RAISECOM

www.raisecom.com

ISCOM2600G (A) Series Configuration Guide (Rel_04)

Raisecom Technology Co., Ltd. provides customers with comprehensive technical support and services. For any assistance, please contact our local office or company headquarters.

Website: http://www.raisecom.com

Tel: 8610-82883305

Fax: 8610-82883056

Email: export@raisecom.com

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

Postal code: 100094

Notice

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

Preface

Objectives

This document describes features supported by the ISCOM2600G series switch, and related configurations, including basic configurations, basic principles and configuration procedures of Ethernet, ring network protection, IP route, reliability, 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 ISCOM2600G series switch, and how to network with the ISCOM2600G series switch.

Versions

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

Product name	Software version	Hardware version
ISCOM2600G series switch	V3.10	A

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.

Symbol	Description
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. One is selected.
[x | y | ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x | y | ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[x | y | ...] *	The parameter before the & sign can be repeated 1 to n times.

Change history

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

Issue 04 (2016-05-12)

Fourth commercial release

- Added descriptions of PoE.

Issue 03 (2015-11-30)

Third commercial release

- Upgraded the software version to V3.10.
- Fixed known bugs.

Issue 02 (2015-11-05)

Second commercial release

- Optimized the document.
- Fixed known bugs.

Issue 01 (2015-08-15)

Initial commercial release

Contents

Figures

Tables

1 Basic configurations

This chapter describes basic configurations and configuration procedures of the ISCOM2600G series switch, and provides related configuration examples, including the following sections:

- CLI
- Accessing device
- Managing files
- Load and upgrade
- Automatically updating version and configurations
- Time management
- Interface management
- Configuring basic information
- Task scheduling
- Watchdog

1.1 CLI

1.1.1 Introduction

The Command-line Interface (CLI) is a medium for you to communicate with the ISCOM2600G series switch. You can configure, monitor, and manage the ISCOM2600G series switch through the CLI.

You can log in to the ISCOM2600G series switch through the terminal equipment or through a computer that runs the terminal emulation program. Enter commands at the system prompt.

The CLI supports the following features:

- Configure the ISCOM2600G series switch locally through the Console interface.
- Configure the ISCOM2600G series switch locally or remotely through Telnet/Secure Shell v2 (SSHv2).
- Commands are classified into different levels. You can execute the commands that correspond to your level only.

- The commands available to you depend on which mode you are currently in.
- Shortcut keys can be used to execute commands.
- Check or execute a history command by checking command history. The last 20 history commands can be saved on the ISCOM2600G series switch.
- Enter a question mark (?) at the system prompt to obtain online help.
- The ISCOM2600G series switch supports multiple intelligent analysis methods, such as fuzzy match and context association.

1.1.2 Levels

The ISCOM2600G series switch uses hierarchy protection methods to divide command line into 16 levels in ascending order.

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

1.1.3 Modes

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

Establish a connection with the ISCOM2600G series switch. If the ISCOM2600G series switch is in default configuration, it will enter user EXEC mode, and the screen will display:

```
Raisecom>
```

Note

Users under level 11 do not need to enter the password when entering privileged EXEC mode.

In privileged EXEC mode, use 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 using the **hostname** *string* command in privileged EXEC mode.
- Commands executed in global configuration mode can also be executed in other modes. The functions vary on command modes.

- You can use the **exit** or **quit** command to return to the upper command mode.
- You can execute the **end** command to return to privileged EXEC mode from any modes but user EXEC mode and privileged EXEC mode.

The ISCOM2600G series switch supports the following command line modes:

Mode	Enter method	Description
Privileged EXEC	In user EXEC mode, enter the **enable** command and correct password.	`Raisecom#`
Global configuration	In privileged EXEC mode, enter the **config terminal** command.	`Raisecom(config)#`

Physical layer interface configuration	In global configuration mode, enter the **interface** { **gigaethernet** | **tengigethernet** } *unit/slot/interface* command.	`Raisecom(config-gigaethernet1/1/`*`interface`*`)#`
		`Raisecom(config-tengigaethernet1/1/`*`interface`*`)#`

SNMP interface configuration	In global configuration mode, enter the **interface fastethernet 1/0/1** command.	`Raisecom(config-fastethernet1/0/1)#`
Loopback interface configuration	In global configuration mode, enter the **interface loopback** *lb-number* command.	`Raisecom(config-loopback)#`
VLAN configuration	In global configuration mode, enter the **vlan** *vlan-id* command.	`Raisecom(config-vlan)#`
Aggregation group configuration	In global configuration mode, enter the **interface port-channel** *channel-number* command.	`Raisecom(config-port-channel)#`
Traffic classification configuration	In global configuration mode, enter the **class-map** *class-map-name* command.	`Raisecom(config-cmap)#`
Traffic policy configuration	In global configuration mode, enter the **policy-map** *policy-map-name* command.	`Raisecom(config-pmap)#`
Traffic policy configuration binding with traffic classification	In floe policy configuration mode, enter the **class-map** *class-map-name* command.	`Raisecom(config-pmap-c)#`
Basic IP ACL configuration	In global configuration mode, enter the **access-list** *acl-number* command. Wherein, *acl-number* ranges from 1000 to 1999.	`Raisecom(config-acl-ipv4-std)#`
Extended IP ACL configuration	In global configuration mode, enter the **access-list** *acl-number* command. Wherein, *acl-number* ranges from 2000 to 2999.	`Raisecom(config-acl-ipv4-ext)#`

Mode	Enter method	Description
MAC ACL configuration	In global configuration mode, enter the **access-list** *acl-number* command. Wherein, *acl-number* ranges from 3000 to 3999.	`Raisecom(config-acl-mac)#`
User ACL configuration	In global configuration mode, enter the **access-list** *acl-number* command. Wherein, *acl-number* ranges from 5000 to 5999.	`Raisecom(config-acl-udf)#`
MST region configuration	In global configuration mode, enter the **spanning-tree region-configuration** command.	`Raisecom(config-region)#`
Profile configuration	In global configuration mode, enter the **igmp filter profile** *profile-number* command.	`Raisecom(config-igmp-profile)#`
cos-remark configuration	In global configuration mode, enter the **mls qos mapping cos-remark** *profile-id* command.	`Raisecom(cos-remark)#`
cos-to-pri configuration	In global configuration mode, enter the **mls qos mapping cos-to-local-priority** *profile-id* command.	`Raisecom(cos-to-pri)#`
dscp-mutation configuration	In global configuration mode, enter the **mls qos mapping dscp-mutation** *profile-id* command.	`Raisecom(dscp-mutation)#`
dscp-to-pri configuration	In global configuration mode, enter the **mls qos mapping dscp-to-local-priority** *profile-id* command.	`Raisecom(dscp-to-pri)#`
SRED profile configuration	In global configuration mode, enter the **mls qos sred profile** *profile-id* command.	`Raisecom(sred)#`
CMAP configuration	In global configuration mode, enter the **class-map** *class-map-name* command.	`Raisecom(config-cmap)#`
Traffic monitoring profile configuration	In global configuration mode, enter the **mls qos policer-profile** *policer-name* [**single**] command.	`Raisecom(traffic-policer)#`
PMAP configuration	In global configuration mode, enter the **policy-map** *policy-map-name* command.	`Raisecom(config-pmap)#`

Mode	Enter method	Description
Traffic policy bound with traffic classification configuration	In PMAP configuration mode, enter the **class-map** *class-map-name* command.	`Raisecom(config-pmap-c)#`
Chinese prompt	In any configuration mode, enter the **language chinese** command.	`Raisecom#`
English prompt	In any configuration mode, enter the **language english** command.	`Raisecom#`

1.1.4 Shortcut keys

The ISCOM2600G series switch supports the following 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.

Shortcut key	Description
Ctrl+A	Move the cursor to the beginning of the command.
Ctrl+B	Identical to the **Left Arrow** key.
Ctrl+C	Interrupt the ongoing command, such as **ping** and **traceroute**.
Ctrl+D or **Delete**	Delete the character at the cursor.
Ctrl+E	Move the cursor to the end of the command.
Ctrl+F	Identical to the Right Arrow key
Ctrl+K	Delete all characters from the cursor to the end of the command.
Ctrl+L	Clear screen information.
Ctrl+S	Identical to the **Down Arrow** key
Ctrl+W	Identical to the **Up Arrow** key
Ctrl+X	Delete all characters before the cursor (except the cursor location).
Ctrl+Y	Show history commands.
Ctrl+Z	Return to privileged EXEC mode from the current mode (except user EXEC mode).
Space bar or **Y**	Scroll down one screen.
Enter	Scroll down one line.

1.1.5 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 as below.

```
clear     Clear screen
enable    Turn on privileged mode command
exit      Exit current mode and down to previous mode
help      Message about help
history  Most recent history command
```

```
language  Language of help message
list      List command
quit      Exit current mode and down to previous mode
terminal  Configure terminal
```

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

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

The command output is 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 bar** 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 as below.

```
<0-254>  IP interface number
```

Incomplete help

You can acquire incomplete help under following three conditions:

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

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

The command output is as below.

```
cache              Cache information
class-map          Set class map
```

```
clear                Clear screen
cluster              Cluster configuration mode
cluster-autoactive   Cluster autoactive function
command-log          Log the command to the file
cpu                  Configure cpu parameters
create               Create static VLAN
```

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

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

The command output is as below.

```
link-aggregation     Link aggregation
link-state-tracking  Link state tracking
```

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

Error messages

The ISCOM2600G series switch prints out the following error messages according to error type when you enter incorrect commands:

Error message	Description
% Incomplete command.	The user has entered an incomplete command.
Error input in the position marked by '^'.	The keyword marked "^" is invalid.
Ambiguous input in the position marked by '^'	The keyword marked "^" is not clear.

Note

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

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

Filtering displayed information

The ISCOM2600G series switch supports a series of commands starting with **show**, to check device configurations, operation and diagnostic information. Generally, these commands can output more information, and then you need to add filtering rules to filter out unnecessary information.

The **show** command on the ISCOM2600G series switch supports three kinds of filter modes:

- | **begin** *string*: show all lines starting from the assigned string.
- | **exclude** *string*: show all lines mismatch with the assigned string.
- | **include** *string*: show all lines only match with the assigned string.

Page-break

Page-break is used to suspend displaying messages when they are displayed at more than one screen. After page-break is enabled, you can use shortcut keys listed in Table 1-1. 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 terminal page-break for the ISCOM2600G series switch as below.

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

1.1.7 Command history

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

Configure the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**terminal history** *number*	(Optional) configure the number of history commands saved in the system.
2	Raisecom#**terminal time-out** *period*	(Optional) configure the Console terminal timeout period.
3	Raisecom#**history**	Show history commands entered by the user.
4	Raisecom#**show terminal**	Show terminal configurations of the user.

1.1.8 Restoring default value of command line

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

- **no** form: be provided in front of a command and used to restore the default value, disable some feature, or delete a configuration. It is used to 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: 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 interface 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 and restore to the default values.
- In physical layer interface configuration mode, the **shutdown** command is used to disable an interface while the **no shutdown** command is used to enable an interface.
- In global configuration mode, the **terminal page-break enable** command is used to enable page-break while the **terminal page-break disable** command is used to disable terminal page-break.

Note

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

1.1.9 Logging command lines

Configure the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**command-log enable** Raisecom(config)#**exit**	Enable command line logging.

1.2 Accessing device

1.2.1 Introduction

The ISCOM2600G series switch can be configured and managed in Command Line Interface (CLI) mode or NView NNM network management mode.

The ISCOM2600G series switch CLI mode has a variety of configuration modes:

- Console mode: it must use Console mode in the first configuration.
- Telnet mode: log on through the Console mode, open Telnet service on the Switch, configure the IP address of the VLAN interface, configure the user name and password, and then take remote Telnet configuration.
- SSH mode: before accessing the ISCOM2600G series switch through SSH, you need to log in to the ISCOM2600G series switch and start the SSH service through the Console interface.

When configuring the ISCOM2600G series switch in network management mode, you must first configure the IP address of the VLAN interface on CLI, and then configure the ISCOM2600G series switch through NView NNM network management platform.

1.2.2 Accessing through Console interface

Introduction

The Console interface is an interface which is commonly used to connect the network device with a PC running terminal emulation programs. You can use this interface to configure and manage local devices. 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 ISCOM2600G series switch through the Console interface when the network fails.

In the following two conditions, you can only log in to the ISCOM2600G series switch and configure it through the Console interface:

- The ISCOM2600G series switch is powered on to start for the first time.
- Accessing the ISCOM2600G series switch through Telnet fails.

Accessing device from RJ45 Console interface

If you wish to access the ISCOM2600G series switch through PC through RJ45 Console interface, connect Console interface and PC RS-232 serial port, as shown in Figure 1-1; then run the terminal emulation program such as Windows XP Hyper Terminal program in PC to configure communication parameters as shown in Figure 1-2, and then log in to the ISCOM2600G series switch.

Figure 1-1 Accessing device through PC connected with RJ45 Console interface

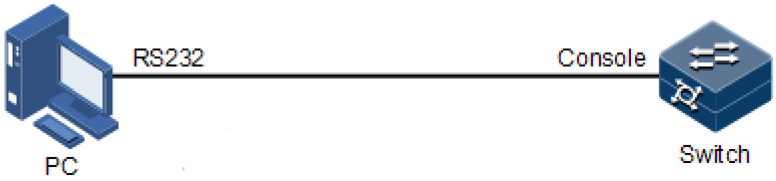
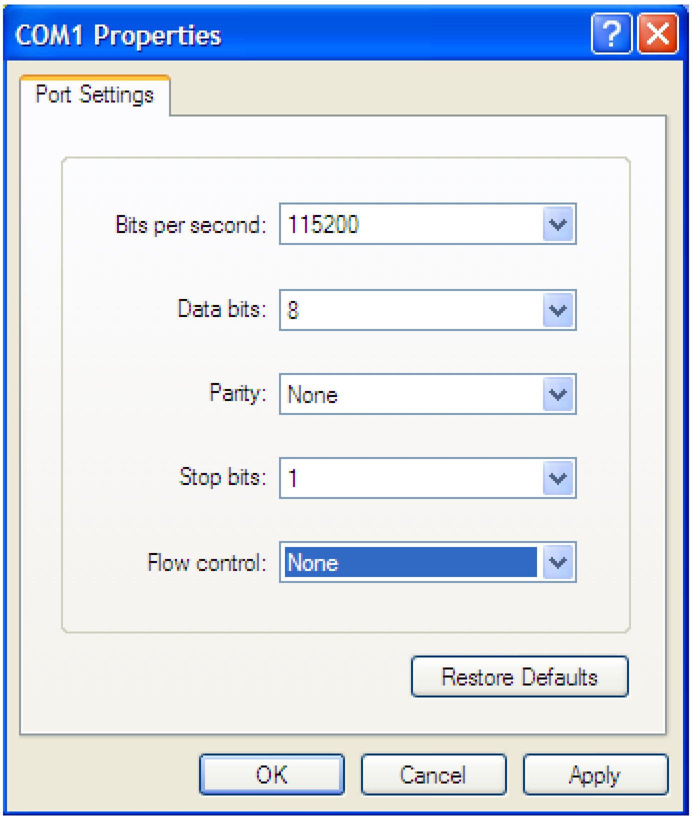


Figure 1-2 Configuring communication parameters in Hyper Terminal



COM1 Properties

Port Settings

Bits per second: 115200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

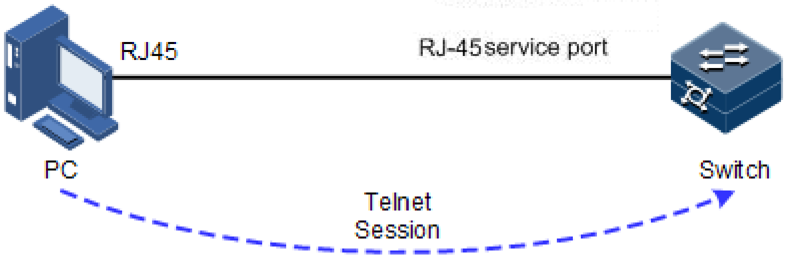
1.2.3 Accessing through Telnet

You can use a PC to log in to the ISCOM2600G series switch remotely through Telnet. You can log in to an ISCOM2600G series switch from PC at first, then Telnet other ISCOM2600G series switch devices on the network. You do not need to connect a PC to each ISCOM2600G series switch.

