qos port** [*port-id*]	Show QoS priority and trust mode on the interface.
2	Raisecom#**show mls qos queue**	Show queue weight information.
3	Raisecom#**show mls qos queue-rate** [**port-list** *port-list*]	Show interface-based queue transmission rate.

5.6 Configuring rate limiting based on interface or VLAN

5.6.1 Preparing for configurations

Scenario

When the network is congested, you wish to restrict burst flow on an interface or VLAN make packets transmitted in a well-proportioned rate to remove network congestion. You need to configure rate limiting based on interface or VLAN.

Prerequisite

Create VLANs.

5.6.2 Configuring rate limiting based on interface

Configure rate limiting based on interface for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**rate-limit port-list** { **all** | *port-list* } { **egress** | **ingress** } *rate-value* [*burst-value*] Raisecom(config)#**rate-limit port-list** { **all** | *port-list* } **both** *rate-value*	Configure rate limiting based on interface.

5.6.3 Configuring rate limiting based on VLAN

Configure rate limiting based on VLAN for the ISCOM21xx as below.

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 rate limiting based on VLAN.

5.6.4 Configuring rate limiting based on QinQ

Configure rate limiting based on QinQ for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`rate-limit double-tagging-vlan outer`** `{` *`outer-vlan-id`* `|` **`any`** `}` **`inner`** `{` *`inner-vlan-id`* `|` **`any`** `}` *`rate-value burst-value`* `[` **`statistics`** `]`	(Optional) configure rate limiting based on QinQ.

5.6.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show rate-limit port-list`** `[` *`port-list`* `]`	Show configurations of rate limiting on specified interfaces.
2	`Raisecom#`**`show rate-limit vlan`**	Show configurations of rate limiting based on VLAN.

5.6.6 Maintenance

Maintain the ISCOM21xx as below.

Command	Description
`Raisecom(config)#`**`clear rate-limit statistics vlan`** `[` *`vlan-id`* `]`	Clear statistics of packet lost due to rate limiting based on VLAN.

5.7 Configuring examples

5.7.1 Example for configuring congestion management

Networking requirements

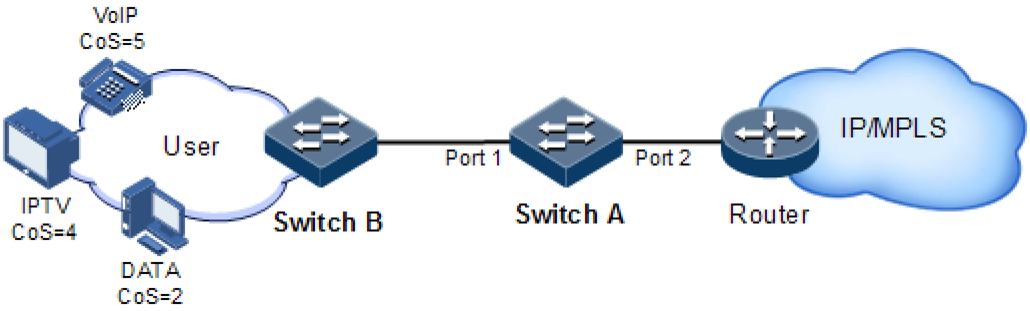
As shown in Figure 5-8, the user uses voice, video and data services.

CoS priority of voice service is 5, CoS priority of video service is 4, and CoS priority of data service is 2. The local priorities for these three types of services are mapping 6, 5, and 2 respectively.

Congestion occurs easily on Switch A. To reduce network congestion; make the following rules according to different services types:

- For voice service, perform SP schedule to ensure this part of flow passes through in prior;
- For video service, perform WRR schedule, with weight value 50;
- For data service, perform WRR schedule, with weight value 20;

Figure 5-8 Queue scheduling networking



Configuration steps

Step 1 Configure interface priority trust mode.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#mls qos enable
SwitchA(config)#interface port 2
SwitchA(config-port)#mls qos trust cos
SwitchA(config-port)#quit
```

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

```
SwitchA(config)#mls qos mapping cos 5 to local-priority 6
SwitchA(config)#mls qos mapping cos 4 to local-priority 5
SwitchA(config)#mls qos mapping cos 2 to local-priority 2
```

Step 3 Conduct SP+WRR queue scheduling in Port 1 egress direction.

```
SwitchA(config)#mls qos queue wrr 1 1 20 1 1 50 0 0
```

Checking results

Use the following command to show interface priority trust mode.

```
SwitchA#show mls qos port 2
Port    Priority    Trust        Flow Modify
-----------------------------------------------------------
  2      0           Cos        Enable
…
```

Use the following command to show mapping between Cos priority and local priority.

```
SwitchA#show mls qos mapping cos
CoS-LocalPriority Mapping:

           CoS:   0   1   2   3   4   5   6   7
  ----------------------------------------------
  LocalPriority:  0   1   2   3   5   6   6   7

SwitchA#show mls qos mapping localpriority
LocalPriority-Queue Mapping:
LocalPriority: 0   1   2   3   4   5   6   7
----------------------------------------------------
        Queue: 1   2   3   4   5   6   7   8
```

Use the following command to show configurations of queue scheduling on the interface.

```
SwitchA#show mls qos queue
Queue    Weight(WRR)
-------------------------
  1      1
  2      1
  3      20
  4      1
  5      1
  6      50
  7      0
  8      0
```

5.7.2 Example for configuring rate limiting based on interface

Networking requirements

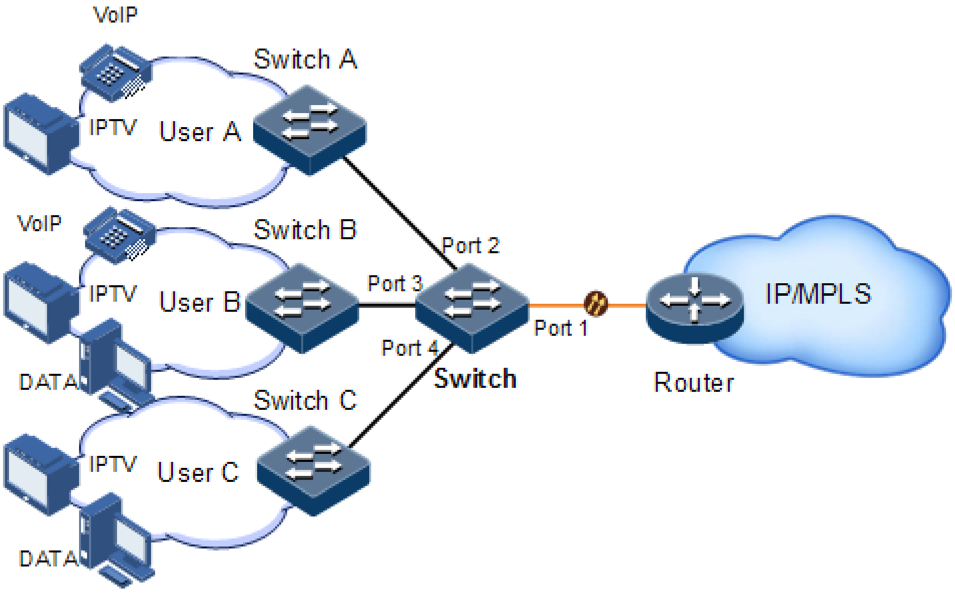
As shown in Figure 5-9, User A, User B, and User C are respectively connected to Switch A, Switch B, Switch C and ISCOM21xx.

User A requires voice and video services, User B requires voice, video and data services, and User C requires video and data services.

According to service requirements, make rules as below.

- For User A, provide 25 Mbit/s assured bandwidth, permitting burst flow 100 Kbytes and discarding redundant flow.
- For User B, provide 35 Mbit/s assured bandwidth, permitting burst flow 100 Kbytes and discarding redundant flow.
- For User C, provide 30 Mbit/s assured bandwidth, permitting burst flow 100 Kbytes and discarding redundant flow.

Figure 5-9 Rate limiting based on interface



Configuration steps

Step 1 Configure rate limiting based on interface.

```
Raisecom#config
Raisecom(config)#rate-limit port-list 2 ingress 25000 100
Raisecom(config)#rate-limit port-list 3 ingress 35000 100
Raisecom(config)#rate-limit port-list 4 ingress 30000 100
```

Checking results

Use the **show rate-limit** *interface-type interface-number* command to show configurations of rate limiting based on interface.

```
Raisecom#show rate-limit port-list 2-4
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)
-------------------------------------------------------------
2       24992         100          0             0
3       34976         100          0             0
4       29984         100          0             0
```

6 Multicast

This chapter describes basic principles and configuration procedures of multicast and provides related configuration examples, including the following sections:

- Overview
- Configuring IGMP Snooping
- Configuring MVR
- Configuring MVR Proxy
- Configuring IGMP filtering
- Maintenance
- Configuration examples

6.1 Overview

With the constant development of Internet, more and more 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.

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 ISCOM21xx 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 ISCOM21xx sends multicast packets from this interface.

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.

Note

The multicast address is the destination address instead of the source 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

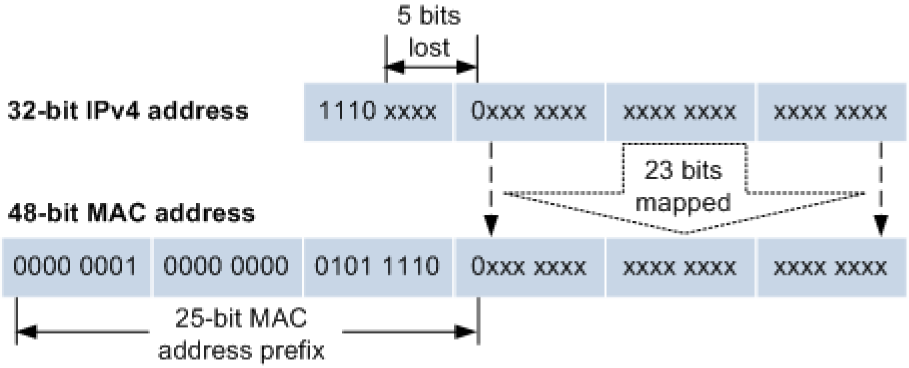
When the Ethernet transmits unicast IP packets, it uses the MAC address of the receiver as the destination MAC address. However, when multicast packets are transmitted, the destination is no longer a specific receiver, but a group with an uncertain number of members, so the Ethernet needs to use the 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.

Figure 6-1 shows mapping between the IPv4 multicast address and MAC address.

Figure 6-1 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 ISCOM21xx may receive extra data besides IPv4 multicast group, and these extra multicast data needs to be filtered by the upper layer on the ISCOM21xx.

Supported multicast features

The ISCOM21xx supports the following multicast features:

- Internet Group Management Protocol Snooping (IGMP) Snooping
- Multicast VLAN Registration (MVR)
- MVR Proxy
- IGMP filtering

Note

- MVR Proxy is usually used with MVR.
- IGMP filtering can be used with IGMP Snooping or MVR.

6.1.2 IGMP Snooping

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 ISCOM21xx to monitor IGMP session between the host and multicast router. When monitoring a group of IGMP Report from host, the ISCOM21xx will add host-related interface to the forwarding entry of this group. Similarly, when a forwarding entry reaches the aging time, the ISCOM21xx will delete host-related interface from forwarding entry.

IGMP Snooping forwards multicast data through Layer 2 multicast forwarding entry. When receiving multicast data, the ISCOM21xx 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 ISCOM21xx effectively.

IGMP Snooping establishes a Layer 2 multicast forwarding table, of which entries can be learnt dynamically or configured manually.

Note

Currently, the ISCOM21xx supports up to 1024 Layer 2 multicast entries.

6.1.3 MVR

Multicast VLAN Registration (MVR) is multicast constraining mechanism running on Layer 2 devices, used for multicast group management and control and achieve Layer 2 multicast.

MVR adds member interfaces belonging to different user VLANs on the Layer device to multicast VLAN by configuring multicast VLAN and makes different VLAN user uses one common multicast VLAN, then the multicast data will be transmitted only in one multicast VLAN without copying one for each user VLAN, thus saving bandwidth. At the same time, multicast VLAN and user VLAN are completely isolated which also increases the security.

Both MVR and IGMP Snooping can achieve Layer 2 multicast, but the difference is: multicast VLAN in IGMP Snooping is the same with user VLAN, while multicast VLAN in MVR can be different with user VLAN.

Note

One switch can be configured with up to 10 multicast VLAN, at least one multicast VLAN and group addresses. It supports up to 1024 multicast groups.

6.1.4 MVR Proxy

MVR Proxy is an MVR protocol proxy mechanism. It runs on Layer 2 devices to assist in managing and controlling multicast groups. MVR Proxy will terminate IGMP packets. It can proxy host function and also proxy multicast router functions for the next agent. The Layer 2 network device enabled with MVR Proxy has two roles:

- On the user side, it is a query builder and undertakes the role of Server, sending Query packets and periodically checking user information, and dealing with the Report and Leave packets from user.
- On the network routing side, it is a host and undertakes the role of Client, responding the multicast router Query packet and sending Report and Leave packets. It sends the user information to the network when they are in need.

The proxy mechanism can control and access user information effectively, at the same time, reducing the network side protocol packet and network load.

MVR Proxy establishes the multicast forwarding table by blocking IGMP packets between users and the multicast router.

Note

MVR Proxy is usually used with MVR.

The following concepts are related to MVR Proxy.

- IGMP packet suppression

IGMP packet suppression means that the Layer 2 device filters identical Report packets. When receiving Report packets from a multicast group member in a query interval, the Layer 2 device sends the first Report packet to the multicast router only rather than other identical Report packets, to reduce packet quantity on the network.

Note

When MVR is enabled, IGMP packet suppression can be enabled or disabled respectively.

- IGMP Querier

If a Layer 2 device is enabled with this function, it can actively send IGMP query packets to query information about multicast members on the interface. If it is disabled with this function, it only forwards IGMP query packets from routers.

Note

When IGMP Snooping is enabled, IGMP Querier can be enabled or disabled respectively.

- Source IP address of query packets sent by IGMP Querier

IGMP querier sends the source IP address of query packets. By default, the IP address of IP interface 0 is used. If the IP address is not configured, 0.0.0.0 is used. When receiving query packets with IP address of 0.0.0.0, some hosts take it illegal and do not respond. Thus, specifying the IP address for the query packet is recommended.

- Query interval

It is the query interval for common groups. The query message of common group is periodically sent by the Layer 2 device in multicast mode to all hosts in the shared network segment, to query which multicast groups have members.

- Maximum response time for query packets

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

- Interval for last member to send query packets

It is also called the specified group query interval. It is the interval for the Layer 2 device continues to send query packets for the specified group when receiving IGMP Leave packet for a specified group by a host.

The query packet for the specified multicast group is sent to query whether the group has members on the interface. If yes, the members must send Report packets within the maximum response time; after the Layer 2 device receives Report packets in a specie period, it continues to maintain multicast forwarding entries of the group; If the members fail to send Report packets within the maximum response time, the switch judges that the last member of the multicast group has left and thus deletes multicast forwarding entries.

6.1.5 IGMP filtering

To control user access, you can configure 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 configured 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 configured on an interface or interface+VLAN.

The maximum group limitation rule determines 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 MVR.

6.2 Configuring IGMP Snooping

6.2.1 Preparing for configurations

Scenario

Multiple hosts in the same VLAN receive data from the multicast source. Enable IGMP Snooping on the Layer 2 device 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.

Prerequisite

Create a VLAN, and add related interfaces to the VLAN.

6.2.2 Default configurations of IGMP Snooping

Default configurations of IGMP Snooping are as below.

Function	Default value
Global IGMP Snooping status	Disable
VLAN IGMP Snooping status	Disable
Aging time of router interface and multicast forwarding entry in IGMP Snooping	300s

6.2.3 Enabling global IGMP Snooping

Enable global IGMP Snooping for the ISCOM21xx as below.

Step	Function	Default value
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`ip igmp snooping`**	Enable global IGMP Snooping.

6.2.4 (Optional) enabling IGMP Snooping on VLANs

When global IGMP Snooping is enabled, IGMP Snooping is enabled on all VLANs by default. In this situation, you can disable or re-enable IGMP Snooping on a VLAN in VLAN configuration mode.

When global IGMP Snooping is disabled, IGMP Snooping is disabled on all VLANs by default. In this situation, you cannot enable IGMP Snooping on a VLAN.

Configuring IGMP Snooping in VLAN configuration mode

In VLAN configuration mode, you can enable IGMP Snooping on only one VLAN at a time.

Configure IGMP Snooping in VLAN configuration mode for the ISCOM21xx as below.

Step	Function	Default value
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`vlan`** *`vlan-id`*	Enable VLAN configuration mode.
3	`Raisecom(config-vlan)#`**`ip igmp snooping`**	Enable IGMP Snooping on a VLAN.

Configuring IGMP Snooping in global configuration mode

In VLAN configuration mode, you can enable IGMP Snooping on multiple VLANs at a time.

Configure IGMP Snooping in global configuration mode for the ISCOM21xx as below.

Step	Function	Default value
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`ip igmp snooping vlan-list`** *`vlan-list`*	Enable IGMP Snooping on VLANs.

6.2.5 Configuring multicast router interface

Configure the multicast router interface for the ISCOM21xx as below.

Step	Function	Default value
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ip igmp snooping mrouter vlan vlan-id port-list port-list`	Configure the multicast router interface of the specified VLAN.

Note

- IGMP Snooping can dynamically learn router interfaces (on the condition that the multicast router is enabled with multicast route protocol, and through IGMP query packets), or you can manually configure dynamic learning so that downstream multicast report and leaving packets can be forwarded to the router interface.
- There is aging time for the router interface dynamically learnt and no aging time for manually configured router interface.

6.2.6 (Optional) configuring aging time of IGMP Snooping

A timer starts on a dynamically learnt router interface in IGMP Snooping, and its timeout is the aging time of IGMP Snooping. If failing to receive any IGMP Query packet before timeout, the router interface will no longer be a multicast router interface. After receiving an IGMP Query packet, the router interface resets the aging time of IGMP Snooping.

The ISCOM21xx starts a timer for each multicast forwarding entry, and the timeout is the aging time of multicast members, namely, aging time of IGMP Snooping. If failing to receive any IGMP Report packet, the ISCOM21xx deletes the multicast member. After receiving an IGMP Report packet, the ISCOM21xx resets the aging time of IGMP Snooping.

Configure the aging time of IGMP Snooping for the ISCOM21xx as below.

Step	Function	Default value
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ip igmp snooping timeout { period | infinite }`	Configure the aging time of router interfaces or multicast forwarding entries.

Note

The aging time of IGMP Snooping configured through the previous command takes effect on all dynamically learnt router interfaces and multicast forwarding entries.

6.2.7 (Optional) configuring immediate leave

In IGMP Snooping, when a user sends a Leave packet, the ISCOM21xx will not delete the corresponding multicast forwarding entry until the multicast forwarding entry is aged. Therefore, when many downstream users who join or leave the network frequently, you can configure this function to immediately delete the corresponding multicast forwarding entries.

Configuring immediate leave in VLAN configuration mode

In VLAN configuration mode, you can enable immediate leave on only one VLAN at a time.

Configure immediate leave in VLAN configuration mode for the ISCOM21xx as below.

Step	Function	Default value
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`vlan`** *`vlan-id`*	Enable VLAN configuration mode.
3	`Raisecom(config-vlan)#`**`ip igmp snooping immediate-leave`**	Configure immediate leave on the VLAN.

Configuring immediate leave in global configuration mode

In global configuration mode, you can configure immediate leave on multiple VLANs at a time.

Configure immediate leave in global configuration mode for the ISCOM21xx as below.

Step	Function	Default value
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`ip igmp snooping vlan-list`** *`vlan-list`* **`immediate-leave`**	Configure immediate leave based on VLAN.

6.2.8 (Optional) configuring static multicast table

An interface is added to the multicast group through the IGMP Report packet sent by a host. Or you can manually add an interface to a multicast group.

Configure the static multicast table for the ISCOM21xx as below.

Step	Function	Default value
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`mac-address-table static multicast`** *`mac-address`* **`vlan`** *`vlan-id`* **`port-list`** *`port-list`*	Add interfaces to the static multicast group.

6.2.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show ip igmp snooping** [**vlan** *vlan-id*]	Show configurations of IGMP Snooping.
2	Raisecom#**show ip igmp snooping mrouter** [**vlan** *vlan-id*]	Show information about the multicast router interface of IGMP Snooping.
3	Raisecom#**show mac-address-table multicast** [**vlan** *vlan-id*] [**count**]	Show information about the Layer 2 multicast MAC address table.

6.3 Configuring MVR

6.3.1 Preparing for configurations

Scenario

Multiple hosts receive data from the multicast sources. These hosts and the multicast router belong to different VLANs. You can enable MVR on the Layer 2 device which connects the router and the host and configure multicast VLAN. In this way, users in different VLANs can share a multicast VLAN to receive the same multicast data, and bandwidth waste is reduced.

Prerequisite

Create VLANs and add related interfaces to VLANs.

6.3.2 Default configurations of MVR

Default configurations of MVR are as below.

Function	Default value
Global MVR status	Disable
Interface MVR status	Disable
Multicast VLAN and group address set	N/A
MVR multicast entity aging time	600s
MVR operation mode	Dynamic
MVR interface immediate leave status	Disable

6.3.3 Configuring MVR basic information

Configure MVR basic information for ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mvr enable**	Enable global MVR. It is disabled by default.
3	Raisecom(config)#**mvr timeout** *period*	(Optional) configure the aging time of MVR multicast entities.
4	Raisecom(config)#**mvr vlan** *vlan-id*	Configure MVR multicast VLAN.
5	Raisecom(config)#**mvr vlan** *vlan-id* **group** *ip-address* [*count*]	Configure group address set for multicast VLAN. Note The **mvr vlan** *vlan-id* **group** *ip-address* [*count*] command is used to configure group address set for multicast VLAN. If the received IGMP Report packet does not belong to group address set of any VLAN, it is not processed and the user cannot make multicast traffic on demand.
6	Raisecom(config)#**mvr mode** { **compatible** | **dynamic** }	(Optional) configure MVR operation mode. The **dynamic** mode allows source interfaces to dynamically join the multicast group; the **compatible** mode does not allow source interfaces to dynamically join the multicast group. Only when the receiving interface has a member which joins the multicast group, the source interface can join the multicast group.

6.3.4 Configuring MVR interface information

Caution

On an aggregation device, configuring immediate leave is not commended on the receiving interface. If multiple users are connected to the receiving interface configured with immediate leave through another device, the aggregation device will delete the receiving interface. As a result, other users that are still connected to the receiving interface will fail to receive multicast traffic.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mvr enable**	Enable global MVR.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#**mvr**	(Optional) enable interface MVR.

Step	Command	Description
5	Raisecom(config-port)#**mvr type { receiver | source }**	Configure the type of interface MVR. By default, the type is non-MVR. To configure it, configure the uplink interface to the source interface to receive multicast data. Users cannot be directly connected to the source interface; all source interfaces must be in the multicast VLAN; configure the interface directly connected to the user to the receiving interface and it cannot belong to the multicast VLAN.
6	Raisecom(config-port)#**mvr immediate**	(Optional) configure immediate leave on the MVR interface. This function can be applied to the receiving interface directly connected to the user.

Note

After global MVR is enabled, interface MVR is enabled as well.

6.3.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show mvr**	Show configurations of MVR.
2	Raisecom#**show mvr vlan group [vlan** *vlan*-6.3*id* **]**	Show MVR multicast VLAN and group address set.
3	Raisecom#**show mvr vlan** *vlan-id* **member**	Show information about MVR multicast member.

6.4 Configuring MVR Proxy

6.4.1 Preparing for configurations

Scenario

In a network with multicast routing protocol widely applied, there are multiple hosts and client subnet receiving multicast information. Enable IGMP Proxy on the Layer 2 device that connects the multicast router and hosts, to block IGMP packets between hosts and the multicast router and relieve the network load.

Configure IGMP Proxy to relive configuration and management of client subnet for the multicast router and to implement multicast connection with the client subnet.

Prerequisite

- Enable MVR.
- Configure multicast VLAN and group address set.
- Configure the source interface and the receiving interface, and add related interfaces to the corresponding VLANs.

6.4.2 Default configurations of IGMP Proxy

Default configurations of IGMP Proxy are as below.

Function	Default value
IGMP Proxy status	Disable
IGMP packet suppression status	Disable
IGMP Querier status	Disable
Source IP address for IGMP Querier and IGMP Proxy to send packets	Use the IP address of IP interface 0. If IP interface 0 is not configured, use 0.0.0.0.
IGMP query interval	60s
Maximum response time to send Query packets	10s
Interval for the last member to send Query packets	1s

6.4.3 Configuring IGMP Proxy

Configure IGMP Proxy for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mvr proxy**	Enable IGMP Proxy. **Note** After global MVR Proxy is enabled, MVR packet suppression and IGMP querier are enabled as well.
3	Raisecom(config)#**mvr proxy suppression**	Enable IGMP packet suppression. IGMP packet suppression can be enabled or disabled when MVR is enabled.
4	Raisecom(config)#**ip igmp querier enable**	(Optional) enable IGMP querier. IGMP querier can be enabled or disabled when IGMP Snooping or MVR is enabled.
5	Raisecom(config)#**mvr proxy source-ip** *ip-address*	(Optional) configure the source IP address for the IGMP querier to send query packets.

Step	Command	Description
6	Raisecom(config)#**ip igmp querier query-interval** *period*	(Optional) configure the IGMP query interval.
7	Raisecom(config)#**mvr proxy query-max-response-time** *period*	(Optional) configure the maximum response time to send query packets.
8	Raisecom(config)#**mvr proxy last-member-query** *period*	(Optional) configure the interval for the last member to send query packets.

Note

When IGMP Proxy is disabled, the following parameters of MVR Proxy can be configured: source IP address, query interval, maximum response time to send Query packets, and interval for the last member to send Query packets. After IGMP Proxy is enabled, these configurations will take effect immediately.

6.4.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show mvr proxy**	Show configurations of IGMP Proxy.
2	Raisecom#**show ip igmp querier vlan**	Show user VLAN information to be queried.

6.5 Configuring IGMP filtering

6.5.1 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 configured.

Prerequisite

- Enable MVR.
- Configure multicast VLAN and group address set.
- Configure the source interface and receiving interfaces, and add the related interfaces to the responding VLANs.

6.5.2 Default configurations of IGMP filtering

Default configurations of IGMP filtering are as below.

Function	Default value
Global IGMP filtering	Disable
IGMP filter profile Profile	N/A
IGMP filter profile action	Refuse
IGMP filtering under interface	No maximum group limit. The largest group action is drop, and no application filter profile.
IGMP filtering under interface+VLAN	No maximum group limit. The largest group action is drop, and no application filter profile.

6.5.3 Enabling global IGMP filtering

Enable global IGMP filtering for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode
2	`Raisecom(config)#`**`igmp filter`**	Enable global IGMP filtering

Note

Before configuring IGMP filter profile or the maximum number of IGMP groups, use the **igmp filter** command to enable global IGMP filtering.

6.5.4 Configuring IGMP filtering rules

Configure the IGMP filter profile for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode
2	`Raisecom(config)#`**`ip igmp profile`** *`profile-number`*	Create an IGMP profile, and enter profile configuration mode.
3	`Raisecom(config-igmp-profile)#{` **`permit`** `|` **`deny`** `}`	Configure IGMP profile action.
4	`Raisecom(config-igmp-profile)#`**`range`** *`start-ip-address`* `[` *`end-ip-address`* `]`	Configure the IP multicast address or range to be controlled for access.

6.5.5 Applying IGMP filtering rules

Apply the IGMP filter profile for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**ip igmp filter** *profile-number*	(Optional) applying IGMP profile filtering rules on the interface. An IGMP profile can be applied to multiple interfaces, but each interface can be configured with only one IGMP profile.
4	Raisecom(config-port)#**exit** Raisecom(config)#**ip igmp filter** *profile-number* **vlan** *vlan-id*	(Optional) applying IGMP profile filtering rules in the VLAN.

6.5.6 Configuring maximum number of multicast groups

You can add the maximum number of multicast groups applied to interface or interface+VLAN.

Configuring maximum number of multicast groups on interface

Configure the maximum number of multicast groups on the interface for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**ip igmp max-groups** *group-number*	Configure the maximum number of multicast groups allowed on the interface.
4	Raisecom(config-port)#**ip igmp max-groups action** { **deny** | **replace** }	(Optional) configure the action when the number of groups exceeds the maximum number of multicast groups allowed on the interface.

Configuring maximum number of multicast groups in VLAN

Configure the maximum number of multicast groups in the VLAN for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode
2	Raisecom(config)#**ip igmp max-group** *max-group* **vlan** *vlan-id*	Configure the maximum number of multicast groups allowed in the VLAN.
3	Raisecom(config)#**ip igmp max-group action** { **deny** | **replace** } **vlan** *vlan-id*	(Optional) configure the action when the number of groups exceeds the maximum number of multicast groups allowed in the VLAN.

Note

By default, there is no limit on the multicast group number. The action for the maximum multicast group is **deny**.

6.5.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show ip igmp filter** [*interface-type interface-number* | **vlan** [*vlan-id*]]	Show application information about IGMP filtering.
2	Raisecom#**show ip igmp profile** [*profile-number*]	Show configurations of IGMP profile filtering rules.

6.6 Maintenance

Maintain the ISCOM21xx as below.

No.	Command	Description
1	Raisecom(config)#**clear mvr** *interface-type* [*interface-number*] **statistics**	Clear MVR statistics on the interface.

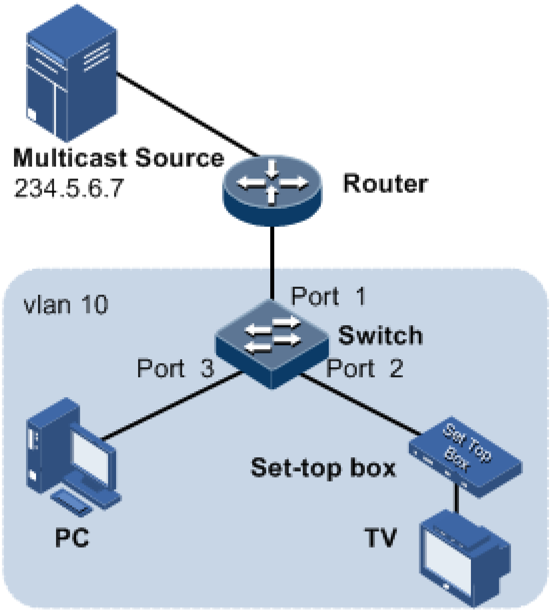
6.7 Configuration examples

6.7.1 Example for configuring IGMP Snooping

Networking requirements

As shown in Figure 6-2, Port 1 on the switch is connected with the multicast router; Port 2 and Port 3 connect users. All multicast users belong to the same VLAN 10; you need to configure IGMP Snooping on the switch to receive multicast data with the address 234.5.6.7.

Figure 6-2 IGMP Snooping networking



Configuration steps

Step 1 Create a VLAN and add interfaces to it.

```
Raisecom#config
Raisecom(config)#create vlan 10 active
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk native vlan 10
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport access vlan 10
Raisecom(config-port)#exit
Raisecom(config)#interface port 3
Raisecom(config-port)#switchport access vlan 10
Raisecom(config-port)#exit
```

Step 2 Enable IGMP Snooping.

```
Raisecom(config)#igmp snooping
Raisecom(config)#igmp snooping vlan-list 10
```

Step 3 Configure the multicast router interface.

```
Raisecom(config)#ip igmp snooping mrouter vlan 1 port 1
```

Checking results

Use the following command to show configurations of IGMP Snooping.

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

6.7.2 Example for configuring MVR and MVR Proxy

Networking requirements

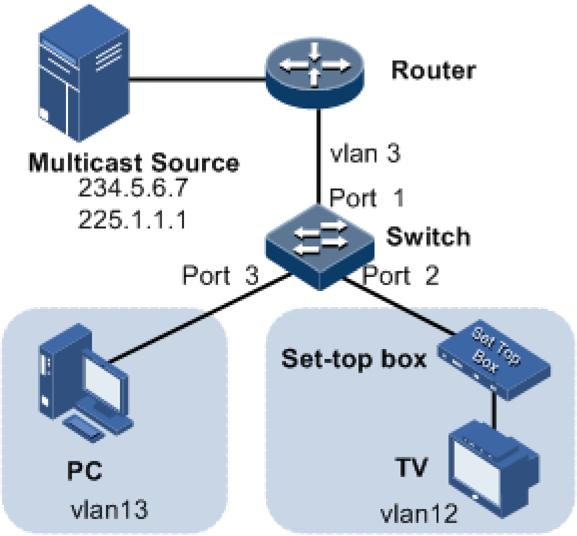
As shown in Figure 6-3, Port 1 on the switch connects with the multicast router, and Port 2 and Port 3 connect with users in different VLANs to receive data from multicast 234.5.6.7 and 225.1.1.1.

Configure MVR on the Switch to designate VLAN 3 as a multicast VLAN, and then the multicast data can only be copied one time in the multicast VLAN instead of copying for each user VLAN, thus saving bandwidth.

Enabling MVR Proxy on the Switch reduces communication between hosts and the multicast router without implementing multicast functions.

When the PC and set-top box are added into the same multicast group, the Switch receives two IGMP Report packets and only sends one of them to the multicast router. The IGMP Query packet sent by multicast will no longer be forwarded downstream, but the switch transmits IGMP Query packet periodically.

Figure 6-3 MVR networking



Configuration steps

Step 1 Create VLANs on Switch A and add interfaces to it.

```
Raisecom(config)#config
Raisecom(config)#creat vlan 3,12,13 active
Raisecom(config)#interface port 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 port 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 port 3
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk native vlan 13
Raisecom(config-port)#switchport trunk untagged vlan 3
```

Step 2 Configure MVR on Switch A.

```
Raisecom(config)#mvr enable
Raisecom(config)#interface port 2
Raisecom(config-port)#mvr
Raisecom(config-port)#exit
Raisecom(config)#interface port 3
Raisecom(config-port)#mvr
```

Step 3 Specify the multicast VLAN and group address set.

```
Raisecom(config)#mvr vlan 3
Raisecom(config)#mvr vlan 3 group 234.5.6.7
Raisecom(config)#mvr vlan 3 group 225.1.1.1
```

Step 4 Enable MVR Proxy.

```
Raisecom(config)#mvr proxy
Raisecom(config)#mvr proxy suppression
Raisecom(config)#ip igmp querier enable
Raisecom(config)#mvr proxy source-ip 192.168.1.2
```

Step 5 Configure source interface information.

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

Step 6 Configure receiving interface information.

```
Raisecom(config)#interface port 2
Raisecom(config-port)#mvr type receiver
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 port 3
Raisecom(config-port)#mvr type receiver
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk native vlan 13
Raisecom(config-port)#switchport trunk untagged vlan 3
```

Checking results

Use the following command to show MVR configurations on the switch.

```
Raisecom#show mvr
MVR Running: Enable
MVR Multicast VLAN(ref):3(2)
MVR Max Multicast Groups: 3840
MVR Current Multicast Groups: 2
MVR Timeout: 600 (second)
MVR Mode: Dynamic
Mvr general query translate vlan: 0
```

Use the following command to show information about the multicast VLAN and group address.

```
Raisecom#show mvr vlan group
Vlan  Group Address
-----------------------------
3    225.1.1.1
3    234.5.6.7

Group address entries for all Vlans:  2
```

Use the following command to show configurations of IGMP Proxy.

```
Raisecom#show mvr proxy
Mvr Proxy Suppression Status:     Enable
Ip Igmp Querier Status:          Enable
Mvr Proxy Source Ip:            192.168.1.2
Mvr Proxy Version:             V2
Ip Igmp Query Interval(s):       60
Query Response Interval(s):      10
Last Member Query Interval(s):    1
Next IGMP General Query(s):      60
```

6.7.3 Example for applying IGMP filtering and maximum number of multicast groups to interface

Networking requirements

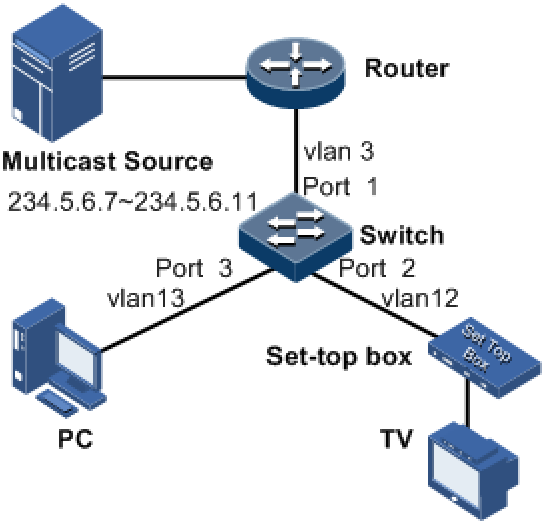
Enable IGMP filtering on the switch. Add filtering rules on the interface to filter multicast users.

As shown in Figure 6-4,

- Create an IGMP filtering rule Profile 1, configure the action to pass for the multicast group ranging from 234.5.6.7 to 234.5.6.10.
- Apply filtering IGMP filtering rule Profile 1 on Port 2, allow the set top box 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 Port 3, and allow PCs to join the 234.5.6.11 multicast group.

Configure the maximum number of multicast groups on Port 2. After the set top box is added to the 234.5.6.7 multicast group, add it to the 234.5.6.8 multicast group. Then, it quits the 234.5.6.7 multicast group.

Figure 6-4 Applying IGMP filtering on the interface



Configuration steps

Step 1 Create a VLAN, and create IGMP filtering rules.

```
Raisecom#config
Raisecom(config)#creat vlan 3,12,13 active
Raisecom(config)#ip igmp profile 1
Raisecom(config-igmp-profile)#range 234.5.6.7 234.5.6.10
Raisecom(config-igmp-profile)#permit
```

Step 2 Enable MVR and IGMP filtering.

```
Raisecom(config)#mvr enable
Raisecom(config)#mvr vlan 3
Raisecom(config)#mvr vlan 3 group 234.5.6.7 5
Raisecom(config)#ip igmp filter
```

Step 3 Configure the source interface.

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

Step 4 Configure the receiving interface on the set top box, and apply IGMP filtering rule and configure the maximum number of multicast groups.

```
Raisecom(config)#interface port 2
Raisecom(config-port)#mvr type receiver
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)#ip igmp filter 1
Raisecom(config-port)#ip igmp max-groups 1
Raisecom(config-port)#ip igmp max-groups action replace
```

Step 5 Configure the receiving interface on the PC.

```
Raisecom(config)#interface port 3
Raisecom(config-port)#mvr type receiver
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk native vlan 13
Raisecom(config-port)#switchport trunk untagged vlan 3
```

Checking results

Use the following command to show configurations of IGMP filtering on the interface.

```
Raisecom#show ip igmp filter port 2
IGMP Filter: 1
Max Groups: 1
Current groups: 0
Action: Replace
```

6.7.4 Example for applying IGMP filtering and maximum number of multicast groups to VLAN

Networking requirements

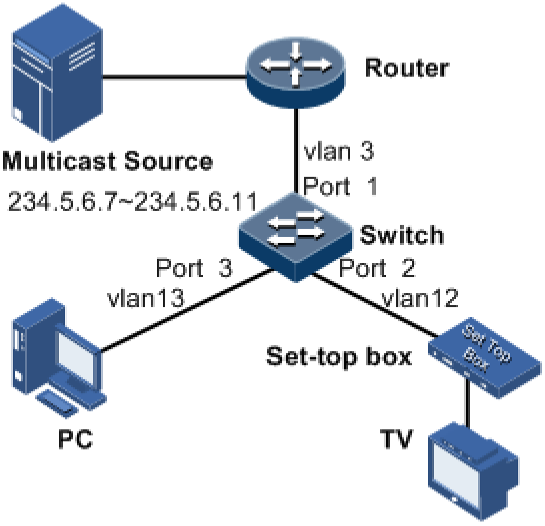
Enable IGMP filtering on the switch. Add filtering rules in the VLAN to filter multicast users.

As shown in Figure 6-5,

- Create an IGMP filtering rule Profile 1, configure the action to pass, and configure the IP address to range from 234.5.6.7 to 234.5.6.10.
- Apply filtering IGMP filtering rule Profile 1 on VLAN 12, allow the set top box 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 VLAN 3, and allow PCs to join the 234.5.6.11 multicast group.

Configure the maximum number of multicast groups in VLAN 12. After the set top box is added to the 234.5.6.7 multicast group, add it to the 234.5.6.8 multicast group. Then, it quits the 234.5.6.7 multicast group.

Figure 6-5 Applying IGMP filtering in the VLAN



Configuration steps

Step 1 Create a VLAN, and create IGMP filtering rules.

```
Raisecom#config
Raisecom(config)#creat vlan 3,12,13 active
Raisecom(config)#ip igmp profile 1
Raisecom(config-igmp-profile)#range 234.5.6.7 234.5.6.10
Raisecom(config-igmp-profile)#permit
```

Step 2 Enable MVR and IGMP filtering.

```
Raisecom(config)#mvr enable
Raisecom(config)#mvr vlan 3
Raisecom(config)#mvr vlan 3 group 234.5.6.7 5
Raisecom(config)#ip igmp filter
```

Step 3 Configure the source interface.

```
Raisecom(config)#ip igmp filter 1 vlan 12
Raisecom(config)#ip igmp max-group 1 vlan 12
Raisecom(config)#ip igmp max-group action replace vlan 12
```

Step 4 Configure the receiving interface on the set top box, and apply IGMP filtering rule and configure the maximum number of multicast groups.

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

Step 5 Configure the receiving interface on the PC.

```
Raisecom(config)#interface port 2
Raisecom(config-port)#mvr type receiver
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 port 3
Raisecom(config-port)#mvr type receiver
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk native vlan 13
Raisecom(config-port)#switchport trunk untagged vlan 3
```

Checking results

Check whether IGMP filtering is correctly configured in the VLAN.