Telnet service provided by the ISCOM2600G series switch including:

- Telnet Server: run the Telnet client program on a PC to log in to the ISCOM2600G series switch, and take configuration and management. As shown in Figure 1-3, ISCOM2600G series switch is providing Telnet Server service at this time.

Figure 1-3 Networking with device as Telnet server

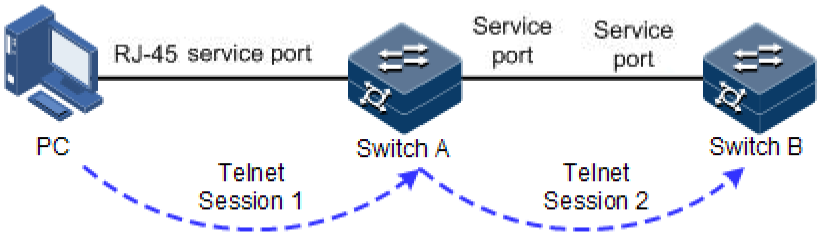


Before accessing the ISCOM2600G series switch through Telnet, you need to log in to the ISCOM2600G series switch through the Console interface and start the Telnet service. Take the following configurations on the ISCOM2600G series switch that needs to start Telnet service.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface fastethernet 1/0/1`	Enter out-of-band network management interface configuration mode
3	`Raisecom(config-fastethernet 1/0/1)#ip address ip-address [ ip-mask ]`	Configure the IP address for the out-of-band network management interface.
4	`Raisecom(config)#telnet-server accept interface-type interface-list`	(Optional) configure the interface in support of Telnet function.
5	`Raisecom(config)#telnet-server close terminal-telnet session-number`	(Optional) release the specified Telnet connection.
6	`Raisecom(config)#telnet-server max-session session-number`	(Optional) configure the maximum number of Telnet sessions supported by the ISCOM2600G series switch. By default, it is 5.

- Telnet Client: when you connect to the ISCOM2600G series switch through the PC terminal emulation program or Telnet client program on a PC, then telnet other ISCOM2600G series switch and configure/manage them. As shown in Figure 1-4, Switch A not only acts as Telnet server but also provides Telnet client service.

Figure 1-4 Networking with device as Telnet client



Configure Telnet Client device as below.

Step	Command	Description
1	`Raisecom#telnet { ip-address | ipv6-address } [ port port-id ]`	Log in to another device through Telnet.

1.2.4 Accessing through SSH

Telnet is lack of security authentication and it transports messages through 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 plain text, 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 provides greater security for remote login and other network services in network environment.

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

Before accessing the ISCOM2600G series switch through SSHv2, you must log in to the ISCOM2600G series switch through the Console interface and start SSH service.

Default configurations for accessing the ISCOM2600G series switch through SSHv2 are as follows.

Function	Default value
SSH server status	Disable
Local SSH key pair length	512 bits
Key renegotiation period	0h
SSH authentication method	password
SSH authentication timeout	600s
Allowable failure times for SSH authentication	20
SSH snooping port number	22
SSH session status	Enable
SSH protocol version	v1 and v2

Configure SSH service for the ISCOM2600G series switch 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. By default, the length is 512 bits.
3	`Raisecom(config)#`**`ssh2 server`**	Start the SSH server. By default, it is not started. Use the **no ssh2 server** command to shut down the SSH server. (Optional) configure SSH key renegotiation period.
4	`Raisecom(config)#`**`ssh2 server authentication`** `{` **`password`** `|` **`rsa-key`** `}`	(Optional) configure SSHv2 authentication mode. By default, it is password.

Step	Command	Description
5	Raisecom(config)#**ssh2 server authentication public-key**	(Optional) record the public key of the client on the ISCOM2600G series switch in rsa-key authentication mode.
6	Raisecom(config)#**ssh2 server authentication-timeout** *period*	(Optional) configure the SSHv2 authentication timeout. The Gazelle S3028 refuses to authenticate the client and then closes the connection when the client authentication time exceeds this upper limit. By default, it is 600s.
7	Raisecom(config)#**ssh2 server authentication-retries** *times*	(Optional) configure the allowable failure times for SSHv2 authentication. The ISCOM2600G series switch refuses to authenticate the client and then closes the connection when the number of client authentication failure times exceeds the upper limit. By default, it is 20.
8	Raisecom(config)#**ssh2 server port** *port-number*	(Optional) configure SSHv2 snooping port number. By default, it is 22. **Note** When configuring SSHv2 snooping port number, the entered parameter cannot take effect until SSH is restarted.
9	Raisecom(config)#**ssh2 server max-session** *session-number*	(Optional) configure the maximum number of SSHv2 sessions.
10	Raisecom(config)#**ssh2 server version** { **both** | **v1** | **v2** }	(Optional) configure the SSHv2 protocol version.
11	Raisecom(config)#**ssh access-list** { *ip access-list number* | *ipv6 access-list number* }	(Optional) configure the ACL number.
12	Raisecom(config)# **ssh2 server close session** *session-number*	(Optional) close the specified SSHv2 session.

1.2.5 Managing users

When you start the ISCOM2600G series switch for the first time, connect the PC through Console interface to the ISCOM2600G series switch, enter the initial user name and password in HyperTerminal to log in and configure the ISCOM2600G series switch.

Note

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

If there is no privilege restriction, any remote user can log in to the ISCOM2600G series switch through Telnet or access network by establishing a PPP (Point to Point Protocol) connection when service interfaces are configured with IP address. This is unsafe to the ISCOM2600G series switch and network. Creating user for the ISCOM2600G series switch and configuring password and privilege helps manage the login users and ensures network and device security.

Default configurations of user management are as below.

Function	Default value
Local user information	● User name: raisecom ● Password: raisecom ● Level: 15
New user right	15
New user activation status	Activate
New user service type	N/A
Enable password	raisecom
User login authentication mode	local-user
Enable login authentication mode	local-user

Configure login user management for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**user name** *user-name* **password** [**cipher** | **simple**] *password*	Create or modify the user name and password.
2	Raisecom#**user** *user-name* **privilege** *privilege-level*	Configure the login user right.
3	Raisecom#**user** *user-name* { **allow-exec** | **disallow-exec** } *first-keyword* [*second-keyword*]	(Optional) configure the priority rule for login user to perform the command line.
4	Raisecom#**user** *user-name* **service-type** { **lan-access** | **ssh** | **telnet** | **web** | **console** | **all** }	(Optional) configure the service type supported by the user.
5	Raisecom#**user login** { **local-radius** | **local-user** | **radius-local** [**server-no-response**] | **radius-user** | **local-tacacs** | **tacacs-local** [**server-no-response**] | **tacacs-user** }	(Optional) configure authentication mode for user login.

Step	Command	Description
6	Raisecom#**enable login { local-radius | local-user | radius-local [server-no-response] | radius-user | local-tacacs | tacacs-local [server-no-response] | tacacs-user }**	(Optional) configure authentication mode of privileged users.
7	Raisecom#**enable password [cipher** *password* **]**	(Optional) modify the password for entering privileged EXEC mode. Users with the level lower than 11 do not need the password for entering privileged EXEC mode.

Note

- Besides the default user raisecom, you can create up to 9 local user accounts.
- The login password is 8–16 characters, mandatorily including digits, case-sensitive letters, and other special characters.
- A local user with a level lower than 15, unless allowed to execute the command to modify the login password, is not allowed to modify the login password.

1.2.6 Checking configurations

Use the following commands to check the configuration results.

No.	Command	Description
1	Raisecom#**show user table**	Show login user information.
2	Raisecom#**show user active**	Show information about users logged in to the ISCOM2600G series switch.
3	Raisecom#**show telnet-server**	Show configurations of the Telnet server.
4	Raisecom#**show ssh public-key [authentication]**	Show the public key used for SSH authentication on the ISCOM2600G series switch and client.
5	Raisecom#**show ssh2 { server | session }**	Show SSHv2 server or session information.

1.2.7 Example for configuring user management

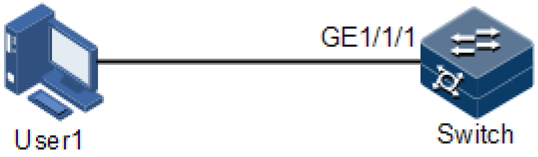
Networking requirements

As shown in Figure 1-5, to prevent malicious users from logging in to the ISCOM2600G series switch and to eliminate risks on the ISCOM2600G series switch, configure user management as below:

- Configure user login mode to local-user.

- Create a local user user1 with plain password of aaAA123@.
- Configure user1 privilege to level 10.
- Configure user1 service type to Telnet.
- Allow user1 to execute commands starting with **mirror**.

Figure 1-5 User management networking



Configuration steps

Step 1 Configure user login authentication mode.

```
Raisecom#user login local-user
```

Step 2 Create a local user user1.

```
Raisecom#user name user1 password simple aaAA123@
```

Step 3 Configure user's privilege.

```
Raisecom#user user1 privilege 10
```

Step 4 Configure the user's service type.

```
Raisecom#user user1 service-type telnet
```

Step 5 Configure user command management.

```
Raisecom#user user1 allow-exec mirror
```

Checking results

Use the **show user table detail** command to show configurations of local users.

```
Raisecom#show user table detail
User Login  :local-user
Enable Login:local-user

Username    :raisecom
Priority    :15
Server     :0.0.0.0
Login      :telnet-1
Status     :online
Service type:console telnet ssh web lan-access
User State  :active

Username    :user1
Priority    :10
Server     :0.0.0.0
Login      :--
Status     :offline
Service type:telnet
User State  :active
User command control config:
--------------------------------------------------------
Type:allow
First keyword :mirror
Second keyword :(null)

--------------------------------------------------------
```

Use the newly-created user name user1 and password aaAA123@ to log in to the ISCOM2600G series switch, and check whether the user right is correctly configured.

```
Login:user1
Password:
Raisecom>enable
Raisecom#config
Raisecom(config)#mirror enable
Set successfully.
```

As you can see above, user1 of privilege 10 can execute the command starting with **mirror** successfully after you configure user command management.

1.3 Managing files

1.3.1 Managing BootROM files

The BootROM files of the ISCOM2600G series switch include small BootROM and big BootROM.

- The small BootROM is used to boot the ISCOM2600G series switch.

- The big BootROM file is used to boot the ISCOM2600G series switch and initialize the ISCOM2600G series switch. You can upgrade the big BootROM file through Trivial File Transfer Protocol (TFTP).

Caution

We do not recommend conducting any operation over the Small BootROM. Contact local Raisecom technical support engineers if required.

After being powered on, the ISCOM2600G series switch runs the BootROM file. When the system prompts "Press Space to enter boot menu", press **Space bar** to enter the big BootROM menu.

In big Boot mode, you can do the following operations.

Operation	Description
t	Update system software to the ISCOM2600G series switch.
m	Update the boot file to the ISCOM2600G series switch.
b	Read system software from the ISCOM2600G series switch, and load it.
s	Specify the sequence of system software to be loaded upon startup.
e	Clear environment variables.
r	Reboot the ISCOM2600G series switch.
p	Configure the BootROM password.
?/h	Show information about system files and help.

Configure the ISCOM2600G series switch 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* }[*dir*]	(Optional) download the big BootROM file through FTP or TFTP.
2	Raisecom#**erase** [*file-name*]	(Optional) delete files saved in the Flash.
3	Raisecom#**upload bootstrap** { **ftp** *ip-address user-name password file-name* | **tftp** *ip-address file-name* }[*dir*]	(Optional) upload the big BootROM file through FTP or TFTP.

Note

The ISCOM2600G series switch does not support upgrading the small BootROM through CLI.

1.3.2 Managing system files

System files are the files needed for system operation (such as system startup software and configuration file). These files are usually saved in the memory. The ISCOM2600G series switch manages them through a file system to facilitate managing the memory. The file system can create, delete, and modify the file and directory.

In addition, the ISCOM2600G series switch supports dual-system. There are 2 independent sets of system software saved at the memory. When the ISCOM2600G series switch fails to work due to upgrade failure, you can use the other set to boot the ISCOM2600G series switch.

Manage system files for the ISCOM2600G series switch as below.

All the following steps are optional and in any sequence.

Step	Command	Description
1	Raisecom#**download system-boot** { **ftp** *ip-address user-name password file-name* | **tftp** *ip-address file-name* } { **system1.z** | **system2.z** }	(Optional) download the system boot file through FTP or TFTP.
2	Raisecom#**erase** [*file-name*]	(Optional) delete files saved in the Flash.
3	Raisecom#**upload system-boot** { **ftp** *ip-address user-name password file-name* | **tftp** *ip-address file-name* } { **system1.z** | **system2.z** }	(Optional) upload the system boot file through FTP or TFTP.

1.3.3 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 ISCOM2600G series switch 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 ISCOM2600G series switch 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 ISCOM2600G series switch uses the default parameters for initialization.

The configuration that is currently used by the ISCOM2600G series switch is called the running configuration.

You can modify the running configuration of ISCOM2600G series switch 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 ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`download startup-config`** `{` **`ftp`** *`ip-address user-name password file-name`* `|` **`tftp`** *`ip-address file-name`* `}[` *`dir`* `]`	(Optional) download the startup configuration file through FTP or TFTP.
2	`Raisecom#`**`download backtup-config`** `{` **`ftp`** *`ip-address user-name password file-name`* `|` **`tftp`** *`ip-address file-name`* `}[` *`dir`* `]`	(Optional) download the backup configuration file through FTP or TFTP.
3	`Raisecom#`**`erase`** `[` *`file-name`* `]`	(Optional) delete files saved in the Flash.
4	`Raisecom#`**`upload startup-config`** `{` **`ftp`** *`ip-address user-name password file-name`* `|` **`tftp`** *`ip-address file-name`* `}[` *`dir`* `]`	(Optional) upload the startup configuration file through FTP or TFTP.
5	`Raisecom#`**`upload backtup-config`** `{` **`ftp`** *`ip-address user-name password file-name`* `|` **`tftp`** *`ip-address file-name`* `}[` *`dir`* `]`	(Optional) upload the backup configuration file through FTP or TFTP.
6	`Raisecom#`**`upload command-log`** `{` **`ftp`** *`ip-address user-name password file-name`* `|` **`tftp`** *`ip-address file-name`* `}[` *`dir`* `]`	(Optional) upload the command line logging file and system logs through FTP or TFTP.
7	`Raisecom#`**`upload logging-file`** `{` **`ftp`** *`ip-address user-name password file-name`* `|` **`tftp`** *`ip-address file-name`* `}`	(Optional) upload the system log file through FTP or TFTP.
8	`Raisecom#`**`write`**	(Optional) save the running configuration file in the Flash.

1.3.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show startup-config`**	Show configurations loaded upon device startup.
2	`Raisecom#`**`show running-config`**	Show the running configurations.

1.4 Load and upgrade

1.4.1 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 ISCOM2600G series switch supports TFTP auto-loading mode.

TFTP auto-loading refers that you can obtain the configuration files from a server and then configure the ISCOM2600G series switch. 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 ISCOM2600G series switch provides several methods to confirm configuration file name on the TFTP server, such as manually entering, obtaining through DHCP, and using default name of the configuration file. Besides, you can assign certain naming conventions for configuration files, and then the ISCOM2600G series switch confirms the name according to naming conventions and its attributes (device type, MAC address, software version, and so on).

Upgrade

The ISCOM2600G series switch needs to be upgraded if you wish to add new features, optimize functions, or fix bugs in the current software version.

The ISCOM2600G series switch supports the following two upgrade modes:

- Upgrade through BootROM
- Upgrade through CLI

1.4.2 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 establish a TFTP environment, and use the PC as the TFTP server and the ISCOM2600G series switch as the client. Basic requirements are as below.

- Configure the TFTP server. Ensure that the TFTP server is available.
- Configure the IP address of the TFTP server; keep it in the same network segment with that of the ISCOM2600G series switch.
- Connect the Ethernet interface on the TFTP server to the SNMP interface on the ISCOM2600G series switch. The default IP address of the SNMP interface is 192.168.0.1 by default.

Upgrade system software through BootROM for the ISCOM2600G series switch as below.

<table>
<tr><th>Step</th><th>Operation</th></tr>
<tr><td>1</td><td>

Log in to the ISCOM2600G series switch through serial interface as the administrator, enter Privileged EXEC mode, and restart the ISCOM2600G series switch with the **reboot** command.

```
Raisecom#reboot
```

</td></tr>
<tr><td>2</td><td>

When the system successfully loads the big BootROM, and it displays "Press space to enter big boot menu", press **Space bar** to enter the interface starting with [raisecom]. The command list is displayed as below:

```
                    BOOT
 **************************************************
         t: Update system from tftp.
         m: Update boot from tftp.
         b: Boot system from flash.
         e: Erase bootline para.
         s: Select system image to boot.
         p: Password setting.
         r: Reboot.
         ?/h: Help menu.
[Raisecom]:
```

</td></tr>
<tr><td>3</td><td>

Type "t" to upgrade system software to the ISCOM2600G series switch.

```
[Raisecom]:t
ipaddr: 192.168.5.100
serverip: 192.168.5.1
filename: uImage

Current system partiton info:
Partition number   Name             Size
----------------------------------------------------
1               iscom2600_image    16320072
2               None              0

Please input system partition number for upgrading(1-2):1
```

</td></tr>
<tr><td>4</td><td>

Type "m" to upgrade the Boot software to the ISCOM2600G series switch.

```
[Raisecom]:m
ipaddr: 192.168.5.100
serverip: 192.168.5.1
filename: uImage mboot.bin

press y to confirm: y
```

</td></tr>
<tr><td>5</td><td>

Type "r" to rapidly execute the big BootROM file. The ISCOM2600G series switch is restarted and will load the downloaded startup file.

</td></tr>
</table>

1.4.3 Upgrading system software through CLI

Before upgrading system software through CLI, you should establish a TFTP environment, and use a PC as the TFTP server and the ISCOM2600G series switch as the client. Basic requirements are as below.

- Connect the Ethernet interface on the TFTP server to the SNMP interface on the ISCOM2600G series switch. The default IP address of the SNMP interface is 192.168.0.1 by default.
- Configure the TFTP server, and ensure that the server is available.
- Configure the IP address of the TFTP server; keep it in the same network segment with that of the ISCOM2600G series switch so that the ISCOM2600G series switch can access the TFTP server.

Upgrade system software through CLI for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**download system-boot** { **ftp** *ip-address user-name password file-name* | **tftp** *ip-address file-name* } { **system1.z** | **system2.z** }	Download the system boot file through FTP.
2	Raisecom#**boot sequence**	(Optional) configure the sequence for loading system software.
3	Raisecom#**reboot** [**now**]	Reboot the ISCOM2600G series switch, and it will automatically load the downloaded system boot file.

1.4.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show startup-config**	Show information about the startup configuration file.
2	Raisecom#**show running-config**	Show information about the running configuration file.
3	Raisecom#**show version**	Show system version.

1.5 Automatically updating version and configurations

1.5.1 Introduction

After being powered on, the ISCOM2600G series switch can automatically obtain the new version and configurations. After obtaining an IP address as a DHCP client, it will automatically download configuration files and system files from the TFTP server to update version and configurations.

1.5.2 Preparing for configurations

Scenario

To use the ISCOM2600G series switch as a DHCP client, you must enable DHCP Client. The DHCP client actively sends a Discover broadcast packet. After receiving the packet, the DHCP server pads information such as assigned IP address to the Offer packet, and sent the packet to the DHCP client. Meanwhile, it pads the IP address of the TFTP server to Option 150 and pads the name of the configuration file or system file to Option 67. After receiving these packets, the DHCP client resolves Option 150 for the IP address of the TFTP server and resolves Option 67 for the name of the configuration file or system file according to naming conversions, resolves Option 17 for the file path.

Prerequisite

- Configure the address pool on the DHCP server and configure Option 67 and Option 150 in the address pool.
- Configure DHCP Client.

1.5.3 Automatically updating version and configurations

Configure automatic update of version and configurations for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface vlan 1**	Enter Layer 3 interface configuration mode.
3	Raisecom(config-vlan1)#**ip address dhcp** [**server-ip** *ip-address*]	Configure the DHCP client to apply for the IP address through DHCP.
4	Raisecom(config-vlan1)#**auto_config enable** Raisecom(config-vlan1)#**exit**	Enable automatic update of version and configurations.
5	Raisecom(config)#**auto_save enable**	(Optional) enable automatic saving of configurations.
6	Raisecom(config)#**auto_load time** *hour minute second*	(Optional) configure the time for saving configuration after successfully loading the configuration file.

Note

- After configuring the ISCOM2600G series switch, save configurations and restart it. Then, it will automatically apply for the IP address and conduct update operations.

- Connect the DHCP client to the DHCP server properly. Connect the DHCP client to the TFTP server properly.

1.5.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show auto_config`	Show configurations of automatic update of version and configurations.
2	`Raisecom#show buffer_config`	Show information about the configuration file in the buffer.

1.5.5 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description
`Raisecom(config)#clear buffer_config`	Clear the configuration file in the buffer.

1.6 Time management

1.6.1 Configuring time and time zone

To make the ISCOM2600G series switch to work coordinately with other devices, you must configure system time and local time zone accurately.

The ISCOM2600G series switch 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
Local time zone	+08:00
Time zone offset	+08:00
DST status	Disable
System clock display mode	Default

Configure time and time zone for the ISCOM2600G series switch 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 the local time zone.
3	Raisecom#**clock display** { **default** | **utc** }	Configure system clock display mode.

1.6.2 Configuring DST

Daylight Saving Time (DST) is a kind of artificial regulation local time system for saving energy. At present, there are nearly 110 countries running DST every summer around the world, but different countries has different stipulations for DST. In this case, you should consider local conditions when configuring DST.

Configure DST for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**clock summer-time enable**	Enable DST.
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 Underlined command lines indicate the termination DST.

Note

- When you configure system time manually, if the system uses DST, such as DST from 2 a.m. on the second Sunday, April to 2 a.m. on the second Sunday, September every year, you have to advance the clock one hour faster during this period, configure time offset as 60 minutes, and the period from 2 a.m. to 3 a.m. on the second Sunday, April each year is inexistent. The time setting by manual operation during this period shows failure.
- The summer time in southern hemisphere is opposite to the northern hemisphere, which is from September to April of next year. If you configure the start time later than the end time, the system will suppose that it is in the Southern Hemisphere. Namely, the summer time is from the start time this year to the ending time of next year.

1.6.3 Configuring NTP

Network Time Protocol (NTP) is a time synchronization protocol defined by RFC1305, used to synchronize time between the 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 ISCOM2600G series switch can provide different application over a unified time. Meanwhile, NTP can ensure very high accuracy, with accuracy of 10ms around.

The ISCOM2600G series switch in support of NTP cannot only receive synchronization from other clock source, but also to synchronize other devices as a clock source.

The ISCOM2600G series switch adopts multiple NTP working modes for time synchronization:

- Server/Client mode

In this mode, the client sends clock synchronization messages to different servers. The servers work in server mode automatically after receiving the synchronization message and sending 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 establishes 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 device is NTP master clock	No
Global NTP server	Inexistent
Global NTP equity	Inexistent
Reference clock source	0.0.0.0

⚠ **Caution**

NTP and SNTP are mutually exclusive, so they cannot be currently configured.

Configure NTP for the ISCOM2600G series switch 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 ISCOM2600G series switch working in symmetric peer mode.

Step	Command	Description
4	Raisecom(config)#**ntp refclock-master** [*ip-address*] [*stratum*]	Configure clock of the ISCOM2600G series switch as NTP reference clock source for the ISCOM2600G series switch.

Note

If the ISCOM2600G series switch is configured as the NTP reference clock source, it cannot be configured as the NTP server or NTP symmetric peer; vice versa.

1.6.4 Configuring SNTP

Simple Network Time Protocol (SNTP) is used to synchronize the system time of the ISCOM2600G series switch 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 settings of time zone.

Default configurations of SNTP are as below.

Function	Default value
IP address of the SNTP server	Inexistent

Configuring unicast feature of SNTP client

Configure unicast feature of SNTP client for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**sntp server** *ip-address*	Configure the IP address of the SNTP unicast server. After the SNTP server is configured with an IP address, the ISCOM2600G series switch tries to get the clock information from the SNTP server every 10s. In addition, the maximum timeout is 60s.

1.6.5 Checking configurations

Use the following commands to check configuration results.

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

No.	Command	Description
3	`Raisecom#show ntp status`	Show NTP configurations.
4	`Raisecom#show ntp associations [ detail ]`	Show information about NTP connection.

1.7 Interface management

1.7.1 Introduction

Ethernet is a very important LAN networking technology which is flexible, simple and easy to implement. The Ethernet interface includes the Ethernet electrical interface and Ethernet optical interface.

The ISCOM2600G series switch supports both Ethernet electrical and optical interfaces.

Auto-negotiation

Auto-negotiation is used to make the devices at both ends of a physical link automatically choose the same working parameters by exchanging information. The auto-negotiation parameters include duplex mode, interface rate, and flow control. Once successful in negotiation, the devices at both ends of the link can work in the same duplex mode and interface rate.

Cable connection

Generally, the Ethernet cable can be categorized as the Medium Dependent Interface (MDI) cable and Medium Dependent Interface crossover (MDI-X) cable. MDI provides physical and electrical connection from terminal to network relay device while MDI-X provides connection between devices of the same type (terminal to terminal). Hosts and routers use MDI cables while hubs and switches use MDI-X interfaces. Usually, the connection of different devices should use the MDI cable while devices of the same type should use the MDI-X cable. Devices in auto-negotiation mode can be connected by the MDI or MDI-X cable.

The Ethernet cable of the ISCOM2600G series switch supports auto-MDI/MDIX.

1.7.2 Default configurations of interface management

Default configurations of interface management are as below.

Function	Default value
Maximum forwarding frame length of interface	2000 bytes
Duplex mode of interface	Auto-negotiation
Interface rate	Auto-negotiation
Interval for monitoring the interface rate	5s
Interface rate statistics status	Disable

Function	Default value
Time interval of interface dynamic statistics	2s
Interface flow control status	Disable
Interface status	Enable
L2protocol peer stp status	Disable

1.7.3 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 attributes to make the devices at both ends match each other.

The Ethernet physical layer works in three modes as below:

- Half duplex: devices can receive or send messages at a time.
- Full duplex: devices can receive and send messages concurrently.
- Auto-negotiation: devices can automatically choose duplex mode by exchanging information. Once successful in negotiation, the devices at both ends of the link can work in the same duplex mode, interface rate, and flow control mode.

Configure the basic attributes of interface for the ISCOM2600G series switch 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-gigaethernet1/1/1)#`**`mtu`** *`max-frame-length`*	Configure the MTU on the interface. When the length of the IP packet to be forwarded exceeds the maximum value, the ISCOM2600G series switch will fragment the IP packet.
4	`Raisecom(config)#`**`interface`** *`interface-type interface-number`*	Enter physical layer interface configuration mode.
5	`Raisecom(config-gigaethernet1/1/1)#`**`duplex`** `{` **`full`** `|` **`half`** `}`	Configure the duplex mode of the interface.
6	`Raisecom(config-gigaethernet1/1/1)#`**`speed`** `{` **`auto`** `|` **`10`** `|` **`100`** `|` **`1000`** `|` **`10000`** `}`	Configure the interface rate. It depends on specifications of the optical module for the optical interface.
7	`Raisecom(config-gigaethernet1/1/1)#`**`tpid`** `{` **`8100`** `|` **`9100`** `|` **`88a8`** `}`	(Optional) configure the interface TPID. By default, it is 0x8100.
8	`Raisecom(config-gigaethernet1/1/1)#`**`jumboframe`** *`frame-size`*	(Optional) configure the maximum framelength allowed to pass by the interface.

Step	Command	Description
9	`Raisecom(config-gigaethernet1/1/1)#mdi { xover | auto | normal }`	(Optional) configure the MDI/MDIX mode of the electrical interface.
10	`Raisecom(config-gigaethernet1/1/1)#vibration-suppress peroid second`	(Optional) configure the period for suppressing vibration on the interface.

1.7.4 Configuring interface rate statistics

Configure interface rate statistics for the ISCOM2600G series switch 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-gigaethernet1/1/1)#clear interface statistics`	Clear statistics of the interface rate.

1.7.5 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 a 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 ISCOM2600G series switch 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-gigaethernet1/1/1)#flowcontrol { receive | send } { off | on }`	Enable/Disable interface flow control over 802.3x packets. By default, it is disabled.

1.7.6 Enabling/Disabling interfaces

Enable/Disable an interface for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**shutdown**	Disable the current interface. Use the **no shutdown** command to re-enable the disabled interface.

1.7.7 Configuring L2Protocol Peer STP

To interconnect with the device that sends STP packets with the destination MAC address of 0180.C200.0008, you need to configure L2Protocol Peer STP on the ISCOM2600G series switch. If this function is enabled, the destination MAC address of BPDU, sent through STP, is 0180.C200.0008; otherwise, it is 0180.C200.0000.