```
Raisecom#show ip igmp filter vlan 12
VLAN  Filter   Max Groups   Current Groups  Action
---------------------------------------------------------------------
12      1               1  0              Replace
```

7 Security

This chapter describes basic principles and configuration procedures of security and provides related configuration examples, including the following sections:

- ACL
- Secure MAC address
- Dynamic ARP inspection
- ND detection
- TACACS+
- Storm control
- 802.1x
- IP Source Guard
- PPPoE+
- Loop detection
- Line detection

7.1 ACL

7.1.1 Introduction

Access Control List (ACL) is a set of ordered rules, which can control the ISCOM21xx to receive or refuse some data packets. You need to configure rules on the network to prevent illegal packets from influencing network performance and determine the packets allowed to pass. These rules are defined by ACL.

ACL is a series of rule composed of permit or deny sentences. The rules are described according to the source MAC address, destination MAC address, source IP address, destination IP address, and port ID of data packets. The ISCOM21xx judges whether to receive or reject packets according to the rules.

7.1.2 Preparing for configurations

Scenario

ACL can help network device recognize filtered objects. The ISCOM21xx recognizes special objects and then permits/denies packets to pass according to the configured policy.

ACL includes the below types:

- IP ACL: make classifications rule according to source or destination address taken by packets IP head, port ID used by TCP or UDP, and other attributes of packets.
- MAC ACL: make classification rules according to attributes, such as source MAC address, destination MAC address, Layer 2 protocol type taken by packets Layer 2 frame header.
- MAP ACL: MAP ACL can define more protocols and more detailed protocol fields than IP ACL and MAC ACL, also can match any bytes of the first 64 bytes of Layer 2 frames according to user's definition.

There are 3 kinds of ACL applications according to difference in application environment: ACL based on whole device, based on interface, and based on VLAN.

Prerequisite

N/A

7.1.3 Default configurations of ACL

Default configurations of ACL are as below.

Function	Default value
Filter effectiveness status	Disable
Non-fragmenting packet message type	Mismatch
ICMP packet message type	Mismatch
Filter function effective status	Take effect
MAC address matching rules	Mismatch
CoS value matching rules	Mismatch
Ethernet frame type matching rules	Mismatch
ARP type matching rules	Mismatch
ARP packet and MAC/IP address matching rules	Mismatch
IP packet address, DSCP, priority, and matching rule between priority and ToS	Mismatch
Matching rule between port ID and protocol Tag bit of TCP packets	Mismatch
Port ID matching rules of UDP packets	Mismatch
IGMP packet message type matching rules	Mismatch

Function	Default value
IPv6 packet matching rules	Mismatch

7.1.4 Configuring IPv4 ACL

Configure IPv4 ACL for the ISCOM21xx as below.

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-address mask* | **any**} { *destination-address mask* | **any** }	Configure IPv4 ACL.
	Raisecom(config)#**ip-access-list** *acl-number* { **deny** | **permit** } { **tcp** | **udp** } { *source-ip-address ip-mask* | **any** } [*source-protocol-port*] { *destination-ip-address ip-mask* | **any** } [*destination-protocol-port*]	
3	Raisecom(config)#**interface ip** *if-number* Raisecom(config-ip)#**ip ip-access-list** { *list-number* | **all** } [**port-list** *port-list*]	Apply ACL on the ISCOM21xx.

7.1.5 Configuring IPv6 ACL

Configure IPv6 ACL for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6-access-list** *acl-number* { **deny** | **permit** } { *source-address mask* | **any**} { *destination-address mask* | **any** }	Apply IPv6 ACL. Use the **no ipv6-access-list** { *acl-id* | **all** } command to delete IPv6 ACL rules.

Note

The **ipv6-access-list permit any** rule and **ipv6-access-list deny any any** rule conflict with each other. When they are concurrently issued, the later takes effect while the former does not. For example:

```
Raisecom#config
Raisecom(config)#ipv6-access-list 1 permit any 2001::1/64
Raisecom(config)#ipv6-access-list 5 deny any any
Raisecom(config)#filter-ipv6 enable
Raisecom(config)#filter ipv6-access-list 5 ingress port 1
Raisecom(config)#filter ipv6-access-list 1 ingress port 1
```

In this case, ipv6-access-list 1 does not take effect.

7.1.6 Configuring MAC ACL

Configure MAC ACL for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mac-access-list** *acl-id* { **deny** | **permit**} [*protocol-id* | **arp** | **ip** | **rarp** | **any**] { *source-mac-address* [**src-mask** *src-mask*] | **any** } { *destination-mac-address* [**dst-mask** *dst-mask*] | **any** }	Configure MAC ACL.

7.1.7 Configuring IPv4 MAP ACL

Configure IPv4 MAP ACL for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**access-list-map** *acl-id* { **deny** | **permit** }	Create a MAP ACL and enter ACLMAP configuration mode.
3	Raisecom(config-aclmap)#**match mac** { **destination** | **source** } *mac-address*	(Optional) define matching rule for the source or destination MAC address.
4	Raisecom(config-aclmap)#**match cos** *cos-value*	(Optional) define matching rules for CoS value.
5	Raisecom(config-aclmap)#**match ethertype** *ethertype* [*ethertype-mask*]	(Optional) define matching rules for Ethernet frame type.
6	Raisecom(config-aclmap)#**match** { **arp** | **eapol** | **flowcontrol** | **ip** | **ipv6** | **loopback** | **mpls** | **mpls-mcast** | **pppoe** | **pppoedisc** | **x25** | **x75** }	(Optional) define matching rules for upper layer protocol type carried by Layer 2 packet head.
7	Raisecom(config-aclmap)#**match arp opcode** { **reply**| **request** }	(Optional) define matching rule for ARP type (reply packet/request packet).
8	Raisecom(config-aclmap)#**match arp** { **sender-mac** | **target-mac** } *mac-address*	(Optional) define matching rules for the MAC address of ARP packets.
9	Raisecom(config-aclmap)#**match arp** { **sender-ip** | **target-ip** } *ip-address* [*ip-address-mask*]	(Optional) define matching rules for the IP address of ARP packets.

Step	Command	Description
10	Raisecom(config-aclmap)#**match ip** { **destination-address** | **source-address** } *ip-address* [*ip-address-mask*]	(Optional) define matching rules for the source or destination IP address.
11	Raisecom(config-aclmap)#**match ip precedence** { *precedence-value* | **critical** | **flash** | **flash-override** | **immediate**| **internet** | **network** | **priority** | **routine** }	(Optional) define matching rules for IP packet priority.
12	Raisecom(config-aclmap)#**match ip tos** { *tos-value* | **max-reliability** | **max-throughput** | **min-delay** | **min-monetary-cost** | **normal** }	(Optional) define matching rules for ToS value of IP packet priority.
13	Raisecom(config-aclmap)#**match ip dscp** { *dscp-value* | **af11** | **af12** | **af13** | **af21** | **af22** | **af23** | **af31** | **af32** | **af33** | **af41**| **af42** |**af43** | **cs1** | **cs2** | **cs3** | **cs4** | **cs5** | **cs6** | **cs7**| **default** | **ef** }	(Optional) define matching rules for DSCP value of IP packets.
14	Raisecom(config-aclmap)#**match ip protocol** *protocol-id*	(Optional) define matching rules for protocol value of IP packets.
15	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 matching rules for port ID of TCP packets.
16	Raisecom(config-aclmap)#**match ip tcp** { **ack** | **fin** | **psh** | **rst** | **syn** | **urg** }	(Optional) define matching rules for TCP protocol Tag.
17	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 matching rules for port ID of UDP packets.
18	Raisecom(config-aclmap)#**match ip icmp** *icmp-type-id* [*icmp-code*]	(Optional) define matching rules for message type of ICMP packets.

Step	Command	Description
19	`Raisecom(config-aclmap)#match ip no-fragments`	(Optional) define matching rules for message type of non-fragment packets.
20	Raisecom(config-aclmap)#**match ip igmp** { *igmp-type-id* | **dvmrp** | **leave-v2**| **pim-v1** | **query** | **report-v1** | **report-v2** |**report-v3** }	(Optional) define matching rules for message type of IGMP packets.
21	Raisecom(config-aclmap)#**match user-define** *rule-string rule-mask offset*	(Optional) configure matching rules for user-defined field, that is, two parameters of rule mask and offset take any byte from bytes 23 to 63 of the first 64 bytes, then comparing with user-defined rule to filter out matched data frame for processing. For example, if you wish to filter all TCP packets, you can define: • Rule: 06 • Rule mask: FF • Offset: 27 The rule mask and offset value work together to filter out content of TCP protocol ID field, then comparing with rule and match with all TCP packets. **Note** The rule number must be a hex digital. Offset includes field 802.1q VLAN Tag, even though the ISCOM21xx receives Untag packets.

7.1.8 Configuring IPv6 MAP ACL

Configure IPv6 MAP ACL for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**access-list-map-ipv6** *acl-list* { **deny** | **permit** }	Create a MAP ACL and enter ACL MAP configuration mode.
3	Raisecom(config-aclmap-ipv6)#**match-ipv6** { **destination-address** | **source-address** } *mac-address*	(Optional) define matching rules for the source or destination MAC address.

Step	Command	Description
4	`Raisecom(config-aclmap-ipv6)#`**`match-ipv6`** `{` **`trafficclass`** *`trafficclass-value`* `|` **`nextheader`** *`nextheader-value`* `|` **`cos`** *`cos-value`* `}`	(Optional) define matching rules for related parameters.
5	`Raisecom(config-aclmap-ipv6)#`**`match-ipv6 mac source`** *`mac-address`*	(Optional) define matching rules for Ethernet frame type.
6	`Raisecom(config-aclmap-ipv6)#`**`match-ipv6 vlan`** *`vlan-id`*	(Optional) define matching rules for VLAN.

7.1.9 Creating ACL group

Create an ACL group for the ISCOM21xx as below.

Note

The ACL group is used to control ACL priority, so its inner ACL rules are sequential. If an ACL group is applied in a filter, it cannot be used to match other flows. The ACL group must be applied to an existing flow only; otherwise, the application will fail and error prompt will appear.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`acl-group`** *`list-number`*	Create an ACL group. Use the **no acl-group** *list-number* command to delete a created ACL group.
3	`Raisecom(config-aclgroup)#`**`acl-group match`** `{` **`ip-access-list`** `|` **`access-list-map`** `|` **`mac-access-list`** `}` *`access-list`*	Configure the flow to be applied to an ACL group. Use the **no acl-group match** { **ip-access-list** | **mac-access-list** | **access-list-map** } *access-list* command to delete a specified flow applied in an ACL group.

7.1.10 Applying IPv4 ACL

Configure IPv4 ACL for the ISCOM21xx as below.

Note

ACL cannot take effect until it is added into a filter. Multiple ACL matching rules can be added into a filter to form multiple filter rules. The priority depends on the sequence of ACL matching rules. The later the rules are added, the higher the priority is. If multiple rules conflict in matching calculation, the higher priority rule prevails.

Pay attention to the order of rules when configuring the commands to filter packets correctly.

Applying IPv4 ACL based on whole device

Apply IPv4 ACL based on whole device for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#filter { ip-access-list | mac-access-list | access-list-map } { acl-list | all } [ statistics ]`	Configure the filter for the device. If the **statistics** parameter is configured, the system will gather statistics according to filter rules.
3	`Raisecom(config)#filter enable`	Enable filter to make rules take effect. Enabling the filter takes effect not only on the filter rules configured before but also on the ones configured later.

Applying IPv4 ACL based on interface

Apply IPv4 ACL based on interface as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#filter { access-list-map | ip-access-list | mac-access-list } { all | acl-list } ingress interface-type interface-list [ statistics ]`	Configure filter on the interface. If the **statistics** parameter is configured, the system will gather statistics according to filtering rules.
3	`Raisecom(config)#filter access-list-mac { all | acl-list } ingress interface-type interface-list valid`	(Optional) enable the filter based on interface. Use the **filter** { **access-list-map** | **ip-access-list** | **mac-access-list** } { **all** | *acl-list* } **ingress** *interface-type interface-list* **invalid** command to disable this function.
4	`Raisecom(config)#filter enable`	Enable filter to make rules take effect. Enabling the filter not only activates the filter rules, but also makes the filter rules configured later take effect.

Applying ACL based on VLAN

Apply ACL based on VLAN as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**filter**{ **ip-access-list**| **mac-access-list** | **access-list-map** } { *acl-list* | **all** } **vlan** *vlan-id* [**double-tagging inner**] [**statistics**]	Configure ACL on the interface. If the **statistics** parameter is configured, the system will gather statistics according to filtering rules.
3	Raisecom(config)#**filter enable**	Enable filter to make rules take effect. Enabling the filter not only activates the filter rules, but also makes the filter rules configured later take effect.

7.1.11 Applying IPv6 ACL

Configure IPv6 ACL for the ISCOM21xx as below.

Note

ACL cannot take effect until ACL is added into a filter. Multiple ACL matching rules can be added into a filter to form multiple filter rules. When you configure the filter, the order to add ACL matching rule determines priority of the rule. The later the rules are added, the higher the priority is. If multiple rules conflict in matching calculation, the higher priority rule prevails. Pay attention to the order of rules when configuring the commands to filter packets correctly.

Applying IPv6 ACL based on whole device

Apply IPv6 ACL based on whole device for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**filter ipv6-access-list** *access-list* **schedule-list** *list-number*	Configure the filter for the whole device.
3	Raisecom(config)#**filter-ipv6 enable**	Enable filter to make rules take effect. Enabling the filter not only activates the filter rules, but also makes the filter rules configured later take effect.

Applying IPv6 ACL based on interface

Apply IPv6 ACL based on interface as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**filter ipv6-access-list** *access-list* **ingress port** *port-list* [**statistics**] **schedule-list** *list-number*	Configure filter on the interface. If the **statistics** parameter is configured, the system will gather statistics according to filtering rules.
3	Raisecom(config)#**filter-ipv6 enable**	Enable filter to make rules take effect. Enabling the filter not only activates the filter rules, but also makes the filter rules configured later take effect.

Applying ACL based on VLAN

Apply ACL based on VLAN as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**filter ipv6-access-list** *access-list* **vlan** *vlan-id* [**statistics**] **schedule-list** *list-number*	Configure ACL on the interface. If the **statistics** parameter is configured, the system will gather statistics according to filtering rules.
3	Raisecom(config)#**filter-ipv6 enable**	Enable filter to make rules take effect. Enabling the filter not only activates the filter rules, but also makes the filter rules configured later take effect.

7.1.12 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show ip-access-list** [*list-number*]	Show configurations of IPv4 ACL.
2	Raisecom#**show mac-access-list** [*list-number*]	Show configurations of MAC ACL.
3	Raisecom#**show access-list-map** [*list-number*]	Show configurations of IPv4 MAP ACL.
4	Raisecom#**show filter** [*filter-number-list*]	Show configurations of IPv4 filters.
5	Raisecom#**show interface ip ip-access-list**	Show configurations of the filter on the Layer 3 interface.
6	Raisecom#**show ipv6-access-list** *acl-list*	Show configurations of IPv6 ACL.

No.	Command	Description
7	`Raisecom#show access-list-map-ipv6 acl-list`	Show configurations of IPv6 MAP ACL.
8	`Raisecom#show filter-ipv6`	Show configurations of IPv6 MAP ACL.
9	`Raisecom#show acl-group`	Show created ACL groups and rules for flows applied to ACL groups.

7.1.13 Maintenance

Maintain the ISCOM21xx as below.

Command	Description
`Raisecom(config)#clear filter statistics`	Clear filter statistics.

7.2 Secure MAC address

7.2.1 Introduction

Port security MAC is used for the switch on the edge of the network user side, which can ensure the security of access data on some interfaces, control the input packets according to source MAC address.

You can enable port security MAC to limit and distinguish which users can access the network through secure port. Only packets from the secure MAC addresses can access the network, and unsecure MAC addresses will be dealt with as configured interface access violation mode.

Classification secure MAC address

Secure MAC addresses supported by the device are divided into the following three categories:

- Static secure MAC address

Static secure MAC address is configured by user on secure interface manually; this MAC address will take effect when port security MAC is enabled. Static secure MAC address does not age and supports loading configuration.

- Dynamic secure MAC address

The dynamic secure MAC address is learnt by the device. You can configure the learnt MAC address to secure MAC address in the range of the maximum number of learnt MAC address. The dynamic secure MAC addresses ages and does not support configuration load.

Dynamic secure MAC address can be converted to sticky secure MAC address if needed, so as not to be aged and support configuration load.

- Sticky secure MAC address

The sticky secure MAC address is generated from the manual configuration of users in secure interface or converted from dynamic secure MAC address. Different from static secure MAC address, sticky secure MAC address needs to be used in conjunction with sticky learning:

  - When sticky learning is enabled, sticky secure MAC address will take effect and this address will not be aged and support loading configurations.
  - When sticky learning is disabled, sticky secure MAC address will lose effectiveness and be saved only in the system.

Note

- When sticky learning is enabled, all dynamic secure MAC addresses learnt from an interface will be converted to sticky secure MAC addresses.
- When sticky learning is disabled, all sticky secure MAC addresses on an interface will be converted to dynamic secure MAC addresses.

Processing mode for violating secure MAC address

When the number of secure MAC addresses has already reached the maximum number, the strange source MAC address packets inputting will be regarded as violation operation. For the illegal user access, there are different processing modes to configure the switch according to secure MAC violation policy:

- Protect mode: for illegal access users, the secure interface will discard the user's packets directly.
- Restrict mode: for illegal access users, the secure interface will discard the user's packets, and the console will print Syslog information and send alarm to the network management system.
- Shutdown mode: for illegal access users, the secure interface will discard the user's packets, and the console will print Syslog information and send alarm to the network management system and then shut down the secure interface.

Caution

When the MAC address is flapping, that is, the secure interface A receives one user access corresponding a secure MAC address on secure interface B, secure interface A will take it as violation processing.

7.2.2 Preparing for configurations

Scenario

To ensure the security of data accessed by the interface of the switch, you can control the input packets according to source MAC address. With secure MAC address, you can configure permitting specified users to access the interface, or permitting specified number of users to access from this interface only. However, when the number of users exceeds the limit, the accessed packets will be processed in accordance with secure MAC address violation policies.

Prerequisite

N/A

7.2.3 Default configurations of secure MAC address

Default configurations of port security MAC are as below.

Function	Default value
Interface secure MAC	Disable
Aging time of dynamic secure MAC address	30min
Dynamic secure MAC sticky learning	Disable
Port secure MAC Trap	Disable
Port secure MAC violation processing mode	Protect
Maximum number of port security MAC	1

7.2.4 Configuring basic functions of secure MAC address

Caution

- We do not recommend enabling port security MAC on member interfaces of the LAG.
- We do not recommend using MAC address management function to configure static MAC addresses when port security MAC is enabled.
- Port security MAC and 802.1x are mutually exclusive. We do not suggest configuring them concurrently.
- Port security MAC and interface-based MAC address limit are mutually exclusive. We do not recommend configuring them concurrently.
- Port security MAC and MAC address number limit based on interface+VLAN are mutually exclusive. We do not recommend configuring them concurrently.

Configure basic functions of secure MAC address for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**switchport port-security**	Enable port security MAC.
4	Raisecom(config-port)#**switchport port-security maximum** *maximum*	(Optional) configure the maximum number of secure MAC addresses.
5	Raisecom(config-port)#**switchport port-security violation** { **protect** | **restrict** | **shutdown** }	(Optional) configure secure MAC violation mode.

Step	Command	Description
6	Raisecom(config-port)#**no port-security shutdown**	(Optional) re-enable the interface which is shut down due to violating the secure MAC address.
7	Raisecom(config-port)#**mac-address-table threshold notification enable**	(Optional) enable Syslog printing.
8	Raisecom(config-port)#**switchport port-security cpu-protect enable**	(Optional) enable CPU protection.

Note

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

7.2.5 Configuring static secure MAC address

Configure static secure MAC address for the ISCOM21xx as below.

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

7.2.6 Configuring dynamic secure MAC address

Configure dynamic secure MAC address for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**port-security aging-time** *period*	(Optional) configure the aging time of dynamic secure MAC address.

Step	Command	Description
3	`Raisecom(config)#interface port` *`port-id`*	Enter physical layer interface configuration mode.
4	`Raisecom(config-port)#switchport port-security`	Enable dynamic secure MAC learning.
5	`Raisecom(config-port)#switchport port-security trap enable`	(Optional) enable port security MAC Trap.

Note

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

7.2.7 Configuring sticky secure MAC address

Configure sticky secure MAC address for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface port` *`port-id`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#switchport port-security`	(Optional) enable port security MAC.
4	`Raisecom(config-port)#switchport port-security mac-address sticky` *`mac-address`* `vlan` *`vlan-id`*	Manually configure sticky secure MAC learning.
5	`Raisecom(config-port)#switchport port-security mac-address sticky`	(Optional) manually configure sticky secure MAC addresses. Note After sticky port secure MAC learning is enabled, dynamic security port AMC is translated into the sticky MAC address. Manually configured sticky security MAC address takes effect.

7.2.8 Checking configurations

Use the following commands to check configuration results.

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

7.2.9 Maintenance

Maintain the ISCOM21xx as below.

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

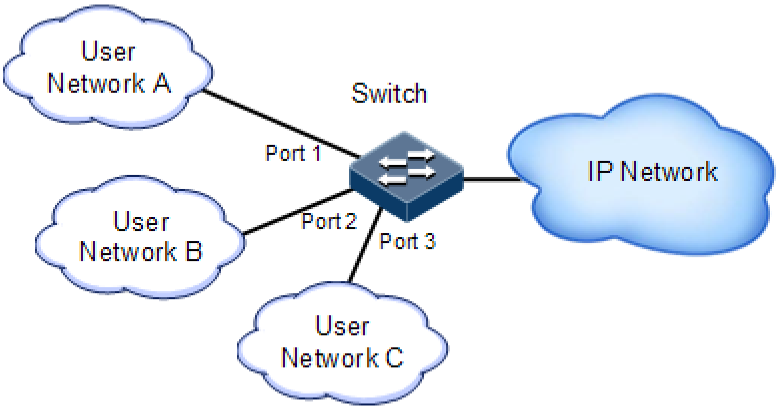
7.2.10 Example for configuring secure MAC address

Networking requirements

As shown Figure 7-1, the switch connects 3 user networks. To ensure the security of switch interface access data, the configuration is as below.

- Port 1 permits 3 users to access network up to. The MAC address of one user is specified to 0000.0000.0001. The other 2 users dynamically learn the MAC addresses; the NView NNM system will receive Trap information once the user learns a MAC address. Violation mode is configured to Protect and the aging time of the two learned MAC addresses is configured to 10min.
- Port 2 permits 2 users to access network up to. The 2 user MAC addresses are confirmed through learning; once they are confirmed, they will not be aged. Violation mode is configured to Restrict mode.
- Port 3 permits 1 user to access network up to. The specified user MAC address is 0000.0000.0002. Whether to age user MAC addresses can be controlled. Violation mode adopts Shutdown mode.

Figure 7-1 Secure MAC address networking



Configuration steps

Step 1 Configure the secure MAC address of Port 1.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport port-security
Raisecom(config-port)#switchport port-security maximum 3
Raisecom(config-port)#switchport port-security mac-address 0000.0000.0001
vlan 1
Raisecom(config-port)#switchport port-security violation protect
Raisecom(config-port)#switchport port-security trap enable
Raisecom(config-port)#exit
Raisecom(config)#port-security aging-time 10
```

Step 2 Configure the secure MAC address of Port 2.

```
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport port-security
Raisecom(config-port)#switchport port-security maximum 2
Raisecom(config-port)#switchport port-security mac-address sticky
Raisecom(config-port)#switchport port-security violation restrict
Raisecom(config-port)#exit
```

Step 3 Configure the secure MAC address of Port 3.

```
Raisecom(config)#interface port 3
Raisecom(config-port)#switchport port-security
Raisecom(config-port)#switchport port-security maximum 1
Raisecom(config-port)#switchport port-security mac-address sticky
0000.0000.0002 vlan 1
Raisecom(config-port)#switchport port-security mac-address sticky
Raisecom(config-port)#switchport port-security violation shutdown
```

Checking results

Use the **show port-security** [**port-list** *port-list*] command to show configurations of port security MAC.

```
Raisecom#show port-security port-list 1-3
Port security aging time:10 (mins)
port status  Max-Num  Cur-Num  His-Num   vio-Count vio-action Dynamic-Trap
-------------------------------------------------------------------------
1    Enable    3        1       0          0       protect      Enable
2    Enable    2        0       0          0       restrict     Disable
3    Enable    1        1       0          0       shutdown     Disable
```

Use the **show port-security mac-address** command to show secure MAC address and configurations of secure MAC address learning on an interface.

```
Raisecom#show port-security mac-address
VLAN  Security-MAC-Address  Flag   Port  Age(min)
-------------------------------------------------
2    0000.0000.0001      static   1    --
2    0000.0000.0002      sticky   3    --
```

7.3 Dynamic ARP inspection

7.3.1 Introduction

Dynamic ARP inspection is used for ARP protection of unsecure interface and prevents from responding ARP packets which do not meet the requirements, thus preventing ARP spoofing attack on the network.

There are 2 modes for dynamic ARP inspection:

- Static binding mode: configure the binding manually.
- Dynamic binding mode: in cooperation with the DHCP snooping to generate dynamic binding. When DHCP Snooping entry is changed, the dynamic ARP inspection will also update dynamic binding entry synchronously.

The ARP inspection table, which is used for preventing ARP attacks, consists of DHCP snooping entries and statically configured ARP inspection rules, including IP address, MAC address, and VLAN binding information. In addition, the ARP inspection table associates this information with specific interfaces. The dynamic ARP inspection binding table supports the combination of following entries:

- Interface+IP
- Interface+IP+MAC
- Interface+IP+VLAN
- Interface+IP+MAC+VLAN

Dynamic ARP inspection interfaces are divided into the following two types according to trust status:

- Trusted interface: the interface will stop ARP inspection, which conducts no ARP protection on the interface. All ARP packets are allowed to pass.
- Untrusted interface: the interface takes ARP protection. Only ARP packets that match the binding table rules are allowed to pass. Otherwise, they are discarded.

Figure 7-2 Principle of dynamic ARP inspection

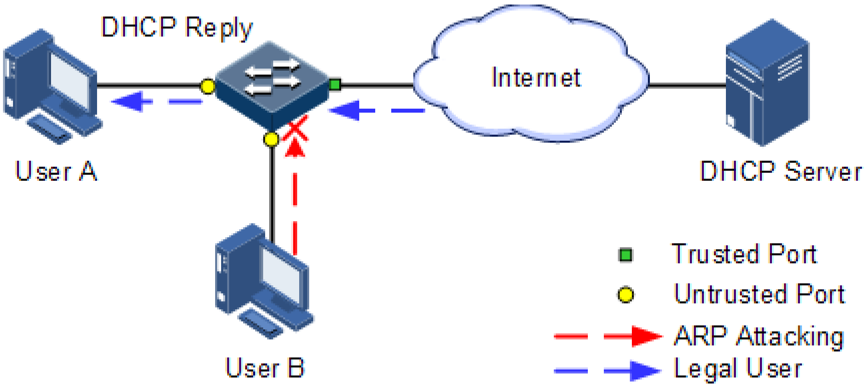


Figure 7-2 shows the principle of dynamic ARP inspection. When the ISCOM21xx receives an ARP packet, it compares the source IP address, source MAC address, interface ID, and VLAN information of the ARP packet with the DHCP Snooping entry information. If matched, it indicates that it is a legal user and the ARP packets are permitted to pass. Otherwise, it is an ARP attack and the ARP packet is discarded.

Dynamic ARP inspection also provides rate limiting on ARP packets to prevent unauthorized users from attacking the ISCOM21xx by sending a large number of ARP packets to the ISCOM21xx.

- When the number of ARP packets received by an interface every second exceeds the threshold, the system will regard that the interface receives an ARP attack, and then discard all received ARP packets to avoid the attack.
- The system provides auto-recovery and supports configuring the recovery time. The interfaces, where the number of received ARP packets is greater than the threshold, will recover to normal Rx/Tx status automatically after the recovery time expires.

Dynamic ARP inspection can also protect the specified VLAN. After the protection VLAN is configured, the ARP packets in specified VLAN on an untrusted interface will be protected. Only the ARP packets, which meet binding table rules, are permitted to pass. Other packets are discarded.

7.3.2 Preparing for configurations

Scenario

Dynamic ARP inspection is used to prevent the common ARP spoofing attacks on the network, which isolates the ARP packets with unsafe sources. Trust status of an interface depends on whether it trusts ARP packets. However, the binding table determines whether the ARP packets meet requirement.

Prerequisite

Enable DHCP Snooping if there is a DHCP user.

7.3.3 Default configurations of dynamic ARP inspection

Default configurations of dynamic ARP inspection are as below.

Function	Default value
Dynamic ARP inspection interface trust status	Untrusted
Dynamic ARP inspection static binding	Disable
Binding status of dynamic ARP inspection and dynamic DHCP Snooping	Disable
Binding status of dynamic ARP inspection and dynamic DHCP Relay	Disable
Dynamic ARP inspection static binding table	N/A
Dynamic ARP inspection protection VLAN	All VLANs
Interface rate limiting status for ARP packets	Disable
Interface rate limiting on ARP packets	100 pps
Auto-recovery rate limiting on ARP packets	Disable
Auto-recovery time for rate limiting on ARP packets	30s

7.3.4 Configuring trusted interfaces of dynamic ARP inspection

Configure trusted interfaces of dynamic ARP inspection for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#`**`ip arp-inspection trust`**	Configure the interface to a trusted interface.

7.3.5 Configuring static binding of dynamic ARP inspection

Configure static binding of dynamic ARP inspection for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`ip arp-inspection static-config`**	Enable global static ARP binding.

Step	Command	Description
3	`Raisecom(config)#`**`ip arp-inspection binding`** *`ip-address`* `[` *`mac-address`* `] [` **`vlan`** *`vlan-id`* `]` **`port`** *`port-id`*	Configure the static binding.

7.3.6 Configuring dynamic binding of dynamic ARP inspection

Caution

Before enabling dynamic binding of dynamic ARP inspection, you need to use the **ip dhcp snooping** command to enable DHCP Snooping.

Configure dynamic binding of dynamic ARP inspection for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`ip arp-inspection`** `{` **`dhcp-snooping`** `|` **`dhcp-relay`** `}`	Enable global dynamic ARP binding.

7.3.7 Configuring protection VLAN of dynamic ARP inspection

Configure protection VLAN of dynamic ARP inspection for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`ip arp-inspection`** `{` **`dhcp-snooping`** `|` **`dhcp-relay`** `}`	Enable global dynamic ARP binding.
3	`Raisecom(config)#`**`ip arp-inspection vlan`** *`vlan-list`*	Configure protection VLAN of dynamic ARP inspection.

7.3.8 Configuring rate limiting on ARP packets on interface

Configure rate limiting on ARP packets on the interface for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#`**`ip arp-rate-limit enable`**	Enable interface ARP packet rate limiting.

Step	Command	Description
4	`Raisecom(config-port)#ip arp-rate-limit rate rate-value`	Configure rate limiting on ARP packets on the interface.

7.3.9 Configuring auto-recovery time for rate limiting on ARP packets

Configure the auto-recovery time for rate limiting on ARP packets for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ip arp-rate-limit recover enable`	Enable auto-recovery for rate limiting on ARP packets.
3	`Raisecom(config)#ip arp-rate-limit recover time time`	Configure the auto-recovery time for rate limiting on ARP packets.

7.3.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show ip arp-inspection`	Show configurations of dynamic ARP inspection.
2	`Raisecom#show ip arp-inspection binding [ port port-id ]`	Show information about the dynamic ARP inspection binding table.
3	`Raisecom#show ip arp-rate-limit`	Show configurations of rate limiting on ARP packets.

7.3.11 Example for configuring dynamic ARP inspection

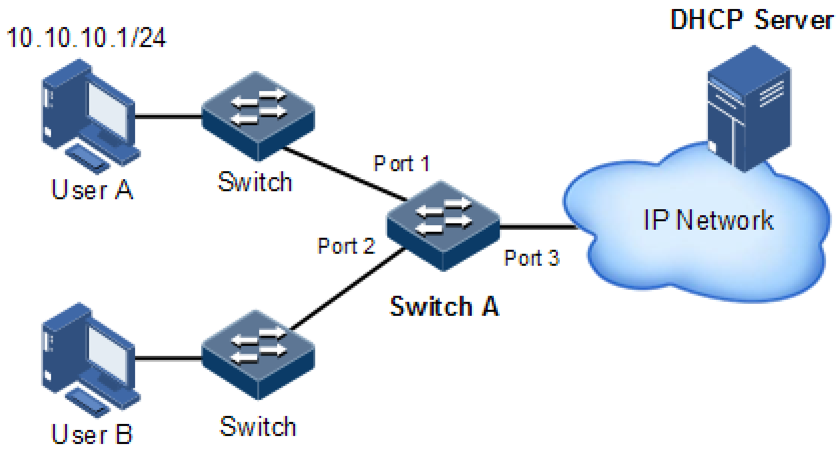
Networking requirements

To prevent ARP attacks, configure dynamic ARP inspection function on Switch A, as shown in Figure 7-3.

- Uplink Port 3 permits all ARP packets to pass.
- Downlink Port 1 permits ARP packets with specified IP address 10.10.10.1 to pass.
- Other interfaces permit ARP packets complying with dynamic binding learnt by DHCP snooping to pass.

- Downlink Port 2 configures rate limiting on ARP packets. The rate threshold is configured to 20 pps and recovery time for rate limiting is configured to 15s.

Figure 7-3 Dynamic ARP inspection networking



Configuration steps

Step 1 Configure Port 3 to the trusted interface.

```
Raisecom#config
Raisecom(config)#interface port 3
Raisecom(config-port)#ip arp-inspection trust
Raisecom(config-port)#exit
```

Step 2 Configure static binding.

```
Raisecom(config)#ip arp-inspection static-config
Raisecom(config)#ip arp-inspection binding 10.10.10.1 port 1
```

Step 3 Enable binding between dynamic ARP inspection and dynamic DHCP Snooping.

```
Raisecom(config)#ip dhcp snooping
Raisecom(config)#ip arp-inspection dhcp-snooping
```

Step 4 Configure ARP packet rate limiting on the interface.

```
Raisecom(config)#interface port 2
Raisecom(config-port)#ip arp-rate-limit rate 20
Raisecom(config-port)#ip arp-rate-limit enable
Raisecom(config-port)#exit
```

Step 5 Configure auto-recovery for rate limiting on ARP packets.

```
Raisecom(config)#ip arp-rate-limit recover time 15
Raisecom(config)#ip arp-rate-limit recover enable
```

Checking results

Use the **show ip arp-inspection** command to show configurations of interface trust status static/dynamic ARP binding.

```
Raisecom#show ip arp-inspection
Static Config ARP Inspection: Enable
DHCP Snooping ARP Inspection: Enable
DHCP Relay ARP Inspection: Disable
ARP Inspection Protect Vlan : 1-4094
Bind Rule Num            : 1
Vlan Acl Num             : 0
Remained Acl Num          : 512
Port   Trust
-------------
1      no
2      no
3      yes
4      no
…
```

Use the **show ip arp-inspection binding** command to show information about the dynamic ARP binding table.

```
Raisecom#show ip arp-inspection binding
Ip Address      Mac Address    VLAN  Port    Type         Inhw
---------------------------------------------------------------------
10.10.10.1      --             --     1      static        yes
Current Rules Num: 1
History Max Rules Num: 1
```

Use the **show ip arp-rate-limit** command to show configurations of rate limiting on the interface and auto-recovery time for rate limiting.

```
Raisecom#show ip arp-rate-limit
arp rate limit auto recover: enable
arp rate limit auto recover time: 15 second
Port   Enable-Status   Rate(Num/Sec)   Overload
--------------------------------------------------
1      Disabled       100            No
```

```
2      Enabled        20           No
3      Disabled       100          No
4      Disabled       100          No
…
```

7.4 ND detection

7.4.1 Introduction

Neighbor Discovery (ND) is a group of messages or processes for determining relations between neighboring nodes. Its messages replace the IPv4 Address Resolution Protocol (ARP), ICMP Router Discovery (RD), and ICMP Redirect messages, and it alsosupports the following functions:

- Detecting address conflicts
- Resolving the neighbor address
- Determining neighbor reachability
- Configuring the IP address of the host

ND detection is used on the ISCOM21xx to check user validity. It normally forwards ND packets of authorized users and discards those of unauthorized users, thus preventing attacks from forged users and gateways.

IPv6 ND detection support static binding instead of dynamic binding at present. Static binding refers to manual binding.

User validity check is used to determine whether a user is an authorized user of the VLAN to which the interface receiving the ND packet belongs, according to the source IPv6 address and source MAC address carried in the ND packet. It consists of the following items:

- Checking static binding entries of IP Source Guard
- Checking ND Snooping entries
- Checking DHCPv6 Snooping security entries

The ND detection binding table supports the following combinations:

- Interface+IP address
- Interface+IP address+MAC address

ND detection divides interfaces of the access device into the following two types:

- ND trusted interface: this interface does not check user validity.
- ND untrusted interface: this interface takes received packets invalid and thus discards them directly.

7.4.2 Preparing for configurations

Scenarios

ND detection is used to prevent common ND spoofing attacks on the network, thus able to isolate ND packets from unauthorized sources. You can configure the trusted status of an interface to trust ND packets or not and configure the binding table to determine whether ND packets comply with requirements.

Prerequisite

N/A

7.4.3 Default configurations of ND detection

Default configurations of ND detection are as below.

Function	Default value
Interface trusted status of ND detection	Untrusted
Static binding status of ND detection	Disable

7.4.4 Enable static binding of ND detection

Enable static binding of ND detection for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`nd-inspection static`**	Enable static binding. Use the **no nd-inspection static** command to disable this function.

7.4.5 Configuring trusted interface of ND detection

Configure the trusted interface of ND detection for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#`**`nd-inspection trust`**	Configure the interface to a trusted interface.

7.4.6 Configuring static binding of ND detection

Configure static binding of ND detection for the ISCOM21xx as below.

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

Step	Command	Description
2	Raisecom(config)#**nd-inspection static**	Configure global static binding.
3	Raisecom(config)#**nd-inspection binding** *ipv6-address* [*mac-address*] **port** *port-id*	Configure static binding. Use the **no nd-inspection binding** *ipv6-address* command to delete a binding relation.

7.4.7 RA Snooping

Note

The Router Advertisement (RA) message carries network configurations, including the default router, network prefix list, and enabling status of DHCP server. If the victim receives the forged RA message, network configurations will be incorrect and thus spoofing attacks are generated.

Configure RA Snooping for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 ra snooping**	Enable global RA Snooping.
3	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#**ipv6 ra snooping trust**	Configure the interface as the trusted interface.

7.4.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show nd-inspection static**	Show static binding and interface trusted status.
2	Raisecom#**show nd-inspection binding** [**port** *port-id*]	Show the binding relation of a specified interface or all interfaces.
3	Raisecom(config)#**show ipv6 ra snooping**	Show configurations of RA Snooping.

7.5 RADIUS

7.5.1 Introduction

Remote Authentication Dial In User Service (RADIUS) is a standard communication protocol that authenticates remote access users intensively. RADIUS uses UDP as the transmission protocol (port 1812 and port 1813) which has a good instantaneity; at the same time, RADIUS supports retransmission mechanism and standby server mechanism which has a good reliability.

RADIUS authentication

RADIUS adopts client/server mode, network access device is used as client of RADIUS server. RADIUS server receives user connecting requests and authenticates users, then reply configurations to all clients for providing services. Control user access device and network and improve network security.

Communication between client and RADIUS server is authenticated by sharing key, which will not be transmitted on network. Besides, all user directions need to be encrypted when transmitting between client device and RADIUS server to ensure security.

RADIUS accounting

RADIUS accounting is used to authenticate users through RADIUS. When logging in, a user sends a starting account packet to the RADIUS accounting server, according to the accounting policy to send update packet to the RADIUS server. When logging off, the user sends a stopping account packet to the RADIUS accounting server, and the packet includes user online time. The RADIUS accounting server can record the access time and operations for each user through packets.

7.5.2 Preparing for configurations

Scenario

You can deploy RADIUS server on the network to take authentication and accounting to control user access to device and network. This device can be used as agent of RADIUS server, which authorizes user accessing according to feedback from RADIUS.

Prerequisite

N/A

7.5.3 Default configurations of RADIUS

Default configurations of RADIUS are as below.

Function	Default value
RADIUS accounting	Disable
IP address of RADIUS server	0.0.0.0
IP address of RADIUS accounting server	0.0.0.0

Function	Default value
Port ID of RADIUS authentication server	1812
Port ID of RADIUS accounting server	1813
Shared key used for communication with the RADIUS accounting server	N/A
Policy for processing failed accounting	Online
Period for sending update packet	0

7.5.4 Configuring RADIUS authentication

Configure RADIUS authentication for the ISCOM21xx 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)#`**`ip address`** *`ip-address`* `[` *`ip-mask`* `] [` *`vlan-list`* `]`	Configure an IPv4 address.
4	`Raisecom(config-ip)#`**`end`**	Return to privileged EXEC mode.
5	`Raisecom#`**`radius`** `[` **`backup`** `]` *`ip-address`* `[` **`auth-port`** *`port-number`* `]`	Assign the IP address and port ID for RADIUS authentication server. Configure the **backup** parameter to assign the backup RADIUS authentication server.
6	`Raisecom#`**`radius-key`** *`string`*	Configure the shared key for RADIUS authentication.
7	`Raisecom#`**`user login`** `{` **`local-radius`** `|` **`local-user`** `|` **`radius-local`** `[` **`server-no-response`** `] |` **`radius-user`** `}`	Configure users to perform login authentication through RADIUS.
8	`Raisecom#`**`enable login`** `{` **`local-radius`** `|` **`local-user`** `|` **`radius-local`** `[` **`server-no-response`** `] |` **`radius-user`** `}`	Configure the authentication mode for users to enter privileged EXEC mode to RADIUS.

7.5.5 Configuring RADIUS accounting

Configure RADIUS accounting for the ISCOM21xx as below.

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

Step	Command	Description
2	Raisecom(config)#**interface ip** *if-number*	Enter Layer 3 interface configuration mode.
3	Raisecom(config-ip)#**ip address** *ip-address* [**sub**] [*ip-mask*] [*vlan-list*]	Configure an IPv4 address.
4	Raisecom(config-ip)#**end**	Return to privileged EXEC mode.
5	Raisecom#**aaa accounting login enable**	Enable RADIUS accounting.
6	Raisecom#**radius** [**backup**] **accounting-server** *ip-address* [*account-port*]	Assign IP address and UDP port ID for the RADIUS accounting server.
7	Raisecom#**radius accounting-server key** *string*	Configure the shared key to communicate with the RADIUS accounting server. The shared key must be identical to the one configured on the RADIUS accounting server. Otherwise, accounting will fail.
8	Raisecom#**aaa accounting fail** { **offline** | **online** }	Configure the processing policy for accounting failure.
9	Raisecom#**aaa accounting update** *period*	Configure the period for sending accounting update packets. If it is configured as 0, no accounting update packet is sent. **Note** The RADIUS accounting server can record access time and operation for each user through accounting starting packets, update packets and accounting end packets.

7.5.6 Checking configurations

Use the following commands to check configuration results.

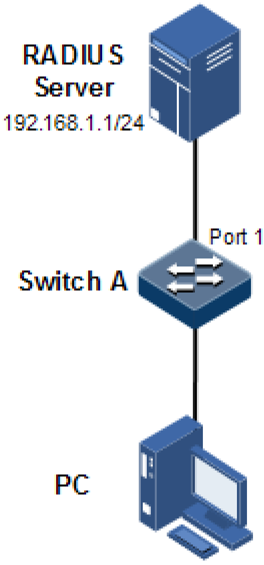
No.	Command	Description
1	Raisecom#**show radius-server**	Show configurations of the RADIUS server.
2	Raisecom#**show aaa accounting**	Show configurations of global accounting.

7.5.7 Example for configuring RADIUS

Networking requirements

As shown in Figure 7-4, configure RADIUS authentication and accounting on Switch A to authenticate login users and record their operations. The period for sending update packets is 2 configured to minutes. The user will be offline if accounting fails.

Figure 7-4 RADIUS networking



Configuration steps

Step 1 Authenticate login users through RADIUS.

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

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 2
```

Checking results

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

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

Use the **show aaa accounting** command to show configurations of RADIUS accounting.

```
Raisecom#show aaa accounting
Accounting login:            enable
Accounting update interval:     2
Accounting fail policy:       offline
```

7.6 TACACS+

7.6.1 Introduction

Terminal Access Controller Access Control System (TACACS+) is a kind of network access authentication protocol similar to RADIUS. The differences between them are:

- TACACS+ uses TCP port 49, which has higher transmission reliability compared with UPD port used by RADIUS.
- TACACS+ encrypts the holistic of packets except the standard head of TACACS+, and there is a field to show whether the data packets are encrypted in the head of packet. Compared to RADIUS user password encryption, the TACACS+ is much safer.
- TACACS+ authentication function is separated from authorization and accounting functions; it is more flexible in deployment.

In a word, TACACS+ is safer and more reliable than RADIUS. However, as an open protocol, RADIUS is more widely used.

7.6.2 Preparing for configurations

Scenario

To control users accessing to the ISCOM21xx and the network, you can authenticate and account users by deploying the TACACS+ server on the network. Compared with RADIUS, TACACS+ is safer and more reliable. The ISCOM21xx can be used as the agent of the TACACS+ server, controlling users according to feedback result from the TACACS+ server.

Prerequisite

N/A

7.6.3 Default configurations of TACACS+

Default configurations of TACACS+ are as below.

Function	Default value
TACACS+ status	Disable
Login mode	Local-user
IP address of TACACS+ authentication server	0.0.0.0, shown as "--"
IP address of TACACS+ accounting server	0.0.0.0, shown as "--"
Shared key used for communication with TACACS+ accounting server	N/A
Policy for processing failed accounting	Online
Period for sending update packet	0

7.6.4 Configuring TACACS+ authentication

Configure TACACS+ authentication for the ISCOM21xx 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)#`**`ip address`** *`ip-address`* [*`ip-mask`*] [*`vlan-list`*]	Configure an IPv4 address.
4	`Raisecom(config-ip)#`**`end`**	Return to privileged EXEC mode.
5	`Raisecom#`**`tacacs-server`** [**`backup`**] *`ip-address`*	Assign the IP address and port ID for the TACACS+ authentication server. Configure the **backup** parameter to assign the backup TACACS+ authentication server.
6	`Raisecom#`**`tacacs-server key`** *`string`*	Configure the shared key for TACACS+ authentication.
7	`Raisecom#`**`user login`** { **`local-tacacs`** | **`local-user`** | **`tacacs-local`** [**`server-no-response`**] | **`tacacs-user`** }	Configure users to perform login authentication through TACACS+.
8	`Raisecom#`**`enable login`** { | **`local-tacacs`** | **`local-user`** | **`tacacs-local`** [**`server-no-response`**] | **`tacacs-user`** }	Configure the authentication mode for users to enter privileged EXEC mode to TACACS+.

7.6.5 Configuring TACACS+ accounting

Configure TACACS+ accounting for the ISCOM21xx 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)#**ip address** *ip-address* [*ip-mask*] [*vlan-list*]	Configure an IPv4 address.
4	Raisecom(config-ip)#**end**	Return to privileged EXEC mode.
5	Raisecom#**aaa accounting login enable**	Enable TACACS+ accounting.
6	Raisecom#**tacacs** [**backup**] **accounting-server** *ip-address*	Assign IP address and UDP port ID for the TACACS+ accounting server.
7	Raisecom#**tacacs-server key** *string*	Configure the shared key to communicate with the TACACS+ accounting server.
8	Raisecom#**aaa accounting fail** { **offline** | **online** }	Configure the processing policy for accounting failure.
9	Raisecom#**aaa accounting update** *period*	Configure the period for sending accounting update packets. If configured as 0, no accounting update packet is sent.

7.6.6 Configuring TACACS+ authorization

Configure TACACS+ authorization for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**tacacs authorization enable**	Enable the TACACS+ authorization server.

7.6.7 Checking configurations

Use the following commands to check configuration results.

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

No.	Command	Description
2	Raisecom#**show radius-server**	Show configurations on the TACACS+ accounting server. **Note** Use the **show radius-server** command to show configurations of TACACS+ and RADIUS accounting. By default, the results are configurations of RADIUS authentication.

7.6.8 Maintenance

Maintain the ISCOM21xx as below.

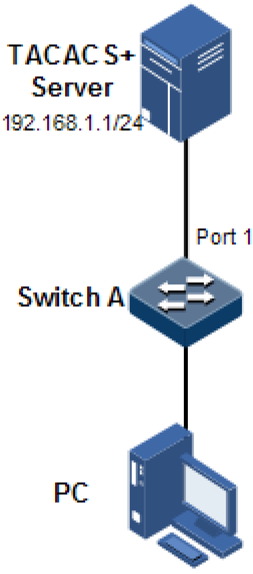
Command	Description
Raisecom#**clear tacacs statistics**	Clear TACACS+ statistics.

7.6.9 Example for configuring TACACS+

Networking requirements

As shown in Figure 7-5, configure TACACS+ authentication on Switch A to authenticate users who log in to the ISCOM21xx.

Figure 7-5 TACACS+ networking



Configuration steps

Authenticate login users through TACACS+.

```
Raisecom#tacacs-server 192.168.1.1
Raisecom#tacacs-server key raisecom
Raisecom#user login tacacs-user
Raisecom#enable login local-tacacs
```

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
Total Packet Sent:   0
Total Packet Recv:   0
Accounting server Address:      --
Backup Accounting server Address: --
```

7.7 Storm control

7.7.1 Introduction

In most Layer 2 network, the unicast traffic is much heavier than the broadcast traffic. If the rate for broadcast traffic is not limited, when a broadcast storm is generated, much bandwidth will be occupied. Therefore, network performance will be reduced and unicast packet cannot be forwarded. In addition, the communication between devices may be interrupted.

Configuring storm control on Layer 2 devices can prevent broadcast storm from occurring when broadcast packets increase sharply on the network. In this case, the unicast packets can be properly forwarded.

Storm control allows an interface to filter broadcast packets received by the interface. After storm control is enabled, when the number of received broadcast packets reaches the pre-configured threshold, the interface will automatically discard the received packets. If storm control is disabled or if the number of received broadcast packets does not reach the pre-configured threshold, the broadcast packets are broadcasted to other interfaces of the switch properly.

7.7.2 Preparing for configurations

Scenario

Configuring storm control on Layer 2 devices can prevent broadcast storm from occurring when broadcast packets increase sharply on the network. In this case, 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 MAC destination address is not in MAC address table. It is broadcasted by Layer 2 devices.
- Unknown multicast traffic: the multicast traffic whose MAC destination address is not in MAC address table. Generally, it is broadcasted by Layer 2 devices.
- Broadcast traffic: the traffic whose MAC destination address is a broadcast MAC address. It is broadcasted by Layer 2 devices.

Prerequisite

Connect the interface and configure its physical parameters to make it Up.

7.7.3 Default configurations of storm control

Default configurations of storm control are as below.

Function	Default value
Broadcast storm control status	Enable
Multicast and unknown unicast storm control status	Disable
Allowed Bytes per second	64 kbit/s
DLF packet forwarding	Enable

7.7.4 Configuring storm control

Configure storm control for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**storm-control { all | broadcast | dlf | multicast } enable port-list** *port-list*	Enable storm control over broadcast traffic, multicast traffic, and unknown unicast traffic.
3	Raisecom(config)#**storm-control bps** *value*	(Optional) configure the number of bytes that are allowed to pass every second.

7.7.5 Configuring DLF packet forwarding

Configure DLF packet forwarding for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**dlf-forwarding enable**	Enable DLF packet forwarding on the interface.

7.7.6 Checking configurations

Use the following commands to check configuration results.

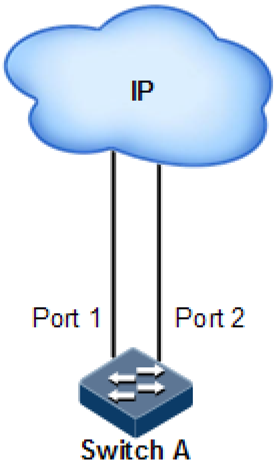
No.	Command	Description
1	`Raisecom#show storm-control`	Show configurations of storm control.
2	`Raisecom(config)#show dlf-forwarding`	Show the status of forwarding DLF packets.

7.7.7 Example for configuring storm control

Networking requirements

As shown in Figure 7-6, to restrict influence on Switch A caused by broadcast storm, you need to configure storm control on Switch A to control broadcast packets and unknown unicast packets. The control threshold is configured to 640 kbit/s, and the burst is configured to 80 Kbytes.

Figure 7-6 Storm control networking



Configuration steps

Step 1 Configure storm control on Switch A.

```
Raisecom#config
Raisecom(config)#storm-control broadcast enable port 1-2
Raisecom(config)#storm-control dlf enable port 1-2
Raisecom(config)#storm-control bps 640 80
```

Checking results

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

```
Raisecom#show storm-control
Threshold: 640 kbps
Burst: 80 kB
Port   Broadcast      Multicast      DLF_Unicast
-----------------------------------------------------------
1        Enable        Disable          Enable
2        Enable        Disable          Enable
3        Enable        Disable          Disable
```

7.8 802.1x

7.8.1 Introduction

802.1x, based on IEEE 802.1x, is a VLAN-based network access control technology. It is used to solve authentication and security problems for LAN users.

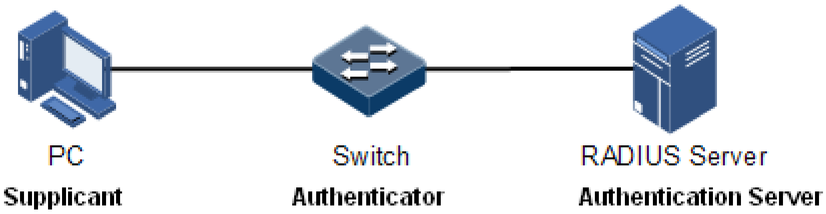
It is used to authenticate and control access devices at the physical later of the network device. It defines a point-to-point connection mode between the device interface and user devices. User devices, connected to the interface, can access resources in the LAN if they are authenticated. Otherwise, they cannot access resources in the LAN through the switch.

802.1x structure

As shown in Figure 7-7, 802.1x authentication uses C/S mode, including the following 3 parts:

- Supplicant: a user-side device installed with the 802.1x client software (such as Windows XP 802.1x client), such as a PC
- Authenticator: an access control device supporting 802.1x authentication, such as a switch
- Authentication Server: a device used for authenticating, authorizing, and accounting users. Generally, the RADIUS server is taken as the 802.1x authentication server.

Figure 7-7 802.1x structure



Interface access control modes

The authenticator uses the authentication server to authenticate clients that need to access the LAN and controls interface authorized/ unauthorized status through the authentication results. You can control the access status of an interface by configuring access control modes on the interface. 802.1x authentication supports the following 3 interface access control modes:

- Protocol authorized mode (auto): the protocol state machine determines the authorization and authentication results. Before clients are successfully authenticated, only EAPoL packets are allowed to be received and sent. Users are disallowed to access network resources and services provided by the switch. If clients are authorized, the interface is switched to the authorized state, allowing users to access network resources and services provided by the switch.
- Force interface authorized mode (authorized-force): the interface is in authorized state, allowing users to access network resources and services provided by the switch without being authorized and authenticated.
- Force interface unauthorized mode (unauthorized-force): the interface is in unauthorized mode. Users are disallowed to access network resources and services provided by the switch, that is, users are disallowed to be authenticated.

802.1x authentication procedure

The supplicant and the authentication server exchange information through the Extensible Authentication Protocol (EAP) packet while the supplicant and the authenticator exchange information through the EAP over LAN (EAPoL) packet. The EAP packet is encapsulated with authentication data. This authentication data will be encapsulated into the RADIUS protocol packet to be transmitted to the authentication server through a complex network.

Both the authenticator and the suppliant can initiate the 802.1x authentication procedure. This guide takes the suppliant for an example, as shown below:

Step 1 The user enters the user name and password. The supplicant sends an EAPoL-Start packet to the authenticator to start the 802.1x authentication.

Step 2 The authenticator sends an EAP-Request/Identity to the suppliant, asking the user name of the suppliant.

Step 3 The suppliant replies an EAP-Response/Identity packet to the authenticator, which includes the user name.

Step 4 The authenticator encapsulates the EAP-Response/Identity packet to the RADIUS protocol packet and sends the RADIUS protocol packet to the authentication server.

Step 5 The authentication server compares with received encrypted password with the one generated by itself.

Step 6 If identical, the authenticator modifies the interface state to authorized state, allowing users to access the network through the interface and sends an EAP-Success packet to the suppliant. Otherwise, the interface is in unauthorized state and sends an EAP-Failure packet to the suppliant.

802.1x timers

During 802.1x authentication, the following 5 timers are involved:

- Reauth-period: re-authorization t timer. After the period is exceeded, the ISCOM21xx re-initiates authorization.

- Quiet-period: quiet timer. When user authorization fails, the ISCOM21xx needs to keep quiet for a period. After the period is exceeded, the ISCOM21xx re-initiates authorization. During the quiet time, the ISCOM21xx does not process authorization packets.
- Tx-period: transmission timeout timer. When the ISCOM21xx sends a Request/Identity packet to users, the ISCOM21xx will initiate the timer. If users do not send an authorization response packet during the tx-period, the ISCOM21xx will re-send an authorization request packet. The ISCOM21xx sends this packet three times in total.
- Supp-timeout: Supplicant authorization timeout timer. When the ISCOM21xx sends a Request/Challenge packet to users, the ISCOM21xx will initiate supp-timeout timer. If users do not send an authorization response packet during the supp-timeout, the ISCOM21xx will re-send the Request/Challenge packet. The ISCOM21xx sends this packet twice in total.
- Server-timeout: Authentication server timeout timer. The timer defines the total timeout period of sessions between authorizer and the RADIUS server. When the configured time is exceeded, the authenticator will end the session with RADIUS server and start a new authorization process.

7.8.2 Preparing for configruations

Scenario

To implement access authentication on LAN users and ensure access user security, you need to configure 802.1x authentication on the ISCOM21xx.

If users are authenticated, they are allowed to access network resources. Otherwise, they cannot access network resources. By performing authentication control on user access interface, you can manage the users.

Prerequisite

If RADIUS authentication server is used, you need to perform following operations before configuring 802.1x authentication:

- Configure the IP address of the RADIUS server and the RADIUS shared key.
- The ISCOM21xx can ping through the RADIUS server successfully.

7.8.3 Default configurations of 802.1x

Default configurations of 802.1x are as below.

Function	Default value
Global 802.1x	Disable
Interface 802.1x	Disable
Interface access control mode	Auto
802.1x authentication method	chap
Interface access control mode of 802.1x authentication	portbase
RADIUS server timout timer time	100s

Function	Default value
802.1x re-authentication	Disable
802.1x re-authentication timer	3600s
802.1x quiet timer time	60s
Request packet retransmission timer timeout	30s
Supplicant authorization timer timeout	30s

7.8.4 Configuring basic functions of 802.1x

Caution

- 802.1x and STP are exclusive on the same interface. You cannot enable them concurrently.
- Only one user authentication request is processed on an interface at a time.

Configure basic functions of 802.1x for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#dot1x enable`	Enable global 802.1x.
3	`Raisecom(config)#interface port port-id`	Enter physical layer interface configuration mode.
4	`Raisecom(config-port)#dot1x authentication-method { chap | eap | pap }`	Configure 802.1x protocol authentication mode.
5	`Raisecom(config-port)#dot1x enable`	Enable interface 802.1x.
6	`Raisecom(config-port)#dot1x auth-control { auto | authorized-force | unauthorized-force }`	Configure access control mode on the interface.
7	`Raisecom(config-port)#dot1x auth-method { macbased | portbased }`	Configure access control mode of 802.1x authentication on the interface.

Note

To configure EAP relay authentication mode, ensure that the RADIUS server supports EAP attributes.

If 802.1x is disabled in global/interface configuration mode, the interface access control mode of 802.1x is configured to force interface authorized mode.

7.8.5 Configuring 802.1x re-authentication

Configure 802.1x re-authentication for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**dot1x reauthentication enable**	Enable 802.1x re-authentication.

Caution

Re-authentication is initiated for authorized users. Before enabling re-authentication, you must ensure that global/interface 802.1x is enabled. Authorized interfaces are still in this mode during re-authentication. If re-authentication fails, the interfaces are in unauthorized state.

7.8.6 Configuring 802.1x timers

Configure 802.1x timers for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**dot1x timer reauth-period** *reauth-period*	Configure the time of the re-authentication timer.
4	Raisecom(config-port)#**dot1x timer quiet-period** *quiet-period*	Configure the time of the quiet timer.
5	Raisecom(config-port)#**dot1x timer tx-period** *tx-period*	Configure the time of the transmission timeout timer.
6	Raisecom(config-port)#**dot1x timer supp-timeout** *supp-timeout*	Configure the time of the supplicant authorization timeout timer.
7	Raisecom(config-port)#**dot1x timer server-timeout** *server-timeout*	Configure the time of the Authentication server timeout timer.

7.8.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show dot1x port-list`** *`port-list`*	Show 802.1x configurations on the interface.
2	`Raisecom#`**`show dot1x port-list`** *`port-list`* **`statistics`**	Show 802.1x statistics on the interface.
3	`Raisecom#`**`show dot1x port-list`** *`port-list`* **`user`**	Show user information of 802.1x authentication on the interface.

7.8.8 Maintenance

Maintain the ISCOM21xx as below.

Command	Description
`Raisecom(config)#`**`clear dot1x port-list`** *`port-list`* **`statistics`**	Clear interface 802.1x statistics.

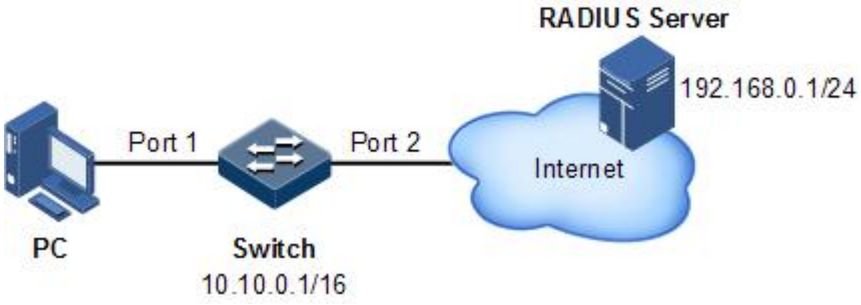
7.8.9 Example for configuring 802.1x

Networking requirements

To make users access external network, you need to configure 802.1x authentication on the switch, as shown in Figure 7-8.

- Configure the switch.
  - IP address: 10.10.0.1
  - Subnet mask: 255.255.0.0
  - Default gateway address: 10.10.0.2
- Perform authorization and authentication through the RADIUS server.
  - IP address of the RADIUS server: 192.168.0.1
  - Password of the RADIUS server: raisecom
- Configure the interface access control mode to protocol authorized mode.
- After authorized successfully, the user can initiate re-authentication in 600 seconds.

Figure 7-8 802.1x networking



Configuration steps

Step 1 Configure the IP addresses of the Switch and RADIUS server.

```
Raisecom#config
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address 10.10.0.1 255.255.0.0 1
Raisecom(config-ip)#exit
Raisecom(config)#ip default-gateway 10.10.0.2
Raisecom(config)#exit
Raisecom#radius 192.168.0.1
Raisecom#radius-key raisecom
```

Step 2 Enable global 802.1x and interface 802.1x.

```
Raisecom#config
Raisecom(config)#dot1x enable
Raisecom(config)#interface port 1
Raisecom(config-port)#dot1x enable
```

Step 3 Configure the authorization mote to protocol authorization mode.

```
Raisecom(config-port)#dot1x auth-control auto
```

Step 4 Enable re-authentication and configure the re-authentication time to 600s.

```
Raisecom(config-port)#dot1x reauthentication enable
Raisecom(config-port)#dot1x timer reauth-period 600
```

Checking results

Use the **show dot1x port-list** *port-list* command to show 802.1x configurations.

```
Raisecom#show dot1x port-list 1
802.1x Global Admin State: Enable
802.1x Authentication Method: Chap
Port 1
--------------------------------------------------------
802.1X Port Admin State:      Enable
PAE:                      Authenticator
PortMethod:                 Portbased
PortControl:                Auto
PortStatus:                 Authorized
```

```
Authenticator PAE State:      Initialize
Backend Authenticator State:   Initialize
ReAuthentication:            Disable
QuietPeriod:               60(s)
ServerTimeout:              100(s)
SuppTimeout:               30(s)
ReAuthPeriod:               3600(s)
TxPeriod:                 30(s)
```

7.9 IP Source Guard

7.9.1 Introduction

IP Source Guard uses a binding table to defend against IP Source spoofing and solve IP address embezzlement without identity authentication. IP Source Guard can cooperate with DHCP Snooping to generate dynamic binding. In addition, you can configure static binding manually. DHCP Snooping filters untrusted DHCP packets by establishing and maintaining the DHCP binding database.

IP Source Guard binding entry

IP Source Guard is used to match packet characteristics, including source IP address, source MAC address, and VLAN Tags, and can support the interface to combine with the following characteristics (hereinafter referred to as binding entries):

- Interface+IP
- Interface+IP+MAC
- Interface+IP+VLAN
- Interface+IP+MAC+VLAN

According to the generation mode of binding entries, IP Source Guard can be divided into static binding and dynamic binding:

- Static binding: configure binding information manually and generate binding entries to complete the interface control. Static binding fits when the number of hosts is small or you need to perform separate binding on a single host.
- Dynamic binding: obtain binding information automatically from DHCP Snooping to complete the interface control. Dynamic binding is suitable when there are many hosts and you need to adopt DHCP to perform dynamic host configurations. Dynamic binding can prevent IP address conflict and embezzlement.

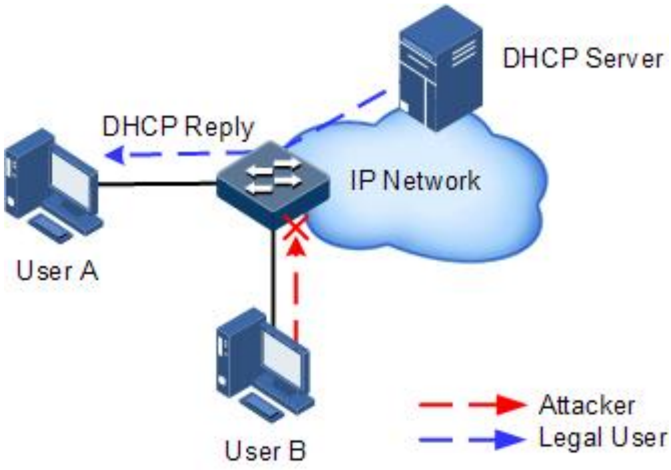
Principle of IP Source Guard

The principle of IP Source Guard is to build an IP source binding table within the ISCOM21xx, based on which packets are examined on each interface. Figure 7-9 shows the principle of IP Source Guard.

- If the received IP packets meet the relationship of Port/IP/MAC/VLAN binding entries in IP source binding table, forward these packets.
- If the received IP packets are DHCP data packets, forward these packets.

- Otherwise, discard these packets.

Figure 7-9 Principle of IP Source Guard



Before forwarding IP packets, the ISCOM21xx compares the source IP address, source MAC address, interface ID, and VLAN ID of the IP packets with binding table information. If the information matches, it indicates that the user is legal and the packets are permitted to forward normally. Otherwise, the user is identified as an attacker and the IP packets are discarded.

7.9.2 Preparing for configurations

Scenario

There are often some IP source spoofing attacks on the network. For example, the attacker impersonates an authorized to send forged IP packets to the server, or the attacker forges the source IP address of another user to communicate. This makes authorized users fail to access network services normally.

IP Source Guard binding can filter and control packets forwarded by the interface, and prevent illegal packets from accessing the interface, thus restricting unauthorized use of network resources and improving interface security.

Prerequisite

Enable DHCP Snooping if there is a DHCP user.

7.9.3 Default configurations of IP Source Guard

Default configurations of IP Source Guard are as below.

Function	Default value
IP Source Guide static binding	Disable
IP Source Guide dynamic binding	Disable
Interface trust status	Untrusted

7.9.4 Configuring interface trusted status of IPv4 Source Guard

Configure interface trusted status of IPv4 Source Guard for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#`**`ip verify source trust`**	Configure the interface as a trusted interface.

7.9.5 Configuring interface trusted status of IPv6 Source Guard

Configure interface trusted status of IPv6 Source Guard for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#`**`ipv6 verify source trust`**	Configure the IPv6 interface as a trusted interface. Use the **no ipv6 verify source trust** command to configure the IPv6 interface as an untrusted interface. In this case, all IP packets except DHCP packets and binding-compliant packets will not be forwarded. In trusted status, the IPv6 interface forwards all packets.

7.9.6 Configuring IPv4 Source Guide binding

Configuring static IPv4 Source Guide binding

Configure IPv4 Source Guide static binding for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`ip verify source`**	Enable static IP Source Guide binding.
3	`Raisecom(config)#`**`ip source binding`** *`ip-address`* `[` *`mac-address`* `] [` **`vlan`** *`vlan-id`* `]` **`port`** *`port-id`*	Configure static binding.
4	`Raisecom(config)#`**`ip verify source set-cos`** *`cos-value`*	Configure CoS of packets.

Step	Command	Description
5	Raisecom(config)#**ip verify source** *ip-address mask* **set-cos** *cos-value* [**rate-limit** *rate-value brust-value*]	Configure inter-segment CoS of packets and rate limit.

Note

- Configured static binding can take effect only when global static binding is enabled; otherwise, it does not effect.
- For an identical IP address, manually-configured static binding will override dynamic binding with the same IP address but existing static binding. When static binding is deleted, the system will automatically recover the overridden dynamic binding.

Configuring dynamic IP Source Guide binding

Configure IP Source Guide dynamic binding for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip verify source** { **dhcp-snooping** | **dhcp-relay** }	Enable IP Source Guide dynamic binding.

Note

- Dynamic binding learnt through DHCP Snooping can take effect only when global dynamic binding is enabled; otherwise, it does not effect.
- If an IP address exists in the static binding table, configuring dynamic binding with the IP address does not override existing dynamic binding and thus will not take effect.

Configuring binding translation

Configure binding translation for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip verify source** { **dhcp-snooping** | **dhcp-relay** }	Enable IP Source Guide dynamic binding.
3	Raisecom(config)#**ip source binding** { **dhcp-snooping** | **dhcp-relay** } **static**	Translate the dynamic binding to the static binding.

Step	Command	Description
4	Raisecom(config)#**ip source binding auto-update**	(Optional) enable auto-translation. After it is enabled, dynamic binding entries learned through DHCP Snooping are directly translated into static binding entries.

7.9.7 Configuring IPv6 Source Guide binding

Configuring static IPv6 Source Guide binding

Configure IPv6 Source Guide static binding for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 verify source**	Enable static IPv6 Source Guide binding.
3	Raisecom(config)#**ipv6 source binding** *ipv6-address* [*mac-address*] **port** *port-id*	Configure static binding. Use the **no ipv6 source binding ipv6-address** command to delete the static binding.

Note

- Configured static binding can take effect only when global static binding is enabled; otherwise, it does not effect.
- For an identical IP address, manually configured static binding will override dynamic binding with the same IP address but existing static binding. When static binding is deleted, the system will automatically recover the overridden dynamic binding.

Configuring dynamic IPv6 Source Guide binding

Configure dynamic IPv6 Source Guide binding for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 verify source dhcp-snooping**	Enable dynamic IPv6 Source Guide dynamic binding.
3	Raisecom(config)#**ipv6 source guard dynamic mode { all | l3 }**	Configure dynamic binding.

Note

- Dynamic binding learnt through DHCP Snooping can take effect only when global dynamic binding is enabled; otherwise, it does not effect.
- If an IPv6 address exists in the static binding table, configuring dynamic binding with the IPv6 address does not override existing dynamic binding and thus will not take effect.

7.9.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show ip verify source`	Show global binding status and interface trusted status.
2	`Raisecom#show ip source binding [ port port-id ]`	Show configurations of CoS priority of matching packets.
3	`Raisecom#show ipv6 verify source`	Show configurations of IP Source Guard binding, interface trusted status, and binding table.
4	`Raisecom#show ipv6 source binding [port port-id]`	Show all dynamic/static bindings on all interfaces or a specified interface.
5	`Raisecom#show ipv6 source guard dynamic mode`	Show dynamic binding mode.
6	`Raisecom#show ip verify source set-cos`	Show information about Configure CoS and rate limiting.

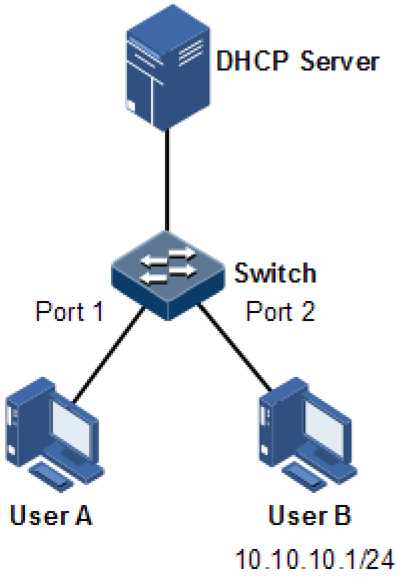
7.9.9 Example for configuring IP Source Guard

Networking requirements

As shown in Figure 7-10, to prevent IP address embezzlement, you need to configure IP Source Guard on the switch.

- The Switch permits all IP packets on Port 1 to pass.
- Port 2 permits IP packets with specified the IP address 10.10.10.1 and subnet mask 255.255.255.0 and the IP packets meeting DHCP Snooping learnt dynamic binding to pass.
- Other interfaces only permit the packets meeting DHCP Snooping learnt dynamic binding to pass.

Figure 7-10 IP Source Guard networking



Configuration steps

Step 1 Configure Port 1 to a trusted interface.

```
Raisecom#config
Raisecom(config)#interface port 1
Raisecom(config-port)#ip verify source trust
Raisecom(config-port)#exit
```

Step 2 Configure static binding.

```
Raisecom(config)#ip verify source
Raisecom(config)#ip source binding 10.10.10.1 port 2
```

Step 3 Enable global dynamic IP Source Guard binding.

```
Raisecom(config)#ip verify source dhcp-snooping
```

Checking results

Use the **show ip source binding** command to show configurations of the static binding table.

```
Raisecom#show ip source binding
History Max Entry Num: 1
```

```
Current Entry Num: 1
Ip Address      Mac Address     VLAN   Port   Type          Inhw
----------------------------------------------------------------------
10.10.10.1      --             --       2     static         yes
```

Use the **show ip verify source** command to show interface trusted status and configurations of IP Source Guard static/dynamic binding.

```
Raisecom#show ip verify source
Static Bind: Enable
Dhcp-Snooping Bind: Enable
Dhcp-Relay Bind: Disable
Port        Trust
--------------------
  1       yes
  2       no
  3       no
…
```

7.10 PPPoE+

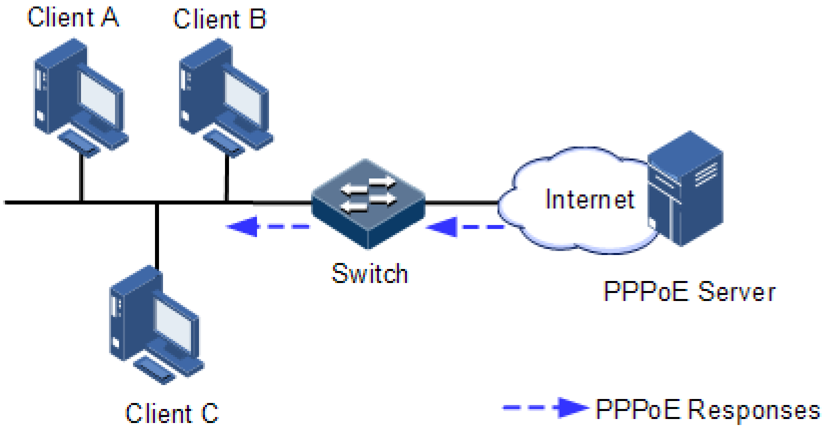
7.10.1 Introduction

PPPoE Intermediate Agent (PPPoE+) is used to process authentication packets. PPPoE+ adds device information into the authentication packet to bind account and access device so that the account is not shared and stolen, and the carrier's and users' interests are protected. This provides the server with enough information to identify users, avoiding account sharing and theft and ensuring the network security.

With PPPoE dial-up mode, you can access the network through various interfaces of the device only when one authentication is successfully. However, the server cannot accurately differentiate users just by the authentication information, which contains the user name and password. With PPPoE+, besides the user name and the password, other information, such as the interface ID, is included in the authentication packet for authentication. If the interface ID identified by the authentication server cannot match with the configured one, authentication will fail. This helps prevent illegal users from stealing accounts of other legal users for accessing the network.

The PPPoE protocol adopts C/S mode, as shown in Figure 7-11. The Switch acts as a relay agent. Users access the network through PPPoE authentication. If the PPPoE server needs to locate users, more information should be contained in the authentication packet.

Figure 7-11 Accessing the network through PPPoE authentication



To access the network through PPPoE authentication, you need to pass through the following 2 stages: discovery stage (authentication stage) and session stage. PPPoE+ is used to process packets at the discovery stage. The following steps show the whole discovery stage.

Step 1 To access the network through PPPoE authentication, the client sends a broadcast packet PPPoE Active Discovery Initiation (PADI). This packet is used to query the authentications server.

Step 2 After receiving the PADI packet, the authentication server replies a unicast packet PPPoE Active Discovery Offer (PADO).

Step 3 If multiple authentication servers reply PADO packets, the client selects one from them and then sends a unicast PPPoE Active Discovery Request (PADR) to the authentication server.

Step 4 After receiving the PADR packet, if the authentication server believes that the user is legal, it sends a unicast packet PPPoE Active Discovery Session-confirmation (PADS) to the client.

PPPoE is used to add user identification information in to PADI and PADR. Therefore, the server can identify whether the user identification information is identical to the user account for assigning resources.

7.10.2 Preparing for configurations

Scenario

To prevent illegal client access during PPPoE authentication, you need to configure PPPoE+ to add additional user identification information in PPPoE packet for network security.

Because the added user identification information is related to the specified switch and interface, the authentication server can bind the user with the switch and interface to effectively prevent account sharing and theft. In addition, this helps users enhance network security.

Prerequisite

N/A

7.10.3 Default configurations of PPPoE+

Default configurations of I PPPoE+ are as below.

Function	Default value
Global PPPoE	Disable
Interface PPPoE	Disable
Padding mode of Circuit ID	Switch
Circuit ID information	Interface ID/VLAN ID/attached string
Attached string of Circuit ID	hostname
Padded MAC address of Remote ID	MAC address of the switch
Padding mode of Remote ID	Binary
Interface trusted status	Untrusted
Tag overriding	Disable

Note

By default, PPPoE packet is forwarded without being attached any information.

7.10.4 Configuring basic functions of PPPoE+

Caution

PPPoE+ is used to process PADI and PADR packets. It is designed for the PPPoE client. Generally, PPPoE+ is only enabled on interfaces that are connected to the PPPoE client. Trusted interfaces are interfaces through which the switch is connected to the PPPoE server. PPPoE+ and trusted interface are exclusive. An interface is either enabled with PPPoE+ or is a trusted interface.

Enabling PPPoE+

After interface PPPoE+ is enabled, PPPoE authentication packets sent to the interface will be attached with user information and then are forwarded to the trusted interface.

Enable PPPoE+ for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#`**`pppoeagent enable`**	Enable interface PPPoE+.

Configuring PPPoE trusted interface

The PPPoE trusted interface can be used to prevent PPPoE server from being cheated and avoid security problems because PPPoE packets are forwarded to other non-service interfaces. Generally, the interface connected to the PPPoE server is configured as the trusted interface. PPPoE packets from the PPPoE client to the PPPoE server are forwarded by the trusted interface only. In addition, only PPPoE received from the trusted interface can be forwarded to the PPPoE client.

Configure the PPPoE trusted interface for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#`**`pppoeagent trust`**	Configure the PPPoE trusted interface.

Note

Because PPPoE+ is designed for the PPPoE client instead of the PPPoE server, downlink interfaces of the device cannot receive the PADO and PADS packets. It means that interfaces, where PPPoE+ is enabled, should not receive PADO and PADS packet. If there interfaces receive these packets, it indicates that there are error packets and the packets should be discarded. However, these interfaces can forward PADO and PADS packets of trusted packet. In addition, PADI and PADR packets are forwarded to the trusted interface only.

7.10.5 Configuring PPPoE+ packet information

PPPoE is used to process a specified Tag in the PPPoE packet. This Tag contains Circuit ID and Remote ID.

- Circuit ID: is padded with the VLAN ID, interface ID, and host name of request packets at the RX client.
- Remote ID: is padded with the MAC address of the client or the switch.

Configuring Circuit ID

The Circuit ID has 2 padding modes: Switch mode and ONU mode. By default, Switch mode is adopted. In ONU mode, the Circuit ID has a fixed format. The following commands are used to configure the padding contents of the Circuit ID in Switch mode.

In switch mode, the Circuit ID supports 2 padding modes:

- Default mode: when customized Circuit ID is not configured, the padding content is the VLAN ID, interface ID, or the attached string. If the attached string is not defined, it is configured to hostname by default.
- Customized mode: when customized Circuit ID is configured, the padding content is the Circuit IS string.

Configure the Circuit ID for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#pppoeagent circuit-id mode { onu | switch }`	Configure the padding mode of the Circuit ID.
3	`Raisecom(config)#pppoeagent circuit-id { attach-string | format | hex } string`	(Optional) configure the attached string of the Circuit ID. The Circuit ID contains a string of hostname, which can be configured though this command.
4	`Raisecom(config)#pppoeagent circuit-id mac-format string`	(Optional) configure the format of the MAC address which is a variable in the Circuit ID.
5	`Raisecom(config)#interface port port-id`	Enter physical layer interface configuration mode.
6	`Raisecom(config-port)#pppoeagent circuit-id string`	(Optional) configure the Circuit ID to the customized string.

The Circuit ID in default format contains an attached string which is the hostname of the ISCOM21xx by default and also can be customized.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#pppoeagent circuit-id attach-string string`	(Optional) configure the attached string of the Circuit ID. This command can add customized information to the Circuit ID if it is in default format.

Configuring Remote ID

The Remote ID is padded with a MAC address of the switch or a client. In addition, you can specify the form (binary/ASCII) of the MAC address.

Configure the Remote ID for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface port port-id`	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#pppoeagent remote-id { client-mac | switch-mac }`	(Optional) configure PPPoE+ Remote ID to be padded with the MAC address.

Step	Command	Description
4	`Raisecom(config-port)#pppoeagent remote-id format { ascii | binary }`	(Optional) configure the padding modes of the PPPoE+ Remote ID.

Configuring Tag overriding

Tags of some fields may be forged by the client because of some reasons. The client overrides the original Tags. After Tag overriding is enabled, if the PPPoE packets contain Tags, these Tags are overridden. If not, add Tags to these PPPoE packets.

Configure Tag overriding for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface port port-id`	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#pppoeagent vendor-specific-tag overwrite enable`	Enable Tag overriding.

7.10.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show pppoeagent [ port-list port-list ]`	Show PPPoE+ configurations.
2	`Raisecom#show pppoeagent statistic [ port-list port-list ]`	Show PPPoE+ statistics.

7.10.7 Maintenance

Maintain the ISCOM21xx as below.

Command	Description
`Raisecom(config)#clear pppoeagent statistic [ port-list port-list ]`	Clear PPPoE+ statistics.

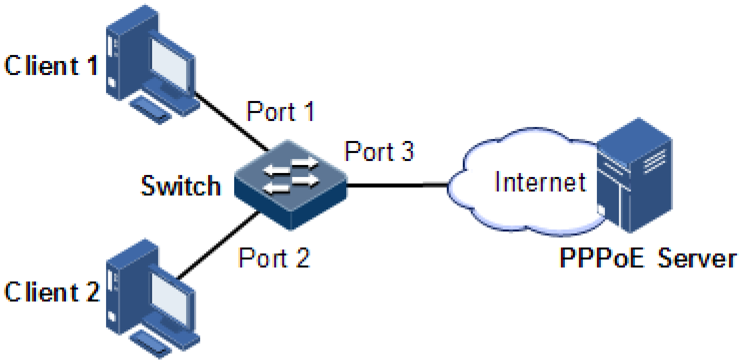
7.10.8 Example for configuring PPPoE+

Networking requirements

As shown in Figure 7-12, to prevent illegal access during PPPoE authentication and to control and monitor users, you need to configure PPPoE+ on the Switch.

- Port 1 and Port 2 are connected to Client 1 and Client 2 respectively. Port 3 is connected to the PPPoE server.
- Enable global PPPoE+ and enable PPPoE+ on Port 1 and Port 2. Configure Port 3 to the trusted interface.
- Configure the attached string of the Circuit ID to raisecom. Configure the padding content of the Circuit ID on Port 1 to user01. Configure the padding content of the Remote ID on Port 2 to the MAC address of the client. The padding contents are in ASCII mode.
- Enable Tag overriding on Port 1 and Port 2.

Figure 7-12 PPPoE+ networking



Configuration steps

Step 1 Configure Port 3 to the trusted interface.

```
Raisecom#config
Raisecom(config)#interface port 3
Raisecom(config-port)#pppoeagent trust
Raisecom(config-port)#exit
```

Step 2 Configure packet information about Port 1 and Port 2.

```
Raisecom(config)#pppoeagent circuit-id attach-string raisecom
Raisecom(config)#interface port 1
Raisecom(config-port)#pppoeagent circuit-id user01
Raisecom(config-port)#exit
Raisecom(config-port)#interface port 2
Raisecom(config-port)#pppoeagent remote-id client-mac
Raisecom(config-port)#pppoeagent remote-id format ascii
Raisecom(config-port)#exit
```

Step 3 Enable Tag overriding on Port 1 and Port 2.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#pppoeagent vendor-specific-tag overwrite enable
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#pppoeagent vendor-specific-tag overwrite enable
Raisecom(config-port)#exit
```

Step 4 Enable PPPoE+ on Port 1 and Port 2.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#pppoeagent enable
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#pppoeagent enable
```

Checking results

Use the **show pppoeagent** [**port-list** *port-list*] command to show PPPoE+ configurations.

```
Raisecom#show pppoeagent port-list 1-3
Attach-string: raisecom
Circuit ID padding mode: switch
Port   Enable Trust-port  Overwrite  Remote-ID   Format-rules  Circuit-ID
----------------------------------------------------------------
1     enable    no      enable   switch-mac   binary        user01
2     enable    no      enable    client-mac   ascii        %default%
3    disable   yes      disable   switch-mac   binary      %default%
**In switch mode, Circuit-ID's default string is: Port\Vlan\Attach-string.
**In onu mode, Circuit-ID's default string is: 0 0/0/0:0.0
0/0/0/0/0/0/MAC 0/0/Port:eth/4096.CVLAN LN.
**Attach-string's default string is the hostname.
```

7.11 Loop detection

7.11.1 Introduction

Loop detection can address the influence on network caused by a loopback, providing the self-detection, fault-tolerance and robustness.