Configure L2Protocol Peer STP for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**l2protocol peer stp**	Enable L2Protocol Peer STP.

1.7.8 Configuring Console interface

Configure the Console interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**console open**	(Optional) enable the Console interface. Use this command in non-Console command lines only. ⚠ **Caution** Using the **console close** command to disable the Console interface causes the ISCOM2600G series switch to be out of control. Use it with care.
3	Raisecom(config)#**login-trap enable**	(Optional) enable sending Trap upon user login or exit.

1.7.9 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show interface** [*interface-type interface-number*]	Show interface status.
2	Raisecom#**show l2protocol peer stp** [*interface-type interface-number*]	Show status of L2protocol Peer STP on the interface.

1.8 Configuring basic information

Configure basic information for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**hostname** *name*	(Optional) configure the device name. By default, the device name is Raisecom. The system supports changing device name to make users distinguish different devices on the network. Once the device name changes, it can be seen in terminal prompt.
2	Raisecom#**language** { **chinese** | **english** }	(Optional) configure language mode. By default, the language is English.
3	Raisecom#**write**	Save configurations. Save configurations to the ISCOM2600G series switch after configurations, and the new configurations will overwrite the original configurations. Without saving, the new configurations will be lost after restarting, and the ISCOM2600G series switch will continue working with the original configurations. ⚠ **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 restart options. When the ISCOM2600G series switch fails, restart it to try to solve the problem according to actual condition.

Caution

- Restarting the ISCOM2600G series switch interrupts services, so use the command with care.
- Save configurations before restarting to avoid loss of configurations.

1.9 Task scheduling

1.9.1 Introduction

To use some commands periodically or at a specified time, configure task scheduling.

The ISCOM2600G series switch supports scheduling tasks by combining the program list with 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 implement the periodic execution of command lines.

1.9.2 Configuring task scheduling

Configure task scheduling for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**schedule-list** *list-number* **start date-time** { *mm-dd-yyyy hh:mm:ss* [**every** { **day** | **week** } **stop** *mm-dd-yyyy hh*:*mm*:*ss*] | **every** *days-interval time-interval* [**stop** *mm-dd-yyyy hh*:*mm*:*ss*] }	Create a schedule list, and configure it.
	Raisecom(config)#**schedule-list** *list-number* **start date-time** *mm-dd-yyyy hh:mm:ss* **every weekday-list** { **fri** | **mon** | **off-day** | **sta** | **sun** | **thu** | **tue** | **wed** | **working-day** | *weekday-list* }	
	Raisecom(config)#**schedule-list** *list-number* **start up-time** *days-after-startup hh*:*mm*:*ss* [**every** *days-interval time-interval* [**stop** *days-after-startup hh*:*mm*:*ss*]]	
3	Raisecom(config)#*command-string* **schedule-list** *list-number*	Bind the command line which needs periodical execution and supports the schedule list to the schedule list.

1.9.3 Checking configurations

Use the following command to check configuration results.

No.	Command	Description
1	`Raisecom#show schedule-list [ list-number ]`	Show configurations of the schedule list.

1.10 Watchdog

1.10.1 Introduction

The external electromagnetic field interferes with the working of the Microcontroller Unit (MCU), and causes program elapsing and endless loop; consequently the system fails to work normally. To monitor the realtime running state of the MCU, a program is specially used, which is commonly known as the Watchdog.

The ISCOM2600G series switch will be restarted when it fails to work due to task suspension or endless loop, and it neither sends signals to restart the waterdog timer.

Watchdog can prevent the system program from endless loop due to uncertain fault, thus improving system stability.

1.10.2 Preparing for configurations

Scenario

By configuring Watchdog, you can prevent the system program from endless loop due to uncertain fault, thus improving system stability.

Prerequisite

N/A

1.10.3 Default configurations of Watchdog

Default configurations of Watchdog are as below.

Function	Default value
Watchdog status	Enable Watchdog.

1.10.4 Configuring Watchdog

Configure Watchdog for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#watchdog enable`	Enable Watchdog.

1.10.5 Checking configurations

Use the following command to check configuration results.

Step	Command	Description
1	`Raisecom#show watchdog`	Show Watchdog status.

1.11 Configuring Banner

1.11.1 Preparing for configurations

Scenario

Banner is a message to display when you log in to or exit the ISCOM2600G series switch, such as the precautions or disclaimer.

You can configure the Banner of the ISCOM2600G series switch as required. In addition, the ISCOM2600G series switch provides the Banner switch. After Banner display is enabled, the configured Banner information appears when you log in to or exit the ISCOM2600G series switch.

After configuring Banner, use the **write** command to save configurations. Otherwise, Banner information will be lost when the ISCOM2600G series switch is restarted.

Prerequisite

N/A

1.11.2 Configuring Banner

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

Step	Command	Description

2	`Raisecom(config)#`**`banner login`** *`word`* `Press Enter.`
	`Enter text message followed by the character ’`*`word`*`’ to finish.User can stop configuration by inputing’ Ctrl+c’`
	`message word`
		Configure the Banner contents. Enter the **banner login** and *word*, press **Enter**, enters the Banner contents, and then end with the *word* character.
		Note
		The *word* parameter is a 1-byte character. It is the beginning and end marker of the Banner contents. These 2 marks must be the identical character. We recommend selecting the specified character that will not occur at the *message*.
		The message parameter is the Banner contents. Up to 2560 characters are supported.

3	`Raisecom(config)#`**`clear banner login`**	(Optional) clear contents of the Banner.

1.11.3 Enabling Banner display

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`banner enable`**	Enable Banner display. By default, Banner display is disabled. Use the **banner disable** command to disable Banner display.

1.11.4 Checking configurations

No.	Command	Description
1	`Raisecom#`**`show banner login`**	Show Banner status and contents of the configured Banner.

2 Ethernet

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

- MAC address table
- VLAN
- QinQ
- VLAN mapping
- STP/RSTP
- MSTP
- Loop detection
- Interface protection
- Port mirroring
- L2CP

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 the MAC address table for the forwarding interface, 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 number
- Interface VLAN ID
- Flag bits

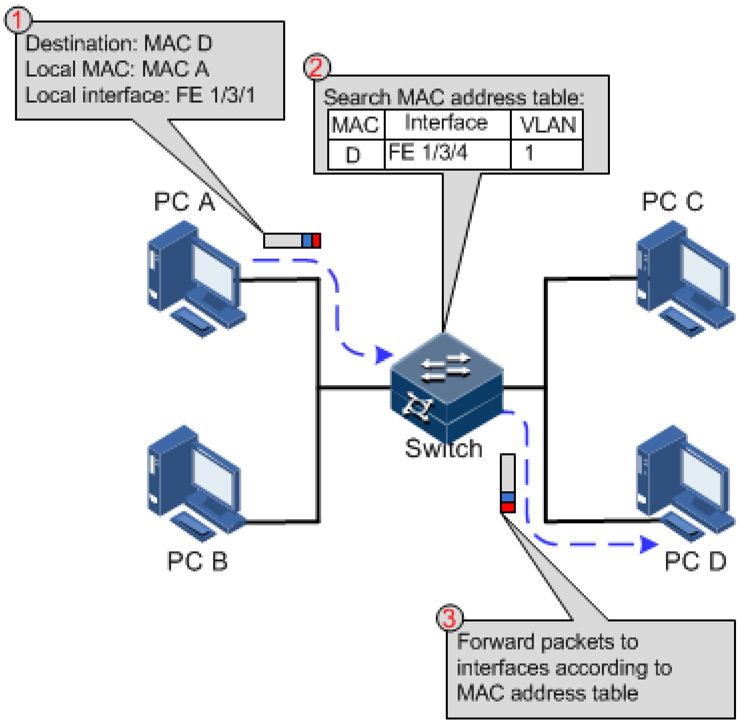
The ISCOM2600G series switch supports showing MAC address information by device, interface, or VLAN.

Forwarding modes of MAC addresses

When forwarding packets, based on the information about MAC addresses, the ISCOM2600G series switch 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 ISCOM2600G series switch 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 ISCOM2600G series switch broadcasts the packet to all interfaces except the receiving interface, as shown in Figure 2-1.

Figure 2-1 Forwarding packets according to the MAC address table


1
Destination: MAC D
Local MAC: MAC A
Local interface: FE 1/3/1
2
Search MAC address table:
MAC | Interface | VLAN
D | FE 1/3/4 | 1
PC A
PC C
Switch
PC B
PC D
3
Forward packets to interfaces according to MAC address table

- Multicast: when the ISCOM2600G series switch receives a packet of which the destination MAC address is a multicast address, it will broadcast the packet. If multicast is enabled and storm control over unknown packets is also enabled, the packet will be sent to the specified Report interface. If no Report interface is specified, the packet will be discarded.
- Broadcast: when the ISCOM2600G series switch receives an all-F packet, or the MAC address is not listed in the MAC address table, the ISCOM2600G series switch forwards the packet to all interfaces except the interface that receives this packet. Broadcast addresses are special multicast addresses.

Classification of MAC addresses

MAC address table is divided into static address entry and dynamic address entry.

- 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, adding static address entry manually can reduce the network broadcast flow, improve the security of the interface, and prevent entries from being lost after the system is reset.

- Dynamic MAC address entry: the ISCOM2600G series switch can add dynamic MAC address entries through MAC address learning. The entries are aged according to the configured aging time, and will be empty after the system is reset.

The ISCOM2600G series switch supports up to 16K dynamic MAC addresses. 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 ISCOM2600G series switch. To maximize the use of the MAC address table, the ISCOM2600G series switch uses the aging mechanism to update the MAC address table. For example, when the ISCOM2600G series switch 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 ISCOM2600G series switch will delete the entry.

The ISCOM2600G series switch 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.

Forwarding policies of MAC addresses

The MAC address table has two forwarding policies:

When receiving packets on an interface, the ISCOM2600G series switch searches the MAC address table for the interface related to the destination MAC address of packets.

- If successful, it forwards packets on the related interface, records the source MAC addresses of packets, interface number of ingress packets, and VLAN ID in the MAC address table. If packets from other interface are sent to the MAC address, the ISCOM2600G series switch can send them to the related interface.
- If failed, 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 used to limit the number of MAC addresses, avoid extending the searching time of forwarding entry caused by a 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), 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
MAC address aging time	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.
2	Raisecom(config)#**mac-address static unicast** *mac-address* **vlan** *vlan-id interface-type interface-number*	Configure static unicast 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 ISCOM2600G series switch is 1024 per interface.

2.1.5 Configuring blackhole MAC address

Configure blackhole MAC addresses as below.

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

Step	Command	Description
2	Raisecom(config)#**mac-address blackhole** *mac-address* **vlan** *vlan-id*	Configure blackhole MAC addresses.

2.1.6 Filtering unknown multicast packets

Filter unknown multicast packets for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mac-address multicast drop-unknown reserved-address**	(Optional) filter unknown multicast packets.

2.1.7 Configuring MAC address learning

Configure MAC address learning for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**mac-address learning enable** { *interface-type interface-number* | **vlanlist** *vlan-list* }	Enable MAC address learning.

2.1.8 Configuring MAC address limit

Configure the MAC address limit for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**mac-address threshold** *threshold-value*	Configure interface-based MAC address limit.

2.1.9 Configuring aging time of MAC addresses

Configure the aging time of MAC addresses for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mac-address aging-time** { **0** | *period* }	Configure the aging time of MAC addresses.

2.1.10 Enabling suppression of MAC address flapping

Configure suppression of MAC address flapping for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mac-address mac-move enable**	Enabling global suppression of MAC address flapping.

2.1.11 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show mac-address static** [*interface-type interface-number* | **vlan** *vlan-id*]	Show static unicast MAC addresses.
2	Raisecom#**show mac-address multicast** [**vlan** *vlan-id*] [**count**]	Show the Layer 2 multicast address or number of existing multicast MAC address.
3	Raisecom#**show mac-address blackhole**	Show the blackhole MAC address.
4	Raisecom#**show mac-address threshold** [*interface-type interface-list*]	Show the dynamic MAC address limit.
5	Raisecom#**show mac aging-time**	Show the aging time of dynamic MAC addresses.
6	Raisecom#**show mac-address learning** [*interface-type interface-list*]	Show status of MAC address learning.
7	Raisecom#**show mac-address count** [**vlan** *vlan-id*] [*interface-type interface-number*]	Show the number of MAC address entries.

2.1.12 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description
`Raisecom(config)#`**`clear mac-address{ all | blackhole | dynamic | static }`**	Clear MAC addresses.
`Raisecom(config)#`**`clear mac-address{ all | dynamic | static } [ vlan`** *`vlan-id`* **`]`** *`interface-type interface-number`*	Clear MAC addresses of a specified interface.
`Raisecom(config)#`**`clear mac-address blackhole vlan`** *`vlan-id`*	Clear blackhole MAC address entries in a specified VLAN.
`Raisecom(config)#`**`search mac-address`** *`mac-address`* **`{ all | dynamic | static } [`** *`interface-type interface-number`* **`] [ vlan`** *`vlan-id`* **`]`**	Search for a MAC address.

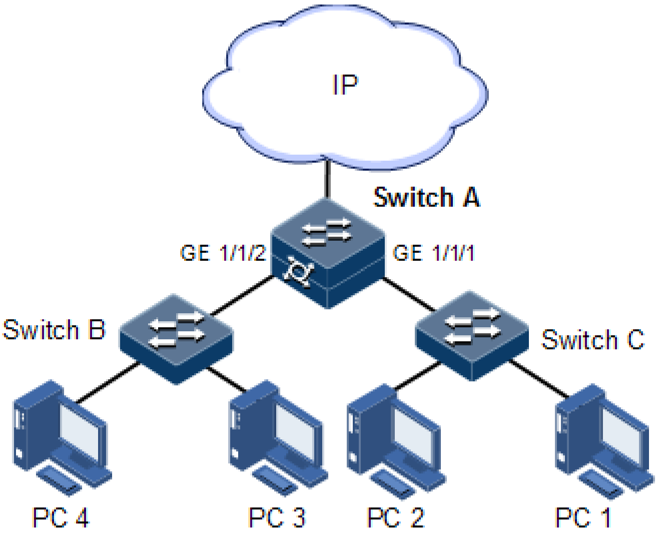
2.1.13 Example for configuring MAC address table

Networking requirements

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

- Configure a static unicast MAC address 0001.0203.0405 on GE 1/1/2 and configure its VLAN to VLAN 10.
- Configure the aging time to 500s.

Figure 2-2 MAC networking



Configuration steps

Step 1 Create VLAN 10 and active it, and add GE 1/1/2 to VLAN 10.

```
Raisecom#config
Raisecom(config)#create vlan 10 active
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport mode access
Raisecom(config-port)#switchport access vlan 10
Raisecom(config-port)#exit
```

Step 2 Configure a static unicast MAC address 0001.0203.0405 on GE 1/1/2, which belongs to VLAN 10.

```
Raisecom(config)#mac-address static unicast 0001.0203.0405 vlan 10
gigaethernet 1/1/2
```

Step 3 Configure the aging time to 500s.