Procedures for loop detection are as below:

Step 1 All interfaces on the ISCOM21xx send the LoopBack-Detection packet periodically (the period can be configured. By default, the interval is 4 seconds).

Step 2 The ISCOM21xx checks the source MAC field of the received packet. If the MAC address of the ISCOM21xx is saved in the source MAC field, it is believed that a loop is detected on an interface of the ISCOM21xx. Otherwise, the packet is discarded.

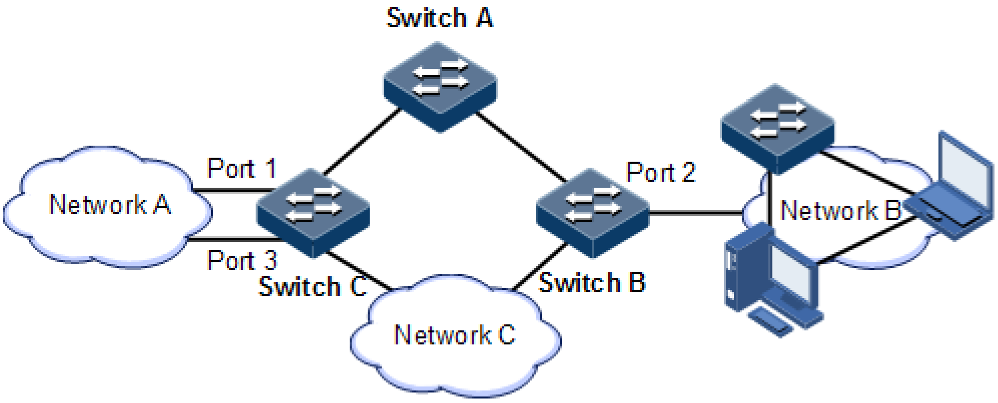
- If the Tx interface ID and Rx interface ID of a packet are identical, the interface will be shut down.
- If the Tx interface ID and Rx interface ID of a packet are different, the interface with a greater interface ID will be shut down and the interface with a smaller interface ID is kept in Up status.

Common loop types are self-loop, internal loop and external loop.

As shown in Figure 7-13, Switch B and Switch C, as edge switches, connect the user network.

- Self-loop: a loop on the same Ethernet interface of the same device. User network B has a loop, which forms a self-loop.
- Internal loop: a loop forming on different Ethernet interfaces of the same device. Fastethernet 1/3/1 and Fastethernet 1/3/3 on Switch C forms an internal loop with the user network A.
- External loop: a loop forming on the Ethernet interface of different devices. Switch A, Switch B, and Switch C form an external loop with user network C.

Figure 7-13 Loop detection networking



In Figure 7-13, assume that both Switch B and Switch connect user network interfaces enabled with loop detection. Loop detection mechanisms for the three types of loops are as below:

- Self-loop: the Rx interface ID and Tx interface ID of the packet on Switch B are the same, so shut down interface 2 to remove the self-loop.
- Internal loop: Switch C receives the loop detection packet sent by it and the Rx interface ID and Tx interface ID of the packet are different, so shut down interface 3 with a greater interface ID to remove the internal loop.
- External loop: Switch B and Switch C receive the loop detection packet from each other. Generally, loop detection does not process the external loop. As a result, Switch B and Switch C send Trap alarms only without blocking any interface. However, you can block one of the interfaces manually, such as the one with a greater MAC address to remove the external loop.

7.11.2 Preparing for configurations

Scenario

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

Prerequisite

Connect the interface and configure its physical parameters to make it Up.

7.11.3 Default configurations of loop detection

Default configurations of loop detection are as below.

Function	Default value
Interface loop detection status	Disable
Automatic recovery time for the blocked interface	No automatic recovery
Loop process mode of loop detection	Trap-only
Loop detection period	4s
Loop detection mode	VLAN
Time for recovering the block interface due to loop detection	Infinite
Loop detection VLAN	VLAN 1

7.11.4 Configuring loop detection

Note

- Loop detection function and STP are exclusive, only one can be enabled at one time.
- The directly connected device cannot be enabled with loop detection at both ends simultaneously; otherwise the interfaces at both ends will be blocked.

Configure loop detection for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**loopback-detection** { **enable** | **disable** } **port-list** *port-list*	Enable loop detection on the interface.

Step	Command	Description
3	Raisecom(config)#**loopback-detectiondestination-address** *mac-address*	(Optional) configure the destination MAC address of loop detection packets. Note Loop detection in the entire topology must be configured the same; otherwise, loop detection may fail.
4	Raisecom(config)#**loopback-detection vlan** *vlan-id*	(Optional) configure the VLAN for loop detection.
5	Raisecom(config)#**loopback-detection hello-time** *period*	Configure the period for sending loop detection packets.
6	Raisecom(config)#**loopback-detection error-device** { **discarding** | **trap-only** } **port-list** *port-list*	(Optional) configure process mode when the interface receives loop detection message from other devices.
7	Raisecom(config)#**loopback-detection down-time** { *time-value* | **trap-only** | **infinite** }	(Optional) configure the time for automatically recover the blocked interface due to loop detection.
8	Raisecom(config)#**interface port** *port-id* Raisecom(config-port)#**no loopback-detection discarding**	Enable the interface blocked due to loop detection.

7.11.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show loopback-detection port-list** *port-list*	Show interface loop detection configuration.
2	Raisecom#**show loopback-detection statistics port-list** *port-list*	Show statistics of loop detection.

7.11.6 Maintenance

Maintain the ISCOM21xx by below commands.

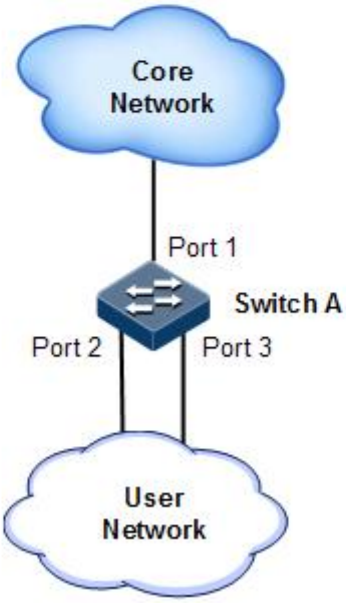
Command	Description
Raisecom(config-port)#**clear loopback-detection statistic**	Clear loop detection statistics.

7.11.7 Example for configuring loop detection

Networking requirements

As shown in Figure 7-14, Port 1 on Switch A is connected to the core network; Port 2 and Port 3 on Switch A are connected to the user network. There is loop in user network. There is a loop on the user network. Enable loop detection on Switch A to detect the loop on user network, and then block the related port.

Figure 7-14 Configuring loop detection



Configuration steps

Step 1 Create VLAN 3, and add Port 2 and Port 3 into VLAN 3.

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

Step 2 Enable loop detection on the specified interface.

```
Raisecom(config)#loopback-detection enable port-list 2-3
Raisecom(config)#loopback-detection vlan 3
Raisecom(config)#loopback-detection hello-time 3
```

Checking configurations

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

```
Raisecom#show loopback-detection port-list 2-3
Destination address: FFFF.FFFF.FFFF
VLAN:3
Period of loopback-detection:3s
Restore time:infinite
Port State Status exloop-act  Last      Last-Occur     Open-Time      vlan
                              Loop-with  (ago)         (ago)
--------------------------------------------------------------------------
2      Ena   no    trap-only   --        --          --            --
3      Ena   no    trap-only   --        --          --            --
```

7.12 Line detection

7.12.1 Introduction

Line detection is a module to detect physical lines and provides you with status query function, so it can help you analyze fault source and maintain the network.

7.12.2 Preparing for configurations

Scenario

With this function, you can query status of physical lines between devices, analyze faults, and thus maintain the network.

Prerequisite

N/A

7.12.3 Configuring line detection

Configure line detection for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**test cable-diagnostics port-list** { **all** | *port-list* }	Detect physical link status.

7.12.4 Checking configurations

Use the following command to check configuration result.

No.	Command	Description
1	`Raisecom#show cable-diagnostics port-list { all	port-list }`	Show information about line detection.

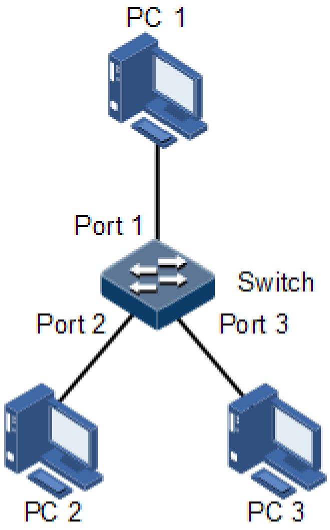
7.12.5 Example for configuring line detection

Networking requirements

As shown in Figure 7-15, to help you analyze fault source, conduct line detection on the Switch.

No line detection is done before.

Figure 7-15 Line detection networking



Configuration steps

Conduct line detection on Ports 1–3 on the ISCOM21xx.

```
Raisecom#test cable-diagnostics port-list 1-3
```

Checking results

Use the **show cable-diagnostics port-list** [**all** | *port-list*] command to show configurations of line detection on the interface.

```
Raisecom#show cable-diagnostics port-list 1-2
Port  Attribute     Time        RX Stat  RX Len(m)  TX Stat  TX Len(m) ----
------------------------------------------------------------------
```

```
1    Issued   01/09/2011 08:13:03  Normal     0       Normal     0
2    Issued   01/09/2011 08:13:03  Normal     0       Normal      0
```

Remove the line that connects PC 1 and the ISCOM21xx from the PC 1, and conduct line detection again. Use the **show cable-diagnostics port-list** [**all** | *port-list*] command again to show configurations of line detection on the interface.

```
Raisecom#show cable-diagnostics port-list 1-2
Port  Attribute      Time        RX Stat   RX Len(m)   TX Stat   TX Len(m)
----------------------------------------------------------------------
1    Issued   01/09/2011 08:18:09  Open       3       Open       3
2    Issued   01/09/2011 08:18:09  Normal     0       Normal      0
```

8 Reliability

This chapter describes basic principles and configuration procedures of reliability and provides related configuration examples.

- Link aggregation
- Interface backup
- Link-state tracking
- STP
- MSTP
- ERPS
- RRPS

8.1 Link aggregation

8.1.1 Introduction

With link aggregation, multiple physical Ethernet interfaces are combined to form a Logical Aggregation Group (LAG). Multiple physical links in one LAG are taken as a logical link. The link aggregation helps share traffics among members in an LAG. Besides effectively improving reliability on links between devices, link aggregation helps gain higher bandwidth without upgrading hardware.

Generally, the link aggregation consists of manual link aggregation, static Link Aggregation Control Protocol (LACP) link aggregation, and dynamic LACP link aggregation.

- Manual link aggregation

Manual link aggregation refers to a process that multiple physical interfaces are aggregated to a logical interface. Links under a logical interface share loads.

- Static LACP link aggregation

Link Aggregation Control Protocol (LACP) is a protocol based on IEEE802.3ad. LACP communicates with the peer through the Link Aggregation Control Protocol Data Unit (LACPDU). In addition, you should manually configure the LAG. After LACP is enabled on an interface, the interface sends a LACPDU to inform the peer of its system LACP protocol priority, system MAC address, interface LACP priority, interface ID, and operation Key.

After receiving the LACPDU, the peer compares its information with the one received by other interfaces to select a selected interface. Therefore, the interface and the peer are in the same Selected state. The operation key is a configuration combination automatically generated based on configurations of the interface, such as the speed, duplex mode, and Up/Down status. In a LAG, interfaces in the Selected state share the identical operation key.

- Dynamic LACP link aggregation

In dynamic LACP link aggregation, the system automatically creates and deletes the LAG and member interfaces through LACP. Interfaces cannot be automatically aggregated into a group unless their basic configurations, speeds, duplex modes, connected devices, and the peer interfaces are identical.

In manual aggregation mode, all member interfaces are in forwarding state, sharing loads. In static/dynamic LACP mode, there are backup links.

Link aggregation is the most widely used and simplest Ethernet reliability technology.

Note

The ISCOM21xx supports manual and static link aggregation only.

8.1.2 Preparing for configurations

Scenario

To provide higher bandwidth and reliability for a link between two devices, configure link aggregation.

With link aggregation, multiple physical Ethernet interface are added into a LAG and are aggregated to a logical link. Link aggregation helps share uplink and downlink traffic among members in one LAG. Therefore, the link aggregation helps obtain higher bandwidth and helps members in one LAG back up data for each other, which improves reliability of Ethernet connection.

Prerequisite

Connect the interface and configure its physical parameters to make it Up.

8.1.3 Default configurations of link aggregation

Default configurations of link aggregation are as below.

Function	Default value
Link aggregation	Enable
Load balancing mode	Sxordmac
LAG	Existing, in manual mode
LACP system priority	32768
LACP interface priority	LACP priority without specifying interface
Interface dynamic LACP link aggregation	Disable

8.1.4 Configuring manual link aggregation

Configure manual link aggregation for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**trunk group** *group-id* **port** *port-list*	Configure LAG.
3	Raisecom(config)#**trunk enable**	Enable LAG.
4	Raisecom(config)#**trunk loading-sharing mode** { **dip** | **dmac** | **sip** |**smac** | **sxordip** | **sxordmac** }	(Optional) configure load sharing mode for link aggregation.

Note

In the same LAG, member interfaces that share loads must be identically configured. These configurations include QoS, QinQ, VLAN, interface properties, and MAC address learning.

- QoS: traffic policing, rate limit, SP queue, WRR queue scheduling, interface priority and interface trust mode
- QinQ: QinQ enabling/disabling 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 or Access) on the interface, subnet VLAN configurations, protocol VLAN configurations, and whether VLAN packets carry Tag
- Port properties: whether the interface is added to the isolation group, interface rate, duplex mode, and link Up/Down status
- MAC address learning: whether enabling the MAC address learning, and whether the MAC address limit is configured on the interface

8.1.5 Configuring static LACP link aggregation

Configure static LACP link aggregation for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**lacp system-priority** *system-priority*	(Optional) configure system LACP priority. The higher priority end is active end. LACP chooses active and backup interfaces according to the active end configuration. The smaller the number is, the higher the priority is. The smaller system MAC address device will be chosen as active end if devices system LACP priorities are identical.
3	Raisecom(config)#**lacp timeout** { **fast** | **slow** }	Configure LACP timeout mode.

Step	Command	Description
4	`Raisecom(config)#trunk group group-id port port-list [ lacp-static ]`	Create a static LACP LAG.
5	`Raisecom(config)#interface port port-id`	(Optional) enter physical layer interface configuration mode.
6	`Raisecom(config-port)#lacp port-priority port-priority`	(Optional) configure LACP priority on the interface. It affects electing the default interface of LACP. The smaller the value is, the higher the priority is.
7	`Raisecom(config-port)#lacp mode { active | passive }`	(Optional) configure LACP mode for member interfaces. If both two ends of a link are in passive mode, LACP connection cannot be established.
8	`Raisecom(config-port)#exit`	Return to global configuration mode.
9	`Raisecom(config)#trunk enable`	Enable LAG.
10	`Raisecom(config)#trunk loading-sharing mode { dip | dmac | sip |smac | sxordip | sxordmac }`	(Optional) configure load sharing mode for the aggregation link.
11	`Raisecom(config)#trunk group group-id min-active links threshold`	(Optional) configure the minimum number of active links in LACP LAG.

Note

- The interface in static LACP LAG can be in active or standby status. Both the active interface and standby interface can receive/send LACP packets, but the standby interface cannot send client packets.
- The system chooses default interface in the order of neighbor discovery, interface maximum speed, interface highest LACP priority, and interface minimum ID. The interface is in active status by default, the interface with identical speed, identical peer and identical device operation key is also in active status; other interfaces are in standby status.

8.1.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show lacp internal`	Show local LACP interface status, Tag, interface priority, administration key, operation key, and interface status machine status.

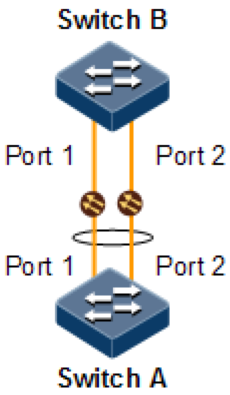
No.	Command	Description
2	`Raisecom#show lacp neighbor`	Show the peer LACP information, including Tag, interface priority, device ID, Age, operation key value, interface ID, and interface status machine status.
3	`Raisecom#show lacp statistics`	Show interface LACP statistics, including total number of received/sent LACP packets, the number of received/sent Marker packets, the number of received/sent Marker Response packets, the number of errored Marker Response packets.
4	`Raisecom#show lacp sys-id`	Show global LACP enabling status of the local system, device ID, including system LACP priority and system MAC address.
5	`Raisecom#show trunk`	Show configurations of all LAGs.

8.1.7 Example for configuring manual link aggregation

Networking requirements

As shown in Figure 8-1, to improve link reliability between Switch A and Switch B, you need to configure manual link aggregation for the two devices. Add Port 1 and Port 2 into the LAG to build up a unique logical interface. The LAG conducts load sharing according to the source MAC address.

Figure 8-1 Manual link aggregation networking



Configuration steps

Step 1 Create a manual LAG.

Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#trunk group 1 port 1-2
```

Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#trunk group 1 port 1-2
```

Step 2 Configure the load sharing mode for aggregated links.

Configure Switch A.

```
SwitchA(config)#trunk loading-sharing mode smac
```

Configure Switch B.

```
SwitchB(config)#trunk loading-sharing mode g smac
```

Step 3 Enable link aggregation.

Configure Switch A.

```
SwitchA(config)#trunk enable
```

Configure Switch B.

```
SwitchB(config)#trunk enable
```

Checking results

Use the **show trunk** command to show global configurations of manual link aggregation.

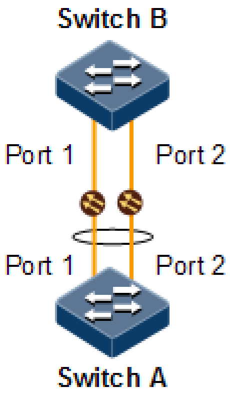
```
SwitchA#show trunk
Trunk: Enable
Loading sharing mode: SMAC
Trunk Group Mode  Member Ports         Efficient Ports
-----------------------------------------------------------
1         manual 1,2                       1,2
```

8.1.8 Example for configuring static LACP link aggregation

Networking requirements

As shown in Figure 8-2, to improve link reliability between Switch A and Switch B, you can configure a static LACP link aggregation between these 2 devices. Add Port 1 and Port 2 into one LAG, where Port 1 is used as the working line and Port 2 is the protection line.

Figure 8-2 Static LACP link aggregation networking



Configuration steps

Step 1 Configure the static LACP LAG on Switch A and configure Switch A to the active end.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#truck group 1 port 1-2 lacp-static
SwitchA(config)#lacp system-priority 1000
SwitchA(config)#trunk group 1 min-active links 1
SwitchA(config)#interface port 1
SwitchA(config-port)#lacp port-priority 1000
SwitchA(config-port)#exit
SwitchA(config)#trunk enable
```

Step 2 Configure the static LACP LAG on Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#truck group 1 port 1-2 lacp-static
SwitchB(config)#lacp system-priority 1000
SwitchB(config)#trunk enable
```

Checking results

Use the **show trunk** command to show global configurations of static LACP link aggregation on Switch A.

```
SwitchA#show trunk
Trunk: Enable
Loading sharing mode: SMAC
Trunk Group Mode  Member Ports         Efficient Ports
-----------------------------------------------------------
1         static 1,2                --
```

Use the **show lacp internal** command to show local system LACP interface state, flag, interface priority, administration key, operation key, and interface state machine state on Switch A.

```
SwitchA#show lacp internal
Flags:
      S - Device is requesting Slow LACPDUs
      F - Device is requesting Fast LACPDUs
      A - Device is in Active mode
      P - Device is in Passive mode
Port State     Flags Port-Pri  Admin-key Oper-key Port-State
---------------------------------------------------------------------
1    down      FA    1000      0x1      0x1     0xF
2    down      FA    32768     0x1      0x1     0xF
```

Use the **show lacp neighbor** command to show peer system LACP interface state, flag, interface priority, administration key, operation key, and interface state machine state on Switch A.

8.2 Interface backup

8.2.1 Introduction

In dual uplink networking, Spanning Tree Protocol (STP) is used to block the redundancy link and implements backup. Though STP can meet users' backup requirements, but it fails to meet switching requirements. Though Rapid Spanning Tree Protocol (RSTP) is used, the convergence is second level only. This is not a satisfying performance parameter for high-end Ethernet switch which is applied to the Carrier-grade network core.

Interface backup, targeted for dual uplink networking, implements redundancy backup and quick switching through working and protection lines. It ensures performance and simplifies configurations.

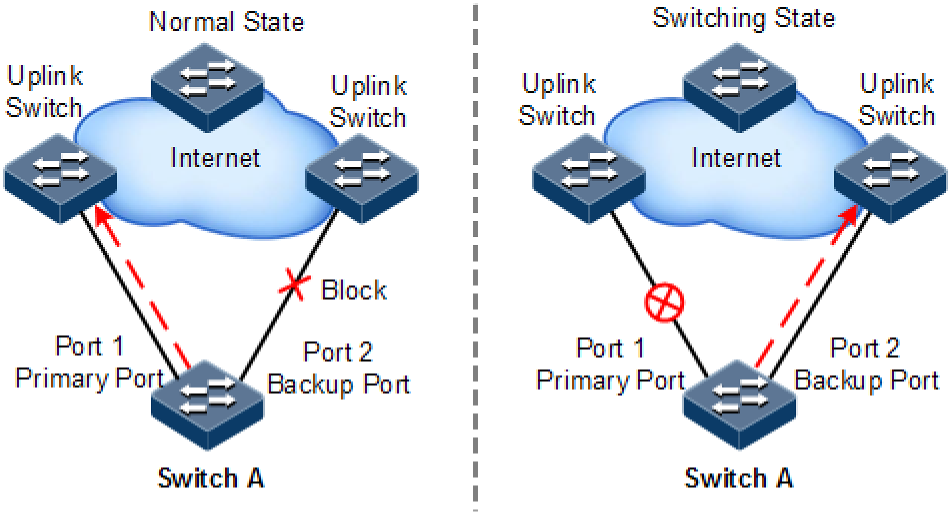
Interface backup is another solution of STP. When STP is disabled, you can realize basic link redundancy by manually configuring interfaces. If the switch is enabled with STP, you should disable interface backup because STP has provided similar functions.

Principle

Interface backup is implemented by configuring the interface backup group. Each interface backup group contains a primary interface and a backup interface. The link, where the primary interface is, is called a primary link while the link, where the backup interface is, is called the backup interface. Member interfaces in the interface backup group supports physical interfaces and LAGs. However, they do not support Layer 3 interfaces.

In the interface backup group, when an interface is in Up status, the other interface is in Standby statue. At any time, only one interface is in Up status. When the Up interface fails, the Standby interface is switched to the Up status.

Figure 8-3 Principles of interface backup



As shown in Figure 8-3, Port 1 and Port 2 on Switch A are connected to their upstream devices respectively. The interface forwarding states are shown as below:

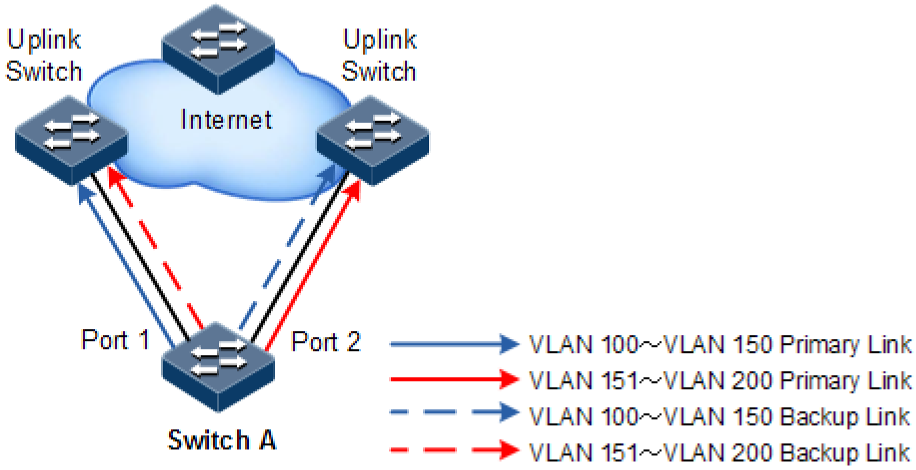
- Under normal conditions, Port 1 is the primary interface while Port 2 is the backup interface. Port 1 and the upstream device forward packet while Port 2 and the upstream device do not forward packets.
- When the link between Port 1 and its upstream device fails, the backup Port 2 and its upstream device forward packets.
- When Port 1 restores normally and keeps Up for a period (restore-delay), Port 1 restores to forward packets and Port 2 restores standby status.

When a switching between the primary interface and the backup interface occurs, the switch sends a Trap to the NView NNM system.

Application of interface backup in different VLANs

By applying interface backup to different VLANs, you can enable two interfaces to share service load in different VLANs, as shown in Figure 8-4.

Figure 8-4 Application of interface backup in different VLANs


Uplink Switch
Internet
Uplink Switch
Port 1
Port 2
Switch A
VLAN 100~VLAN 150 Primary Link
VLAN 151~VLAN 200 Primary Link
VLAN 100~VLAN 150 Backup Link
VLAN 151~VLAN 200 Backup Link

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

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

Interface backup is used share service load in different VLANs without depending on configurations of uplink switches, thus facilitating users' operation.

8.2.2 Preparing for configurations

Scenario

When STP is disabled, by configuring interface backup, you can realize redundancy backup and fast switching of primary/backup link, and load sharing between different interfaces.

Compared with STP, interface backup not only ensures millisecond level fast switching, also simplifies configurations.

Prerequisite

- Create VLANs.
- Add interfaces to VLANs.
- Disable STP.

8.2.3 Default configurations of interface backup

Default configurations of interface backup are as below.

Function	Default value
Interface backup group	N/A
Restore-delay	15s
Restoration mode	Interface connection mode (port-up)

8.2.4 Configuring basic functions of interface backup

Configure basic functions of interface backup for the ISCOM21xx as below.

Caution

Interface backup and STP, loop detection, Ethernet ring, or ELPS, and ERPS may interfere with each other. Configuring both of them on an interface is not recommended.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#`**`switchport backup port`** *`port-id`* [**`vlanlist`** *`vlan-list`*]	Configure the interface backup group.
4	`Raisecom(config-port)#`**`exit`**	Return to global configuration mode.
5	`Raisecom(config)#`**`switchport backup restore-delay`** *`period`*	(Optional) configure the restore-delay period.
6	`Raisecom(config)#`**`switchport backup restore-mode`** { **`disable`** | **`neighbor-discover`** | **`port-up`** }	(Optional) configure restoration mode.

Note

- In an interface backup group, an interface is either a primary interface or a backup interface.
- In a VLAN, an interface or a LAG cannot be a member of two interface backup groups simultaneously.
- If you configure a LAG as a member of interface backup group, you need to configure the member with the minimum interface ID in the LAG as the member. When the member is in Up status, this indicates that the LAG has a Up interface. When the member is in Down status, this indicates that all interfaces in the LAG are Down.

8.2.5 (Optional) configuring FS on interfaces

Caution

- After FS is successfully configured, the primary/backup link will be switched; namely, the working line is switched to the backup link (without considering Up/Down status of the primary/backup interface). For example, when both the primary interface and backup interface are in Up status, the primary link transmits data. In this situation, if you perform forcible switchover, the working line changes from the primary link to the backup link.
- In the FS command, the backup interface ID is optional. If the primary interface is configured with multiple interface backup groups, you should input the backup interface ID.

Configure FS on interfaces for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**switchport backup** [**port** *port-id*] **force-switch**	Configure FS on the interface.

8.2.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show switchport backup**	Show related status information of interface backup, including restoration delay time, restoration mode, and interface backup groups.

8.2.7 Example for configuring interface backup

Networking requirements

When only link aggregation is configured, all VLAN data comes from only one interface, where packet discarding occurs and services are impacted. In this situation, you can configure two LAGs to sharing VLAN data to two interfaces so that load balancing can work and the protection feature of LAGs can be inherited.

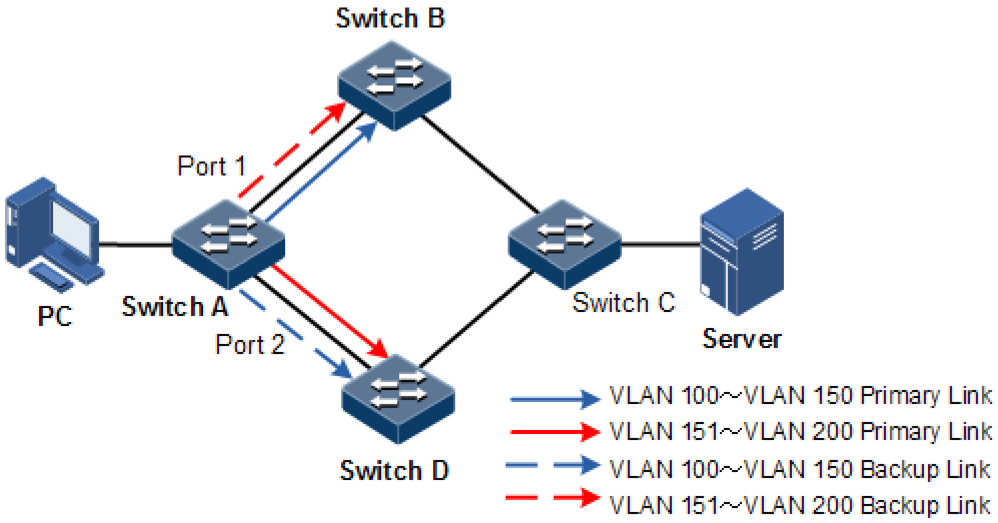
As shown in Figure 8-5, the PC accesses the server through switches. To realize a reliable remote access from the PC to the server, configure an interface backup group on Switch A and specify the VLAN list so that the two interfaces concurrently forward services in different VLANs and share load. Configure Switch A as below:

- Switch A is in VLANs 100–150. Port 1 is the primary interface and Port 2 is the backup interface.
- Switch A is in VLANs 151–200. Port 2 is the primary interface and Port 1 is the backup interface.

When Port 1 or its link fails, the system switches to the backup Port 2 to resume the link.

Switch A should support interface backup while Switch B, Switch C, and Switch D do not need to support interface backup.

Figure 8-5 Interface backup networking


Switch B
Port 1
PC
Switch A
Port 2
Switch C
Server
Switch D
VLAN 100~VLAN 150 Primary Link
VLAN 151~VLAN 200 Primary Link
VLAN 100~VLAN 150 Backup Link
VLAN 151~VLAN 200 Backup Link

Configuration steps

Step 1 Create VLANs 100–200 and add Port 1 and Port 2 to VLANs 100–200.

```
Raisecom#config
Raisecom(config)#create vlan 100-200 active
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 100-200 confirm
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport mode trunk
Raisecom(config-port)#switchport trunk allowed vlan 100-200 confirm
Raisecom(config-port)#exit
```

Step 2 Configure Port 1 to the primary interface and configure Port 2 to the backup interface in VLANs 100–150.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#switchport backup port 2 vlanlist 100-150
Raisecom(config-port)#exit
```

Step 3 Configure Port 2 to the primary interface and configure Port 1 to the backup interface in VLANs 151–200.

```
Raisecom(config)#interface port 2
Raisecom(config-port)#switchport backup port 1 vlanlist 151-200
```

Checking results

Use the **show switchport backup** command to view status of interface backup under normal or faulty conditions.

When both Port 1 and Port 2 are Up, Port 1 forwards traffic of VLANs 100–150, and Port 2 forwards traffic of VLANs 151–200.

```
Raisecom#show switchport backup
Restore delay: 15s.
Restore mode: port-up.
Active Port(State)    Backup Port(State)    Vlanlist
-------------------------------------------------------
1      (Up)           2   (Standby)    100-150
2      (Up)           1   (Standby)    151-200
```

Manually disconnect the link between Switch A and Switch B to emulate a fault. Then, Port 1 becomes Down, and Port 2 forwards traffic of VLANs 100–200.

```
Raisecom#show switchport backup
Restore delay: 15s
Restore mode: port-up
Active Port(State)   Backup Port(State)   Vlanlist
---------------------------------------------------------------
1 (Down)        2    (Up)            100-150
2 (Up)         1    (Down)           151-200
```

When Port 1 resumes and keeps Up for 15s (restore-delay), it forwards traffic of VLANs 100–150 while Port 2 forwards traffic of VLANs 151–200.

8.3 Link-state tracking

8.3.1 Introduction

Link-state tracking is used to provide port linkage scheme for specific application and it can extend range of link backup. By monitoring uplinks and synchronizing downlinks, you can add uplink and downlink interfaces to a link-state group. Therefore, faults of upstream devices can be informed to the downstream devices to trigger switching. Link-state tracking can be used to prevent traffic loss due to uplink failure.

Once all uplink interfaces fail, down link interfaces are in Down status. When at least one uplink interface recovers, downlink interface recovers to Up status. Therefore, faults of upstream devices can be informed to the downstream devices immediately. Uplink interfaces are not influenced when downlink interfaces fail.

8.3.2 Preparing for configurations

Scenario

When uplink fails, traffic cannot switch to the standby link if it cannot notify downstream devices in time, and then traffic will be broken.

Link-state tracking can be used to add downlink interfaces and uplink interfaces of the middle device to a link-state group and monitor uplink interfaces. When all uplink interfaces fails, faults of upstream devices can be informed to the downstream devices to trigger switching.

Prerequisite

Connect the interface and configure its physical parameters to make it Up.

8.3.3 Default configurations of link-state tracking

Default configurations of link-state tracking are as below.

Function	Default value
Failover group	N/A

8.3.4 Configuring link-state tracking

Configure link-state tracking for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**link-state-tracking group** *group-number* { **upstream cfm-mepid** *mep-id* }	Create the link-state group and enable link-state tracking.
3	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#**link-state-tracking group** *group-number* { **downstream** | **upstream** }	Configure the link-state group of the interface and interface type. One interface can only belong to one link-state group and can be either the uplink interface or downlink interface. When the link-state group is configured with CFM network or G.8031 network in uplink, the interface can be configured to downlink interface only.

Note

- One link-state group can contain several uplink interfaces. Link-state tracking will not be performed when at least one uplink interface is Up. Only when all uplink interfaces are Down, link-state tracking occurs.
- In global configuration mode, use the **no link-state-tracking group** *group-number* command to disable link-state tracking. The link-state group will be deleted if there is no interface in it.
- Use the **no link-state-tracking group** command to delete an interface from the link-state group in physical layer interface configuration mode. If there is no other interface and link-state tracking is disabled, the link-state group will be deleted when the interface is deleted.

8.3.5 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	Raisecom#**show link-state-tracking group** *group-number*	Show configurations and status of the link-state group.
2	Raisecom#**show link-admin-status port** *port-list*	Show interface Up/Down status configured on each functional module on the interface.

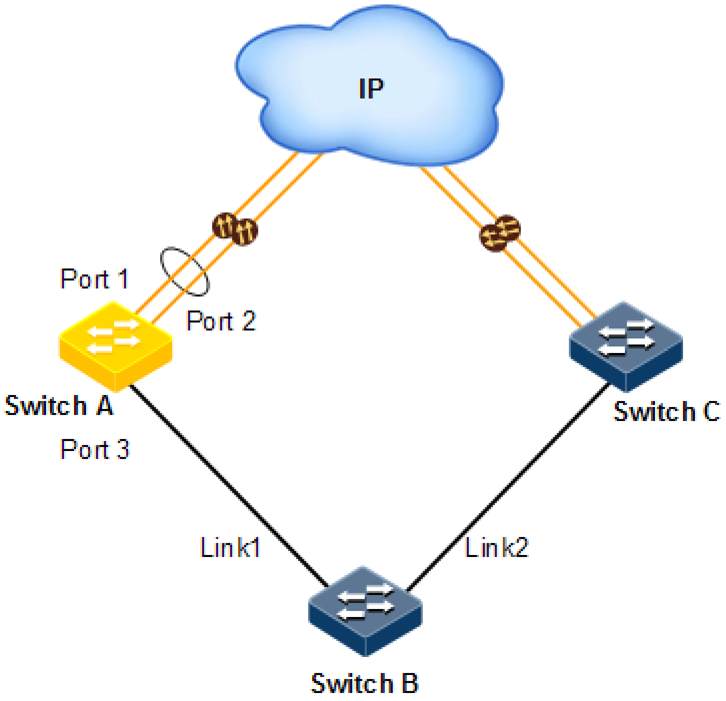
8.3.6 Example for configuring link-state tracking

Networking requirements

As shown in Figure 8-6, to improve network reliability, Link 1 and Link 2 of Switch B are connected to Switch A and Switch C respectively. Link 1 is the primary link and Link 2 is the standby link. Link 2 will not be used to forward data until Link 1 is fault.

Switch A and Switch C are connected to the uplink network in link aggregation mode. When all uplink interfaces on Switch A and Switch C fails, Switch B needs to sense fault in time switches traffic to the standby link. Therefore, you should deploy link-state tracking on Switch A and Switch C.

Figure 8-6 Link-state tracking networking



Configuration steps

Step 1 Configure link-state tracking on Switch A.

Create the link-state group.

```
Raisecom#config
Raisecom(config)#link-state-tracking group 1
```

Add uplink interfaces to the link-state group.

```
Raisecom(config)#interface port 1
Raisecom(config-port)#link-state-tracking group 1 upstream
Raisecom(config-port)#exit
Raisecom(config)#interface port 2
Raisecom(config-port)#link-state-tracking group 1 upstream
Raisecom(config-port)#exit
```

Add downlink interfaces to the link-state group.

```
Raisecom(config)#interface port 3
Raisecom(config-port)#link-state-tracking group 1 downstream
```

Step 2 Configure link-state tracking on Switch C.

Configurations are identical to the ones on Switch A.

Checking results

Take configurations on Switch A for example.

Use the **show link-state-tracking group** command to show configurations of the link-state group.

```
SwitchA#show link-state-tracking group 1
Link State Tracking Group: 1 (Enable)
Status:  Normal
Fault type:  None
Upsteam Mep: --
Upstream Interfaces:
  Port 1(Up)  Port 2(Up)
Downstream Interfaces:
  Port 3(Up)
```

Use the **show link-state-tracking group** command to show configurations of the link-state group after all uplinks of Switch A fails. In this case, you can learn that downlink Port 3 is disabled.

```
SwitchA#show link-state-tracking group 1
Link State Tracking Group: 1 (Enable)
Status:  Failover
Fault type:  Port-down
Upsteam Mep: --
Upstream Interfaces:
   Port 1(Down)   Port 2(Down)
Downstream Interfaces:
   Port 3(Disable)
```

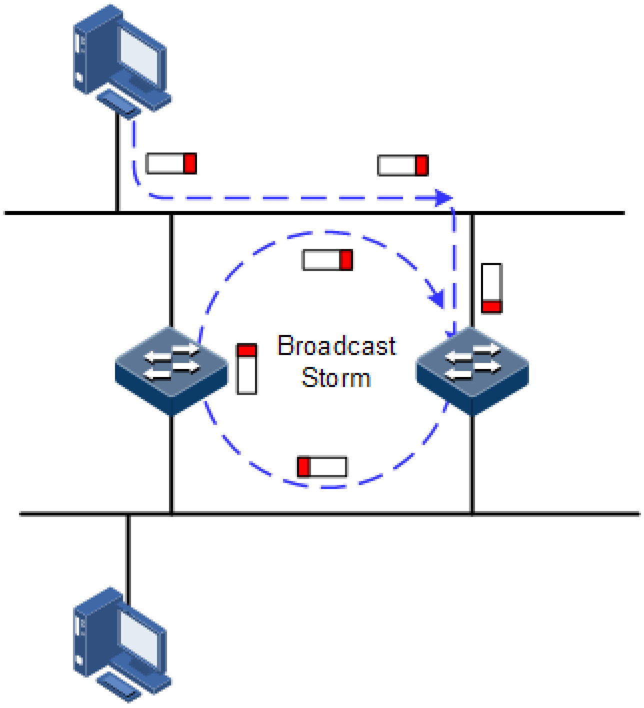
8.4 STP

8.4.1 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. The network storm caused by the loop is shown in Figure 8-7.

Figure 8-7 Network storm due to loop

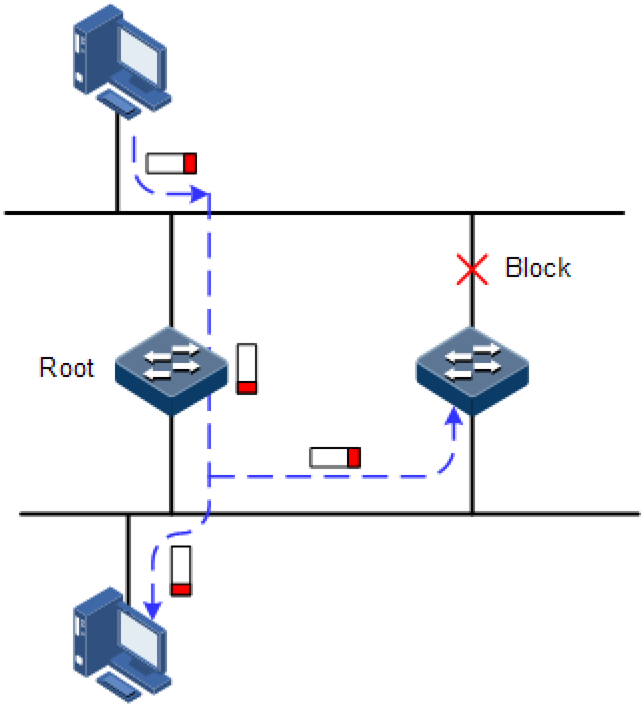


Spanning Tree Protocol (STP) is compliant to IEEE 802.1d standard and used to remove data physical loop in data link layer in LAN.

The ISCOM21xx running STP can process Bridge Protocol Data Unit (BPDU) packet 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 ISCOM21xx logically according to the selection results, and finally trims the loop network structure to tree network structure without loop which takes an ISCOM21xx 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 8-8 shows loop networking with STP.

Figure 8-8 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 convergence speed.

RSTP

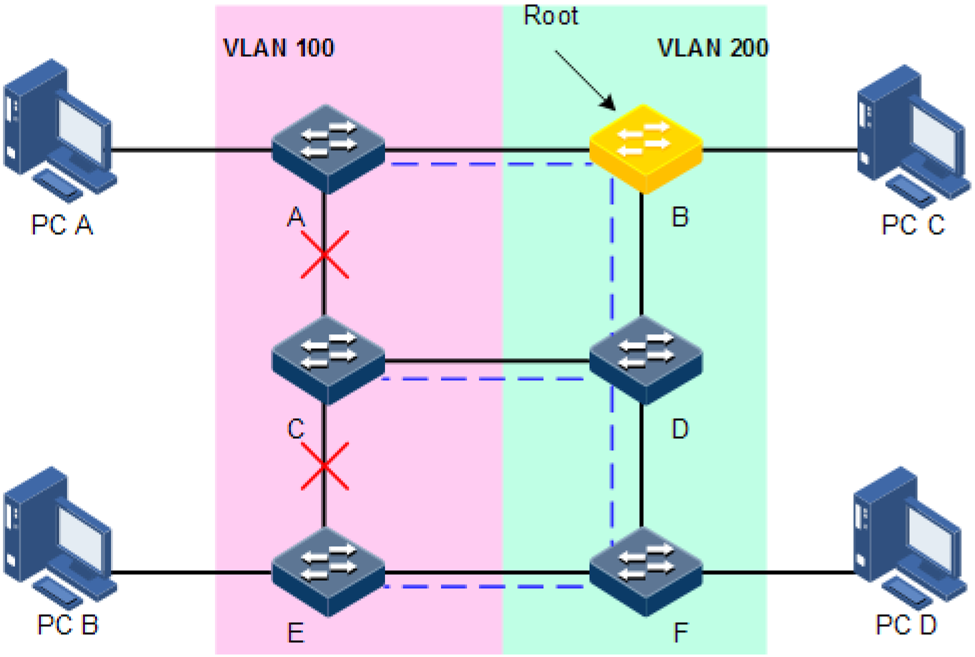
For improving the slow convergent speed of STP, IEEE 802.1w establishes Rapid Spanning Tree Protocol (RSTP), which increases the mechanism to change interface blocking state to forwarding state, speed up the topology convergence rate.

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 the below problems:

- The whole switching network has only one spanning tree, which will lead to longer convergence time on a larger network.
- Waste of bandwidth since a link does not carry any flow after it is blocked.
- Packet of partial VLAN cannot be forwarded when network structure is unsymmetrical. As shown in Figure 8-9, Switch B is the root switch; RSTP blocks the link between Switch A and Switch C logically and makes that the VLAN 100 packet cannot be transmitted and Switch A and Switch C cannot communicate.

Figure 8-9 VLAN packet forward failure due to RSTP



8.4.2 Preparation for configuration

Networking situation

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 down caused by quick copy and transmission of data frame. STP calculation can block one interface in a broken loop and ensure that there is only one path from data flow to the destination host, which is also the best path.

Preconditions

Connect the interface and configure its physical parameters to make it Up.

8.4.3 Default configurations of STP

Default configurations of STP are as below.

Function	Default value
Global STP status	Disable
Interface STP status	Enable
STP priority of device	32768
STP priority of interface	128
Interface path cost	0
max-age timer	20s
hello-time timer	2s

Function	Default value
forward-delay timer	15s

8.4.4 Enabling STP

Configure STP for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`spanning-tree enable`**	Enable STP.

8.4.5 Configuring STP parameters

Configure STP parameters for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`spanning-tree priority`** *`priority-value`*	(Optional) configure device priority.
3	`Raisecom(config)#`**`spanning-tree root`** `{` **`primary`** `|` **`secondary`** `}`	(Optional) configure the ISCOM21xx as the root or backup device.

4	`Raisecom(config)#`**`interface port`** *`port-id`*
	`Raisecom(config-port)#`**`spanning-tree priority`** *`priority-value`*
		(Optional) configure device interface priority.

5	`Raisecom(config-port)#`**`spanning-tree inter-path-cost`** *`cost-value`*
	`Raisecom(config-port)#`**`exit`**
		(Optional) configure interface path cost.

6	`Raisecom(config)#`**`spanning-tree hello-time`** *`value`*	(Optional) configure Hello Time.
7	`Raisecom(config)#`**`spanning-tree transit-limit`** *`value`*	(Optional) configure maximum transmission rate of interface.
8	`Raisecom(config)#`**`spanning-tree forward-delay`** *`value`*	(Optional) configure forward delay.
9	`Raisecom(config)#`**`spanning-tree max-age`** *`value`*	(Optional) configure maximum age.
10	`Raisecom(config)#`**`spanning-tree edged-port bpdu-filter`** `{` **`enable`** `|` **`disable`** `}` **`port-list`** `{` **`all`** `|` *`port-list`* `}`	(Optional) enable BPDU filtering.

8.4.6 Checking configurations

Use the following commands to check configuration results.

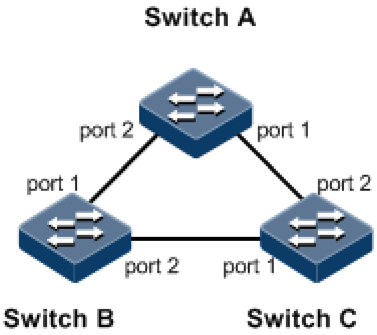
No.	Command	Description
1	`Raisecom#show spanning-tree [ detail ]`	Show basic STP configurations.
2	`Raisecom#show spanning-tree port-list port-list [ detail ]`	Show STP configurations on the interface.

8.4.7 Example for configuring STP

Networking requirements

As shown in Figure 8-10, Switch A, Switch B, and Switch C forms a ring network, so the loopback problem must be solved in the situation of a physical ring. Enable STP on them, configure the priority of Switch A to 0, and path cost from Switch B to Switch A to 10.

Figure 8-10 STP networking



Configuration steps

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

Configure Switch A.

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

Configure Switch B.

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

Configure Switch C.

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

Step 2 Configure interface mode on three switches.

Configure Switch A.

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

Configure Switch B.

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

Configure Switch C.

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

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

Configure Switch A.

```
SwitchA(config)#spanning-tree priority 0
SwitchA(config)#interface port 2
SwitchA(config-port)#spanning-tree inter-path-cost 10
```

Configure Switch B.

```
SwitchB(config)#interface port 1
SwitchB(config-port)#spanning-tree inter-path-cost 10
```

Checking results

Use the **show spanning-tree** command to show bridge status.

Take Switch A for example.

```
SwitchA#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
```

Use the **show spanning-tree port-list** *port-list* command to show interface status.

Take Switch A for example.

```
SwitchA#show spanning-tree port-list 1,2
Port1
PortEnable: admin: enable   oper: enable
Rootguard:  disable
Loopguard:  disable
ExternPathCost:10
EdgedPort:  admin: auto         oper: no            BPDU Filter: disable
LinkType:  admin: auto          oper: point-to-point
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>)
Instance PortState  PortRole   PortCost(admin/oper) PortPriority
-----------------------------------------------------------------
0      discarding disabled    200000/200000      0

Port2
PortEnable: admin: enable    oper: enable
Rootguard:  disable
Loopguard:  disable
ExternPathCost:200000
EdgedPort:  admin: auto         oper: no            BPDU Filter: disable
LinkType:  admin: auto          oper: point-to-point
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>)
Instance PortState  PortRole   PortCost(admin/oper) PortPriority
------------------------------------------------------------
0      discarding disabled   10/10           0
```

8.5 MSTP

8.5.1 Introduction

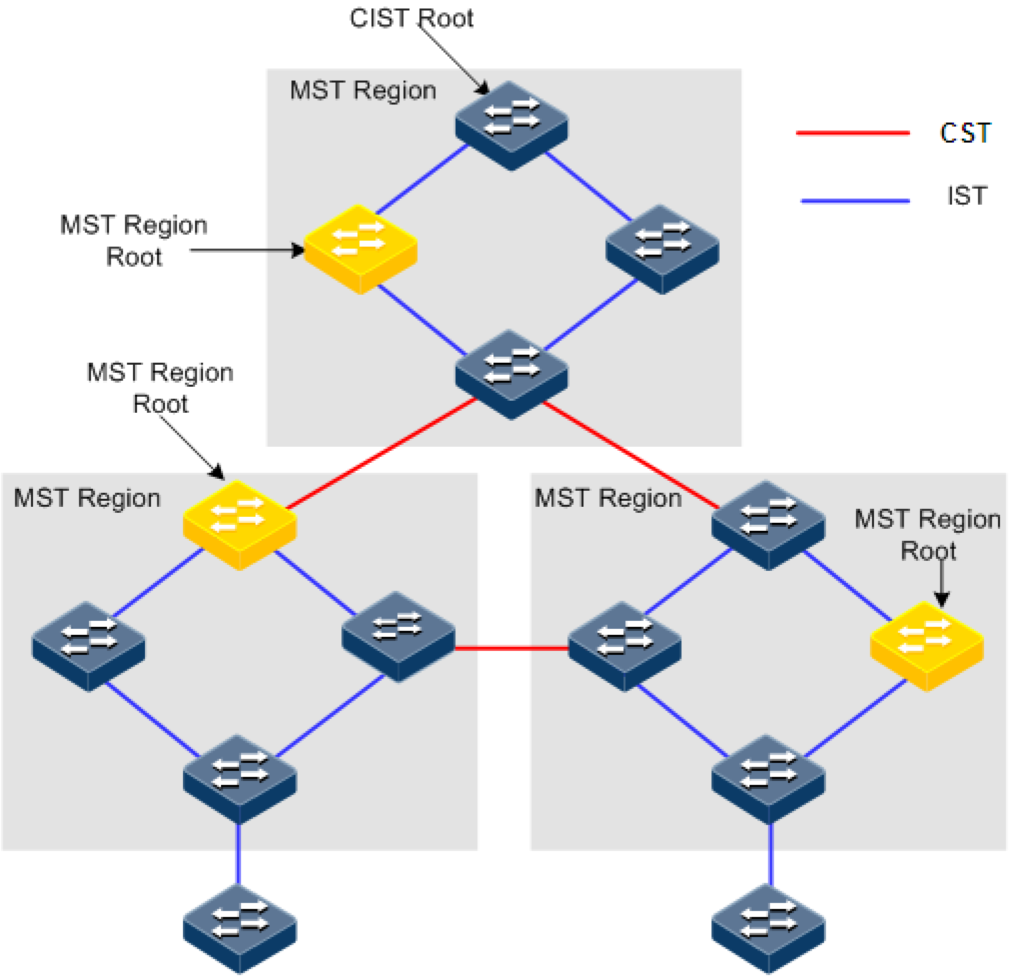
Multiple Spanning Tree Protocol (MSTP) is defined by IEEE 802.1s. Recovering the disadvantages of STP and RSTP, the MSTP implements fast convergence and distributes different VLAN flow following its own path to provide an excellent load sharing mechanism.

MSTP divides a switch 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.

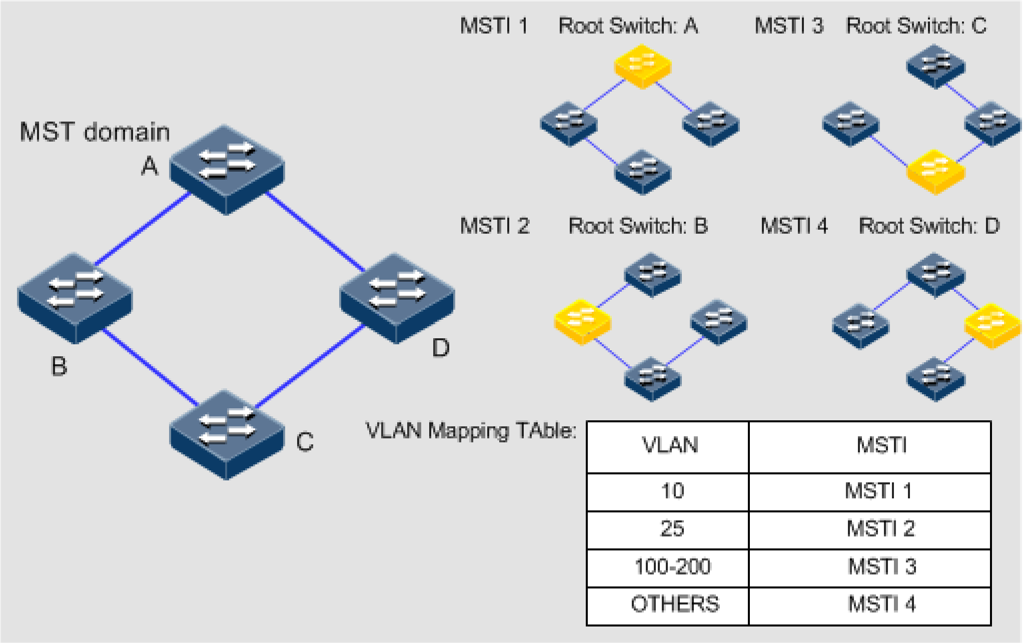
Compared with STP and RSTP, MSTP also introduces total root (CIST Root) and domain root (MST Region Root) concepts. The total root is a global concept; all switches running STP/RSTP/MSTP can have only one total root, which is the CIST Root. The domain root is a local concept, which is relative to an instance in a domain. As shown in Figure 8-11, 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 8-11 Basic concepts of the MSTI network



There can be different MST instance in each MST domain, which associates VLAN and MSTI by configuring the VLAN mapping table (relationship table of VLAN and MSTI). The concept sketch map of MSTI is shown as below.

Figure 8-12 MSTI concepts



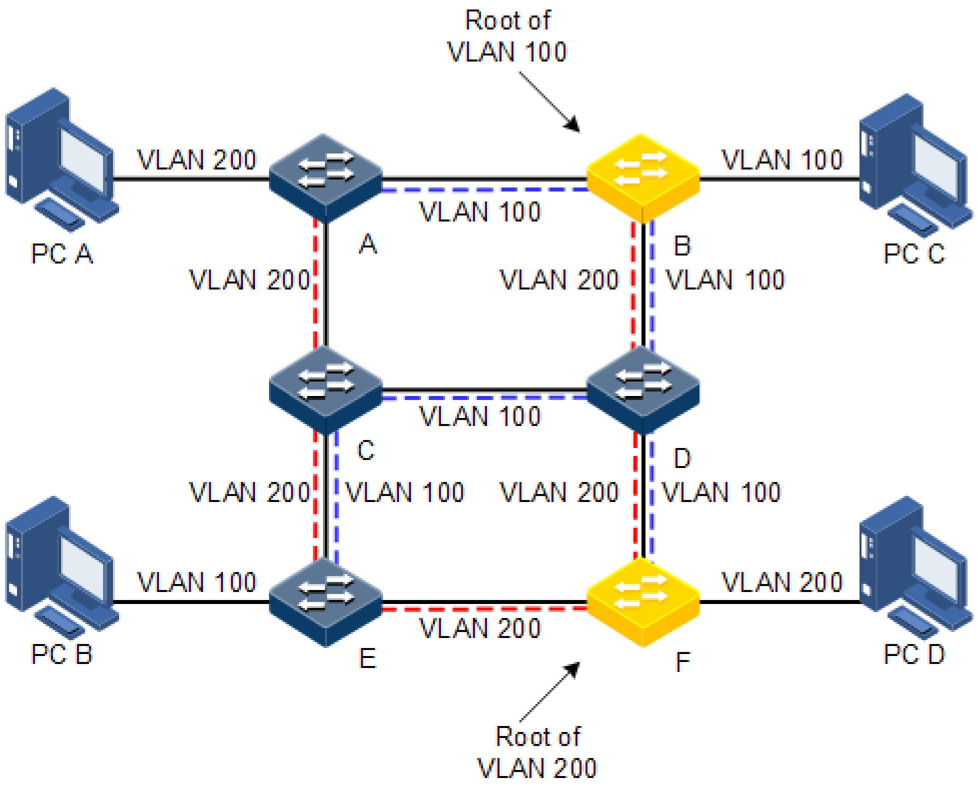
VLAN	MSTI
10	MSTI 1
25	MSTI 2
100-200	MSTI 3
OTHERS	MSTI 4

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 VLAN.

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 VLAN to one MST instance to reduce resource occupancy rate. In addition, MSTP running devices on the network are also compatible with the devices running STP and RSTP.

Figure 8-13 Networking with multiple spanning trees instances in MST domain



Applying MSTP in the network as Figure 3-10 above, after calculation, there are two spanning trees generated at last (two MST instances):

- MSTI1 takes Switch B as the root switch, forwarding packet of VLAN100.
- MSTI2 takes Switch F as the root switch, forwarding packet of VLAN200.

In this way, all VLANs can communicate at internal, different VLAN packets are forwarded in different paths to share loading.

8.5.2 Preparation for configuration

Scenario

In a big LAN or residential region aggregation, the aggregation device creates a ring for link backup, avoids loop, and implements service load sharing. MSTP can select different and unique forwarding paths for each one or a group of VLANs.

Prerequisite

Connect the interface and configure its physical parameters to make it Up.

8.5.3 Default configurations of MSTP

Default configurations of MSTP are as below.

Function	Default value
Global MSTP status	Disable
Interface MSTP status	Enable
Maximum number of hops for MST domain	20
MSTP priority of device	32768
MSTP priority of interface	128
Path cost of interface	0
Maximum number of packets sent within each Hello time	3
Max Age timer	20s
Hello Time timer	2s
Forward Delay timer	15s
Revision level of MST domain	0

8.5.4 Enable MSTP

Configure MSTP for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#spanning-tree enable`	Enable global STP.

8.5.5 Configuring MST domain and its maximum number of hops

You can configure domain information for the ISCOM21xx when it is running in MSTP mode. The device MST domain is decided by domain name, VLAN mapping table and configuration of MSTP revision level. You can configure 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 ISCOM21xx 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 ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#spanning-tree region-configuration`	Enter MST domain configuration mode.

Step	Command	Description
3	`Raisecom(config-region)#name name`	Configure MST domain name.
4	`Raisecom(config-region)#revision-level level-value`	Configure revision level for MST domain.

5	`Raisecom(config-region)#instance instance-id vlan vlan-list`
	`Raisecom(config-region)#exit`
		Configure 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.

8.5.6 Configuring root bridge/backup bridge

Two methods for determining the MSTP root /backup bridge are as below:

- STP calculation based on configuration of the device priority
- Manual configuration through a command

When the root bridge has a fault or is powered off, the backup bridge can replace the root bridge of related instance. In this case, if a new root bridge is assigned, the backup bridge will not become the root bridge. If multiple backup bridges for a spanning tree are configured, once the root bridge stops working, MSTP will choose the backup root with the lowest MAC address as the new root bridge.

Caution

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

Configure root bridge or backup bridge for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#spanning-tree [ instance instance-id ] root { primary | secondary }`	Configure the ISCOM21xx as root bridge or backup bridge for a STP instance.

Note

- You can confirm the effective instance of the root bridge or backup bridge through the parameter **instance** *instance-id*. The current device will be assigned as the root bridge or backup bridge of CIST if instance-id is 0 or parameter **instance** *instance-id* is omitted.
- The roots in device instances are independent mutually, that is to say, they cannot only be the root bridge or backup bridge of one instance, but also the root bridge or backup bridge of other spanning tree instances. However, in the same spanning tree instance, the same device cannot be used as the root bridge and backup bridge at the same time.
- You cannot assign two or more root bridges for one spanning tree instance, but can assign several backup bridges for one spanning tree. Generally speaking, you had better assign one root bridge and several backup bridges for a spanning tree.

8.5.7 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 determines whether the ISCOM21xx can be selected as the root of the spanning tree. Configuring smaller priority helps obtain smaller Bridge ID and designate the ISCOM21xx as the root. If priorities of two ISCOM21xx devices are identical, the ISCOM21xx with lower 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 ISCOM21xx as below.

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

Note

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

8.5.8 Configuring network diameter for switch 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 ISCOM21xx is configured as the CIST root device can this configuration take effect. MSTP will automatically configure the Hello Time, Forward Delay and Max Age parameters to a privileged value through calculation when configuring the network diameter.

Configure the network diameter for the switching network as below.

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

8.5.9 Configuring inner path coast 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 ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port`** *`port-id`*	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.

8.5.10 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 ISCOM21xx as below.

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

8.5.11 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 ISCOM21xx as below.

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

8.5.12 Configuring MSTP timer

- Hello Time: the ISCOM21xx sends the interval of bridge configurations (BPDU) regularly to check whether there is failure in detection link of the ISCOM21xx. The ISCOM21xx 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 ISCOM21xx 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 ISCOM21xx as below.

Step	Command	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.

8.5.13 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 configure the Ethernet interface connected to user client as the edge interface to make it quickly adapt to forwarding 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 ISCOM21xx are configured in auto-detection attribute.

Configure the edge interface for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port`** *`port-id`*	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.

8.5.14 Configuring STP/MSTP mode switching

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

- STP compatible mode: the ISCOM21xx 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.
- MSTP mode: the ISCOM21xx 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 ISCOM21xx as below.

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

8.5.15 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 ISCOM21xx as below.

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

8.5.16 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 ISCOM21xx as below.

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

8.5.17 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 packets 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 ISCOM21xx as below.

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

8.5.18 Executing mcheck operation

Interface on MSTP device has two working modes: STP compatible mode and MSTP mode. Suppose the interface of MSTP device in a switch network is connected to the ISCOM21xx running STP, the interface will change to work in STP compatible mode automatically. But the interface cannot change to work in MSTP mode if the ISCOM21xx running STP is removed, i.e. the interface still works in STP compatible mode. You can execute the **mcheck** command to force the interface working in MSTP mode. If the interface receives new STP packet again, it will return to STP compatible mode.

Execute mcheck operation for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#`**`spanning-tree mcheck`**	Execute mcheck operation, force to remove interface to MSTP mode.

8.5.19 Checking configurations

Use the following commands to check configuration results.

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

8.5.20 Maintenance

Maintain the ISCOM21xx as below.

No.	Command	Description
1	`Raisecom(config-port)#`**`spanning-tree clear statistics`**	Clear statistics of spanning tree on the interface.

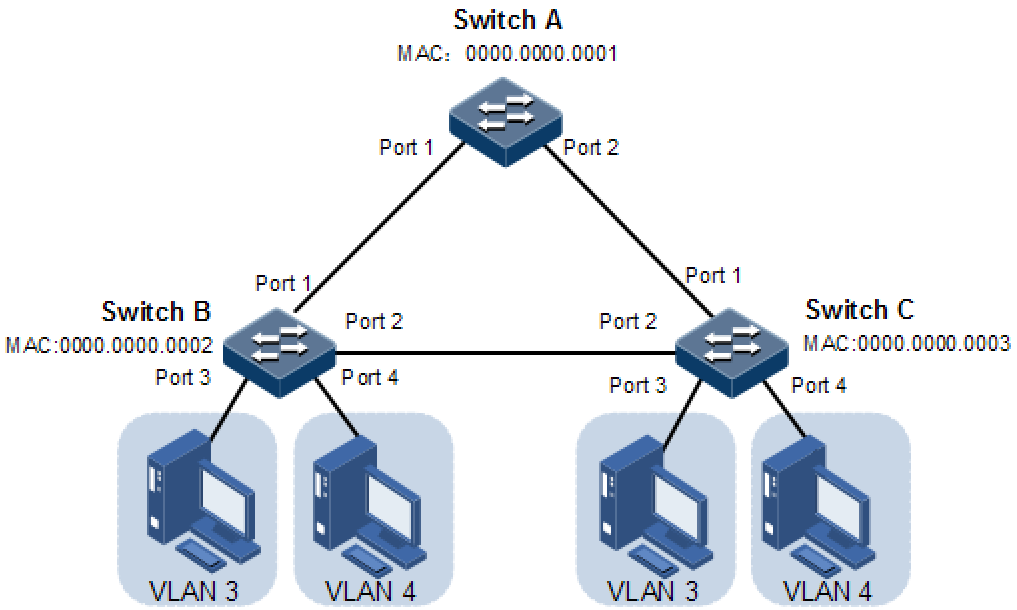
8.5.21 Example for configuring MSTP

Networking requirements

As shown in Figure 8-14, three ISCOM21xx devices are connected to form a ring network through MSTP, with the domain name aaa. Switch B, connected with a PC, belongs to VLAN 3. Switch 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 Switch B so that packets of VLAN 3 and VLAN 4 are forwarded respectively in two paths, which eliminates loopback and implements load sharing.

Figure 8-14 MSTP networking



Configuration steps

Step 1 Create VLAN 3 and VLAN 4 on Switch A, Switch B, and switch C respectively, and activate them.

Configure Switch A.

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

Configure Switch B.

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

Configure Switch C.

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

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

Configure Switch A.

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

Configure Switch B.

```
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
SwitchB(config)#interface port 3
SwitchB(config-port)#switchport access vlan 3
SwitchB(config-port)#exit
SwitchB(config)#interface port 4
SwitchB(config-port)#switchport access vlan 4
SwitchB(config-port)#exit
```

Configure Switch C.

```
SwitchC(config)#interface port 1
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#exit
SwitchC(config)#interface port 2
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#exit
SwitchC(config)#interface port 3
SwitchC(config-port)#switchport access vlan 3
SwitchC(config-port)#exit
SwitchC(config)#interface port 4
SwitchC(config-port)#switchport access vlan 4
SwitchC(config-port)#exit
```

Step 3 Configure spanning tree mode of Switch A, Switch B, and Switch C to MSTP, and enable STP. Enter MSTP configuration mode, and configure 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 Switch A.

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

Configure Switch B.

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

Configure Switch C.

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

Step 4 Configure the inner path coast of Port 1 of spanning tree instance 3 to 500000 on Switch B.

```
SwitchB(config)#interface port 1
SwitchB(config-port)#spanning-tree instance 3 inter-path-cost 500000
```

Checking results

Use the **show spanning-tree region-operation** command to show configurations of the MST domain.

```
Raisecom#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.

- Switch A

```
SwitchA#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   TrunkPort
-------------------------------------------------------------------------
1      forwarding  designated 200000    128        point-to-point  no
2      forwarding  designated 200000    128        point-to-point  no
```

- Switch B

```
SwitchB#show spanning-tree instance 3
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
MST ID: 3
-----------------------------------------------------------
BridgeId:    Mac 0000.0000.0002  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost
500000
PortId  PortState   PortRole   PathCost  PortPriority  LinkType   TrunkPort
-------------------------------------------------------------------------
1      discarding  alternate  500000    128        point-to-point  no
3      forwarding  root      200000    128        point-to-point  no
…
```

- Switch C

```
SwitchC#show spanning-tree instance 3
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
MST ID: 3
-----------------------------------------------------------
BridgeId:    Mac 0000.0000.0003  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost
200000
PortId  PortState   PortRole   PathCost  PortPriority  LinkType   TrunkPort
-------------------------------------------------------------------------
2      forwarding  root       200000   128       point-to-point  no
3      forwarding  designated 200000   128        point-to-point  no
…
```

Use the **show spanning-tree instance 4** command to check whether basic information about spanning tree instance 4 is correct.

- Switch A

```
SwitchA#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    TrunkPort
-------------------------------------------------------------------------
1     discarding  disabled   200000   128        point-to-point  yes
2     disabled   disabled   200000   128        point-to-point  yes
…
```

- Switch B

```
SwitchB#show spanning-tree instance 4
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
MST ID: 4
-----------------------------------------------------------
BridgeId:    Mac 0000.0000.0002  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost
200000
PortId  PortState   PortRole   PathCost  PortPriority  LinkType   TrunkPort
-------------------------------------------------------------------------
1      forwarding  root      200000   128        point-to-point  no
3      forwarding  designated 200000   128       point-to-point  no
…
```

- Switch C

```
SwitchC#show spanning-tree instance 4
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP
MST ID: 4
-----------------------------------------------------------
BridgeId:    Mac 0000.0000.0003  Priority 32768
RegionalRoot: Mac 0000.0000.0001  Priority 32768   InternalRootCost
200000
PortId  PortState   PortRole   PathCost  PortPriority  LinkType  TrunkPort
-------------------------------------------------------------------------
2      forwarding  root       200000   128        point-to-point  no
3      discarding  alternate  200000   128        point-to-point  no
…
```

8.6 ERPS

8.6.1 Introduction

Ethernet Ring Protection Switching (ERPS) is an APS protocol over ITU-T G.8032 recommendation. It is specially used in Ethernet ring link protocol. Generally, ERPS can avoid broadcast storm caused by data loopback. When Ethernet has loop or device malfunction, ERPS can switch the link to the backup link and ensure service restoration quickly.

ERPS uses the control VLAN on a ring network to transmit ring network control information and meanwhile, combining with the topology feature of ring network to discover network fault quickly and enable backup link to restore service fast.

8.6.2 Preparing for configurations

Scenario

With the development from Ethernet to the telecom-grade network, voice and video multicast services bring forth higher requirements on Ethernet redundant protection and fault-restore time. The fault-restore convergent time of current STP system is in second level that is far away to meet requirement. ERPS can blocks a loop to avoid broadcast storm by defining different roles in the ring under normal situations. ERPS can switch the service link to the backup link if the ring link or node fails, thus eliminating loops, conducting fault Automatic Protection Switching (APS) and automatic fault restoration. In addition, the APS time is shorter than 50ms. It supports the single ring, intersecting ring, and tangent rings networking modes.

ERPS supports fault detection in two modes:

- Fault detection based on physical interface status: to obtain link fault and implement quick switching, available to neighbor devices
- Fault detection based on CFM: used in unidirectional fault detection or on multiple devices

Prerequisite

- Connect the interface and configure its physical parameters to make it Up.
- Create VLAN, and add interfaces to the VLAN.
- CFM detection is configured between devices which are configured to neighbor relations (for CFM mode).

8.6.3 Default configurations of ERPS

Default configurations of ERPS are as below.

Function	Default value
Protocol VLAN	1
Protection ring mode	Revertive
Protocol version	1
Ring WTR timer	5min
Ring protocol version	2
Guard timer	500ms
Ring HOLDOFF timer	0ms
ERPS fault information reported to network management system	Disable
Subring virtual circuit mode in intersecting node	with
Ring Propagate switch in intersecting node	Disable
Fault detection mode	Physical interface

8.6.4 Creating ERPS ring

Configure ERPS ring for the ISCOM21xx as below.

Note

The ISCOM2110 series do not support ERPS.

Caution

- Only one device can be configured as the RPL (Ring Protection Link) Owner in a ring, and one device as the RPL Neighbour, other devices can only be configured as ring forwarding nodes.
- A tangent ring can be taken as two independent rings in fact, and its configurations are identical to common single rings. The intersecting ring has a main ring and a tributary ring; for its configurations, see section 8.6.5 (Optional) creating ERPS tributary ring.

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

Step	Command	Description
2	Raisecom(config)#**ethernet ring-protection** *ring-id* **east** { **port** *port-id* | **port-channel** *port-channel-number* } **west** { **port** *port-id* | **port-channel** *port-channel-number* } [**node-type rpl-owner rpl** { **east** | **west** }] [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create a ring, and configure the node as the RPL Owner. A protection ring changes to non-revertive mode if configured with the **not-revertive** parameter. Traffic switches back to the working line from protection line after the fault of the working line is cleared; however, traffic does not switch in non-revertive mode. Note The east-bound and western-bound interface cannot be identical.
	Raisecom(config)#**ethernet ring-protection** *ring-id* **east port** *port-id* **west port** *port-id* **node-type rpl-neighbour rpl** { **east** | **west**} [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create a ring, and configure the node as the RPL Neighbour.
	Raisecom(config)#**ethernet ring-protection** *ring-id* **east port** *port-id* **west port** *port-id* [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create a ring, and configure node as ring forwarding node.
3	Raisecom(config)#**ethernet ring-protection** *ring-id* **name** *string*	(Optional) configure the ring name. The length of name cannot exceed 32 characters.
4	Raisecom(config)#**ethernet ring-protection** *ring-id* **version** { **1** | **2** }	(Optional) configure protocol version. All nodes in one ring must be consistent. Version 1 differentiates rings through protocol VLAN, so different rings need to be configured with different protocol VLANs. So does version 2.
5	Raisecom(config)#**ethernet ring-protection** *ring-id* **guard-time** *guard-time*	(Optional) after configured with the Guard timer, the faulty node does not process APS protocol packets during restoration time. In some big ring network, restoring node fault immediately may receive fault notice from neighbor nodes and cause link Down. Configuring the Guard timer of the ring can solve this problem.

Step	Command	Description
6	`Raisecom(config)#ethernet ring-protection ring-id wtr-time wtr-time`	(Optional) configure the WTR timer of the ring. In revertive mode, wait the WTR timer to expire to switch back working line when the working line restores from a fault.
7	`Raisecom(config)#ethernet ring-protection ring-id holdoff-time holdoff-time`	(Optional) the system delays reporting the fault when the working line becomes faults after configuring the HOLDOFF timer of the ring; namely, traffic will be switched to the protection line after a delayed time. This can avoid working line switching frequently. Note If the HOLDOFF timer is configured over great, the performance of 50ms switching will be affected. Thus it is configured to 0 by default.
8	`Raisecom(config)#ethernet ring-protection trap enable`	(Optional) enable ERPS fault information to be reported to NMS.

8.6.5 (Optional) creating ERPS tributary ring

Caution

- Only the intersecting ring network contains the main ring and tributary ring.
- Configurations of a main ring are identical to configurations of a single ring or tangent ring. For details, see section 8.6.4 Creating ERPS ring.
- Configurations of a Non-intersecting node in a tributary ring are identical to configurations of a single ring or tangent ring. For details, see section 8.6.4 Creating ERPS ring.

Configure the ERPS tributary ring for ISCOM21xx as below.

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

Step	Command	Description
2	Raisecom(config)#**ethernet ring-protection** *ring-id* **east** { **port** *port-id* | **port-channel** *port-channel-number* } **west** { **port** *port-id* | **port-channel** *port-channel-number* } [**node-type rpl-owner rpl** { **east** | **west** }] [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create a tributary ring and configure the node as the RPL Owner on the intersecting node. A protection ring changes to non-revertive mode if configured with the **not-revertive** parameter. Traffic switches back to the working line from protection line after the fault of the working line is cleared; however, traffic does not switch in non-revertive mode. Note The link between two intersecting nodes in intersecting rings belongs to the main ring, so either east-bound or wester-bound interface can be configured for tributary ring.
	Raisecom(config)#**ethernet ring-protection** *ring-id* **east port** *port-id* **west port** *port-id* **node-type rpl-neighbour rpl** { **east** | **west**} [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create a tributary ring, and configure the node as the RPL Neighbour on intersecting nodes.
	Raisecom(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } { **port** *port-id* | **port-channel** *port-channel-number* } [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create a tributary ring, and configure the node as ring forwarding node on intersecting nodes.
3	Raisecom(config)#**ethernet ring-protection** *ring-id* **raps-vc** { **with** | **without** }	(Optional) configure tributary ring virtual circuit mode on the intersecting node. Protocol packets transmitted in the tributary ring are different from that transmitted on the main ring, including with mode and without mode: ● with: the primary ring transmits tributary ring protocol packets. ● without: the tributary ring protocol VLAN transmits tributary ring protocol packets, so it cannot be included in the blocked VLAN list. Configuration mode of two intersecting nodes must be consistent.

Step	Command	Description
4	Raisecom(config)#**ethernet ring-protection** *ring-id* **propagate enable**	Enable the ring Propagate switch on intersecting nodes. Tributary ring data needs to be forwarded by the main ring, so the tributary ring MAC address table also exists on the main ring device. When the tributary ring has fault, the Propagate switch notifies the main ring of refreshing the MAC address table in time and thus avoids flow loss. By default, the Propagate switch is disabled. Use the **ethernet ring-protection** *ring-id* **propagate disable** command to disable this function.

8.6.6 Configuring ERPS fault detection

Configure ERPS fault detection for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } **failure-detect physical-link**	Configure physical interface fault detection mode.
	Raisecom(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } **failure-detect cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	Configure CC fault detection mode. The fault detection mode will not take effect unless CFM is configured. MA must be under md the level if MD is configured.
	Raisecom(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } **failure-detect physical-link-or-cc** [**md** *md-name*] **ma** *ma-name* **level** *level* **mep** *local-mep-id remote-mep-id*	Configure fault detection mode as physical interface or CC. Namely, the system reports fault either in physical link or CC mode. The fault detection mode will not take effect unless CFM is configured. MA must be under the md level if MD is configured.

8.6.7 (Optional) configuring ERPS switching control

Note

By default, traffic will switch to the protection line when the working line fails. Thus ERPS is needed in some special conditions.

Configure ERPS switching control for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ethernet ring-protection ring-id force-switch { east | west }`	Configure Forced Switching (FS) of ring flow to east or west.
3	`Raisecom(config)#ethernet ring-protection ring-id manual-switch { east | west }`	Configure Manual Switching (MS) of traffic on the ring to east or west. MS has a lower priority than FS or APS upon fault of the working line.
4	`Raisecom(config)#clear ethernet ring-protection ring-id command`	Clear switch control command, including **force-switch** and **manual-switch**.

8.6.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show ethernet ring-protection`	Show ERPS ring configuration.
2	`Raisecom#show ethernet ring-protection status`	Show ERPS ring status information.
3	`Raisecom#show ethernet ring-protection statistics`	Show ERPS ring statistics.

8.6.9 Maintenance

Maintain the ISCOM21xx as below.

No.	Command	Description
1	`Raisecom(config)#clear ethernet ring-protection ring-id command`	Clear the effect of ring switching control commands (FS and MS)
2	`Raisecom(config)#clear ethernet ring-protection ring-id statistics`	Clear protection ring statistics.

8.7 RRPS

8.7.1 Introduction

With the development of Ethernet to the MAN, voice, video and multicast services have come up with higher requirements to the Ethernet redundancy protection and fault recovery time.

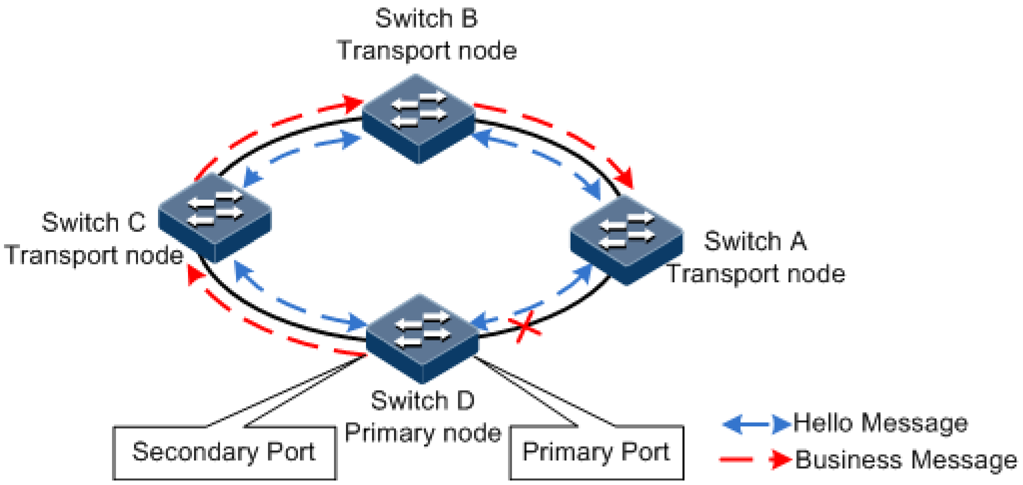
The fault recovery convergence time of original STP mechanism is in the second level, which is far from meeting the fault recovery time requirements of MAN.

Raisecom Ring Protection Switching (RRPS) technology is RAISECOM independent research and development protocol, which can ensure that there is data loop in Ethernet by blocking some interface on the ring. RRPS solves the problems of weak protection to traditional data network and long time to fault recovery, which, in theory, can provide 50ms rapid protection features.

As shown in Figure 8-15, the blocked interface node is the master node, other nodes are transmission nodes. The master node is generated by election. Each node can specify one loop interface as the first interface, the other as the second interface. The master node usually sends Hello packets periodically from the first interface and receives Hello packet sent by itself in the second interface under the circumstance of complete Ethernet ring. Then the master node will block the first interface immediately to ensure there is no loop when the ring network is in a complete state. For the other nodes on the RRPS, the first interface ID and the second interface ID play the same role basically.

RRPS generates the master node by election, so each node needs to collect device information on RRPS, only the right collection leads to correct election. Topology collection is completed by Hello packets, which contain all nodes information collected from the other interface. The normal state of RRPS is shown in Figure 8-15.

Figure 8-15 RRPS in normal status



According to the interface state of node ring, the ring node state can be divided into three types:

- Down: At least one of the two RRPS node interfaces is Down, then the node is Down.
- Block: At least one of the two RRPS node interfaces is Block, then the node is Block.
- Two-Forwarding: Both RRPS node interfaces are Forwarding, then the node is Two-Forwarding.

The election rules of master node are as below:

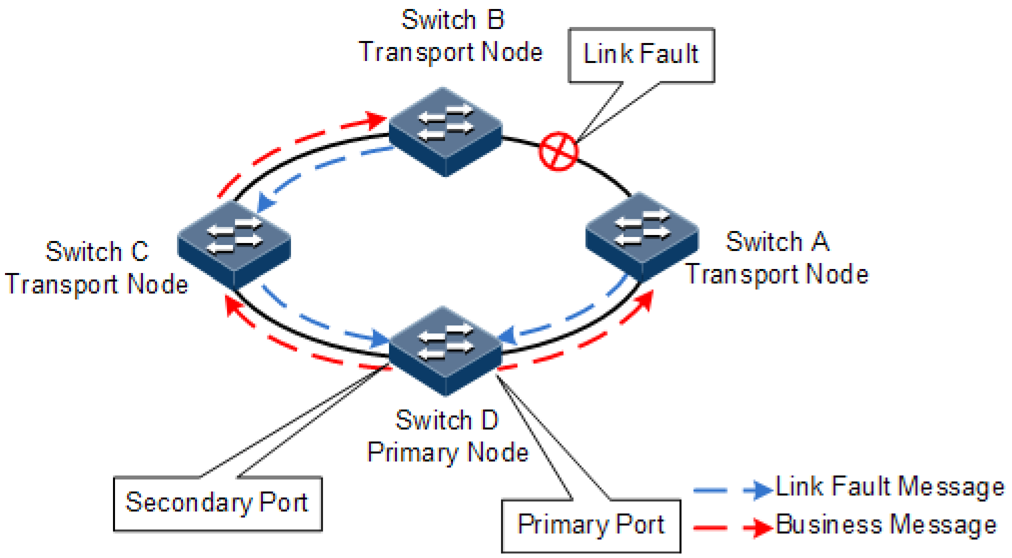
- In all nodes on the ring, node with Down state is prior for master node, followed by Block and Two-Forward.
- If the nodes are in the same state, the node with high-priority Bridge is master node.
- If the nodes have the same state and priority, the node with large MAC address is master node.

Interface Block rules:

- All Link Down interfaces are Block.
- If the node is not master node, all Link Up ring interfaces are Forwarding.
- If the node is master node, then one of two interfaces is Block, the other is Forwarding. Rules are as below:
  - Both interfaces are Up, the Block is the first interface;
  - If one interface is Down, then Block this interface.

The RRPS link failure is shown in Figure 8-16.

Figure 8-16 RRPS in switching status



Once there is link failure (such as link break), the node or interface adjacent to the failure will check the fault immediately, and send link failure packets to the master node. The master node will enable the primary interface once receiving the packets; in the meantime, it sends packets to notify other transmission nodes of the link failure and inform them of changing transmission direction. Traffic will be switched to a normal link after the transmission nodes updates forwarding entry.

When the failed link is restored, the failed node does not enable the blocked port immediately until the new topology collection is stable. The original node will find itself the master node; after some time delay, it will block the first interface, and send Change packets to notify the failed node of enabling the blocked interface.

8.7.2 Preparing for configurations

Scenario

As a Metro Ethernet technology, the Ethernet ring solves the problems of weak protection over traditional data network and long time to fault recovery, which, in theory, can provide 50ms rapid protection switching and is compatible with traditional Ethernet protocol. The Ethernet ring is an important technical choice and solution to optimization and transformation of metro broadband access network.