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

Checking results

Use the **show mac-address** to show configurations of MAC addresses.

```
Raisecom#show mac-address all gigaethernet 1/1/2
Aging time: 500 seconds
Mac Address      Port               Vlan    Flags
-------------------------------------------------------
0001.0203.0405   gigaethernet1/1/2   10      Static
```

2.2 VLAN

2.2.1 Introduction

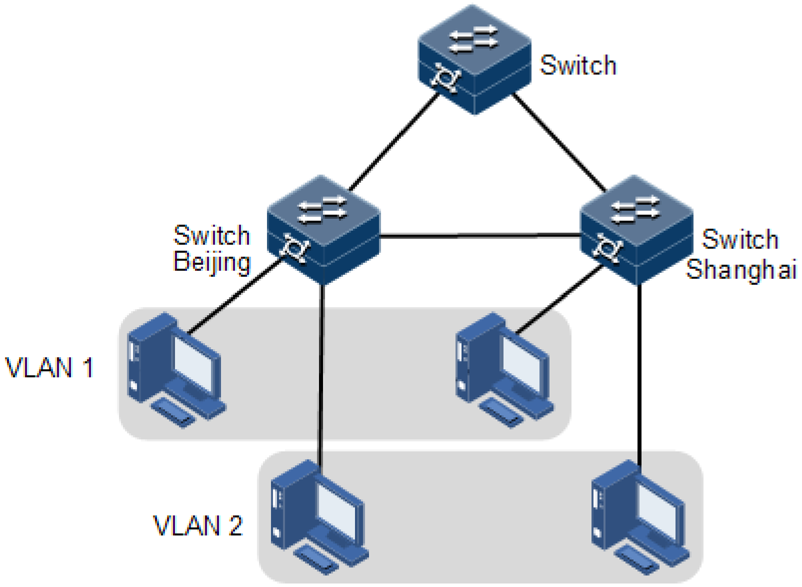
Overview

Virtual Local Area Network (VLAN) is a protocol to solve Ethernet broadcast and security problem. It is a Layer 2 isolation technique that partitions a LAN into different broadcast domains logically rather than physically, and then the different broadcast domains can work as virtual groups without any influence from one another. In terms of functions, VLAN has the same features as LAN, but members in one VLAN can access one another without restriction by physical location.

Partitioning VLANs

There are multiple ways of partitioning VLANs, such as by interface, by MAC address, and by IP subnet, as shown in Figure 2-3.

Figure 2-3 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 ISCOM2600G series switch complies with IEEE 802.1Q standard VLAN and supports 4094 concurrent VLANs.

- Partitioning VLANs by interface

The ISCOM2600G series switch supports VLAN partitioning by interface. The ISCOM2600G series switch has two interface modes: Access mode and Trunk mode. The method of dealing with packet for the two modes shows as below.

Table 2-1 Interface mode and packet processing

Interface type	Processing ingress packets		Processing egress packets
	Untagged packets	Tag packets	
Access	Add Access VLAN Tag into the packet.	• If VLAN ID of the packet is equal to Access VLAN ID, receive the packet. • If VLAN ID of the packet is not equal to Access VLAN ID, discard the packet.	• If the VLAN ID of the packet is equal to Access VLAN ID, remove the Tag and send the packet. • If the packet VLAN ID is not included in the VLAN ID list allowed to pass by the interface, discard the packet.

Interface type	Processing ingress packets		Processing egress packets
	Untagged packets	Tag packets	
Trunk	Add Native VLAN Tag into 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 of the packet is equal to Native VLAN ID, remove the Tag and send the packet. • If the VLAN ID of the packet is not equal to Native VLAN ID and the interface allows the packet to pass, keep the original Tag and send the packet.

- Partitioning VLANs by MAC address

This refers to partitioning VLANs by the source MAC address of the packet.

  - When an interface receives an Untagged packet, it matches the source MAC address of the packet with the VLAN MAC addresses. If they are the same, the match is successful. In this case, the interface adds the VLAN ID specified by VLAN MAC addresses, and forwards the packet. If they are different, the interface continues to match the packet with the IP address-based VLAN and interface-based VLAN in descending order.
  - When a Tag packet reaches an interface, if its VLAN ID is in the VLAN ID list allowed to pass by the interface, the interface receives it; otherwise, the interface discards it.

- Partitioning VLANs by IP subnet

This refers to partitioning VLANs by the source IP subnet of the packet.

  - When an interface receives an Untagged packet, it determines the VLAN of the packet by the source IP subnet of the packet, and then transmits the packet in the specified VLAN.
  - When a Tag packet reaches an interface, if its VLAN ID is in the VLAN ID list allowed to pass by the interface, the interface receives it; otherwise, the interface discards it.

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, such as routers, are required if users want to communicate among different VLANs. 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 and VLAN 4093
Active status of static VLAN	Active
Interface mode	Access
Access VLAN	VLAN 1
Native VLAN of Trunk interface	VLAN 1
Allowable VLAN in Trunk mode	VLAN 1
Allowable Untag VLAN in Trunk mode	VLAN 1
VLAN mapping table ID	VLAN ID

2.2.4 Configuring VLAN attributes

Configure VLAN attributes for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`create vlan`** *`vlan-list`* **`active`**	Create a VLAN. The command can also be used to create VLANs in batches.
3	`Raisecom(config)#`**`vlan`** *`vlan-id`*	Enter VLAN configuration mode.
4	`Raisecom(config-vlan)#`**`name`** *`vlan-name`*	(Optional) configure the VLAN name.

Note

- The VLAN created by the **vlan** *vlan-id* command is in active status.
- All configurations of VLAN do not take until the VLAN is activated.

2.2.5 Configuring interface mode

Configure interface mode for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**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 ISCOM2600G series switch 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-gigaethernet1/1/1)#**switchport mode access** Raisecom(config-gigaethernet1/1/1)#**switchport access vlan** *vlan-id*	Configure the interface to Access mode, and add the Access interface to the VLAN.
4	Raisecom(config-gigaethernet1/1/1)#**switchport access egress-allowed vlan** { **all** | [**add** | **remove**] *vlan-list* }	(Optional) configure the VLAN allowed to pass by the Access interface.

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 the Access VLAN manually, the system will automatically configure the interface Access VLAN as the default VLAN.
- When configuring interface Access VLAN as non-default Access VLAN, default Access VLAN 1 is the VLAN allowed by the Access the egress interface, you can

delete Access VLAN 1 from allowed VLAN list of Access the egress interface by deleting this 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 cluster VLAN, GVRP dynamic VLAN.

2.2.7 Configuring VLAN on Trunk interface

Configure VLAN on the Trunk interface for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**switchport mode trunk**	Configure the interface to Trunk mode.
4	Raisecom(config-gigaethernet1/1/1)#**switchport trunk native vlan** *vlan-id*	Configure the Native VLAN of the interface.
5	Raisecom(config-gigaethernet1/1/1)#**switchport trunk allowed vlan** { **all** | [**add** | **remove**] *vlan-list* }	(Optional) configure VLANs allowed to pass by the Trunk interface.
6	Raisecom(config-gigaethernet1/1/1)#**switchport trunk untagged vlan** { **all** | [**add** | **remove**] *vlan-list* }	(Optional) configure VLANs from which the Trunk interface can remove Tag.

Note

- 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 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.
- When configuring Trunk Untagged VLAN list, the system automatically adds all Untagged VLAN to 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 cluster VLAN, GVRP dynamic VLAN.

2.2.8 Checking configurations

Use the following commands to check configuration results.

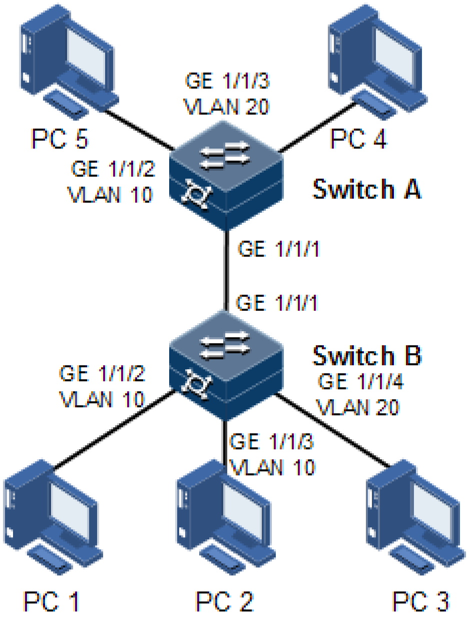
No.	Command	Description
1	`Raisecom#show vlan [ vlan-list | static ]`	Show VLAN configurations.
2	`Raisecom#show switchport interface-type interface-number`	Show VLAN configurations on the interface.

2.2.9 Example for configuring VLAN

Networking requirements

As shown in Figure 2-4, PC 1, PC 2, and PC 5 belong to VLAN 10, PC 3 and PC 4 belong to VLAN 20; Switch A and Switch B are connected by the Trunk interface; PC 3 and PC 4 cannot communicate because VLAN 20 is not allowed to pass in the link; PC 1 and PC 2 under the same Switch B are enabled with interface protection function so that they cannot communicate with each other, but can respectively communicate with PC 5.

Figure 2-4 VLAN and interface protection networking



Configuration steps

Step 1 Create VLAN 10 and VLAN 20 on the two Switch devices respectively, and activate them.

Configure Switch A.

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

Configure Switch B.

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

Step 2 Add GE 1/1/2 and GE 1/1/3 as Access mode on Switch B to VLAN 10, add GE 1/1/4 as Access mode to VLAN 20, configure GE 1/1/1 to Trunk mode, and allow VLAN 10 to pass.

```
SwitchB(config)#interface gigaethernet1/1/2
SwitchB(config-gigaethernet1/1/2)#switchport mode access
SwitchB(config-gigaethernet1/1/2)#switchport access vlan 10
SwitchB(config-gigaethernet1/1/2)#exit
SwitchB(config)#interface gigaethernet1/1/3
SwitchB(config-gigaethernet1/1/3)#switchport mode access
SwitchB(config-gigaethernet1/1/3)#switchport access vlan 10
SwitchB(config-gigaethernet1/1/3)#exit
SwitchB(config)#interface gigaethernet1/1/4
SwitchB(config-gigaethernet1/1/4)#switchport mode access
SwitchB(config-gigaethernet1/1/4)#switchport access vlan 20
SwitchB(config-gigaethernet1/1/4)#exit
SwitchB(config)#interface gigaethernet1/1/1
SwitchB(config-gigaethernet1/1/1)#switchport mode trunk
SwitchB(config-gigaethernet1/1/1)#switchport trunk allowed vlan 10
confirm
SwitchB(config-gigaethernet1/1/1)#exit
```

Step 3 Add GE 1/1/2 as Access mode on Switch A to VLAN 10, add GE 1/1/3 as Access mode to VLAN 20, configure GE 1/1/1 to Trunk mode, and allow VLAN 10 to pass.

```
SwitchA(config)#interface gigaethernet1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode access
SwitchA(config-gigaethernet1/1/2)#switchport access vlan 10
SwitchA(config-gigaethernet1/1/2)#exit
SwitchA(config)#interface gigaethernet1/1/3
SwitchA(config-gigaethernet1/1/3)#switchport mode trunk
SwitchA(config-gigaethernet1/1/3)#switchport trunk native vlan 20
SwitchA(config-gigaethernet1/1/3)#exit
SwitchA(config)#interface gigaethernet1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#switchport trunk allowed vlan 10
confirm
```

Checking results

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

Take Switch B for example.

```
SwitchB#show vlan
Switch Mode: --
VLAN Name          State   Status  Priority Member-Ports
------------------------------------------------------------------------
1    Default       active  static  --       P 1-6
2    VLAN0002      active  other   --       P 1-28
10   VLAN0010      active  static  --      gigaethernet1/1/2
gigaethernet1/1/3
20   VLAN0020      active  static  --       gigaethernet1/1/4
```

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

Take Switch B for example.

```
SwitchB#show switchport interface gigaethernet1/1/2
Interface: gigaethernet1/1/2
Switch Mode: switch
Reject frame type: none
Administrative Mode: access
Operational Mode: access
Access Mode VLAN: 10
Administrative Access Egress VLANs:
Operational Access Egress VLANs: 10
Trunk Native Mode VLAN: 1
Trunk Native VLAN: untagged
Administrative Trunk Allowed VLANs:
Operational Trunk Allowed VLANs: 1
Administrative Trunk Untagged VLANs:
Operational Trunk Untagged VLANs: 1
Administrative private-vlan host-association:  1
Administrative private-vlan mapping: 1
Operational private-vlan: --
```

Check whether the Trunk interface permitting VLAN passing is correct by making PC 1 ping PC 5, PC 2 ping PC 5, and PC 3 ping PC 4.

- PC 1 can ping through PC 5, so VLAN 10 communication is normal.
- PC 2 can ping through PC 5, so VLAN 10 communication is normal.
- PC 3 fails to ping through PC 4, so VLAN 20 communication is abnormal.

2.3 QinQ

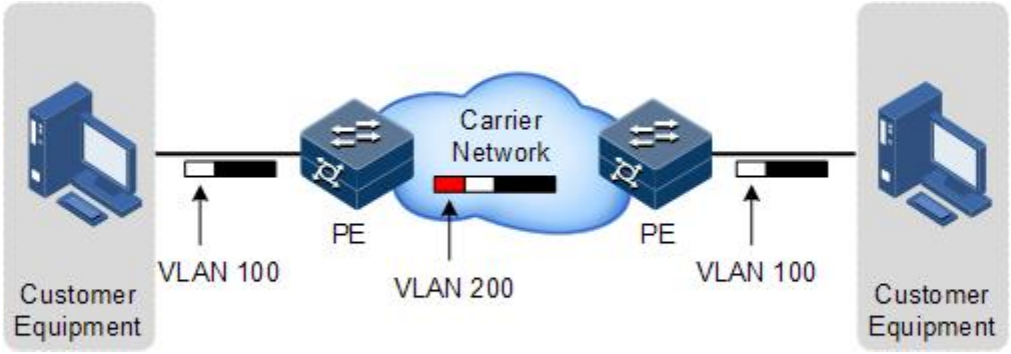
2.3.1 Introduction

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

Basic QinQ

Basic QinQ is a simple Layer 2 VPN tunnel technique, which encapsulates outer VLAN Tag for user private network packets at carrier access end, then the packet with double VLAN Tag traverse backbone network (public network) of the carrier. On the public network, packets are transmitted according to outer VLAN Tag (namely the public network VLAN Tag), the user private network VALN Tag is transmitted as data in packets.

Figure 2-5 Principles of basic QinQ



Typical networking of basic QinQ is shown as Figure 2-5; wherein, the ISCOM2600G series switch is the PE.

Packets are transmitted from the user device to the PE, and the VLAN ID of packet tag is 100. Packet will be added with outer tag with VLAN 1000 when traversing from the PE device at the network side interface to the carrier network.

Packets with the VLAN 1000 outer Tag are transmitted to PE device on the other side by the carrier, and then the PE will remove the outer tag VLAN 1000 and send packets to the user device. Now the packets return to carrying only one tag VLAN 100.

This technique can save public network VLAN ID resources. You can plan private network VLAN ID to avoid conflict with public network VLAN ID.