RRPS technology is Raisecom independent research and development protocol, which through simple configuration implements the elimination of ring loop, fault protection switching, and automatic fault restoration and makes the fault APS time less than 50ms.

RRPS technology supports both single ring and tangent ring networking modes, instead of intersecting ring networking. The tangent ring is actually two separate single rings, which has same configurations with those of a common single ring.

Preconditions

Connect the interface and configure its physical parameters to make it Up.

8.7.3 Default configurations of RRPS

Default configurations of RRPS are as below.

Function	Default value
RRPS status	Disable
Hello packets transmitting time	1s
Fault recovery delay time	5s
RRPS description	Ethernet ring X; X indicates RRPS ID.
Bridge priority	1
Ring interface aging time	15s
Ring protocol packets VLAN	2

8.7.4 Creating RRPS

Create a RRPS as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode. This interface is the first interface on the ring node.
3	`Raisecom(config-port)#`**`ethernet ring`** *`ring-id secondary-interface-number`*	Create a ring and configure corresponding ring interface. This interface is the second interface of ring node.

4	`Raisecom(config-port)#`**`exit`**
	`Raisecom(config)#`**`ethernet ring`** *`ring-id`* **`enable`**
		Enable Ethernet ring.

8.7.5 Configuring basic functions of RRPS

Caution

- For all devices in the same ring, we recommend configuring the fault recovery time and Hello packets interval, ring protocol VLAN, and aging time of ring interface separately for the same value.
- The aging time of an interface must be greater than twice of Hello time.

Configure basic functions of RRPS for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet ring** *ring-id* **hello-time** *hello-time*	(Optional) configure the transmitting time for Hello packets in RRPS.
3	Raisecom(config)#**ethernet ring** *ring-id* **restore-delay** *delay-time*	(Optional) configure fault restoration delay time for RRPS. The link can be restored to the original working line until the restoration delay time expires.
4	Raisecom(config)#**ethernet ring** *ring-id* **priority** *priority*	(Optional) configure the bridge priority for RRPS.
5	Raisecom(config)#**ethernet ring** *ring-id* **description** *string*	(Optional) configure ring description. It should be within 32 characters.
6	Raisecom(config)#**ethernet ring** *ring-id* **hold-time** *hold-time*	(Optional) configure the aging time of the interface for RRPS. If a RRPS interface has not received Hello packets in the aging time, the system ages this interface and considers that the link circuit on link ring is fault. If the node interface is in Block state, it will enable the blocked interface temporarily to ensure the normal communication of all nodes on RRPS.
7	Raisecom(config)#**ethernet ring** *ring-id* **protocol-vlan** *vlan-id*	(Optional) configure RRPS VLANs.
8	Raisecom(config)#**ethernet ring upstream-group** *group-list*	(Optional) configure RRPS uplink interface group. Note The uplink interface group must be used with link-state tracking. It supports dual homing topology. The uplink interface group corresponds to the link-state group in one-to-one relationship.

Note

Master node election: at the beginning, all nodes consider themselves the master node, and one of two interfaces on a node is blocked; so no data loop forms on the ring. When two interfaces on a ring node receive the same Hello packets for many times, the node considers that the ring topology is stable and can elect the master node. Other nodes will release the blocked interface. Usually there is only one master node, which ensures only one blocked interface, and ensures the connectivity of the nodes in the ring.

8.7.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show ethernet ring** [*ring-id*]	Show RRPS information.
2	Raisecom#**show ethernet ring port**	Show RRPS interface information.
3	Raisecom#**show ethernet ring port statistic**	Show statistics of RRPS interface packets.

8.7.7 Maintenance

Maintain the ISCOM21xx as below.

Command	Description
Raisecom(config)#**clear ethernet ring** *ring-id* **statistics**	Clear RRPS interface statistics, including RRPS ID, ring interface ID, Hello packet, Change packet, and Flush packet.

8.7.8 Example for configuring Ethernet ring

Networking requirements

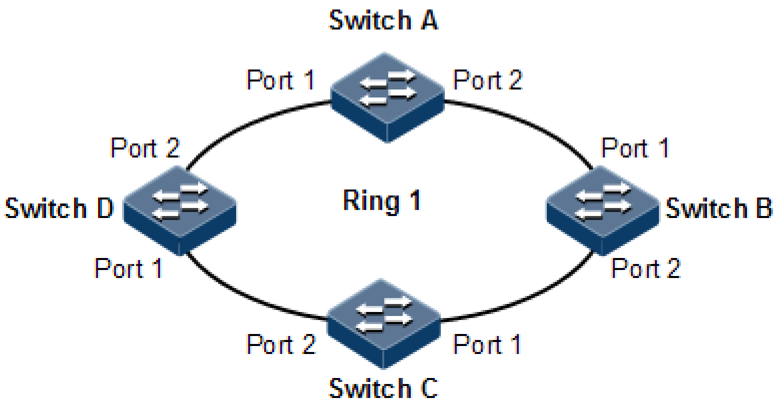
As shown in Figure 8-17, to improve the reliability of Ethernet, Switch A, Switch B, Switch C, Switch D form an Ethernet single ring Ring 1.

The four switches are added to Ring 1 through interfaces. MAC addresses are as below:

- Switch A: 000E.5E00.000A
- Switch B: 000E.5E00.000B
- Switch C: 000E.5E00.000C
- Switch D: 000E.5E00.000D

The status and priority of four switches are the same. The MAC address of Switch D is biggest, so Switch D is the master node of RRPS.

Figure 8-17 RRPS networking



Configuration steps

Step 1 Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#interface port 1
SwitchA(config-port)#ethernet ring 1 port 2
SwitchA(config-port)#exit
SwitchA(config)#ethernet ring 1 enable
```

Step 2 Configure Switch B, Switch C, and Switch D. Their configurations are the same as configurations of Switch A.

Checking results

Use the **show ethernet ring** command to show RRPS configurations.

Take Switch D for example. When the loop is normal, the first ring interface of the master node Switch D is Port 1, and data loop is cleared.

```
SwitchD#show ethernet ring
Ethernet Ring Upstream-Group:--
Ethernet Ring 1:
Ring Admin:     Enable
Ring State:      Enclosed
Bridge State:     Block
Ring state duration: 0 days, 3 hours, 30 minutes, 15 seconds
Bridge Priority:   1
Bridge MAC:     000E.5E00.000D
Ring DB State:      Block
Ring DB Priority:    1
Ring DB:           000E.5E00.000D
Hello Time:      1
Restore delay:     5
Hold Time:      15
```

```
Protocol Vlan:    2
```

Disconnect the link to emulate a fault between Switch A and Switch B manually, so Port 1 on Switch D will change its status from Block to Forwarding, Port 1 on Switch B will change its status from Forwarding to Block. Check RRPS status again.

```
SwitchD#show ethernet ring
Ethernet Ring Upstream-Group:1
Ethernet Ring 1:
Ring Admin:     Enable
Ring State:       Unenclosed
Bridge State:     Two-Forward
Ring state duration: 0 days, 3 hours, 30 minutes, 15 seconds
Bridge Priority:   1
Bridge MAC:     000E.5E00.000D
Ring DB State:       Forwarding
Ring DB Priority:    1
Ring DB:           000E.5E00.000D
Hello Time:       1
Restore delay:     15
Hold Time:      15
Protocol Vlan:    2
```

9 OAM

This chapter describes basic principles and configuration procedures of OAM, and provides related configuration examples, including the following sections:

- EFM
- CFM

9.1 EFM

9.1.1 Introduction

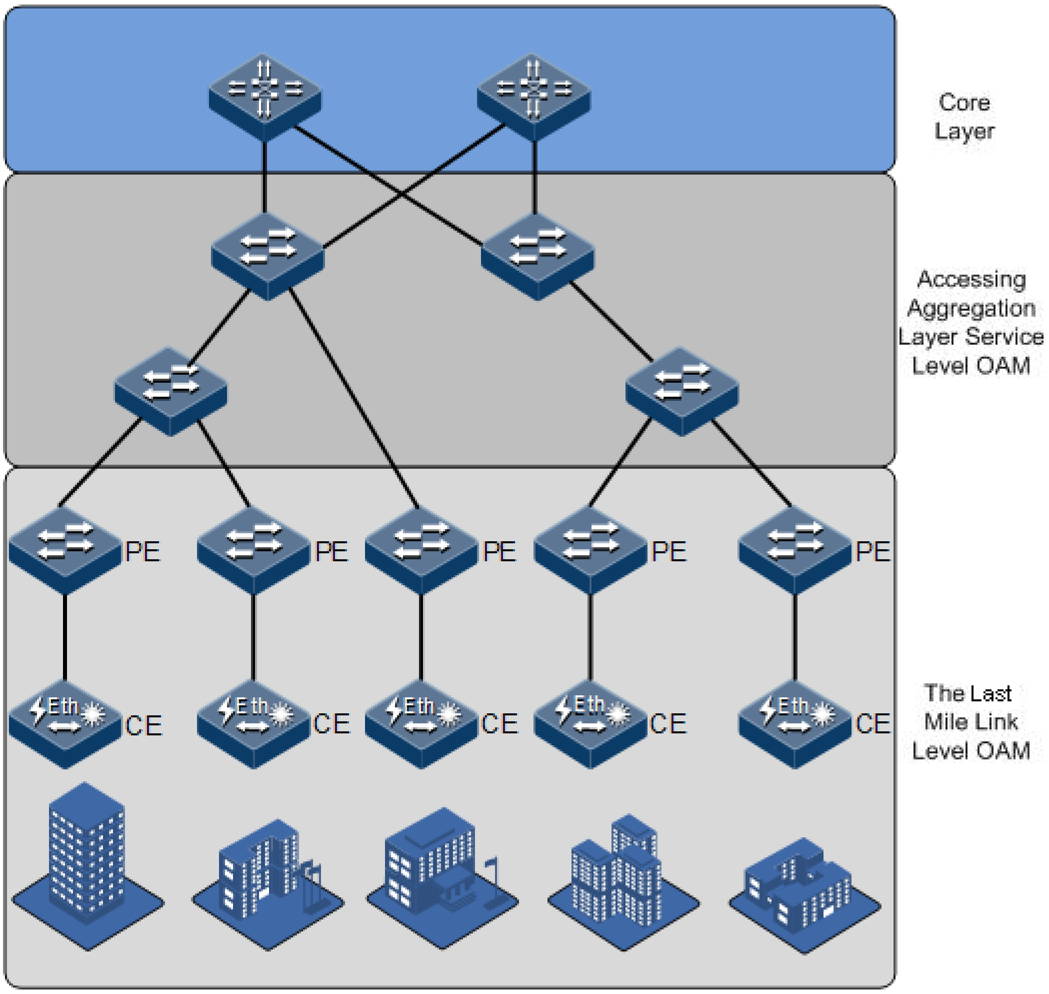
Initially, Ethernet is designed for LAN. Operation, Administration, and Maintenance (OAM) is weak for its small scale and a NE-level administrative system. With continuous development of Ethernet technology, the application scale of Ethernet in telecom network becomes wider and wider. Compared with LAN, the link length and network scale for telecom network is bigger and bigger. The lack of effective management and maintenance mechanism has seriously obstructed Ethernet technology to be applied to the telecom network.

To confirm connectivity of Ethernet virtual connection, effectively detect, confirm and locate faults on Ethernet layer, balance network utilization, measure network performance, and provide service according Service Level Agreement (SLA), implementing OAM on Ethernet has becoming an inevitable developing trend.

Ethernet OAM is implemented in different levels, as show in Figure 9-1, and there are two levels:

- Link-level Ethernet OAM: it is applied in Ethernet physical link (that is the first mile) between Provider Edge (PE) and Customer Edge (CE), which is used to monitor link state between the user network and carrier network, and the typical protocol is Ethernet in the First Mile (EFM) OAM protocol.
- Business-level Ethernet OAM: it is applied in access aggregation layer of network, which is used to monitor connectivity of the whole network, locate connectivity fault of network, monitor and control performance of link, and the typical protocol is Connectivity Fault Management (CFM) OAM protocol.

Figure 9-1 OAM classification


Core Layer
Accessing Aggregation Layer Service Level OAM
PE
PE
PE
PE
PE
Eth
CE
CE
CE
CE
CE
The Last Mile Link Level OAM

Complied with IEEE 802.3ah protocol, Ethernet in the First Mile (EFM) is a link-level Ethernet OAM technology. It provides the link connectivity detection, link fault monitor, and remote fault notification, and so on for a link between two directly connected devices.

"The first mile" in EFM is the connection between local device of telecom operator and client device. The target is that Ethernet technology will be extended to access network market of telecom users, to improve network performance, and reduce cost of device and running. EFM is used in Ethernet link of user access network edge.

The ISCOM21xx provides EFM with IEEE 802.3ah standard.

9.1.2 Preparing for configurations

Scenario

To improve the management and maintenance capability of Ethernet links and ensure network running smoothly, you can deploy EFM between directly connected devices.

Prerequisite

Connect the interface and configure its physical parameters to make it Up.

9.1.3 Default configurations of EFM

Default configurations of EFM are as below.

Function	Default value
EFM working mode	Passive mode
Sending interval of messages	10 ×100ms
Timeout of links	5s
OAM	Disable
Remote OAM event alarm function	Disable
EFM remote loopback state	Not response
Monitor window of errored frame event	1s
Monitor threshold of errored event	1 errored frame
Monitor window of errored frame period event	1000ms
Monitor threshold of errored frame period event	1 errored frame
Monitor window of link errored frame second statistics event	60s
Monitor threshold of link errored frame second statistics event	1s
Monitor window of link errored coding statistics event	100ms
Monitor threshold of errored coding statistic event	1s
Fault indication	Enable
Local OAM event alarm	Disable

9.1.4 Configuring basic functions of EFM

Configure basic functions of EFM for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#oam { active | passive }`	Configure work mode for EFM. ● Active: the device actively initiates OAM peer discovery process. In addition, the device supports responding to remote loopback command and variable obtaining request. ● Passive: the device does not initiate OAM peer discovery process. In addition the device does not support sending remote loopback command and variable obtaining request.

Step	Command	Description
3	Raisecom(config)#**oam send-period** *period-number*	(Optional) OAM link connection is created by sending INFO message. Use this command to configure the interval for sending messages and control communication period of link. The unit is 100ms.
4	Raisecom(config)#**oam timeout** *period-number*	(Optional) Configure OAM link timeout. When both ends of OAM link do not receive OAM message in the interval and the interval is longer than the timeout, the OAM link breaks down. The unit is second.
5	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
6	Raisecom(config-port)#**oam enable**	Enable EFM OAM on an interface.

9.1.5 Configuring active functions of EFM

Configure active functions of EFM for the ISCOM21xx as below.

Note

The active EFM must be configured when the ISCOM21xx is in active mode.

(Optional) configuring device to initiate EFM remote loopback

Configure the ISCOM21xx to initiate EFM remote loopback as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port** *port-id*	Enter physical interface configuration mode.
3	Raisecom(config-port)#**oam remote-loopback**	Configure initiating EFM remote loopback on an interface. The remote loopback can be initiated only when EFM is connected and configured working in active mode.
4	Raisecom(config-port)#**no oam remote-loopback**	(Optional) disable remote loopback. After detection, disable remote loopback immediately.

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 loopback status, the ISCOM21xx detects all packets but OAM packets received by the link. Therefore, disable this function immediately when no detection is needed.

(Optional) configuring peer OAM event alarm

Configure peer OAM event alarm for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**oam peer event trap enable**	Enable peer OAM event trap and then link monitoring event can be reported to NMS center in time. By default, device does not report trap to NMS center through SNMP TRAP when receiving peer link monitoring event.

(Optional) showing current variable information about peer device

Show current variable information about the peer device for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**show oam peer** [**link-statistic** | **oam-info**] [**port-list** *port-list*]	Obtain OAM information or variable values about the peer device.

Note

By obtaining the current variable of the peer, you can learn status of working line. IEEE802.3 Clause 30 defines and explains supported variable and its denotation obtained by OAM in details. The variable takes object as the maximum unit. Each object contains Package and Attribute. A package contains several attributes. Attribute is the minimum unit of a variable. When getting an OAM variable, it defines object, package, branch and leaf description of attributes by Clause 30 to describe requesting object, and the branch and leaf are followed by variable to denote object responds variable request. The ISCOM21xx supports obtaining OAM information and interface statistics.

Peer variable cannot be obtained until EFM is connected.

9.1.6 Configuring passive functions of EFM

Configure passive functions of EFM for the ISCOM21xx as below.

Note

The passive EFM can be configured regardless the ISCOM21xx is in active or passive mode.

(Optional) configuring device to respond to EFM remote loopback

Configure the ISCOM21xx to respond to EFM remote loopback as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface port port-id`	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#oam loopback { ignore | process }`	Configure the ISCOM21xx responding to/ignoring EFM remote loopback. By default, the ISCOM21xx responds to OAM remote loopback.

Note

The peer EFM remote loopback will not take effect until the remote loopback response is configured on the local device.

(Optional) configuring OAM link monitoring

Configure OAM link monitoring for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface port port-id`	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 errored frame event.
4	`Raisecom(config-port)#oam errored-frame-period window window threshold threshold`	Configure the monitor window and threshold for an errored frame period event.
5	`Raisecom(config-port)#oam errored-frame-seconds window window threshold threshold`	Configure the monitor window and threshold for an errored frame seconds event.
6	`Raisecom(config-port)#oam errored-symbol-period window window threshold threshold`	Configure the monitor window and threshold for an errored symbol period event.

Note

The OAM link monitoring is used to detect and report link errors in different conditions. When detecting a fault on a link, the ISCOM21xx provides the peer with the generated time, window, threshold configurations, and so on by OAM event notification packets. The peer receives event notification and reports it to the NMS center through SNMP Trap. Besides, the local device can directly report events to the NMS center through SNMP Trap.

By default, the system configures default value for error generated time, window and threshold configurations.

(Optional) configuring OAM fault indication

Configure OAM fault indication for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**oam notify** { **critical-event** | **dying-gasp** | **errored-frame** | **errored-frame-period** | **errored-frame-seconds** | **errored-symbol-period** } { **disable** | **enable** }	Configure OAM fault indication, which is used to inform the peer when the local fails. Faults that can be notified to the peer contain link-fault, dying-gasp, and critical-event. By default, OAM fault indication is enabled. When a fault occurs, the local device notifies the peer through OAM. The link-fault fault must be notified to the peer while the dying-gasp and critical-event faults can be cleared through this command.

(Optional) configuring local OAM event alarm

Configure local OAM event alarm for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**oam event trap enable**	Enable local OAM event alarm and then link monitoring event can be reported to NMS center in time.

9.1.7 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	Raisecom#**show oam** [**port-list** *port-list*]	Show EFM basic information.
2	Raisecom#**show oam loopback** [**port-list** *port-list*]	Show configurations of EFM remote loopback.
3	Raisecom#**show oam notify** [**port-list** *port-list*]	Show configurations of OAM link monitoring and fault indication.
4	Raisecom#**show oam statistics** [**port-list** *port-list*]	Show OAM statistics.
5	Raisecom#**show oam trap** [**port-list** *port-list*]	Show configurations of OAM event alarm.
6	Raisecom#**show oam event** [**port-list** *port-list*] [**critical**]	Show information about local critical faults detected on an interface.
7	Raisecom#**show oam peer event** [**port-list** *port-list*] [**critical**]	Show information about critical faults sent by the peer.

9.1.8 Maintenance

Maintain the ISCOM21xx as below.

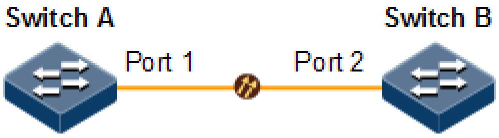
Command	Description
Raisecom(config-port)#**clear oam statistics**	Clear EFM OAM interface link statistics.
Raisecom(config-port)#**clear oam event**	Clear EFM OAM interface link event information.

9.1.9 Example for configuring EFM

Networking requirements

As shown in Figure 9-2, to improve the management and maintenance capability of the Ethernet link between Switch A and Switch B, deploy EFM on Switch A. Switch A works in active mode and is deployed with OAM event alarm function.

Figure 9-2 EFM networking



Configuration steps

Step 1 Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#oam active
SwitchA(config)#interface port 1
SwitchA(config-port)#oam enable
SwitchA(config-port)#oam event trap enable
SwitchA(config-port)#oam peer event trap enable
```

Step 2 Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#interface port 1
SwitchB(config-port)#oam enable
```

Checking results

Use the **show oam** command to show EFM configurations on Switch A.

```
SwitchA#show oam port-list 1
Port: 1
Mode:Active
Administrate state: Enable
Operation state: Operational
Max OAMPDU size: 1518
Send period: 1000 ms
Link timeout :  5 s
Config revision:  1
Supported functions: Loopback, Event, Variable
```

Use the **show oam trap** command to show configurations of OAM event alarm.

```
SwitchA#show oam trap port-list 1
Port:  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
```

9.2 CFM

9.2.1 Introduction

Connectivity Fault Management (CFM) is end to end service level Ethernet OAM technology, implementing end-to-end connectivity fault detection, fault notification, judgement and location functions. This function is used to actively diagnose fault for Ethernet Virtual Connection (EVC) and provide cost-effective network maintenance solution through fault management function and improve network maintenance.

The Device provides CFM function that compatible ITU-Y.1731 and IEEE802.1ag recommendations.

CFM Component

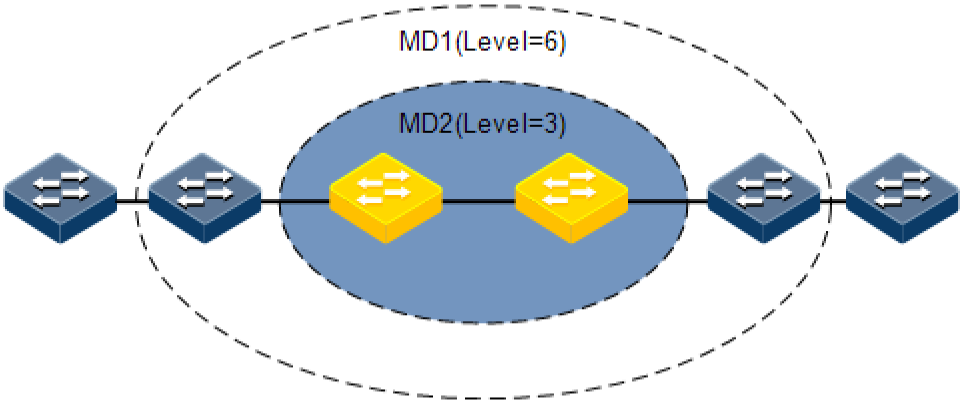
CFM is made from below components:

- MD

Maintenance Domain (MD, also called MEG, Maintenance Entity Group) is a network that runs CFM function. It defines network range for OAM management. MD has level property with 8 different levels (level 0 to level 7), the greater the number is, the higher the level is, and the larger the range is. Protocol packets of a lower level MD will be discarded when entering a higher level MD; while the higher level MD packets can transmit through the lower level MD. In one VLAN range, different MDs can be adjacent, embedded, crossed over.

As shown in Figure 9-3, MD2 is contained in MD1. MD1 packets need to transmit through MD2. Configure MD1 level as 6, and MD2 level as 3. Then MD1 packets can traverse through MD2 and implement connectivity fault management of whole MD1, but MD2 packets will not diffuse into MD1. MD2 is server layer and MD1 is client layer.

Figure 9-3 Different MD levels



- Service instance

Service Instance also called Maintenance Association (MA) is part of MD. One MD can be divided into one or multiple service instances. One service instance corresponds to one service, mapping to one VLAN group, VLAN of different service instances cannot crossover. Though service instance can mapping to multiple VLAN, one instance can use one VLAN for transmitting or receiving OAM packets. The VLAN is master VLAN of the instance.

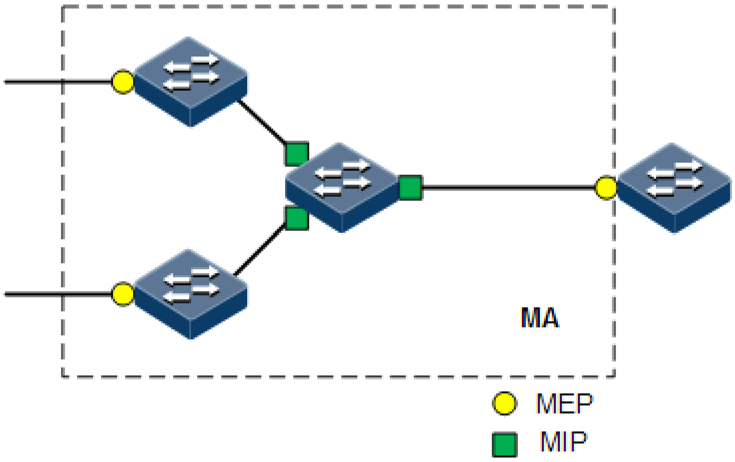
- MEP

As shown in Figure 9-4, Maintenance associations End Point (MEP) is edge node of service instance. MEP can transmit and deal with CFM packets, instance that MEP located and MD decide MEP transmit and receive packets VLAN and level.

MEP on any device configured to run CFM on the network is called local MEP; MEP on other devices in this instance is called Remote Maintenance association End Point (RMEP).

One instance can configure multiple MEP, packets sent by MEP in one instance take identical S-VLAN TAG and with identical priority and C-VLAN TAG. MEP can receive OAM packets sent by other MEP in the instance and stop packets with the same level or lower than itself.

Figure 9-4 MEP and MIP networking



- MIP

As shown in Figure 9-4, Maintenance association Intermediate Point (MIP) is inner node of service instance, automatically created by the ISCOM21xx. MIP cannot send CFM packets actively but can process and answer LinkTrace Message (LTM) and LoopBack Message (LBM) packets.

- MP

MEP and MIP are Maintenance Points (MPs).

9.2.2 Preparing for configurations

Scenario

To develop Ethernet technology application in telecommunication network, Ethernet needs to implement service level identical to telecommunication transmission network. CFM provides full OAM tool to solve this problem through telecommunication Ethernet.

CFM provides the below OAM functions:

- Fault detection function (CC, Continuity Check)

  This function is implemented by MEP sends Continuity Check Packet (CCM) periodically, other MEP in one service instance receives packet to confirm status of RMEP. If the ISCOM21xx faulty or link configuration is incorrect, MEP cannot receive and process CCM from RMEP. If MEP has not received remote CCM packet in 3.5 CCM intervals, the link is considered to be fault, system will send fault trap according to alarm priority configuration.

- Fault acknowledgement function (LB, LoopBack)

  This function confirms connectivity between two MP by sending LBM from source MEP and answering LoopBack Reply (LBR) by destination MP. Source MEP sends LBM to MP for fault acknowledgement, the MP receives LBR and sends a LBR to source MEP, if source MEP received LBR the path is connective, if source MEP does not receive LBR the path is not connective.

- Fault location function (LT, LinkTrace)

  Source MEP sends LTM (LinkTrace Packet) to destination MP, each MP device on LTM transmitting path answers LTR (LinkTrace Reply) to source MEP, the function records efficient LTR and LTM fault location point.

Anyway, CFM implements end-to-end service OAM technology, reducing carriers' operation cost and improving competitiveness.

Prerequisite

- Connect the interface and configure its physical parameters to make it Up.
- Create VLANs.
- Add interfaces into VLANs.

9.2.3 Default configurations of CFM

Default configurations of CFM are as below.

Function	Default value
Global CFM status	Disable
CFM status on interface	Enable
MEP status based on service instance	Up direction
Aging time of RMEP	100min
Storage time of errored CCM packet	100min
MEP sending CCM packet status	Not send
MEP sending CCM packet mode	Passive mode
CCM packet sending interval	1s
Dynamic import function of service instance RMEP learning	Not take effect
cc check function of RMEP	Disable
Priority of CFM OAM packet	6
Layer-2 ping status	The number of sending LBM packets is 5; the length of packet TLV is 64.
Switch status of fault location database	Disable
Storage time of fault location database	100min
Alarm suppression status	Enable

9.2.4 Enabling CFM

Enable CFM for the ISCOM21xx as below.

Note

CFM fault detection, location function cannot take effect unless enables CFM function on the ISCOM21xx.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet cfm enable**	Enable global CFM function.
3	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#**ethernet cfm enable**	Enable CFM on interface. Use the **ethernet cfm disable** command to disable this function. After it is disabled, the interface cannot receive or send CFM packets.

9.2.5 Configuring basic functions of CFM

Configure basic functions of CFM for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet cfm domain** [**md-name** *domain-name*] **level** *level*	Create maintain domain. Use the parameter **md-name** to assign name for MD in 802.1ag style. MA and CCM packets under MD are both in 802.1ag style; do not assign name, the MD is in Y.1731 style, MA and CCM packets under this MD are both in Y.1731 style. If user assigns name for MD, the name must be unique in global, or else MD configuration will be failure. Note Level of different MD must be different; otherwise MD configuration will fail.
3	Raisecom(config)#**service** *cisid* **level** *level*	Create service instance and enter instance configuration mode (MD name and service instance name). Character string is unique in global range. If service instance existed, this command will direct lead to service instance configuration mode.

Step	Command	Description
4	Raisecom(config-service)#**service vlan-list** *vlan-list*	Configure service application VLAN map. VLAN list permits up to 32 VLAN. The smallest VLAN will be taken as primary VLAN of service instance. All MEP in service instance transmit and receive packets through primary VLAN. **Note** Since using primary VLAN to transmit and receive packets, all of other VLAN in the list are mapped to primary VLAN. This logical VLAN mapping is globally; VLAN mapping of different level can be identical but cannot crossover. For example: instance 1 mapping to VLAN 10-20, instance 2 mapping to VLANs 15-30, the configuration is illegal because VLANs 15-20 are crossed.
5	Raisecom(config-service)#**service mep [up | down] mpid** *mep-id* **port** *port-id*	Configure MEP over service instance. Service instance must map to VLAN when configuring this kind MEP. By default, MEP is Up direction, namely interface uplink direction detects fault.

9.2.6 Configuring fault detection

Configure fault detection for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet cfm remote mep age-time** *minute*	(Optional) configure RMEP aging time.
3	Raisecom(config)#**ethernet cfm errors archive-hold-time** *minute*	(Optional) configure hold time for errored CCM packets. The ISCOM21xx saves all fault information of reported by MEP. By default, hold time for errored CCM packets is 100 minutes. It check data in database once system configures new hold time, clear data immediately if there is data over time.
4	Raisecom(config)#**ethernet cfm mode { slave | master }**	Configure the mode for all service instances to send CCM packets.
5	Raisecom(config)#**service** *cisid* **level** *level*	Enter service instance configuration mode.

Step	Command	Description
6	Raisecom(config-service)#**service cc interval** { **1** | **10** | **100ms** | **60** | **600** }	(Optional) configure service instance CCM packets sending time interval. By default, CCM packets sending time interval is 10 seconds. Cannot modify CCM packets sending interval when CCM packets sending function enable.
7	Raisecom(config-service)#**service cc enable mep** { *mep-list* | **all** }	Enable MEP sending CCM packets. By default, MEP does not send CCM packet.
8	Raisecom(config-service)#**service remote-mep** *mep-list*	(Optional) configure static RMEP. Used cooperated with cc check function.
9	Raisecom(config-service)#**service remote-mep learning active**	(Optional) configure RMEP learning dynamic import function. Service instance transfer dynamic RMEP to static RMEP by automation every time receiving of CCM packets. By default, this function does not take effective.
10	Raisecom(config-service)#**service remote-mep cc-check enable**	(Optional) configure RMEP cc check function. After this function is enabled, system checks dynamic learned RMEP ID consistent with static RMEP ID when receiving CCM packets, if not consistent, the CCM packets are considered as incorrect.
11	Raisecom(config-service)#**service cvlan** *vlan-id*	(Optional) configure client VLAN of CFM OAM packets, just need configure in QinQ networking environment. By default, CFM OAM packets do not take C-TAG. After configuring client VLAN for service instance, all MEP under the instance send CCM, LTM, LBM, DMM with double TAG. Hereinto, C-TAG uses this command to configure client VLAN.
12	Raisecom(config-service)#**service priority** *priority*	(Optional) configure CFM OAM packets priority. After configuring packets priority, all CCM, LBM, LTM, DMM sent by MEP use assigned priority.

Step	Command	Description
13	`Raisecom(config-service)#snmp-server trap cfm { all | ccmerr | macremerr | none | remerr | xcon } mep { all | mep-list }`	(Optional) configure CFM permits sending fault trap type. CC function of CFM can detect fault in 5 levels, the order from high to low: level 5–cross connection, level 4-CCM error, level 3-loss of RMEP, level 2-interface status fault, level 1-RDI. By default, it is macremerr, namely permit fault trap on level 2-5. Note • When CFM detected fault, identical level or lower level fault will not generate trap again before removing fault; • Wait for 10s until the fault status is cleared after removing CFM fault.

9.2.7 Configuring fault acknowledgement

Configure fault acknowledgement for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#service cisid level level`	Enter service instance configuration mode.
3	`Raisecom(config-service)#ping { mac-address | mep rmep-id } [ count count ] [ size size ] [ source mep-id ]`	Execute Layer 2 ping function for acknowledging fault. By default, sending LBM packets number is 5, packets TLV size is 64, search an available source MEP by automation. CFM needs to find destination MEP MAC address to execute ping operation if perform Layer 2 ping operation by assigning destination MEPID. After source MEP discovers RMEP and becomes stable, it saves data information of RMEP in RMEP database, and then RMEP MAC address can be found from RMEP database according to MEPID.

Note

- Enable global CFM before using this command; otherwise the command will fail to be executed.
- If there is no MEP configured in service instance, ping unsuccessfully because of failing to find the source MEP.

- If assigned source MEP is invalid, ping unsuccessfully. For example, assigned source MEP does not exist or CFM of the source MEP interface is disabled.
- If assigning destination MEP ID to perform ping operation, ping unsuccessfully when fail to find destination MEP MAC address according to MEPID.
- Operation unsuccessful if other users are using the assigned source MEP to perform ping operation.

9.2.8 Configuring fault location

Configure fault location for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#` **`ethernet cfm traceroute cache enable`**	(Optional) enable fault location database. In enable status, system trace route information through database storing protocol, the **show ethernet cfm traceroute cache** command can show at any time. In disable status, result of traceroute will be cleared after executing traceroute. By default, this function is disabled. Use the **ethernet cfm traceroute cache disable** command to disable it.
3	`Raisecom(config)#` **`ethernet cfm traceroute cache hold-time`** *`minute`*	(Optional) configure data hold time for fault location database. You can configure data hold time when fault location database is enabled. Hold time is 100 minutes by default.
4	`Raisecom(config)#` **`ethernet cfm traceroute cache size`** *`size`*	(Optional) configure saved data amount. You can configure the saved data amount when the function is enabled. It is 100 by default; does not save data if the function is disabled.
5	`Raisecom(config)#` **`service`** *`cisid`* **`level`** *`level`*	Enter service instance configuration mode.
6	`Raisecom(config-service)#`**`traceroute`** `{` *`mac-address`* `|` **`mep`** *`mep-id`* `}` `[` **`ttl`** *`ttl`* `]` `[` **`source`** *`mep-id`* `]`	Execute Layer 2 Traceroute for fault locating. By default, packets TLV size is 64, search an available source MEP by automation. CFM should find MAC address of destination MEP by mep-id to complete traceroute operation if Layer 2 traceroute operation is operated by specified destination mep-id. Users can find the following content by data base of RMEP: data information of RMEP is saved in RMEP database in MEP after source MEP found RMEP and it is stable, you can find MAC address of RMEP according to mep-id in RMEP database.

Note

- Enable global CFM before using this command; otherwise the command will fail to be executed.
- If there is no MEP configured in service instance, Traceroute unsuccessfully because of fail to find source MEP.
- If assigned source MEP is invalid, Traceroute unsuccessfully. For example, assigned source MEP does not exist or CFM of the source MEP interface is disabled.
- If assigning destination MEPID to perform Traceroute operation, Traceroute unsuccessfully when fail to find destination MEP MAC address according to MEPID.
- If CC function is not effective, configure static RMEP and assign MAC address to ensure Layer 2 traceroute operating successfully.
- Operation unsuccessful if other users are using the assigned source MEP to perform Traceroute operation.

9.2.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show ethernet cfm**	Show CFM global configuration.
2	Raisecom#**show ethernet cfm domain** [**level** *level*]	Show MD and service instance configuration.
3	Raisecom#**show ethernet cfm errors** [**level** *level*]	Show errored CCM database information.
4	Raisecom#**show ethernet cfm local-mp** [**interface port** *port-id* | **level** *level*]	Show Ethernet locked signals.
5	Raisecom#**show ethernet cfm remote-mep** [**static**]	Show local MEP configuration.
7	Raisecom#**show ethernet cfm remote-mep** [**level** *level* [**service** *name* [**mpid** *local-mep-id*]]]	Show static RMEP information.
8	Raisecom#**show ethernet cfm traceroute-cache**	Show RMEP discovery information.
9	Raisecom#**show ethernet cfm traceroute-cache**	Show database trace route information.

9.2.10 Maintenance

Maintain the ISCOM21xx as below.

Command	Description
Raisecom(config)#**clear ethernet cfm errors** [**level** *level*]	Clear CCM errored database information.

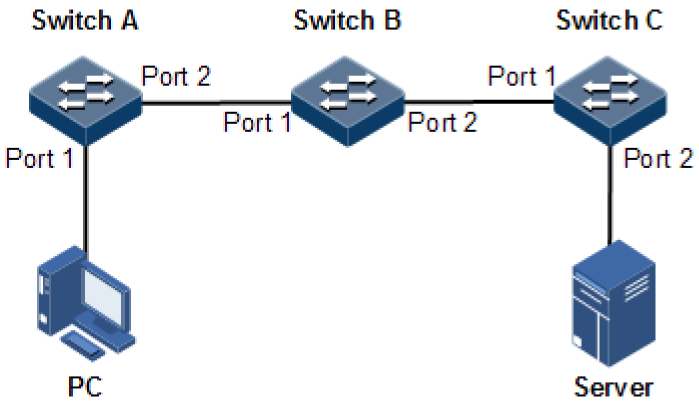
Command	Description
`Raisecom(config)#clear ethernet cfm remote-mep [ level level ]`	Clear RMEP.
`Raisecom(config)#clear ethernet cfm traceroute-cache`	Clear traceroute cache database.

9.2.11 Example for configuring CFM

Networking requirements

As shown in Figure 9-5, the PC communicates with the server through the network consisting of by Switch A, Switch B and Switch C. You can deploy CFM feature on Switch Device to implement active fault detection, acknowledgement and location, then make Ethernet link between PC and Server achieving telecommunication service level. Switch A and Switch C are MEP, Switch B is MIP, detecting Ethernet fault from Switch A Port 1 to Switch C Port 2, maintenance domain level is 3.

Figure 9-5 CFM networking



Configuration steps

Step 1 Add ports into the VLAN.

Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#create vlan 100 active
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport access vlan 100
SwitchA(config-port)#exit
SwitchA(config)#interface port 2
SwitchA(config-port)#switchport mode trunk
SwitchA(config-port)#exit
```

Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#interface port 1
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
SwitchB(config)#interface port 2
SwitchB(config-port)#switchport mode trunk
SwitchB(config-port)#exit
```

Configure Switch C.

```
Raisecom#hostname SwitchC
SwitchC#config
SwitchC(config)#create vlan 100 active
SwitchC(config)#interface port 2
SwitchC(config-port)#switch access vlan 100
SwitchC(config-port)#exit
SwitchC(config)#interface port 1
SwitchC(config-port)#switchport mode trunk
SwitchC(config-port)#exit
```

Step 2 Configure CFM fault detection.

Configure Switch A.

```
SwitchA(config)#ethernet cfm domain level 3
SwitchA(config)#service ma1 level 3
SwitchA(config-service)#service vlan-list 100
SwitchA(config-service)#service mep up mpid 301 port 1
SwitchA(config-service)#service remote-mep 302
SwitchA(config-service)#service cc enable mep all
SwitchA(config-service)#exit
SwitchA(config)#ethernet cfm enable
```

Configure Switch B.

```
SwitchB(config)#ethernet cfm domain level 3
SwitchB(config)#service ma1 level 3
SwitchB(config-service)#service vlan-list 100
SwitchB(config-service)#exit
SwitchB(config)#ethernet cfm enable
```

Configure Switch C.

```
SwitchC(config)#ethernet cfm domain level 3
SwitchC(config)#service ma1 level 3
SwitchC(config-service)#service vlan-list 100
SwitchC(config-service)#service mep up mpid 302 port 2
SwitchC(config-service)#service remote mep 301
SwitchC(config-service)#service cc enable mep all
SwitchC(config-service)#exit
SwitchC(config)#ethernet cfm enable
```

Step 3 Execute CFM fault acknowledgement.

Take Switch A for example.

```
Switch(config)#service ma1 level 3
Switch(config-service)#ping mep 302 source 301
Sending 5 ethernet cfm loopback packets to 000e.5e03.688d, timeout is 2.5
seconds:
!!!!!
Success rate is 100 percent (5/5).
Ping statistics from 000e.5e03.688d:
Received loopback replys:< 5/0/0 > (Total/Out of order/Error)
Ping successfully.
```

Step 4 Execute CFM fault location.

Take Switch A for example.

```
SwitchA(config-service)#traceroute mep 302 source 301
TTL: <64>
Tracing the route to 000E.5E00.0002 on level 3, service ma1.
Traceroute send through port1.
-------------------------------------------------------------------------
Hops  HostMac       Ingress/EgressPort  IsForwarded  RelayAction  NextHop
-------------------------------------------------------------------------
 1    000E.5E00.0003      2/1        Yes         rlyFdb      000E.5E00.0003
 2    000E.5E00.0003      1/2        Yes         rlyFdb      000E.5E00.0001
3   000E.5E00.0001      1/-         No         rlyHit      000E.5E00.0002
```

Checking results

Show CFM configuration on Switch by the command of **show ethernet cfm**.

Take Switch A for example.