Selective QinQ

Selective QinQ is an enhancement to basic QinQ, which classifies flow according to user data features, then encapsulates different types flow into different outer VLAN Tags. This technique is implemented by combination of 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, encapsulate different outer Tags for users in different classes. On the public network, you can configure

QoS policy according to outer Tag and configure data transmission priority flexibly to make users in different classes receive corresponding services.

2.3.2 Preparing for configurations

Scenario

Basic QinQ configuration and selective QinQ configuration for the ISCOM2600G series switch are based on different service requirements.

- Basic QinQ

With application of basic QinQ, you can add outer VLAN Tag to plan Private VLAN ID freely to make the user device data at both ends of carrier network transparently transmitted without conflicting with VLAN ID on the service provider network.

- Selective QinQ

Different from basic QinQ, outer VLAN Tag of selective QinQ can be selectable according to different services. There are multiple services and different private VLAN ID on the user network which are divided by adding different outer VLAN Tag for voice, video, and data services, then implementing different distributaries and inner and outer VLAN mapping for forwarding different services.

Prerequisite

- Connect the interfaces.
- 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 VLAN Tag TPID	0x8100
Basic QinQ status	Disable
Selective QinQ status	Disable

2.3.4 Configuring basic QinQ

Configure basic QinQ on the ingress interface for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**dot1q-tunnel**	Enable basic QinQ on the interface.
4	Raisecom(config-gigaethernet1/1/1)#**switchport reject-frame** { **tagged** | **untagged** }	Configure the types of packets disallowed to be forwarded.

Note

- To use basic QinQ functions on an interface, configure its attributes first by configuring it to the Access or Trunk interface and configuring the default VLAN.
- When basic QinQ is enabled on the interface, all packets are processed as Untagged packets. If you configure the Untagged packets to be discarded, Tagged packets are discarded as well.

2.3.5 Configuring selective QinQ

Configure selective QinQ on the ingress interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gigaethernet1/1/1**	Enter physical layer interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#**dot1q-tunnel**	Enable basic QinQ on the interface.
4	Raisecom(config-gigaethernet1/1/1)#**switchport vlan-mapping cvlan** *custom-vlan-list* [**cos** *cos-value*] **add-outer** *outer-vlan-id*	(Optional) configure selective QinQ, and add the outer VLAN ID based on inner VLAN.
5	Raisecom(config-gigaethernet1/1/1)#**switchport vlan-mapping-miss discard**	Configure the interface to discard Tagged packets that fail to match selective QinQ or VLAN mapping rules.
6	Raisecom(config-gigaethernet1/1/1)#**switchport vlan-mapping ethertype** { **arp** | **eapol** | **flowcontro l ip** | **ipv6** / **loopback** | **mpls** | **mpls-mcast** | **pppoe** | **pppoedisc** | **user-define** *protocol id* | **x25** | **x75** }**add-outer** *outer-vlan-id*	Configure EtherType selective QinQ, and add mapping rules for Tag VLAN.

Step	Command	Description
7	Raisecom(config-gigaethernet1/1/1)#**switchport vlan-mapping both**{ **priority-tagged** | **cvlan** *custom-vlan-list* | *custom-vlan-id* }**add-outer** *outer-vlan-id* {**remove** | **translate** *vlan-id* } Raisecom(config-gigaethernet1/1/1)#**switchport vlan-mapping both** { **untag** | **inner** *inner -vlan-id* }**add-outer** *outer-vlan-id*	(Optional) configure bidirectional selective QinQ, and add outer VLAN rules.

Note

Before configuring selective QinQ, configure basic QinQ.

2.3.6 Configuring network-side interface toTrunk mode

Configure the network-side interface to Trunk mode for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**switchport mode trunk**	Configure interface trunk mode, permit double Tag packet to pass.

2.3.7 Configuring TPID

Configure TPID on the network side interface for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**tpid** *tpid*	Configure the TPID of the outer VLAN Tag on the interface.

2.3.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show dot1q-tunnel`	Show configurations of basic QinQ.
2	`Raisecom#show vlan-mapping both interface` *`interface-number`*	Show configurations of selective QinQ.

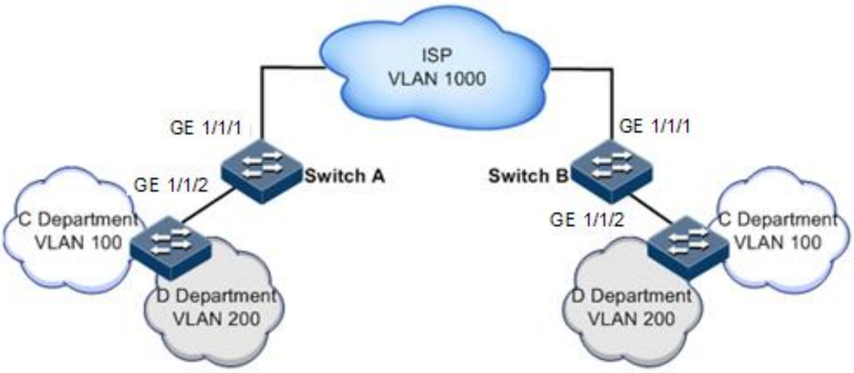
2.3.9 Example for configuring basic QinQ

Networking requirements

As shown in Figure 2-6, Switch A and Switch B are connected to VLAN 100 and VLAN 200 respectively. Two branches of Department C need to communicate through the carrier network, and so are those of Department D. However, different departments' network should be required. The carrier TPID is 9100.

Configure basic QinQ on Switch A and Switch B to enable normal communication inside a department through the carrier's network.

Figure 2-6 Basic QinQ networking



Configuration steps

Configure Switch A and Switch B.

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

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

```
Raisecom#config
Raisecom(config)#create vlan 100,200,1000 active
Raisecom(config)#interface gigaethernet1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport mode trunk
Raisecom(config-gigaethernet1/1/1)#switchport trunk allowed vlan 1000
Raisecom(config-gigaethernet1/1/1)#tpid 9100
Raisecom(config-gigaethernet1/1/1)#exit
```

Step 2 Configure basic QinQ on the interface.

```
Raisecom(config)#interface gigaethernet1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport mode trunk
Raisecom(config-gigaethernet1/1/2)#switchport trunk native vlan 1000
Raisecom(config-gigaethernet1/1/2)#dot1q-tunnel
Raisecom(config-gigaethernet1/1/2)#switchport qinq default-cvlan 100
Raisecom(config-gigaethernet1/1/2)#switchport qinq default-cvlan 200
Raisecom(config-gigaethernet1/1/2)#exit
```

Checking results

Use the **show dot1q-tunnel** command to show QinQ configurations.

```
Raisecom# show dot1q-tunnel
Interface          QinQ Status  Outer TPID on port  Cos override Vlan-
map-miss
-------------------------------------------------------
gigaethernet1/1/1     Enable      0x9100     -
gigaethernet1/1/2     Enable      0x8100     -
```

2.3.10 Example for configuring selective QinQ

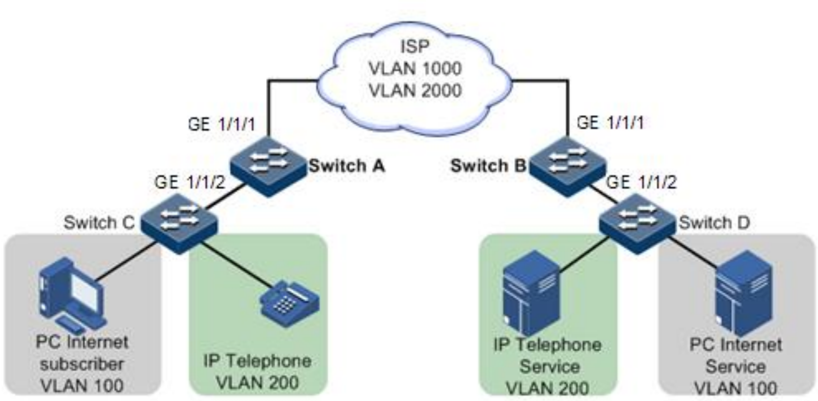
Networking requirements

As shown in Figure 2-7, the carrier network contains common PC Internet access service and IP phone service. PC Internet access 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 the user and server communicate through the carrier network:

- Add outer Tag VLAN 1000 to VLAN 100 assigned to PC Internet access service.
- Add outer Tag 2000 to VLAN 200 for IP phone service.
- The carrier TPID is 9100.

Figure 2-7 Selective QinQ networking



Configuration steps

Configure Switch A and Switch B.

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

Step 1 Create and activate VLAN 100, VLAN 200, VLAN 1000, and VAN 2000. The TPID is 9100.

```
Raisecom#name SwitchA
SwitchA#config
SwitchA(config)#create vlan 100,200,1000,2000 active
SwitchA(config)#interface gigaethernet1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#switchport trunk allowed vlan 1000,2000
SwitchA(config-gigaethernet1/1/1)#tpid 9100
SwitchA(config-gigaethernet1/1/1)#exit
```

Step 2 Enable selective QinQ on GE 1/1/2.

```
SwitchA(config)#interface gigaethernet1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
Raisecom(config-gigaethernet1/1/2)#dot1q-tunnel
Raisecom(config-gigaethernet1/1/2)#switchport qinq default-cvlan 100
Raisecom(config-gigaethernet1/1/2)#switchport qinq default-cvlan 200
SwitchA(config-gigaethernet1/1/2)#switchport vlan-mapping cvlan 100 add-
outer 1000
SwitchA(config-gigaethernet1/1/2)#switchport vlan-mapping cvlan 200 add-
outer 2000
SwitchA(config-gigaethernet1/1/2)#exit
```

Checking results

Use the **show switchport interface** *interface-type interface-number* **vlan-mapping add-outer** command to show configurations of selective QinQ.

Take Switch A for example.

```
SwitchA#show switchport port-list 2 vlan-mapping add-outer
Based inner VLAN flexible QinQ mapping rule:
Interface CVLAN   Add-SVlan    Cos   CVlan-Action Translate-CVlan Hardware
-----------------------------------------------------------------------
gigaethernet1/1/1    100     1000       0     Reserve     -
Yes
gigaethernet1/1/2    200     2000       0     Reserve     -
Yes
```

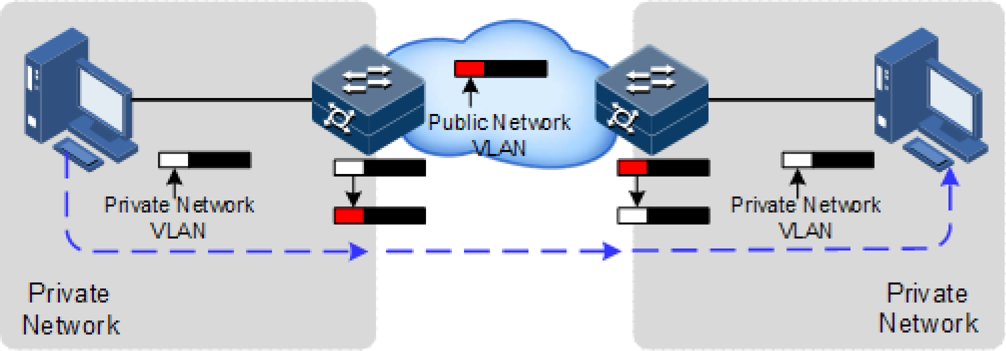
2.4 VLAN mapping

2.4.1 Introduction

VLAN mapping is used to replace the private VLAN Tag of Ethernet packets with carrier's VLAN Tag, making packets transmitted according to carrier'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 2-8 shows principles of VLAN mapping.

Figure 2-8 Principles of VLAN mapping



After receiving a VLAN Tag contained in a user private network packet, the ISCOM2600G series switch matches the packet according to configured VLAN mapping rules. If successful, it maps the packet according to configured VLAN mapping rules.

By supporting 1: 1 VLAN mapping, the ISCOM2600G series switch replaces the VLAN Tag carried by a packet from a specified VLAN to the new 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 rule.

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 interfaces.
- Configure its physical parameters to make it Up.
- Create VLANs.

2.4.3 Default configurations of VLAN mapping

Default configurations of VLAN mapping are as below.

Function	Default value
VLAN mapping status	Disable

2.4.4 Configuring 1:1 VLAN mapping

Configure 1:1 VLAN mapping for the ISCOM2600G series switch 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-gigaethernet1/1/1)#`**`switchport vlan-mapping ingress`** *`outer-vlan-id`* **`translate`** *`outer-new-vlan-id`*	Configure the VLAN mapping rule based on outer VLAN Tag in the ingress direction of the interface, translating the outer VLAN Tag only.
4	`Raisecom(config-gigaethernet1/1/1)#`**`switchport vlan-mapping egress`** *`outer-vlan-id`* **`translate`** *`outer-new-vlan-id`*	Configure the VLAN mapping rule based on outer VLAN Tag in the egress direction of the interface, translating the outer VLAN Tag only.

Step	Command	Description
5	Raisecom(config-gigaethernet1/1/1)#**switchport vlan-mapping egress outer** {**all** | *outer-vlan-id* } {**inner** *inner-vlan-id*| **outer** *outer-vlan-id* }{ **translate** *vlan-id* | **remove** | **tagged** | **unchanged** }{ **inner** | **outer** }{ **translate** *vlan-id* | **remove** | **tagged** }]	Configure the VLAN mapping rule based on outer VLAN Tag and inner VLAN Tag in the ingress direction of the interface, translating both the outer VLAN Tag and inner VLAN Tag.
6	Raisecom(config-gigaethernet1/1/1)#**switchport vlan-mapping ingress outer** { **all** | *outer-vlan-id* } **inner** { **all** | *inner-vlan-id* } **translate outer** *outer-new-vlan-id*	Configure the VLAN mapping rule based on outer VLAN Tag and inner VLAN Tag in the egress direction of the interface, translating both the outer VLAN Tag and inner VLAN Tag.
7	Raisecom(config-gigaethernet1/1/1)#**switchport vlan-mapping both add-outer** *vlan-id* [**inner** *inner -vlan-id*] **translate outer** *vlan-id* [**inner** *inner -vlan-id*]	Configure the VLAN mapping rule based on inner/outer VLAN in both the ingress and egress directions.

2.4.5 Checking configurations

Use the following commands to check configuration results.