```
SwitchA#show ethernet cfm
Global cfm Status: enable
Port CFM Enabled Portlist: 1-10
Archive hold time of error CCMs: 100(Min)
Remote mep aging time: 100(Min)
```

```
Device mode: Slave
```

10 System management

This chapter describes basic principles and configuration procedures of system management and maintenance, and provides related configuration examples, and including the following sections:

- SNMP
- KeepAlive
- RMON
- LLDP
- Extended OAM
- Optical module DDM
- System log
- Power monitoring
- CPU monitoring
- Ping
- Traceroute

10.1 SNMP

10.1.1 Introduction

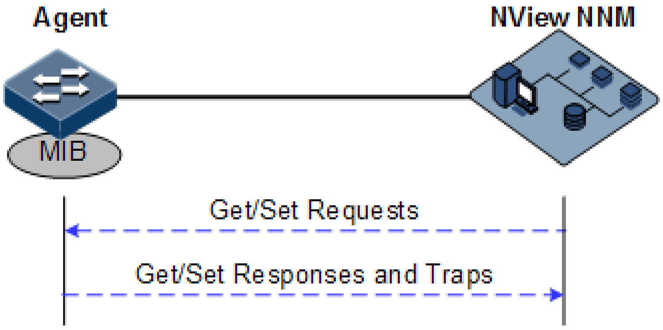
Simple Network Management Protocol (SNMP) is designed by the Internet Engineering Task Force (IETF) to resolve problems in managing network devices connected to the Internet. Through SNMP, a network management system can manage all network devices that support SNMP, including monitoring network status, modifying configurations of a network device, and receiving network alarms. SNMP is the most widely used network management protocol in TCP/IP networks.

Principle of SNMP

SNMP involves two parts: the Agent and NMS. The Agent and NMS communicate through SNMP packets sent through UDP.

Figure 10-1 shows the principle of SNMP.

Figure 10-1 Principle of SNMP



Raisecom NView NNM system can provide friendly Human Machine Interface (HMI) to facilitate network management. The following functions can be implemented through it:

- Send request packets to the managed device.
- Receive reply packets and Trap packets from the managed device, and show result.

The Agent is a program installed in the managed device, realizing the following functions:

- Receive/reply request packets from NView NNM system
- Read/write packets and generate response packets according to the packets type, then return the result to NView NNM system
- Define trigger condition according to protocol modules, enter/exit from system or reboot device when conditions are satisfied; reply module sends Trap packets to NView NNM system through agent to report current status of device.

Note

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

Protocol versions

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

- SNMPv1 uses community name authentication mechanism. The community name, a string defined by an agent, acts like a secret. The network management system can visit the agent only by specifying its community name correctly. If the community name carried in a SNMP packet is not accepted by the ISCOM21xx, the packet will be dropped.
- Compatible with SNMPv1, SNMPv2c also uses community name authentication mechanism. SNMPV2c supports more operation types, data types, and errored codes, and thus better identifying errors.
- SNMPv3 uses User-based Security Model (USM) authentication and View-based Access Control Model (VACM) mechanism. You can configure whether USM authentication is enabled and whether encryption is enabled to provide higher security. USM authentication mechanism allows authenticated senders and prevents unauthenticated senders. Encryption is to encrypt packets transmitted between the network management system and agents, thus preventing interception.

The ISCOM21xx supports SNMPv1, SNMPv2c, and SNMPv3.

MIB

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

- Name
- Access right
- Data type

The device-related statistic contents can be reached by accessing data items. Each proxy has its own MIB. MIB can be taken as an interface between NMS and Agent, through which NMS can read/write every managed object in Agent to manage and monitor the ISCOM21xx.

MIB stores information in a tree structure, and its root is on the top, without name. Nodes of the tree are the managed objects, which take a uniquely path starting from root (OID) for identification. SNMP protocol packets can access network devices by checking the nodes in MIB tree directory.

The ISCOM21xx supports standard MIB and Raisecom-customized MIB.

10.1.2 Preparing for configurations

Scenario

When you need to log in to the ISCOM21xx through NMS, please configure SNMP basic functions for ISCOM21xx in advance.

Prerequisite

- Configure the IP address of the SNMP interface.
- Configure the routing protocol and ensure that the route between the ISCOM21xx and NMS is reachable.

10.1.3 Default configurations of SNMP

Default configurations of SNMP are as below.

Function	Default value
SNMP view	system and internet views (default)
SNMP community	public and private communities (default) Index CommunityName ViewName Permission 1 public internet ro 2 private internet rw
SNMP access group	initialnone and initial access groups (default)
SNMP user	none, md5nopriv, and shanopriv users (default)

Function	Default value
Mapping between SNMP user and access group	Index GroupName UserName SecModel -- 0 initialnone none usm 1 initial md5nopriv usm 2 initial shanopriv usm
Logo and the contact method of administrator	support@Raisecom.com
Device physical location	world china raisecom
Trap	Enable
SNMP target host address	N/A
SNMP engine ID	800022B603000E5E13D266

10.1.4 Configuring basic functions of SNMPv1/SNMPv2c

To protect itself and prevent its MIB from unauthorized access, SNMP Agent proposes the concept of community. The management station in the same community must use the community name in all Agent operating. Otherwise, their requests will not be accepted.

The community name uses different SNMP string to identify different groups. Different communities can have read-only or read-write access authority. Groups with read-only authority can only query the device information, while groups with read-write authority can configure the ISCOM21xx and query the device information.

SNMPv1/SNMPv2c uses the community name authentication scheme, and the SNMP packets which are inconsistent to the community name will be discarded.

Configure basic functions of SNMPv1/SNMPv2c for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server view** *view-name* *oid-tree* [*mask*] { **excluded** | **included** }	(Optional) create SNMP view and configure MIB variable range. The default view is internet view. The MIB variable range contains all MIB variables below "1.3.6" node of MIB tree.
3	Raisecom(config)#**snmp-server community** *com-name* [**view** *view-name*] { **ro** | **rw** }	Create community name and configure the corresponding view and authority. Use default view internet if **view** *view-name* option is empty.

Step	Command	Description
4	Raisecom(config)#**snmp-server access** *group-name* [**read** *view-name*] [**write** *view-name*] [**notify** *view-name*] { **v1sm** | **v2csm** }	(Optional) create and configure SNMPv1/SNMPv2c access group.
5	Raisecom(config)#**snmp-server group** *group-name* **user** *user-name* { **v1sm** | **v2csm** | **usm** }	(Optional) configure the mapping between users and access groups. SNMPv1/SNMPv2c can specify the group for the community, and configure the security model of the group. When the security model is v1sm or v2csm, the security level will automatically change to noauthnopriv.

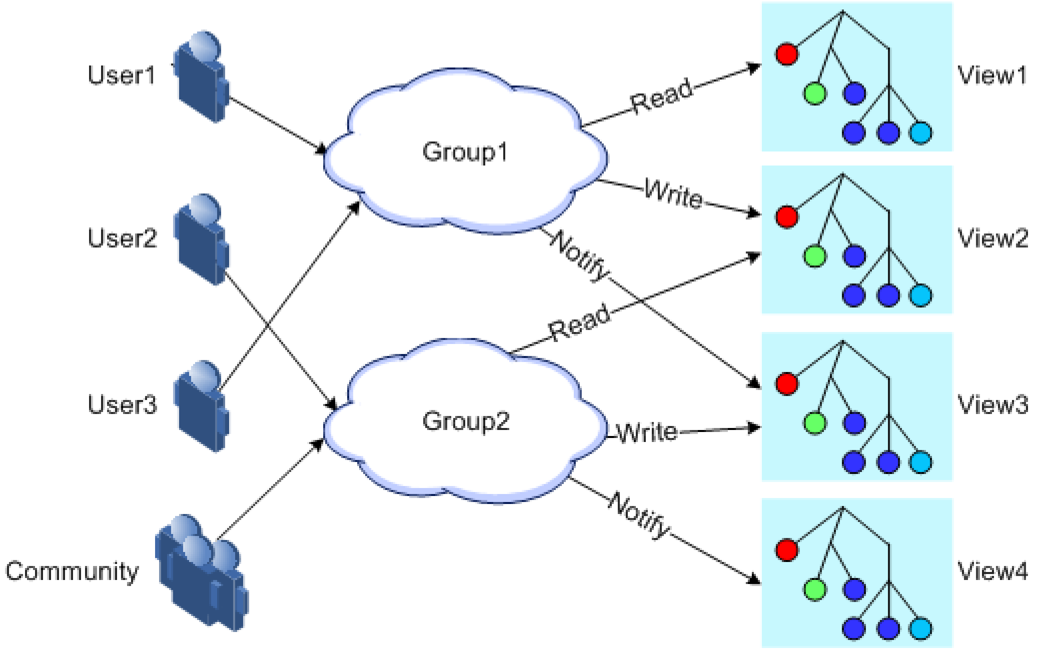
10.1.5 Configuring basic functions of SNMP v3

SNMPV3 uses USM mechanism. USM comes up with the concept of access group. One or more users correspond to one access group. Each access group configures the related read, write, and notification views. Users in an access group have access authorities of this view. The access group of users, who send Get and Set requests, must have authorities corresponding to the requests. Otherwise, the requests will not be accepted.

As shown in Figure 10-2, to access the switch through SNMP v3, you should perform the following configurations:

- Configure users.
- Configure the access group of users.
- Configure the view authority of the access group.
- Create views.

Figure 10-2 SNMP v3 authentication mechanism



Configure basic functions of SNMPv3 for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#snmp-server view view-name oid-tree [ mask ] { excluded | included }`	(Optional) create SNMP view and configure MIB variable range.
3	`Raisecom(config)#snmp-server user user-name [ remote engine-id ] [ authentication { md5 | sha } authpassword ] [ privacy privacypassword ]`	Create users and configure authentication modes.
4	`Raisecom(config)#snmp-server user user-name [ remote engine-id ] [ authkey { md5 | sha } keyword ]`	(Optional) modify the authentication key and the encryption key.
5	`Raisecom(config)#snmp-server access group-name [ read view-name ] [ write view-name ] [ notify view-name ] [ context context-name { exact | prefix } ] usm { authnopriv | noauthnopriv }`	Create and configure the SNMPv3 access group.
6	`Raisecom(config)#snmp-server group group-name user user-name { usm | v1sm | v2csm }`	Configure the mapping between users and the access group.

10.1.6 Configuring other information about SNMP

Other information about SNMP is as below:

- Logo and contact method of the administrator, which is used to identify and contact the administrator
- Physical location of the device: describes where the device is located

SNMPv1, SNMPv2c, and SNMPv3 support configuring this information.

Configure other information of SNMP for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#snmp-server contact contact`	(Optional) configure the logo and contact method of the administrator. Note For example, configure the Email as the ID and contact of the administrator.
3	`Raisecom(config)#snmp-server location location`	(Optional) specify the physical location of the ISCOM21xx.

10.1.7 Configuring Trap

Note

Trap configurations on SNMPv1, SNMPv2c, and SNMPv3 are identical except for Trap target host configurations. Configure Trap as required.

Trap is unrequested information sent by the ISCOM21xx to the NMS automatically, which is used to report some critical events.

Before configuring Trap, you need to perform the following configurations:

- Configure basic functions of SNMP. SNMP v1 and v2c need to configure the community name; SNMPv3 needs to configure the user name and SNMP view.
- Configure the routing protocol and ensure that the route between the ISCOM21xx and NMS is reachable.

Configure Trap of SNMP for the ISCOM21xx 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)#ip address ip-address [ ip-mask ] vlan-list`	Configure the IP address of the Layer 3 interface.

Step	Command	Description
4	Raisecom(config-ip)#**exit**	Exit from global configuration and enter privileged EXEC mode.
5	Raisecom(config)#**snmp-server host** *ip-address* **version 3 { authnopriv | noauthnopriv }** *user-name* [**udpport** *port-id*]	(Optional) configure the SNMPv3 Trap target host.
	Raisecom(config)#**snmp-server host ipv6** *ipv6-address* **version 3 { authpriv | authnopriv | noauthnopriv }** *user-name* [**udpport** *port-id*]	(Optional) configure the IPv6 SNMPv3 Trap target host.
	Raisecom(config)#**snmp-server host** *ip-address* **version { 1 | 2c }** *com-name* [**udpport** *udpport*]	(Optional) configure the SNMPv1/SNMPv2c Trap target host.
	Raisecom(config)#**snmp-server host ipv6** *ipv6-address* **version { 1 | 2c }** *com-name* [**udpport** *udpport*]	(Optional) configure the IPv6 SNMPv1/SNMPv2c Trap target host.
6	Raisecom(config)#**snmp-server enable traps**	Enable Trap sending.

10.1.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show snmp access**	Show SNMP access group configurations.
2	Raisecom#**show snmp community**	Show SNMP community configurations.
3	Raisecom#**show snmp config**	Show SNMP basic configurations, including local SNMP engine ID, ID and contact of the network management personnel, device location, and Trap switch status.
4	Raisecom#**show snmp group**	Show the mapping between SNMP users and the access group.
5	Raisecom#**show snmp host**	Show Trap target host information.
6	Raisecom#**show snmp statistics**	Show SNMP statistics.
7	Raisecom#**show snmp user**	Show SNMP user information.
8	Raisecom#**show snmp view**	Show SNMP view information.

No.	Command	Description
9	`Raisecom#show snmp trap remote`	Show remote Trap configurations of SNMP.

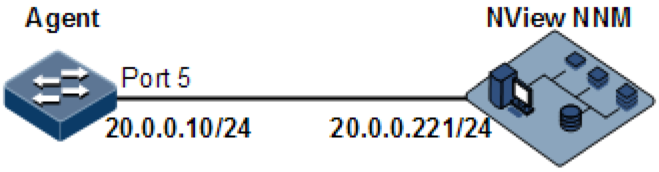
10.1.9 Example for configuring SNMPv1/SNMPv2c and Trap

Networking requirements

As shown in Figure 10-3, the route between the NView NNM system and Agent is reachable. The NView NNM system can view MIBs in the view of the remote switch through SNMPv1/SNMPv2c. And the switch can automatically send Trap to NView NNM in emergency.

By default, there is VLAN 1 in the ISCOM21xx and all physical interfaces belong to VLAN 1.

Figure 10-3 SNMPv1/SNMPv2c and Trap networking



Configuration steps

Step 1 Configure the IP address of the switch.

```
Raisecom#config
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address 20.0.0.10 255.255.255.0 1
Raisecom(config-ip)#exit
```

Step 2 Configure the SNMPv1/SNMPv2c view.

```
Raisecom(config)#snmp-server view mib2 1.3.6.1.2.1 included
```

Step 3 Configure the SNMPv1/SNMPv2c community.

```
Raisecom(config)#snmp-server community raisecom view mib2 ro
```

Step 4 Configure Trap.

```
Raisecom(config)#snmp-server enable traps
Raisecom(config)#snmp-server host 20.0.0.221 version 2c raisecom
```

Checking results

Use the **show interface ip** command to show configurations of IP addresses.

```
Raisecom#show interface ip
Index    Ip Address      NetMask        Vid            Status    Mtu
------------------------------------------------------------------------
0       20.0.0.10    255.255.255.0   1              active   1500
```

Use the **show snmp view** command to show view configurations.

```
Raisecom#show snmp view
Index:    0
  View Name: mib2
  OID Tree:  1.2.6.1.2.1
  Mask:     --
  Type:     included

  Index:    1
  View Name: system
  OID Tree:  1.3.6.1.2.1.1
  Mask:     --
  Type:     included

  Index:    2
  View Name: internet
  OID Tree:  1.3.6
  Mask:     --
  Type:     included
```

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

```
Raisecom#show snmp community
Index  Community Name      View Name         Permission
------------------------------------------------------------
1      public             internet          ro
2      private            internet          rw
3      raisecom           mib2              ro
```

Use the **show snmp host** command to show configurations of the Trap target host.

```
Raisecom#show snmp host
Index:          0
```

```
IP address:     20.0.0.221
Port:           162
User Name:      raisecom
SNMP Version:    v2c
Security Level: noauthnopriv
TagList:        bridge config interface rmon snmp ospf
```

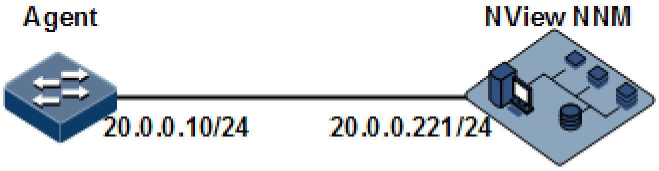
10.1.10 Example for configuring SNMPv3 and Trap

Networking requirements

As shown in Figure 10-4, the route between the NView NNM system and Agent is reachable. The NView NNM system monitors the Agent through SNMPv3. The Agent can automatically send Trap to NView NNM in emergency.

By default, there is VLAN 1 in the ISCOM21xx and all physical interfaces belong to VLAN 1.

Figure 10-4 SNMPv3 and Trap networking



Configuration steps

Step 1 Configure the IP address of the switch.

```
Raisecom#config
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address 20.0.0.10 255.255.255.0 1
Raisecom(config-ip)#exit
```

Step 2 Configure SNMPv3 access.

Configure access view mib2, including all MIB variables under 1.3.6.x.1.

```
Raisecom(config)#snmp-server view mib2 1.3.6.1.2.1 1.1.1.1.0.1 included
```

Create user gusterusr1. Adopt md5 authentication algorithm. Configure the password to raisecom.

```
Raisecom(config)#snmp-server user guestuser1 authentication md5 raisecom
```

Create a guestgroup access group. Configure the security mode to usm. Configure the security level to authnopriv. Configure the name of the read-only view to mib2.

```
Raisecom(config)#snmp-server access guestgroup read mib2 usm authnopriv
```

Map user gudestuser1 to the access group guestgroup.

```
Raisecom(config)#snmp-server group guestgroup user guestuser1 usm
```

Step 3 Configure Trap.

```
Raisecom(config)#snmp-server enable traps
Raisecom(config)#snmp-server host 20.0.0.221 version 3 authnopriv
 guestuser1
```

Checking results

Use the **show snmp access** command to show configurations of the SNMP access group.

```
Index:        0
  Group:        initial
  Security Model: usm
  Security Level: authnopriv
  Context Prefix: --
  Context Match:  exact
  Read View:     internet
  Write View:    internet
  Notify View:   internet

  Index:        1
  Group:        guestgroup
  Security Model: usm
  Security Level: authnopriv
  Context Prefix: --
  Context Match:  exact
  Read View:     mib2
  Write View:    --
  Notify View:   internet

  Index:        2
  Group:        initialnone
  Security Model: usm
  Security Level: noauthnopriv
  Context Prefix: --
  Context Match:  exact
```

```
Read View:     system
Write View:    --
Notify View:   internet
```

Use the **show snmp group** command to show the mapping between users and the access group.

```
Raisecom#show snmp group
Index   GroupName         UserName          SecModel
-----------------------------------------------------------
0      initialnone        none             usm
1      initial           md5nopriv         usm
2      initial           shanopriv         usm
3      guestgroup        guestuser1        usm
```

Use the **show snmp host** command to show configurations of the Trap target host.

```
Raisecom#show snmp host
Index:        0
IP address:    20.0.0.221
Port:         162
User Name:     guestuser1
SNMP Version:   v3
Security Level: authnopriv
TagList:      bridge config interface rmon snmp ospf
```

10.2 KeepAlive

10.2.1 Introduction

KeepAlive packet is a kind of KeepAlive mechanism running in High-Level Data Link Control (HDLC) link layer protocol. The ISCOM21xx will send a KeepAlive packet to confirm whether the peer is online every several seconds to implement neighbour detection mechanism.

Trap is the unrequested information sent by the ISCOM21xx actively to NMS, used to report some urgent and important events.

The ISCOM21xx sends KeepAlive Trap packet actively to the NView NNM system. The KeepAlive Trap packet includes the basic information of ISCOM21xx, such as the name, OID, MAC address, and IP address. The NView NNM system synchronizes device information based on IP address to discover NEs in a short time. This helps improve working efficiency and reduce working load of the administrator.

10.2.2 Preparing for configurations

Scenario

The ISCOM21xx sends KeepAlive Trap packet actively to the NView NNM system. Therefore, the NView NNM system can discover NEs in a short time. This helps improve working efficiency and reduce working load of the administrator. You can enable or disable KeepAlive Trap and configure the period for sending KeepAlive Trap. When KeepAlive Trap is enabled, if configured with **snmp enable traps** and Layer 3 IP address, the ISCOM21xx will send a KeepAlive Trap to all target hosts with Bridge Trap every KeepAlive Trap interval.

Prerequisite

- Configure the IP address of the SNMP interface.
- Configure basic functions of SNMP. SNMPv1 and SNMPv2c need to configure the community name; SNMPv3 needs to configure the user name and SNMP view.
- Configure the routing protocol and ensure that the route between the ISCOM21xx and NMS is reachable.

10.2.3 Default configurations of KeepAlive

Default configurations of KeepAlive are as below.

Function	Default value
KeepAlive Trap	Disable
KeepAlive Trap period	300s

10.2.4 Configuring KeepAlive

Configure KeepAlive for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`snmp-server keepalive-trap enable`**	Enable KeepAlive Trap.
3	`Raisecom(config)#`**`snmp-server keepalive-trap interval`** *`period`*	(Optional) configure the period for sending KeepAlive Trap.

Caution

To avoid multiple devices sending KeepAlive Trap at the same time according to the same period and causing heavy network management load, the real transmission period of KeepAlive Trap is timed as period+5s random transmission.

10.2.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show keepalive`	Show KeepAlive configurations.

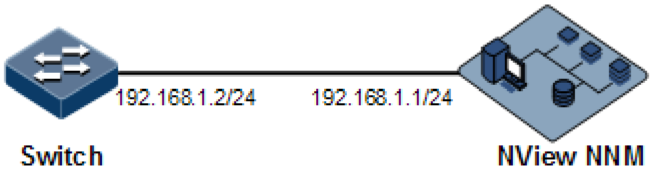
10.2.6 Example for configuring KeepAlive

Networking requirements

As shown in Figure 10-5, configure KeepAlive as below:

- IP address of the switch: 192.169.1.2
- IP address of the SNMPv2c Trap target host: 192.168.1.1
- Name of the read-write community: public
- SNMP version: SNMPv2c
- Period for sending KeepAlive Trap: 120s
- KeepAlive Trap: enabled

Figure 10-5 KeepAlive networking



Configuration steps

Step 1 Configure the management IP address of the switch.

```
Raisecom#config
Raisecom(config)#interface ip 0
Raisecom(config-ip)#ip address 192.168.1.2 255.255.255.0 1
Raisecom(config-ip)#exit
```

Step 2 Configure the IP address of the SNMP Trap target host.

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

Step 3 Enable KeepAlive Trap.

```
Raisecom(config)#snmp-server keepalive-trap enable
Raisecom(config)#snmp-server keepalive-trap interval 120
```

Checking results

Use the **show keepalive** command to show KeepAlive configurations.

```
Raisecom#show keepalive
Keepalive Admin State:Enable
Keepalive trap interval:120s
Keepalive trap count:1
```

10.3 RMON

10.3.1 Introduction

Remote Network Monitoring (RMON) is a standard stipulated by IETF (Internet Engineering Task Force) for network data monitoring through different network Agent and NMS.

RMON is achieved based on SNMP architecture, including the network management center and the Agent running on network devices. On the foundation of SNMP, increase the subnet flow, statistics, and analysis to achieve the monitoring to one network segment and the whole network, while SNMP only can monitor the partial information of a single device and it is difficult for it to monitor one network segment.

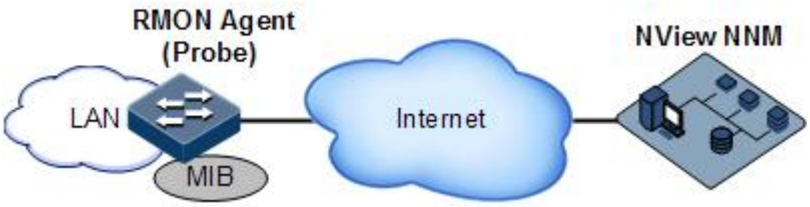
RMON Agent is commonly referred to as the probe program; RMON Probe can take the communication subnet statistics and performance analysis. Whenever it finds network failure, RMON Probe can report network management center, and describes the capture information under unusual circumstances so that the network management center does not need to poll the device constantly. Compared with SNMP, RMON can monitor remote devices more actively and more effectively, network administrators can track the network, network segment or device malfunction more quickly. This approach reduces the data flows between network management center and Agent, makes it possible to manage large networks simply and powerfully, and makes up the limitations of SNMP in growing distributed Internet.

RMON Probe data collection methods:

- Distributed RMON: network management center obtains network management information and controls network resources directly from RMON Probe through dedicated RMON Probe collection data.
- Embedded RMON: embed RMON Agent directly to network devices (such as switches) to make them with RMON Probe function. Network management center will collect network management information through the basic operation of SNMP and the exchange data information of RMON Agent.

The ISCOM21xx adopts embedded RMON, as shown in Figure 10-6. The ISCOM21xx implements RMON Agent. Through this function, the management station can obtain the overall flow, error statistics, and performance statistics of this network segment connected to the managed network device interface to a monitor the network segment.

Figure 10-6 RMON



RMON MIBs are grouped into 9 groups according to functions. Currently, there are 4 groups achieved: statistics group, history group, alarm group, and event group.

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

10.3.2 Preparing for configurations

Scenario

RMON helps monitor and account network traffic.

Compared with SNMP, RMON is a more efficient monitoring method. After you specify the alarm threshold, the ISCOM21xx actively sends alarms when the threshold is exceeded without obtaining variable information. This helps reduce traffic of Central Office (CO) and managed devices and facilitates network management.

Prerequisite

The route between the ISCOM21xx and the NView NNM system is reachable.

10.3.3 Default configurations of RMON

Default configurations of RMON are as below.

Function	Default value
Statistics group	Enabled on all interfaces (including Layer 3 interfaces and physical interfaces)
History group	Disable
Alarm group	N/A
Event group	N/A

10.3.4 Configuring RMON statistics

RMON statistics is used to gather statistics on an interface, including the number of received packets, undersized/oversized packets, collision, CRC and errors, discarded packets, fragments, unicast packets, broadcast packets, and multicast packets, as well as received packet size.

Configure RMON statistics for the ISCOM21xx as below.

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

Note

When using the **no rmon statistics**{ **port-list** *port-list* | **ip** *if-number* } command to disable RMON statistics on an interface, you cannot continue to obtain the interface statistics, but the interface can still count data.

10.3.5 Configuring RMON historical statistics

Configure RMON historical statistics for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**rmon history** { **ip** *if-number* | **port-list** *port- list* } [**shortinterval** *short-period*] [**longinterval** *long-period*] [**buckets** *buckets-number*] [**owner** *owner-name*]	Enable RMON historical statistics on an interface and configure related parameters.

Note

When you use the **no rmon history**{ **ip** *if-number* | **port-list** *port-list* } command to disable RMON historical statistics on an interface, the interface will not count data and clear all historical data collected previously.

10.3.6 Configuring RMON alarm group

You can monitor a MIB variable (mibvar) by configuring a RMON alarm group instance (*alarm-id*). An alarm event is generated when the value of the monitored data exceeds the defined threshold. And then record the log or send Trap to the NView NNM system according to the definition of alarm events.

The monitored MIB variable must be real, and the data value type is correct.

- If the configured variable does not exist or value type variable is incorrect, the system returns an error.
- For the successfully-configured alarm, if the variable cannot be collected later, close the alarm. Reset it if you need to monitor the variable again.

By default, the triggered event ID is 0, which indicates that no event is triggered. If the number is not configured to 0 and there is no event configured in the event group, the event will not be successfully triggered when the monitored variable is abnormal. The event cannot be successfully trigged unless the event is established.

The alarm will be triggered as long as the upper or lower threshold of the event in the event table is matched. The alarm is not generated even when alarm conditions are matched if the event related to the upper/lower threshold (*rising-event-id* or *falling-event-id*) is not configured in the event table.

Configure RMON alarm group for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**rmon alarm** *alarm-id mibvar* [**interval** *period*] { **absolute** | **delta** } **rising-threshold** *rising-value* [*rising-event-id*] **falling-threshold** *falling-value* [*falling-event-id*] [**owner** *owner-name*]	Add alarm instances to the RMON alarm group and configure related parameters.

10.3.7 Configuring RMON event group

Configure the RMON event group for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**rmon event** *event-id* [**log**] [**trap**] [**description** *string*] [**owner** *owner-name*]	Add events to the RMON event group and configure processing modes of events.

10.3.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show rmon**	Show RMON configurations.
2	Raisecom#**show rmon alarms**	Show information about the RMON alarm group.

No.	Command	Description
3	`Raisecom#show rmon events`	Show information about the RMON event group.
4	`Raisecom#show rmon statistics [ port port-id | ip if-number ]`	Show information about the RMON statistics group.
5	`Raisecom#show rmon history { port port-id | ip if-number }`	Show information about the RMON history group.

10.3.9 Maintenance

Maintain the ISCOM21xx as below.

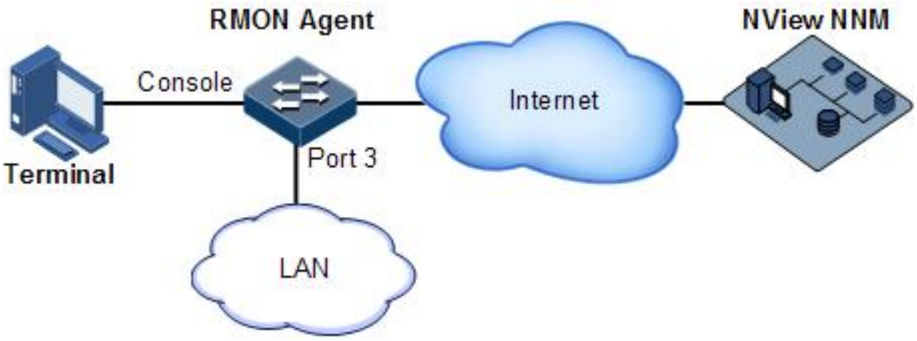
Command	Description
`Raisecom(config)#clear rmon`	Clear all RMON configurations.

10.3.10 Example for configuring RMON alarm group

Networking requirements

As shown in Figure 10-7, the ISCOM21xx is the Agent, connected to terminal through the Console interface, connected to remote NNM system through Internet. Enable RMON statistics and perform performance statistics on Port 3. When the number of packets received by Port 2 exceeds the threshold in a period, the ISCOM21xx records logs and sends Trap alarm to the NView NNM system.

Figure 10-7 RMON alarm group networking



Configuration steps

Step 1 Create event 1. Event 1 is used to record and send the log information which contains the string High-ifOutErrors. The owner of the log information is configured to system.

```
Raisecom#config
```

```
Raisecom(config)#rmon event 1 log description High-ifOutErrors owner
system
```

Step 2 Create alarm 10. Alarm 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 configured 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
```

Checking results

Use the **show rmon alarms** command to show information about the alarm group.

```
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 information about the event group on the ISCOM21xx.

```
Raisecom#show rmon events
Event 1 is active, owned by system
Description is:  High-ifOuterErrors.
Event generated at 0:0:0
Send TRAP when event is fired.
```

When an alarm event is triggered, you can show related records at the alarm management dialog box of the NView NNM system.

10.4 LLDP

10.4.1 Introduction

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

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

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

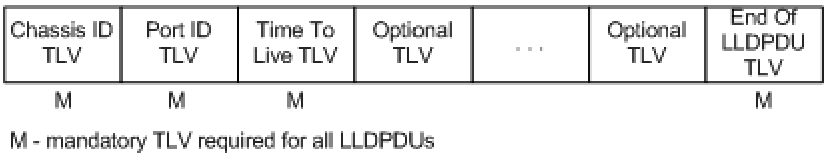
Basic concepts

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

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

As shown in Figure 10-9, LLDPDU is made by several TLV, including 4 mandatory TLV and several optional TLV.

Figure 10-8 LLDPDU structure



TLV: unit combining LLDPDU, which refers to the unit describing the object type, length and information.

As shown in Figure 10-9, each TLV denotes piece of information at local, such as device ID, interface ID, related Chassis ID TLV, and Port ID TLV fixed TLV.

Figure 10-9 Basic TLV structure

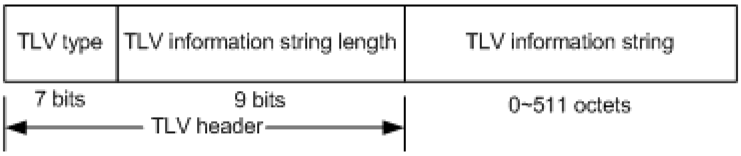


Table 10-1 lists TLV type. At present only types 0–8 are used.

Table 10-1 TLV types

TLV type	Description	Optional/Required
0	End Of LLDPDU	Required
1	Chassis ID	Required
2	Port ID	Required
3	Time To Live	Required
4	Port Description	Optional

TLV type	Description	Optional/Required
5	System Name	Optional
6	System Description	Optional
7	System Capabilities	Optional
8	Management Address	Optional

Principle of LLDP

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

The procedure of packet exchange is as below:

- When the local device transmits packet, it obtains system information required by TLV from NView NNM (Network Node Management), obtains configurations from LLDP MIB, generates TLV, makes LLDPDU, encapsulates information to LLDP packets, and send LLDP packets to the peer end.
- The peer end receives LLDPDU and analyzes TLV information. If there is any change, the information will be updated in neighbor MIB table of LLDP and the NView NNM system will be notified.

The aging time of Time To Live (TTL) in local device information in the neighbour node can be adjusted by modifying the parameter values of aging coefficient, sends LLDP packets to neighbour node, after receiving LLDP packets, neighbour node will adjust the aging time of its neighbour nodes (sending side) information. Aging time formula, TTL = Min {65535, (interval × hold-multiplier)}:

- Interval: indicate the period for sending LLDP packets from the neighbor node.
- Hold-multiplier: the aging coefficient of device information in neighbor node.

10.4.2 Preparing for configurations

Scenario

When you obtain connection information between devices through NView NNM system for topology discovery, the ISCOM21xx needs to enable LLDP, notify their information to the neighbours mutually, and store neighbour information to facilitate the NView NNM system queries.

Prerequisite

N/A

10.4.3 Default configurations of LLDP

Default configurations of LLDP are as below.

Function	Default value
Global LLDP status	Disable
Interface LLDP status	Enable
Delay timer	2s
Period timer	30s
Aging coefficient	4
Restart timer	2s
LLDP alarm status	Enable
Alarm notification timer	5s

10.4.4 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.

When you obtain connection information between devices through the NView NNM system for topology discovery, the ISCOM21xx needs to enable LLDP, sends their information to the neighbours mutually, and stores neighbour information to facilitate query by the NView NNM system.

Enable global LLDP for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#lldp enable`	Enable global LLDP. After global LLDP is enabled, use the **lldp disable** command to disable this function.

10.4.5 Enabling interface LLDP

Enable interface LLDP for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface port` *`port-id`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#lldp enable`	Enable LLDP on an interface. Use the **lldp disable** command to disable this function.

10.4.6 Configuring basic functions of LLDP

Caution

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

Configure basic functions of LLDP for the ISCOM21xx as below.

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.
3	Raisecom(config)#**lldp message-transmission delay** *period*	(Optional) configure the delay timer of the LLDP packet.
4	Raisecom(config)#**lldp message-transmission hold-multiplier** *hold-multiplier*	(Optional) configure the aging coefficient of the LLDP packet.
5	Raisecom(config)#**lldp restart-delay** *period*	(Optional) restart the timer. When configuring the delay timer and period timer, the value of the delay timer should be smaller than or equal to a quarter of the period timer value.

10.4.7 Configuring LLDP alarm

When the network changes, you need to enable LLDP alarm notification function to send topology update alarm to the NView NNM system immediately.

Configure LLDP alarm for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server lldp-trap enable**	Enable LLDP alarm.
3	Raisecom(config)#**lldp trap-interval** *period*	(Optional) configure the period timer of LLDP alarm Trap.

Note

After being enabled with LLDP alarm, the ISCOM21xx sends Traps upon detecting aged neighbours, newly-added neighbours, and changed neighbour information.

10.4.8 Checking configurations

Use the following commands to check configuration results.

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

10.4.9 Maintenance

Maintain the ISCOM21xx as below.

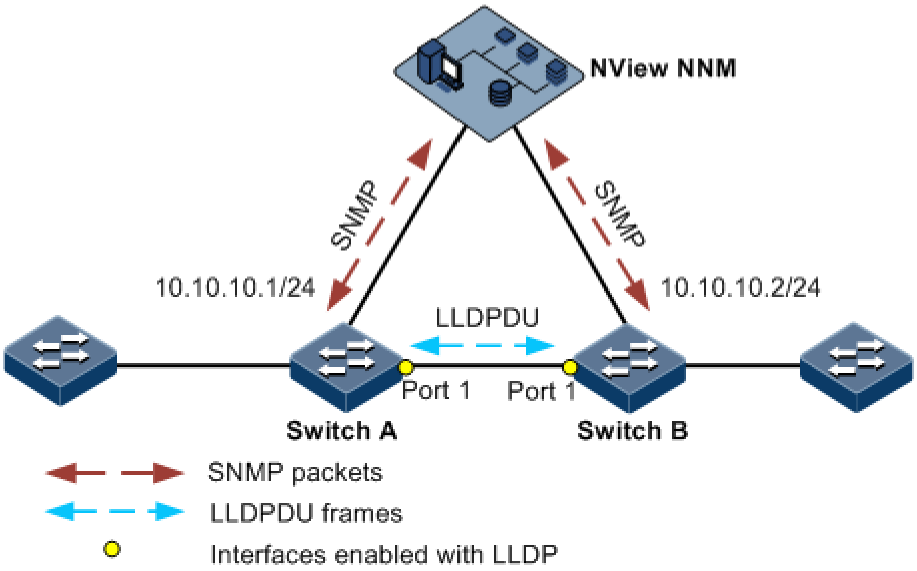
No.	Command	Description
1	`Raisecom(config)#`**clear lldp statistic** [**port-list** *port-id*]	Clear LLDP statistics.
2	`Raisecom(config)#`**clear lldp remote-table** [**port-list** *port-id*]	Clear information about the LLDP neighbor.

10.4.10 Example for configuring basic functions of LLDP

Networking requirements

As shown in Figure 10-10, Switches are connected to the NView NNM system. Enable LLDP on links between Switch A and Switch B. And then you can query the Layer 2 link changes through the NView NNM system. If the neighbour is aged, the neighbour is added, or the neighbour information changes, Switch A and Switch B sends LLDP alarm to the NView NNM system.

Figure 10-10 LLDP networking



Configuration steps

Step 1 Enable LLDP globally and enable LLDP alarm.

Configure Switch A.

```
Raisecom#hostname SwitchA
SwitchA#config
SwitchA(config)#lldp enable
SwitchA(config)#snmp-server lldp-trap enable
```

Configure Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#lldp enable
SwitchB(config)#snmp-server lldp-trap enable
```

Step 2 Configure management IP addresses.

Configure Switch A.

```
SwitchA(config)#create vlan 1024 active
SwitchA(config)#interface port 1
SwitchA(config-port)#switchport access vlan 1024
SwitchA(config-port)#exit
SwitchA(config)#interface ip 1
SwitchA(config-ip)#ip address 10.10.10.1 1024
SwitchA(config-ip)#exit
```

Configure Switch B.

```
SwitchB(config)#create vlan 1024 active
SwitchB(config)#interface port-list 1
SwitchB(config-port)#switchport access vlan 1024
SwitchB(config)#interface ip 1
SwitchB(config-ip)#ip address 10.10.10.2 1024
SwitchB(config-ip)#exit
```

Step 3 Configure LLDP properties.

Configure Switch A.

```
SwitchA(config)#lldp message-transmission interval 60
SwitchA(config)#lldp message-transmission delay 9
SwitchA(config)#lldp trap-interval 10
```

Configure Switch B.

```
SwitchB(config)#lldp message-transmission interval 60
SwitchB(config)#lldp message-transmission delay 9
SwitchB(config)#lldp trap-interval 10
```

Checking results

Use the **show lldp local config** command to show local LLDP configurations.

```
SwitchA#show lldp local config
System configuration:
--------------------------------------------------------------------------
LLDP enable status: enable  (default is disabled)
LLDP enable ports: 1-10
LldpMsgTxInterval: 60     (default is 30s)
LldpMsgTxHoldMultiplier:4      (default is 4)
LldpReinitDelay: 2     (default is 2s)
LldpTxDelay: 9     (default is 2s)
LldpNotificationInterval:10     (default is 5s)
LldpNotificationEnable:enable  (default is enabled)

SwitchB#show lldp local config
System configuration:
--------------------------------------------------------------------------
LLDP enable status: enable  (default is disabled)
LLDP enable ports: 1
LldpMsgTxInterval: 60     (default is 30s)
LldpMsgTxHoldMultiplier:4      (default is 4)
```

```
LldpReinitDelay:2      (default is 2s)
LldpTxDelay:9      (default is 2s)
LldpNotificationInterval:10     (default is 5s)
LldpNotificationEnable:enable  (default is enabled)
```

Use the **show lldp remote** command to show information about the LLDP neighbour.

```
SwitchA#show lldp remote
Port   ChassisId          PortId        SysName   MgtAddress    ExpiredTime
--------------------------------------------------------------------------
port1  000E.5E02.B010    port 1        SwitchB  10.10.10.2    106
……
SwitchB#show lldp remote
Port   ChassisId          PortId        SysName   MgtAddress    ExpiredTime
--------------------------------------------------------------------------
port1  000E.5E12.F120    port 1        SwitchA  10.10.10.1    106
```

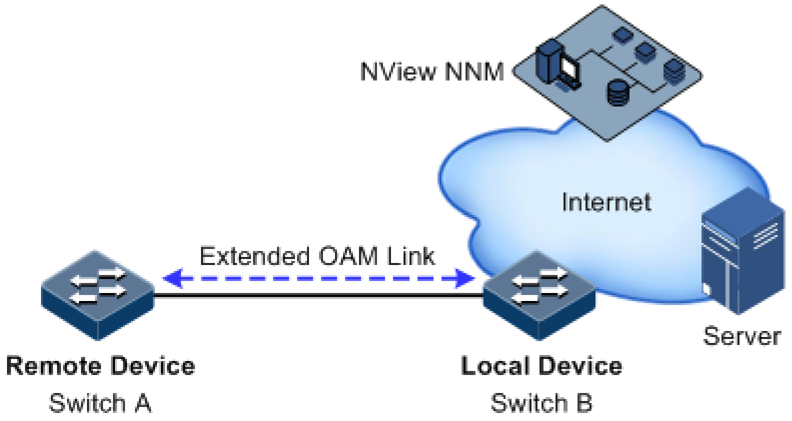
10.5 Extended OAM

10.5.1 Introduction

Extended OAM is based on IEEE 802.3ah OAM links. Based on standard OAM extendibility, it enhances OAM functions, including remote configurations and monitoring.

As shown in Figure 10-11, establish an extended OAM link between the remote switch A and Central Office (CO) Switch B directly connected to the NView NNM system, to enable Switch B to manage Switch A.

Figure 10-11 Extended OAM networking



Extended OAM functions including remote configurations and monitoring, with details as below:

- Obtain attributes of the remote device: the CO device can obtain attributes, configurations, and statistics of the remote device through extended OAM.

- Configure basic functions for the remote device: through extended OAM, the CO device can configure some functions for the remote device, including host name, interface enabling/disabling status, rate, duplex mode, bandwidth, and link-state tracking status.
- Configure network management parameters for the remote device: the CO device can configure network management parameters for remote SNMP-supportive devices, such as IP address, gateway, management IP address, and read/write community, and then implement overall network management through SNMP.
- Support remote Trap: when an interface on a remote device is Up or Down, it sends an extended OAM notification to the CO device which will then send Trap message of the remote device to the NMS.
- Reboot the remote device: the CO device can send a command to reboot the remote device.
- Support other remote management functions: as the remote functions increase, the CO device can manage more remote functions through extended OAM protocols, such as SFP and QinQ.

Note

When the ISCOM21xx works as the CO device, different remote devices may support different extended OAM functions. Whether an extended OAM function is supported depends on the remote device. For details, see the corresponding manuals.

For example, the remote device is the RC551E, which supports to be configured with the following extended OAM functions:

- Configure the IP address (including the default gateway and IP address of the out-of-band interface).
- Configure the name of the remote host.
- Configure network management of the remote device.
- Manage configuration files of the remote device.
- Reboot the remote device.
- Clear statistics of extended OAM links.
- Show extended OAM capabilities of the remote device.
- Show basic information about the remote device.
- Show interface information about the remote device.
- Show Trap status of the remote device.
- Show extended OAM link status.

10.5.2 Preparation for configuration

Scenario

Extended OAM is used to establish connection between Central Office (CO) device and remote device to achieve remote management.

Prerequisite

- Establish OAM link between devices to establish extended OAM link.
- The following configurations take ISCOM21xx as the CO device. For different remote devices, the extended OAM networking situation and configuration commands may be

different; configure the ISCOM21xx according to the specific remote networking situation.

10.5.3 Default configurations of extended OAM

Default configurations of extended OAM are as below.

Function	Default value
OAM status	Disable
OAM working mode	passive
Remote Trap status	Enable

10.5.4 Establishing OAM link

Note

You need to establish OAM link between devices to establish extended OAM link and both sides of devices are OAM active mode and passive mode respectively.

Establish OAM link on the CO device and remote device as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**oam** { **active** | **passive** }	Configure OAM working mode. Establish both sides of OAM link; configure the CO device to active mode and remote device to passive mode.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-port)#**oam enable**	Enable interface OAM.

10.5.5 Configure extended OAM protocols

Configure extended OAM protocols for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**extended-oam config-request enable**	Enable power-on configuration request.
3	Raisecom(config)#**extended-oam notification enable**	Enable sending extended OAM notification packets.

10.5.6 Entering remote configuration mode

Note

The interface can enter remote configuration mode only when OAM link is established between CO device and remote device.

Enter remote configuration mode for the CO device as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**remote-device**	Enter remote configuration mode.
4	Raisecom(config-remote)#**interface client** *client-id* Raisecom(config-remoteport)#	(Optional) enter remote interface configuration mode.

10.5.7 (Optional) showing remote extended OAM capacity

Caution

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

On the CO device, you can use the **show oam capability** command to show remote device extended OAM capacity, and then take configuration according to the specific device.

Show remote extended OAM capacity on the CO device as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**remote-device**	Enter remote configuration mode.
4	Raisecom(config-remote)#**show oam capability**	Show remote device extended OAM management capacity.

10.5.8 Configuring remote host name

Note

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Configure remote host name on the CO device as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**remote-device**	Enter remote configuration mode.
4	Raisecom(config-remote)#**hostname** *hostname*	Configure remote host name.

10.5.9 Configuring MTU for remote device

Caution

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Configure MTU for remote device as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**remote-device**	Enter remote configuration mode.
4	Raisecom(config-remote)#**system mtu** *size*	Configure MTU for the remote device.

10.5.10 Configuring IP address of remote device

Note

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Configure the IP address of the remote device as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface interface-type interface-number`	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#remote-device`	Enter remote configuration mode.
4	`Raisecom(config-remote)#ip address ip-address [ ip-mask ] vlan-list`	Configure remote device IP address. Configure the IP address of IP interface 0 on the remote device to take effect. IP address configuration needs to specify management VLAN, if this VLAN does not exist, create VLAN and take all interfaces as member interface by default; if associated VLAN exists, do not modify the member interface configuration.
5	`Raisecom(config-remote)#ip default-gateway ip-address`	(Optional) configure remote device default gateway. The default gateway and configured IP address of IP interface 0 need to be in the same network segment.

10.5.11 Configuring interface parameters on remote device

Note

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Configure different remote interface parameters in different mode:

- In remote interface configuration mode, configure remote interface Up/Down, speed and working mode, and so on.
- In remote configuration mode, configure remote interface auto-negotiation, interface bandwidth, and link-state tracking, and so on.

Configuring interface parameters in remote interface configuration mode

In remote interface configuration mode, configure remote interface Up/Down, rate and working mode, and so on.

Configure interface parameters in remote interface configuration mode as below.

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

Step	Command	Description
3	Raisecom(config-port)#**remote-device**	Enter remote configuration mode.
4	Raisecom(config-remote)#**interface client** *client-id*	Enter remote interface configuration mode.
5	Raisecom(config-remoteport)#**shutdown**	(Optional) shut down the remote interface.
6	Raisecom(config-remoteport)#**speed** { **auto** | **10**| **100** }	(Optional) configure the interface rate on the remote device.
7	Raisecom(config-remoteport)#**duplex** { **full** | **half** }	(Optional) configure remote device Client interface duplex mode. **Note** The OAM link maybe disconnect after configuring remote interface duplex mode.
8	Raisecom(config-remoteport)#**flowcontrol** { **on** | **off** }	(Optional) enable/disable flow control on the user interface of the remote device.

Configuring interface parameters in remote configuration mode

In remote configuration mode, configure remote interface auto-negotiation, interface bandwidth, and link-state tracking, and so on.

Configure interface parameters in remote configuration mode as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**remote-device**	Enter remote configuration mode.
4	Raisecom(config-remote)#**description** { **line** *line-id* | **client** *client-id* } *string*	(Optional) configure description of the interface on the remote device.
5	Raisecom(config-remote)#**line-speed auto**	(Optional) configure rate auto-negotiation on the Line interface of the remote device. You can configure the optical interface with auto-negotiation when the interface connecting remote device and CO device is the 1000 Mbit/s optical interface.

Step	Command	Description
6	Raisecom(config-remote)#**rate-limit** *interface-type interface-number* **ingress** *rate*	(Optional) configure ingress bandwidth of the remote interface.
7	Raisecom(config-remote)#**fault-pass enable**	(Optional) enable remote link-state tracking. The fault optical interface on the remote device changes to electrical port after being enabled with remote link-state tracking.
8	Raisecom(config-remote)#**inside-loopback** [**crc-recalculate**]	(Optional) enable inner loopback on the optical interface on the remote device.
9	Raisecom(config-remote)#**test cable-diagnostics**	Conduct virtual line detection on the remote device.

Note

For the above interface configuration in remote configuration mode:

- If the command line provides specified interface parameters, the corresponding configuration will take effect on specified interface.
- If the command line does not provide specified interface parameters, the corresponding configuration will take effect on all interfaces of the corresponding type on the remote device.

10.5.12 Uploading and downloading files on remote device

Downloading files from the server to the remote device

The system bootstrap file, system startup file, configuration files, and FPGA file can be forwarded from the CO device to the remote device, which can be initiated by the CO device or the remote device. If the CO device initiates this, it can upgrade multiple remote devices.

On the CO device, download files from the FTP/TFTP server to the remote device as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**remote-device**	Enter remote configuration mode.
4	Raisecom(config-remote)#**download** { **bootstrap** | **startup-config** | **system-boot** | **fpga** } { **ftp** *ip-address user-name password file-name* | **tftp** *ip-address file-name* }	On the CO device, download files from the FTP/TFTP server to the remote device.

On the remote device, download files from the FTP/TFTP server to the remote device as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**download** { **bootstrap** | **startup-config** | **system-boot** | **fpga** } { **ftp** *ip-address user-name password file-name* | **tftp** *ip-address file-name* }	On the remote device, download files from the FTP/TFTP server to the remote device.

Uploading files from the remote device to the server

The system bootstrap file, system startup file, configuration files, and FPGA file can be forwarded from the remote device to the server, which can be initiated by the CO device or the remote device. If the CO device initiates this, it cannot upgrade multiple remote devices.

On the CO device, upload files from the remote device to the server as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**remote-device**	Enter remote configuration mode.
4	Raisecom(config-remote)#**upload** { **startup-config** | **system-boot** } { **ftp** *ip-address user-name password file-name* | **tftp** *ip-address file-name* }	On the CO device, upload files from the remote device to the server.

On the remote device, upload files from the remote device to the server as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**upload** { **startup-config** | **system-boot** } { **ftp** *ip-address user-name password file-name* | **tftp** *ip-address file-name* }	On the remote device, upload files from the remote device to the server.

Downloading remote device files from the server to the CO device

The system bootstrap file, system startup file, configuration files, and FPGA file of the remote device can be downloaded through FTP or TFTP from the server to the CO device, and saved with a specified name in the flash of the remote device. This is prepared for further upgrading of the remote device.

Download remote device files from the server to the CO device as below.

Step	Command	Description
1	Raisecom#**download** { **remote-bootstrap** | **remote-system-boot** | **remote-startup-config** | **remote-fpga** } { **ftp** *ip-address user-name password file-name local-file-name* | **tftp** *ip-address file-name local-file-name* }	Download remote device files from the server to the CO device.

Uploading remote device files from the CO device to the server

Upload remote device files from the CO device to the server as below.

Step	Command	Description
1	Raisecom#**upload** { **remote-bootstrap** | **remote-system-boot** | **remote-startup-config** | **remote-fpga** } { **ftp** *ip-address user-name password file-name local-file-name* | **tftp** *ip-address file-name local-file-name* }	Upload remote device files from the CO device to the server.

Downloading files from the CO device to the remote device

The remote device files saved in the flash of the CO device can be downloaded to the remote device through extended OAM protocols, which can be initiated by the CO device or the remote device. If the CO device initiates this, it can upgrade multiple remote devices.

On the CO device, download files from the CO device to the remote device as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**remote-device**	Enter remote configuration mode.
4	Raisecom(config-remote)#**download** { **bootstrap** | **system-boot** | **fpga** } *file-name*	Download the system bootstrap file, system startup file, and FPGA file from the CO device to the remote device.
5	Raisecom(config-remote)#**download startup-config** [*file-name*]	Download configuration files from the CO device to the remote device.

On the remote device, download files from the CO device to the remote device as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface`** *`interface-type interface-number`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#`**`download`** `{` **`bootstrap`** `|` **`system-boot`** `|` **`fpga`** `}` *`file-name`*	Download the system bootstrap file, system startup file, and FPGA file from the CO device to the remote device.
4	`Raisecom(config-port)#`**`download startup-config`** `[` *`file-name`* `]`	Download configuration files from the CO device to the remote device.

10.5.13 Configuring remote network management

Caution

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Configuring remote network management

Configure the CO device as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port`** *`port-id`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#`**`remote-device`**	Enter remote configuration mode.
4	`Raisecom(config-remote)#`**`snmp-server community`** *`community-name`* `{` **`ro`** `|` **`rw`** `}`	Configure remote read/write community and read/write authority.

Configuring remote Trap

The remote device generates Trap information, which will be sent to CO device through OAM notification packet and then CO device will send the Trap to network management system.

To configure network management system to accept remote Trap, you need to enable remote Trap function on CO device and maybe enable to send extended OAM notification function on remote device.

Configure remote Trap for the CO device as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#snmp trap remote enable`	Enable remote device to send Trap function.

Note

To configure remote Trap, some remote devices need to perform the command of **extended-oam notification enable** to enable to send extended OAM notification function in remote configuration mode.

10.5.14 Configuring remote VLAN

Caution

- Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.
- Different remote devices may have different configuration commands.

You can configure remote VLAN and process packets received by the remote device according to VLAN configurations, such as configuring remote VLAN status and VLAN Tag property and creating remote VLAN group.

Remote VLAN status:

- **dot1q**: remote VLAN mode is Dot1q; the packets entering device interface will be forwarded in accordance with dot1q mode.
- **forbid**: forbid remote VLAN function; the packets entering device interface will be forwarded in accordance with transparent transmission mode.
- **port**: remote VLAN is Port mode.

Enable remote VLAN CoS function, deal with the packets entering device interface according to VLAN priority, high priority first and low priority second.

Configure remote VLAN for the CO device as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface port` *`port-id`*	Enter physical layer interface configuration mode.
3	`Raisecom(config-port)#remote-device`	Enter remote configuration mode.
4	`Raisecom(config-remote)#vlan { dot1q | forbid | port }`	(Optional) configure remote VLAN status.
5	`Raisecom(config-remote)#vlan cos enable`	(Optional) enable remote VLAN CoS.

Step	Command	Description
6	Raisecom(config-remote)#**vlan { cable-port | cpu-port | fiber-port } { tag | untag } priority** *priority* **pvid** *pvid*	(Optional) configure remote VLAN Tag property.
7	Raisecom(config-remote)#**vlan group** *group-id* **vid** *vid* **member-list** *member-list*	(Optional) create remote VLAN group.

10.5.15 Configuring remote QinQ

Note

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Configure remote QinQ for the CO device as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**remote-device**	Enter remote configuration mode.
4	Raisecom(config-remote)#**switch-mode transparent**	(Optional) configure the remote device to work in full transparent transmission mode.
5	Raisecom(config-remote)#s**witch-mode dot1q-vlan native-vlan** *vlan-id* [**line**]	(Optional) enable the remote device to work single Tag forwarding mode.
6	Raisecom(config-remote)#**switch-mode double-tagged-vlan** [**tpid** *tpid*] **native-vlan** *vlan-id* [**line**]	(Optional) configure the remote device to work in double Tag forwarding mode.

Note

- To configure remote device to work in full transparent transmission mode, do not deal with data packets.
- To configure remote device to work in single Tag mode, after the ISCOM21xx is configured to single Tag mode, the data packets without Tag from user interface will be marked with Tag with local VLAN ID; do nothing if there is Tag.
- To configure remote device to work in double Tag mode, after the ISCOM21xx is configured to double Tag mode, the data packets without Tag from user interface will be marked with outer Tag with specified TPID and local VLAN ID.

10.5.16 Managing remote configuration files

Note

Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Manage remote configuration files on the CO device as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**remote-device**	Enter remote configuration mode.
4	Raisecom(config-remote)#**write**	(Optional) save remote device configuration files in remote device flash.
5	Raisecom(config-remote)#**write local**	(Optional) save remote device configuration files in CO device flash.
6	Raisecom(config-remote)#**erase**	(Optional) delete remote device configuration files.

10.5.17 Rebooting remote device

Note

- During resetting or rebooting remote device, OAM link maybe disconnect and the CO device will not connect with remote device.
- Whether the remote device supports this function varies with the specific remote device. For details, see the corresponding manuals.

Configure rebooting the remote device on the CO device as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port** *port-id*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**remote-device**	Enter remote configuration mode.
4	Raisecom(config-remote)#**reboot**	Reboot remote device.

10.5.18 Checking configurations

Note

Whether the remote device supports the following items varies with the specific remote device. For details, see the corresponding manuals.

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom(config-remote)#show remote-device information`	Show basic information about the remote device.
2	`Raisecom#show extended-oam status [ port-list port-list ]`	Show extended OAM link status.
3	`Raisecom(config-remote)#show interface port [ detail | statistics ]`	Show information about the remote device interfaces.
4	`Raisecom(config-remote)#show cable-diagnostics`	Show information about line diagnosis.
5	`Raisecom(config-remote)#show inside-loopback`	Show loopback status on the optical interface on the remote device and loopback parameters.
6	`Raisecom(config-remote)#show oam capability`	Show OAM capabilities supported by the remote device.
7	`Raisecom(config-remote)#show remote-device information`	Show basic information about the remote device.
8	`Raisecom(config-remote)#show vlan basic-information`	Show basic information about VLANs on the remote device.
9	`Raisecom(config-remote)#show vlan group-information { all | group-id }`	Show information about VLAN groups on the remote device.
10	`Raisecom#show extended-oam statistics [ port-list port-list ]`	Show statistics of extended OAM frames.
11	`Raisecom#show snmp trap remote`	Show Trap enabling status on the remote device.

10.5.19 Maintenance

Maintain the ISCOM21xx as below.

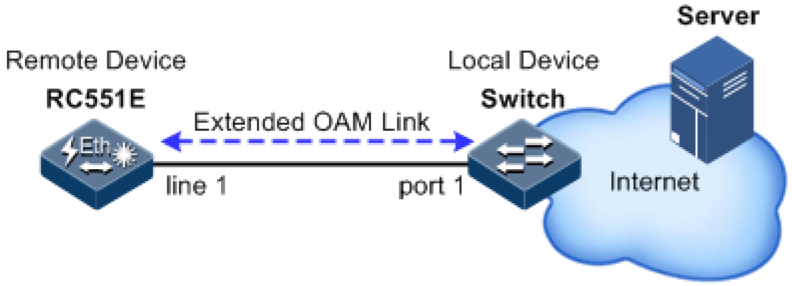
Command	Description
`Raisecom(config)#clear extended-oam statistics [ port-list port-list ]`	Clear statistics of extended OAM packets.

10.5.20 Example for configuring extended OAM to manage remote device

Networking requirements

As shown in Figure 10-12, the RC551E is connected to the Switch. Configured with extended OAM, the Switch can remotely manage the RC551E. Configure the host name and IP address of the RC551E on the Switch.

Figure 10-12 Configuring extended OAM to manage the remote device



Configuration steps

Step 1 Establish an OAM link between the RC551E and the switch.

Configure the RC551E to work in OAM passive mode, and enable OAM.

```
Raisecom#hostname RC55x
RC55x#config
RC55x(config)#oam passive
RC55x(config)#interface line 1
RC55x(config-port)#oam enable
```

Configure the switch to work in OAM active mode, and enable OAM.

```
Raisecom#hostname Switch
Switch#config
Switch(config)#oam active
Switch(config)#interface port 1
Switch(config-port)#oam enable
```

Step 2 Configure the host name and IP address of the RC551E on the switch.

```
Switch(config-port)#remote-device
Switch(config-remote)#hostname RC551E
Switch(config-remote)#ip address 192.168.18.100 255.255.255.0 200
```

Checking results

Use the following command to show configurations of the remote device on the switch.

```
Raisecom(config-remote)#show remote-device information
Local port:port1
Product Name:                           RC551E-4GEF
Hostname:                               RC551E
Operation Software Version:             ROS_4.14.1670.RC551E-
4GEF.39.20110914
Hardware Version:                        Hardware RC551E-4GEF
Main chip id:                            N/A
Total ports:                             6
FPGA chip id:                            N/A
FPGA soft version:                       N/A
IP Address/mask:                         192.168.18.100/255.255.255.0
IP Interface Vlan:                       0
Vlan member Port:
Untag port:
IP Default-gateway:                      0.0.0.0
OutBand-port IP/Mask:                     N/A/N/A
Community Name/Access:                    N/A/N/A
OAM Notification:
Device current temperature(Celsius):     0(Celsius)
Device voltage:                         low
Ref. Volt(mv)       Current Volt(mv)
3300           01
2500           01
1800           01
1200           01
```

10.6 Optical module DDM

10.6.1 Introduction

Digital Diagnostic Monitoring (DDM) on the ISCOM21xx supports diagnosing the Small Form-factor Pluggable (SFP) module.

SFP DDM provides a method for monitoring performance. By analyzing monitored data provides by the SFP module, the administrator can predict the lifetime for the SFP module, isolate system faults, as well as verify the compatibility of the SFP module.

The SFP module offers 5 performance parameters:

- Module temperature
- Internal Power Feeding Voltage (PFV)
- Launched bias current
- Launched optical power
- Received optical power

When SFP performance parameters exceed thresholds or when SFP state changes, related Trap is generated.

10.6.2 Preparing for configurations

Scenario

SFP DDM provides a method for monitoring performance parameters of the SFP module. By analyzing monitored data, you can predict the lifetime of the SFP module, isolate system faults, as well as verify the compatibility of the SFP module.

Prerequisite

N/A

10.6.3 Default configurations of optical module DDM

Default configurations of optical module DDM are as below.

Function	Default value
Optical module DDM	Disable
Optical module DDM sending Trap status	Enable

10.6.4 Enabling optical module DDM

Enable optical module DDM for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#transceiver digitaldiagnotic enable`	Enable optical module DDM.

10.6.5 Enabling optical module DDM to send Trap

Enable optical module DDM to send Trap for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#snmp trap transceiver enable`	Enable optical module DDM to send Trap.

10.6.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show interface port [ port-id ] transceiver [ detail ]`	Show configurations of optical module DDM.
2	`Raisecom#show interface port [ port-id ] transceiver [ detail ] threshold-violations`	Show performance parameters and thresholds of optical module DDM.
3	`Raisecom#show interface port [ port-id ] transceiver information`	Show information about the optical module DDM.

10.7 System log

10.7.1 Introduction

The system log means that the ISCOM21xx records the system information and debugging information in a log and sends the log to the specified destination. When the ISCOM21xx fails to work, you can check and locate the fault easily.

The system information and some scheduling output will be sent to the system log to deal with. According to the configuration, the system will send the log to various destinations. The destinations that receive the system log are divided into:

- Console: send the log message to the local console through the Console interface.
- Host: send the log message to the host.
- Monitor: send the log message to the monitor, such as Telnet terminal.
- File: send the log message to the Flash of the device.

The system log is usually in the following format:

```
timestamp  module-level- Message content
```

The following is an example of system log content.

```
FEB-22-2005 14:27:33  CONFIG-7-CONFIG:USER "raisecom"  Run "logging on"
FEB-22-2005 06:46:20  CONFIG-6-LINK_D:port 2 Link Down
FEB-22-2005 06:45:56  CONFIG-6-LINK_U:port 2 Link  UP
```

The format for outputting to the logging server is as below:

```
timestamp  module-level- Message content
```

The following is an example of log content for the logging server.

```
07-01-200811:31:28Local0.Debug20.0.0.6JAN 01 10:22:15 ISCOM2110: CONFIG-
7-CONFIG:USER " raisecom "  Run " logging on "
07-01-200811:27:41Local0.Debug20.0.0.6JAN 01 10:18:30 ISCOM2110: CONFIG-
7-CONFIG:USER " raisecom "  Run " ip address 20.0.0.6 255.0.0.0 1 "
```

The log is classified into 8 severity levels, as listed in Table 10-2.

Table 10-2 Log levels

Severity	Level	Description
Emergency	0	The system cannot be used.
Alert	1	Need to deal immediately.
Critical	2	Serious status
Error	3	Errored status
Warning	4	Warning status
Notice	5	Normal but important status
Informational	6	Informational event
Debug	7	Debugging information

Note

The severity of output information can be manually configured. When you send information according to the configured severity, you can just send the information whose severity is less than or equal to that of the configured information. For example, when the information is configured with the level 3 (or the severity is errors), the information whose level ranges from 0 to 3,that is, the severity ranges from emergencies to errors, can be sent.

10.7.2 Preparing for configurations

Scenario

The ISCOM21xx generates critical information, debugging information, or error information of the system to system logs and outputs the system logs to log files or transmit them to the host, Console interface, or monitor for viewing and locating faults.

Prerequisite

N/A

10.7.3 Default configurations of system log

Default configurations of system log are as below.

Function	Default value
System log	Enable
Output log information to Console	Enable, the default level is information (6).
Output log information to host	N/A, the default level is information (6).
Output log information to file	Disable, the fixed level is warning (4).
Output log information to monitor	Disable, the default level is information (6).
Log Debug level	Low
Transmitting rate of system log	No limit

10.7.4 Configuring basic information of system log

Configure basic information of system log for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#logging on`	(Optional) Enable system log.
3	`Raisecom(config)#logging time-stamp { date-time | null | relative-start }`	(Optional) configure timestamp for system log.
4	`Raisecom(config)#logging rate log-num`	(Optional) configure transmitting rate of system log.

10.7.5 Configuring system log output

Configure system log output for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#logging console { log-level | alerts | critical | debugging | emergencies | errors | informational | notifications | warnings }`	(Optional) output system logs to the Console.

Step	Command	Description
3	`Raisecom(config)#logging host ip-address { local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7 } { log-level | alerts | critical | debugging | emergencies | errors | informational | notifications | warnings }`	(Optional) output system logs to the log server. Up to 10 log servers are supported.
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`	(Optional) output system logs to the Flash of the ISCOM21xx. Only warning-level logs are available.

10.7.6 Checking configurations

Use the following commands to check configuration results.

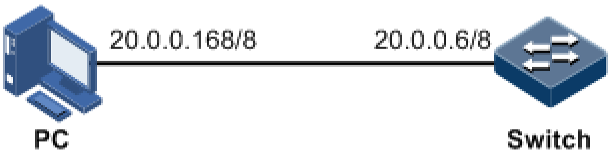
No.	Command	Description
1	`Raisecom#show logging`	Show configurations of system log.
2	`Raisecom#show logging file`	Show contents of system log.

10.7.7 Example for outputting system logs to log server

Networking requirements

As shown in Figure 10-13, configure system log to output system logs of the switch to the log server, facilitating view them at any time.

Figure 10-13 Outputting system logs to log servers



Configuration steps

Step 1 Configure the IP address of the switch.

```
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 server.

```
Raisecom(config)#logging on
Raisecom(config)#logging time-stamp date-time
Raisecom(config)#logging rate 2
Raisecom(config)#logging host 20.0.0.168 local3 warnings
```

Checking results

Use the **show logging** command to show configurations of system log.

```
Raisecom#show logging
Syslog logging:Enable, 0 messages dropped, messages rate-limited 2 per
second
Console logging:Enable, level=informational, 19 Messages logged
Monitor logging:Disable, level=informational, 0 Messages logged
Time-stamp logging messages: date-time

Log host information:
Target Address      Level          Facility     Sent      Drop
----------------------------------------------------------------------
20.0.0.168         warnings        local3       0        0
```

10.8 Power monitoring

10.8.1 Introduction

The ISCOM21xx supports monitoring power alarm, namely, Dying Gasp alarm.

10.8.2 Preparing for configurations

Scenario

You can configure the power alarm function to monitor faults. When the power is abnormal, the system generates the Syslog or sends Trap message, informing you to take actions accordingly to avoid power failure.

Prerequisite

N/A

10.8.3 Default configurations of power monitoring

Default configurations of power monitoring are as below.

Function	Description
Power alarm Trap sending status	Enable

10.8.4 Configuring power monitoring alarm

Configure power monitoring alarm for the ISCOM21xx as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`alarm power`**	Enable sending power alarm Trap.

10.8.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show alarm power`**	Show power alarm status.

10.9 CPU monitoring

10.9.1 Introduction

The ISCOM21xx supports CPU monitoring. It can monitor state, CPU utilization, and stack usage in real time. It helps to locate faults.

CPU monitoring can provide the following functions:

- View CPU utilization

It can be used to view CPU unitization in each period (5s, 1 minute, 10 minutes, and 2 hours). Total CPU unitization in each period can be shown dynamically or statically.

It can be used to view the operating status of all tasks and the detailed running status of assigned tasks.

It can be used to view history CPU utilization in each period.

It can be used to view death task information.

- CPU unitization threshold alarm

If system CPU utilization changes below lower threshold or above upper threshold in a specified sampling period, an alarm will be generated and a Trap message will be sent. The Trap message provides serial number and CPU utilization of 5 tasks whose CPU unitization is the highest in the latest period (5s, 1 minute, 10 minutes).

10.9.2 Preparing for configurations

Scenario

CPU monitoring can monitor state, CPU utilization, and stack usage in real time, provide CPU utilization threshold alarm, detect and eliminate hidden dangers, or help the administrator with fault location.

Prerequisite

When the CPU monitoring alarm needs to be output in Trap mode, configure Trap output target host address, which is IP address of NView NNM system.

10.9.3 Default configurations of CPU monitoring

Default configurations of CPU monitoring are as below.

Function	Default value
CPU utilization rate alarm Trap output	Disable
Upper threshold of CPU utilization alarm	100%
Lower threshold of CPU utilization alarm	1%
Sampling period of CPU utilization	60s

10.9.4 Showing CPU monitoring information

Show CPU monitoring information for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**show cpu-utilization** [**dynamic** | **history** { **10min** | **1min** | **2hour** | **5sec** }]	Show CPU utilization.
2	Raisecom#**show process** [**dead** | **sorted** { **normal-priority** | **process-name** } | *taskname*]	Show states of all tasks.
3	Raisecom#**show process cpu** [**sorted** [**10min** | **1min** | **5sec** | **invoked**]]	Show CPU utilization of all tasks.

10.9.5 Configuring CPU monitoring alarm

Configure CPU monitoring alarm for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server traps enable cpu-threshold**	Enable CPU threshold alarm Trap.
3	Raisecom(config)#**cpu rising-threshold** *rising-threshold-value* [**falling-threshold** *falling-threshold-value*] [**interval** *interval-value*]	(Optional) configure CPU alarm upper threshold, lower threshold, and sampling interval. The upper threshold must be greater than the lower threshold. After CPU threshold alarm Trap is enabled, the system will automatically send Trap if the CPU utilization changes below lower threshold or above upper threshold in a specified sampling period.

10.9.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show cpu-utilization**	Show CPU utilization and related configurations.

10.10 Ping

Configure Ping for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**ping** *ip-address* [**count** *count*] [**size** *size*] [**waittime** *period*]	(Optional) test the connectivity of the IPv4 network through the **ping** command.
2	Raisecom#**ping6** *ipv6-address* [**scopeid** *scopeid*] [**count** *count*] [**size** *size*] [**waittime** *waittime*]	(Optional) test the connectivity of the IPv6 network through the **ping** command.

Note

The ISCOM21xx cannot carry out other operations in the process of executing the **ping** command. You can perform other operations only after Ping is finished or press **Ctrl**+**C** to forcibly interrupt the process.

10.11 Traceroute

Before using Traceroute, you should configure the IP address and default gateway of the ISCOM21xx.

Configure Traceroute for the ISCOM21xx as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip default-gateway** *ip-address*	Configure the default gateway.
3	Raisecom(config)#**exit** Raisecom#**traceroute** *ip-address* [**firstttl** *first-ttl*] [**maxttl** *max-ttl*] [**port** *port-id*] [**waittime** *second*] [**count** *times*]	Test the connectivity of the IPv4 network, and show nodes traversed by the packet.
4	Raisecom#**traceroute ipv6** *ipv6-address* [**firstttl** *first-ttl*] [**maxttl** *max-ttl*] [**port** *port-id*] [**waittime** *second*] [**count** *times*]	Test the connectivity of the IPv6 network, and show nodes traversed by the packet.

11 Appendix

This chapter lists terms, acronym, and abbreviations involved in this document, including the following sections:

- Terms
- Acronyms and abbreviations

11.1 Terms

A

Access Control List (ACL)	A series of ordered rules composed of permit | deny sentences. These rules are based on the source MAC address, destination MAC address, source IP address, destination IP address, interface ID, and so on. The device decides to receive or refuse the packets based on these rules.
Automatic Laser Shutdown (ALS)	The technology that is used for automatically shutting down the laser to avoid the maintenance and operation risks when the fiber is pulled out or the output power is over great.
Auto-negotiation	The interface automatically chooses the rate and duplex mode according to the result of negotiation. The auto-negotiation process is: the interface adapts its rate and duplex mode to the highest performance according to the peer interface, that is, both ends of the link adopt the highest rate and duplex mode they both support after auto-negotiation.
Automatic Protection Switching (APS)	APS is used to monitor transport lines in real time and automatically analyze alarms to discover faults. When a critical fault occurs, through APS, services on the working line can be automatically switched to the protection line, thus the communication is recovered in a short period.

B

Bracket	Small parts at both sides of the chassis, used to install the chassis into the cabinet

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.

Challenge Handshake Authentication Protocol (CHAP)

CHAP is a widely supported authentication method in which a representation of the user's password, rather than the password itself, is sent during the authentication process. With CHAP, the remote access server sends a challenge to the remote access client. The remote access client uses a hash algorithm (also known as a hash function) to compute a Message Digest-5 (MD5) hash result based on the challenge and a hash result computed from the user's password. The remote access client sends the MD5 hash result to the remote access server. The remote access server, which also has access to the hash result of the user's password, performs the same calculation using the hash algorithm and compares the result to the one sent by the client. If the results match, the credentials of the remote access client are considered authentic. A hash algorithm provides one-way encryption, which means that calculating the hash result for a data block is easy, but determining the original data block from the hash result is mathematically infeasible.

D

Dynamic ARP Inspection (DAI)

A security feature that can be used to verify the ARP data packets in the network. With DAI, the administrator can intercept, record, and discard ARP packets with invalid MAC address/IP address to prevent common ARP attacks.

Dynamic Host Configuration Protocol (DHCP)

A technology used for assigning IP address dynamically. It can automatically assign IP addresses for all clients in the network to reduce workload of the administrator. In addition, it can implement centralized management of IP addresses.

E

Ethernet in the First Mile (EFM)

Complying with IEEE 802.3ah protocol, EFM is a link-level Ethernet OAM technology. It provides the link connectivity detection, link fault monitoring, and remote fault notification, and so on for a link between two directly-connected devices. EFM is mainly used for the Ethernet link on edges of the network accessed by users.

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

Full duplex

In a communication link, both parties can receive and send data concurrently.

G

GFP encapsulation

Generic Framing Procedure (GFP) is a generic mapping technology. It can group variable-length or fixed-length data for unified adaption, making data services transmitted through multiple high-speed physical transmission channels.

Ground cable

The cable to connect the device to ground, usually a yellow/green coaxial cable. Connecting the ground cable properly is an important guarantee to lightning protection, anti-electric shock, and anti-interference.

H

Half duplex

In a communication link, both parties can receive or send data at a time.

I

Institute of Electrical and Electronics Engineers (IEEE)

A professional society serving electrical engineers through its publications, conferences, and standards development activities. The body responsible for the Ethernet 802.3 and wireless LAN 802.11 specifications.

Internet Assigned Numbers Authority (IANA)

The organization operated under the IAB. IANA delegates authority for IP address-space allocation and domain-name assignment to the NIC and other organizations. IANA also maintains a database of assigned protocol identifiers used in the TCP/IP suite, including autonomous system numbers.

Internet Engineering Task Force (IETF)

A worldwide organization of individuals interested in networking and the Internet. Managed by the Internet Engineering Steering Group (IESG), the IETF is charged with studying technical problems facing the Internet and proposing solutions to the Internet Architecture Board (IAB). The work of the IETF is carried out by various working groups that concentrate on specific topics, such as routing and security. The IETF is the publisher of the specifications that led to the TCP/IP protocol standard.

L

Label

Symbols for cable, chassis, and warnings

Link Aggregation

With link aggregation, multiple physical Ethernet interfaces are combined to form a logical aggregation group. Multiple physical links in one aggregation group are taken as a logical link. Link aggregation helps share traffic among member interfaces in an aggregation group. In addition to effectively improving the reliability on links between devices, link aggregation can help gain greater bandwidth without upgrading hardware.

Link Aggregation Control Protocol (LACP)

A protocol used for realizing link dynamic aggregation. The LACPDU is used to exchange information with the peer device.

Link-state tracking

Link-state tracking 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.

M

Multi-mode fiber

In this fiber, multi-mode optical signals are transmitted.

N

Network Time Protocol (NTP)

A time synchronization protocol defined by RFC1305. It is used to synchronize time between distributed time server and clients. NTP is used to perform clock synchronization on all devices that have clocks in the network. Therefore, the devices can provide different applications based on a unified time. In addition, NTP can ensure a very high accuracy with an error of 10ms or so.

O

Open Shortest Path First (OSPF)

An internal gateway dynamic routing protocol, which is used to decide the route in an Autonomous System (AS)

Optical Distribution Frame (ODF)

A distribution connection device between the fiber and a communication device. It is an important part of the optical transmission system. It is mainly used for fiber splicing, optical connector installation, fiber adjustment, additional pigtail storage, and fiber protection.

P

Password Authentication Protocol (PAP)	PAP is an authentication protocol that uses a password in Point-to-Point Protocol (PPP). It is a twice handshake protocol and transmits unencrypted user names and passwords over the network. Therefore, it is considered unsecure.
Point-to-point Protocol over Ethernet (PPPoE)	PPPoE is a network protocol for encapsulating PPP frames in Ethernet frames. With PPPoE, the remote access device can control and account each access user.
Private VLAN (PVLAN)	PVLAN adopts Layer 2 isolation technology. Only the upper VLAN is visible globally. The lower VLANs are isolated from each other. If you partition each interface of the switch or IP DSLAM device into a lower VLAN, all interfaces are isolated from each other.

Q

QinQ	802.1Q in 802.1Q (QinQ), also called Stacked VLAN or Double VLAN, is extended from 802.1Q and defined by IEEE 802.1ad recommendation. This VLAN feature allows the equipment to add a VLAN Tag to a Tagged packet. The implementation of QinQ is to add a public VLAN Tag to a packet with a private VLAN Tag, making the packet encapsulated with two layers of VLAN Tags. The packet is forwarded over the ISP's backbone network based on the public VLAN Tag and the private VLAN Tag is transmitted as the data part of the packet. In this way, the QinQ feature enables the transmission of the private VLANs to the peer end transparently. There are two QinQ types: basic QinQ and selective QinQ.
Quality of Service (QoS)	A network security mechanism, used to solve problems of network delay and congestion. When the network is overloaded or congested, QoS can ensure that packets of important services are not delayed or discarded and the network runs high efficiently. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio.

R

Rapid Spanning Tree Protocol (RSTP)	Evolution of the Spanning Tree Protocol (STP), which provides improvements in the speed of convergence for bridged networks
Remote Authentication Dial In User Service (RADIUS)	RADIUS refers to a protocol used to authenticate and account users in the network. RADIUS works in client/server mode. The RADIUS server is responsible for receiving users' connection requests, authenticating users, and replying configurations required by all clients to provide services for users.

S

Simple Network Management Protocol (SNMP)	A network management protocol defined by Internet Engineering Task Force (IETF) used to manage devices in the Internet. SNMP can make the network management system to remotely manage all network devices that support SNMP, including monitoring network status, modifying network device configurations, and receiving network event alarms. At present, SNMP is the most widely-used network management protocol in the TCP/IP network.
Simple Network Time Protocol (SNTP)	SNTP is mainly used for synchronizing time of devices in the network.
Single-mode fiber	In this fiber, single-mode optical signals are transmitted.
Spanning Tree Protocol (STP)	STP can be used to eliminate network loops and back up link data. It blocks loops in logic to prevent broadcast storms. When the unblocked link fails, the blocked link is re-activated to act as the backup link.

V

Virtual Local Area Network (VLAN)	VLAN is a protocol proposed to solve broadcast and security issues for Ethernet. It divides devices in a LAN into different segments logically rather than physically, thus implementing multiple virtual work groups which are based on Layer 2 isolation and do not affect each other.
VLAN mapping	VLAN mapping is mainly used to replace the private VLAN Tag of the Ethernet service packet with the ISP's VLAN Tag, making the packet transmitted according to ISP's VLAN forwarding rules. When the packet is sent to the peer private network from the ISP network, the VLAN Tag is restored to the original private VLAN Tag according to the same VLAN forwarding rules. Thus, the packet is sent to the destination correctly.

11.2 Acronyms and abbreviations

A

AAA	Authentication, Authorization and Accounting
ABR	Area Border Router
AC	Alternating Current
ACL	Access Control List
ANSI	American National Standards Institute
APS	Automatic Protection Switching
ARP	Address Resolution Protocol

AS	Autonomous System
ASCII	American Standard Code for Information Interchange
ASE	Autonomous System External
ATM	Asynchronous Transfer Mode
AWG	American Wire Gauge

B

BC	Boundary Clock
BDR	Backup Designated Router
BITS	Building Integrated Timing Supply System
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
BTS	Base Transceiver Station

C

CAR	Committed Access Rate
CAS	Channel Associated Signaling
CBS	Committed Burst Size
CE	Customer Edge
CHAP	Challenge Handshake Authentication Protocol
CIDR	Classless Inter-Domain Routing
CIR	Committed Information Rate
CIST	Common Internal Spanning Tree
CLI	Command Line Interface
CoS	Class of Service
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
CST	Common Spanning Tree

D

DAI	Dynamic ARP Inspection
DBA	Dynamic Bandwidth Allocation

DC	Direct Current
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Service
DNS	Domain Name System
DRR	Deficit Round Robin
DS	Differentiated Services
DSL	Digital Subscriber Line
E	
EAP	Extensible Authentication Protocol
EAPoL	EAP over LAN
EFM	Ethernet in the First Mile
EMC	Electro Magnetic Compatibility
EMI	Electro Magnetic Interference
EMS	Electro Magnetic Susceptibility
ERPS	Ethernet Ring Protection Switching
ESD	Electro Static Discharge
EVC	Ethernet Virtual Connection
F	
FCS	Frame Check Sequence
FE	Fast Ethernet
FIFO	First Input First Output
FTP	File Transfer Protocol
G	
GARP	Generic Attribute Registration Protocol
GE	Gigabit Ethernet
GMRP	GARP Multicast Registration Protocol
GPS	Global Positioning System
GVRP	Generic VLAN Registration Protocol
H	

HDLC	High-level Data Link Control
HTTP	Hyper Text Transfer Protocol

I

IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IE	Internet Explorer
IEC	International Electro technical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IS-IS	Intermediate System to Intermediate System Routing Protocol
ISP	Internet Service Provider
ITU-T	International Telecommunications Union - Telecommunication Standardization Sector

L

LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit
LAN	Local Area Network
LCAS	Link Capacity Adjustment Scheme
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit

M

MAC	Medium Access Control
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface cross-over
MIB	Management Information Base
MSTI	Multiple Spanning Tree Instance
MSTP	Multiple Spanning Tree Protocol
MTBF	Mean Time Between Failure

MTU	Maximum Transmission Unit
MVR	Multicast VLAN Registration

N

NMS	Network Management System
NNM	Network Node Management
NTP	Network Time Protocol
NView NNM	NView Network Node Management

O

OAM	Operation, Administration and Management
OC	Ordinary Clock
ODF	Optical Distribution Frame
OID	Object Identifiers
Option 82	DHCP Relay Agent Information Option
OSPF	Open Shortest Path First

P

P2MP	Point to Multipoint
P2P	Point-to-Point
PADI	PPPoE Active Discovery Initiation
PADO	PPPoE Active Discovery Offer
PADS	PPPoE Active Discovery Session-confirmation
PAP	Password Authentication Protocol
PDU	Protocol Data Unit
PE	Provider Edge
PIM-DM	Protocol Independent Multicast-Dense Mode
PIM-SM	Protocol Independent Multicast-Sparse Mode
Ping	Packet Internet Grope
PPP	Point to Point Protocol
PPPoE	PPP over Ethernet
PTP	Precision Time Protocol

Q

QoS	Quality of Service

R

RADIUS	Remote Authentication Dial In User Service
RCMP	Raisecom Cluster Management Protocol
RED	Random Early Detection
RH	Relative Humidity
RIP	Routing Information Protocol
RMON	Remote Network Monitoring
RNDP	Raisecom Neighbor Discover Protocol
ROS	Raisecom Operating System
RPL	Ring Protection Link
RRPS	Raisecom Ring Protection Switching
RSTP	Rapid Spanning Tree Protocol
RSVP	Resource Reservation Protocol
RTDP	Raisecom Topology Discover Protocol

S

SCADA	Supervisory Control And Data Acquisition
SF	Signal Fail
SFP	Small Form-factor Pluggable
SFTP	Secure File Transfer Protocol
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SP	Strict-Priority
SPF	Shortest Path First
SSHv2	Secure Shell v2
STP	Spanning Tree Protocol

T

TACACS+	Terminal Access Controller Access Control System

TC	Transparent Clock
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TLV	Type Length Value
ToS	Type of Service
TPID	Tag Protocol Identifier
TTL	Time To Live

U

UDP	User Datagram Protocol
UNI	User Network Interface
USM	User-Based Security Model

V

VLAN	Virtual Local Area Network
VRRP	Virtual Router Redundancy Protocol

W

WAN	Wide Area Network
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