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

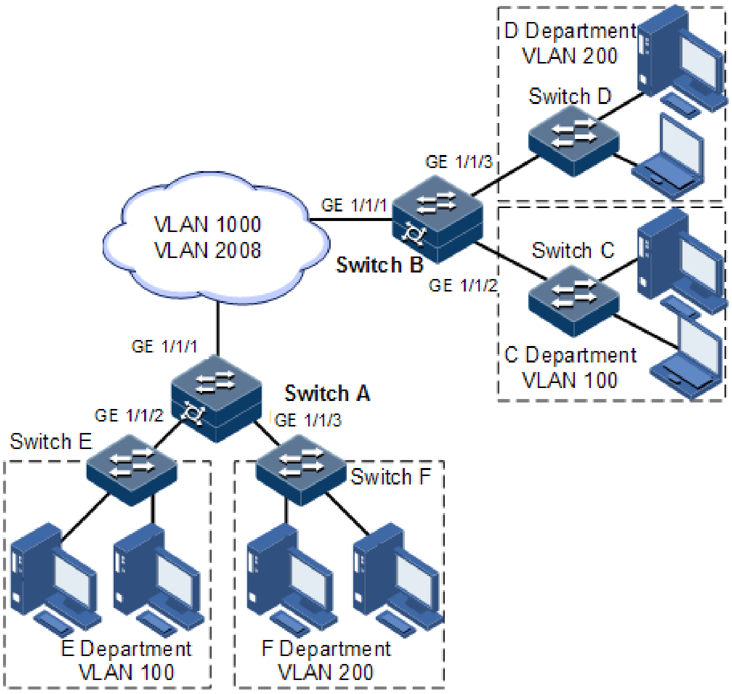
2.4.6 Example for configuring VLAN mapping

Scenario

As shown in Figure 2-9, GE 1/1/2 and GE 1/1/3 on Switch A are connected to Department E using VLAN 100 and Department F using VLAN 200; GE 1/1/2 and GE 1/1/3 on Switch A are connected to Department C using VLAN 100 and Department D using VLAN 200. The carrier's network uses VLAN 1000 to transmit services between Department E and Department C and uses VLAN 2008 to transmit services between Department F and Department D.

Configure 1:1 VLAN mapping between Switch A and Switch B to implement normal communication inside each department.

Figure 2-9 VLAN mapping networking



Configuration steps

Configure Switch A and Switch B.

Configuration steps for Switch A and Switch B are the same. Take Switch A for example.

Step 1 Create VLANs 100, 200, 1000, and 2008, and activate them. Enable VLAN mapping.

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

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

```
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#switchport trunk allowed vlan 1000,2008
confirm
SwitchA(config-gigaethernet1/1/1)#exit
```

Step 3 Configure GE 1/1/2 to Trunk mode, allowing VLAN 100 packets to pass. Configure VLAN mapping rules.

```
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
SwitchA(config-gigaethernet1/1/2)#switchport trunk allowed vlan 100
confirm
SwitchA(config-gigaethernet1/1/2)#switchport vlan-mapping ingress 100
translate 1000
SwitchA(config-gigaethernet1/1/2)#switchport vlan-mapping egress 1000
translate 100
SwitchA(config-gigaethernet1/1/2)#exit
```

Step 4 Configure GE 1/1/3 to Trunk mode, allowing VLAN 200 packets to pass. Configure VLAN mapping rules.

```
SwitchA(config)#interface gigaethernet 1/1/3
SwitchA(config-gigaethernet1/1/3)#switchport mode trunk
SwitchA(config-gigaethernet1/1/3)#switchport trunk allowed vlan 200
confirm
SwitchA(config-gigaethernet1/1/3)#switchport vlan-mapping ingress 200
translate 2008
SwitchA(config-gigaethernet1/1/3)#switchport vlan-mapping egress 2008
translate 200
```

Checking results

Use the **show vlan-mapping interface gigaethernet 1/1/2 egress translate** command to show configurations of 1:1 VLAN mapping.

```
SwitchA#show interface gigaethernet 1/1/2
Interface  : gigaethernet1/1/2
Hardware-ID: 2
Original Outer VLANs: 1000
Original Outer COS:   --
Original Inner VLANs: --
Original Inner COS:   --
Outer-tag Mode:      Translate
New Outer-VID:       100
New Outer-COS:       --
Inner-tag Mode:      --
New Inner-VID:       --
New Inner-COS:       --
```

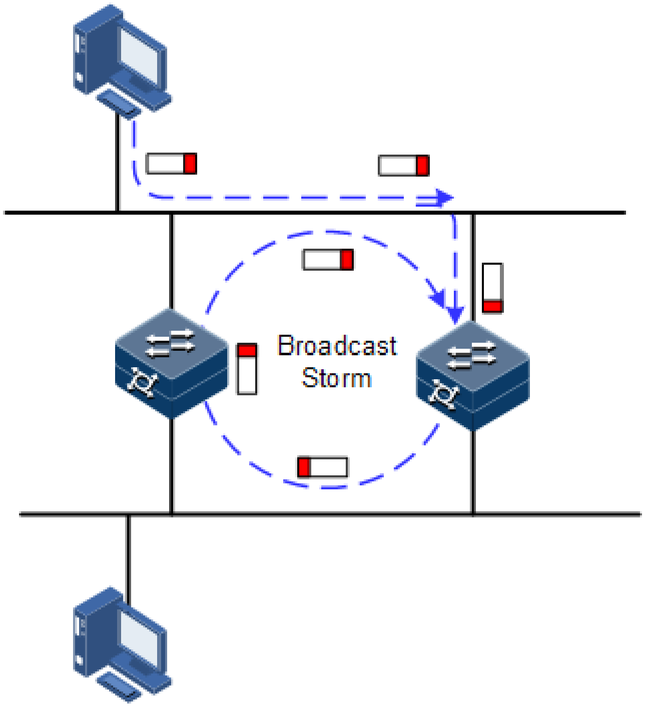
2.5 STP/RSTP

2.5.1 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 2-10.

Figure 2-10 Network storm due to loopback

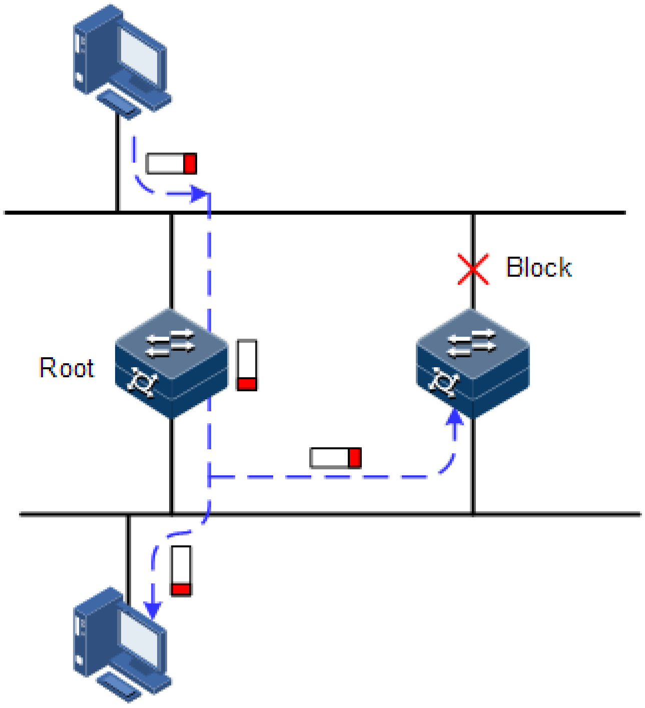


Spanning Tree Protocol (STP) is compliant to IEEE 802.1d standard and used to remove data physical loop in data link layer in the LAN.

The ISCOM2600G series switch running STP can process Bridge Protocol Data Unit (BPDU) with each other for the election of root switch and selection of root port and designated port. It also can block loop interface on the ISCOM2600G series switch logically according to the selection results, and finally trims the loop network structure to tree network structure without loop which takes an ISCOM2600G series switch as root. This prevents the continuous proliferation and limitless circulation of packet on the loop network from causing broadcast storms and avoids declining packet processing capacity caused by receiving the same packets repeatedly.

Figure 2-11 shows loop networking with STP.

Figure 2-11 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

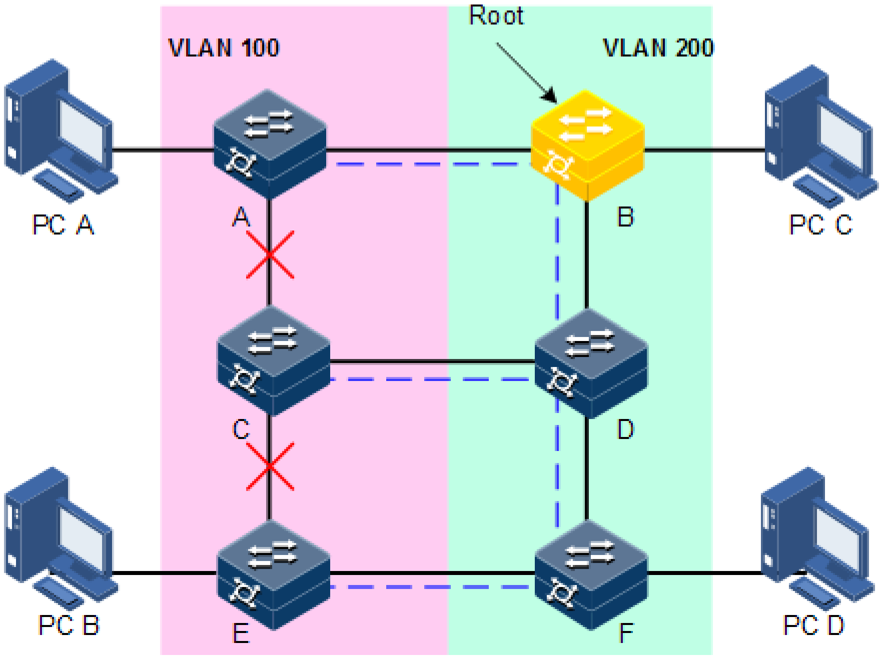
For improving the slow convergent speed of STP, IEEE 802.1w establishes Rapid Spanning Tree Protocol (RSTP), which increases the mechanism to change interface blocking state to forwarding state, speed up the topology convergence rate.

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 to the following problems:

- The whole switching network has only one spanning tree, which will lead to longer convergence time on a larger network.
- After a link is blocked, it does not carry traffic any more, causing waste of bandwidth.
- Packet of partial VLAN cannot be forwarded when network structure is unsymmetrical. As shown in Figure 2-12, 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 2-12 Failure to forward VLAN packets due to RSTP



2.5.2 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

N/A

2.5.3 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
Path cost of interface	0
Max Age timer	20s
Hello Time timer	2s

Function	Default value
Forward Delay timer	15s

2.5.4 Enabling STP

Configure STP for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`spanning-tree enable`**	Enable global STP.
3	`Raisecom(config)#`**`spanning-tree mode`** `{` **`stp`** `|` **`rstp`** `}`	Configure spanning tree mode.
4	`Raisecom(config)#`**`interface`** *`interface-type interface-number`*	Enter physical layer interface configuration mode.
5	`Raisecom(config-gigaethernet1/1/1)#`**`spanning-tree enable`**	Enable interface STP.

2.5.5 Configuring STP parameters

Configure STP parameters for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`spanning-tree priority`** *`priority-value`*	(Optional) configure device priorities.
3	`Raisecom(config)#`**`spanning-tree root`** `{` **`primary`** `|` **`secondary`** `}`	(Optional) configure the ISCOM2600G series switch as the root or backup device.

4	`Raisecom(config)#`**`interface`** *`interface-type interface-number`*
	`Raisecom(config-gigaethernet1/1/1)#`**`spanning-tree priority`** *`priority-value`*
		(Optional) configure interface priorities on the ISCOM2600G series switch.

5	`Raisecom(config-gigaethernet1/1/1)#`**`spanning-tree extern-path-cost`** *`cost-value`*
	`Raisecom(config-gigaethernet1/1/1)#`**`exit`**
		(Optional) configure the path cost of interfaces on the ISCOM2600G series switch.

6	`Raisecom(config)#`**`spanning-tree hello-time`** *`value`*	(Optional) configure the value of Hello Time.
7	`Raisecom(config)#`**`spanning-tree transit-limit`** *`value`*	(Optional) configure the maximum transmission rate of the interface

Step	Command	Description
8	`Raisecom(config)#spanning-tree forward-delay value`	(Optional) configure forward delay.
9	`Raisecom(config)#spanning-tree max-age value`	(Optional) configure the maximum age.

2.5.6 (Optional) configuring RSTP edge interface

The edge interface indicates that the interface neither directly connects to any devices nor indirectly connects to any device through the 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 edge interface to make it quick to change to forward status.

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

By default, all interfaces on the ISCOM2600G series switch are configured in auto-detection attribute.

Configure the edge interface for the ISCOM2600G series switch 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-gigaethernet1/1/1)#spanning-tree edged-port { auto | force-true | force-false }`	Configure attributes of the RSTP edge interface.

2.5.7 (Optional) configuring RSTP link type

Two interfaces connected by a point-to-point link can quickly transit to forward status by transmitting synchronization packets. By default, MSTP configures the link type of interfaces according to duplex mode. The full duplex interface is considered as the point-to-point link, and the half duplex interface is considered as the shared link.

You can manually configure the current Ethernet interface to connect to a point-to-point link, but the system will fail if the link is not point to point. Generally, we recommend configuring 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 ISCOM2600G series switch 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-gigaethernet1/1/1)#**spanning-tree link-type** { **auto** | **point-to-point** | **shared** }	Configure link type for interface.

2.5.8 Checking configurations

Use the following commands to check configuration results.

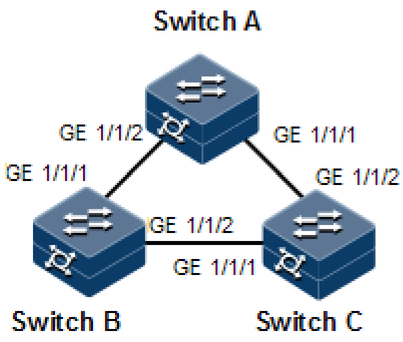
No.	Command	Description
1	Raisecom#**show spanning-tree**	Show basic configurations of STP.
2	Raisecom#**show spanning-tree** *interface-type interface-list* [**detail**]	Show STP configuration on the interface.

2.5.9 Example for configuring STP

Networking requirements

As shown in Figure 2-13, Switch A, Switch B, and Switch C forms a ring network, so the loop must be eliminated in the situation of a physical link forming a 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 2-13 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 modes on three switches.

Configure Switch A.

```
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#exit
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
SwitchA(config-gigaethernet1/1/2)#exit
```

Configure Switch B.

```
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)#switchport mode trunk
SwitchB(config-gigaethernet1/1/1)#exit
SwitchB(config)#interface gigaethernet 1/1/2
SwitchB(config-gigaethernet1/1/2)#switchport mode trunk
SwitchB(config-gigaethernet1/1/2)#exit
```

Configure Switch C.

```
SwitchC(config)#interface gigaethernet 1/1/1
SwitchC(config-gigaethernet1/1/1)#switchport mode trunk
SwitchC(config-gigaethernet1/1/1)#exit
SwitchC(config)#interface gigaethernet 1/1/2
SwitchC(config-gigaethernet1/1/2)#switchport mode trunk
SwitchC(config-gigaethernet1/1/2)#exit
```

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

Configure Switch A.

```
SwitchA(config)#spanning-tree priority 0
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#spanning-tree extern-path-cost 10
```

Configure Switch B.

```
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)#spanning-tree extern-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
           MaxHops   20  Diameter 7
```

Use the **show spanning-tree port-list** *port-list* command to show interface status.

Take Switch A for example.

```
SwitchA#show spanning-tree gigaethernet 1/1/1
GE1/1/1
PortProtocolEnable: admin: enable oper: enable Rootguard:  disable
Loopguard:  disable
Bpduguard:  disable
ExternPathCost:200000
```

```
Partner STP Mode: stp
Bpdus send:   0     (TCN<0>  Config<0>  RST<0>  MST<0>)
Bpdus received:0     (TCN<0>  Config<0>  RST<0>  MST<0>)
State:blocking   Role:non-designated  Priority:128    Cost: 200000
Root:           Mac 0000.0000.0000  Priority 0      RootCost       0
DesignatedBridge: Mac 0000.0000.0000  Priority 0      DesignatedPort   0
```

2.6 MSTP

2.6.1 Introduction

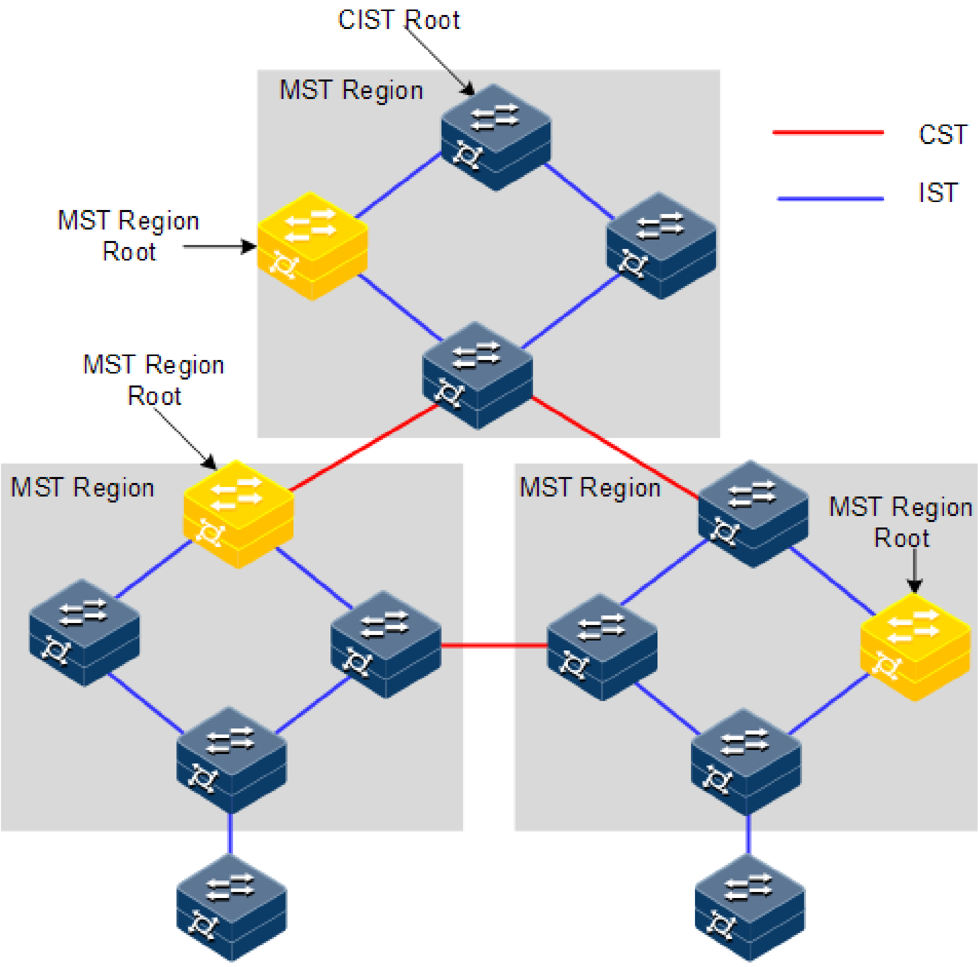
Multiple Spanning Tree Protocol (MSTP) is defined by IEEE 802.1s. Recovering the disadvantages of STP and RSTP, the MSTP implements fast convergence and distributes different VLAN flow following its own path to provide an excellent load balancing mechanism.

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.

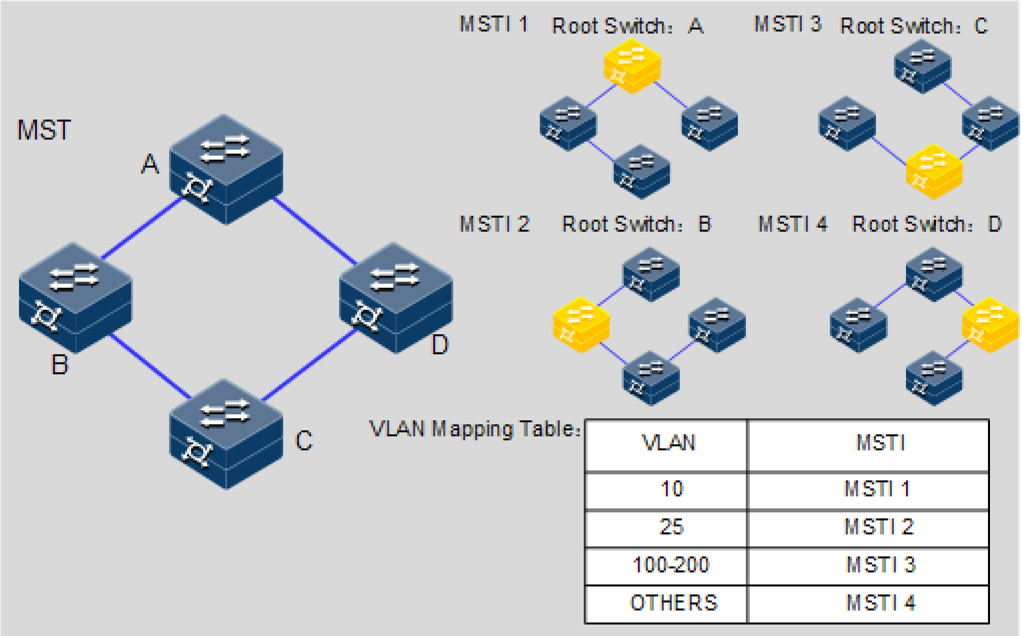
Compared with STP and RSTP, MSTP also introduces total root (CIST Root) and domain root (MST Region Root) concepts. The total root is a global concept; all switches running STP/RSTP/MSTP can have only one total root, which is the CIST Root. The domain root is a local concept, which is relative to an instance in a domain. As shown in Figure 2-14, all connected devices only have one total root, and the number of domain root contained in each domain is associated with the number of instances.

Figure 2-14 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 in Figure 2-15.

Figure 2-15 MSTI concepts



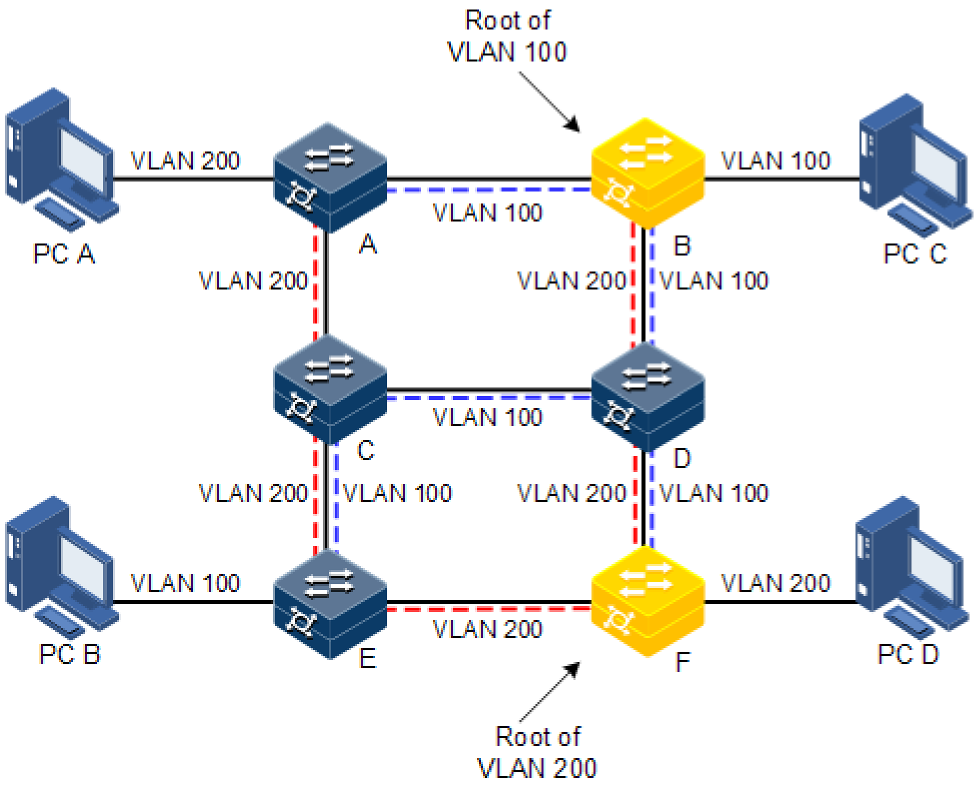
VLAN	MSTI
10	MSTI 1
25	MSTI 2
100-200	MSTI 3
OTHERS	MSTI 4

Note

Each VLAN can map to one MSTI; namely, data of one VLAN can only be transmitted in one MSTI but one MSTI may correspond to several VLANs.

Compared with STP and RSTP mentioned previously, MSTP has obvious advantages, including cognitive ability of VLAN, load balancing, similar RSTP interface status switching, and binding multiple VLAN to one MST instance, to reduce resource occupancy rate. In addition, devices running MSTP on the network are also compatible with the devices running STP and RSTP.

Figure 2-16 Networking with multiple spanning trees instances in MST domain



Apply MSTP to the network as shown in Figure 2-16. After calculation, there are two spanning trees generated at last (two MST instances):

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

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

2.6.2 Preparation for configuration

Scenario

In a big LAN or residential region aggregation, the aggregation devices make up a ring for link backup, avoiding loop and realizing load balancing. MSTP can select different and unique forwarding paths for each one or a group of VLANs.

Prerequisite

N/A

2.6.3 Default configurations of MSTP

Default configurations of MSTP are as below.

Function	Default value
Global MSTP status	Disable
Interface MSTP status	Enable
Maximum numbers of hops in the MST domain	20
MSTP priority of the device	32768
MSTP priority of the interface	128
Path cost of the 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

2.6.4 Enabling MSTP

Enable MSTP for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`spanning-tree mode mstp`**	Configure spanning tree for MSTP.
3	`Raisecom(config)#`**`spanning-tree enable`**	Enable global STP.
4	`Raisecom(config)#`**`interface`** *`interface-type interface-number`*	Enter physical layer interface configuration mode.
5	`Raisecom(config-gigaethernet1/1/1)#`**`spanning-tree enable`**	Enable interface STP.

2.6.5 Configuring MST domain and its maximum number of hops

You can configure domain information about the ISCOM2600G series switch when it is running in MSTP mode. The device MST domain is determined by the 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 ISCOM2600G series switch 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 ISCOM2600G series switch as below.

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

Note

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

2.6.6 Configuring root/backup bridge

Two methods for MSTP root selection are as below:

- To configure device priority and calculated by STP to confirm STP root bridge or backup bridge
- To assign MSTP root directly by a command

When the root bridge has a fault or powered off, the backup bridge can replace of 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 several 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.

Note

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

Configure the root bridge or backup bridge for the ISCOM2600G series switch as below.

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

Step	Command	Description
2	Raisecom(config)#**spanning-tree** [**instance** *instance-id*] **root** { **primary** | **secondary** }	Configure the ISCOM2600G series switch as the root bridge or backup bridge of a STP instance.

Note

- You can confirm the effective instance of the root bridge or backup bridge through the **instance** *instance-id* parameter. The current device will be assigned as the root bridge or backup bridge of CIST if instance-id is 0 or the **instance** *instance-id* parameter is omitted.
- The roots in device instances are mutually independent; namely, 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 a spanning tree instance, a device cannot be used as the root bridge and backup bridge concurrently.
- You cannot assign two or more root bridges for one spanning tree instance, but can assign several backup bridges for one spanning tree. Generally, you had better assign one root bridge and several backup bridges for a spanning tree.

2.6.7 Configuring interface priority 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 ISCOM2600G series switch can be selected as the root of the spanning tree. Configuring smaller priority helps obtain smaller Bridge ID and designate the ISCOM2600G series switch as the root. If priorities of two ISCOM2600G series switch devices are identical, the ISCOM2600G series switch 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 ISCOM2600G series switch 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-gigaethernet1/1/1)#**spanning-tree** [**instance** *instance-id*] **priority** *priority-value* Raisecom(config-gigaethernet1/1/1)#**exit**	Configure interface priority for a STP instance.

Step	Command	Description
4	Raisecom(config)#**spanning-tree** [**instance** *instance-id*] **priority** *priority-value*	Configure system priority for a STP instance.

Note

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

2.6.8 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 on the entire 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 greater the network diameter is, the larger the network scale is.

Similar to the maximum number of hops of MST domain, only when the ISCOM2600G series switch 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.

2.6.9 Configuring internal path cost of interface

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 internal path cost for instance through the **instance** *instance-id* parameter. Configure internal 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 internal path cost for the ISCOM2600G series switch 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-gigaethernet1/1/1)#`**`spanning-tree`** `[` **`instance`** *`instance-id`* `]` **`inter-path-cost`** *`cost-value`*	Configure the internal path cost of the interface.

2.6.10 Configuring external path cost of 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 ISCOM2600G series switch 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-gigaethernet1/1/1)#`**`spanning-tree extern-path-cost`** *`cost-value`*	Configure the external path cost of the interface.

2.6.11 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 ISCOM2600G series switch as below.

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

2.6.12 Configuring MSTP timer

- Hello Time: the ISCOM2600G series switch sends the interval of bridge configurations (BPDU) regularly to check whether there is failure in detection link of the ISCOM2600G series switch. The ISCOM2600G series switch 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 ISCOM2600G series switch 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 a too great 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 ISCOM2600G series switch 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.

2.6.13 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 edge interface to make it quick to change to forward status.

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

By default, all interfaces on the ISCOM2600G series switch are configured in auto-detection attribute.

Configure the edge interface for the ISCOM2600G series switch 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-gigaethernet1/1/1)#`**`spanning-tree edged-port`** `{` **`auto`** `|` **`force-true`** `|` **`force-false`** `}`	Configure attributes of the RSTP edge interface.

2.6.14 Configuring BPDU filtering

After being enabled with BPDU filtering, the edge interface does not send BPDU packets nor process received BPDU packets.

Configure BPDU filtering for the ISCOM2600G series switch 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-gigaethernet1/1/1)#`**`spanning-tree edged-port bpdu-filter enable`** *`interface-type interface-number`*	Enable BPDU filtering on the edge interface.

2.6.15 Configuring BPDU Guard

On a switch, interfaces directly connected with non-switch devices, such as terminals (such as a PC) or file servers, are configured as edge interfaces to implement fast transition of these interfaces.

In normal status, these edge interfaces do not receive BPDUs. If forged BPDU attacks the switch, the switch will configure these edge interfaces to non-edge interfaces when these edge interfaces receive forged BPDUs and re-perform spanning tree calculation. This may cause network vibration.

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

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

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**spanning-tree bpduguard enable**	Enable BPDU Guard.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-gigaethernet1/1/1)#**no spanning-tree bpduguard shutdown port**	Manually restore interfaces that are shut down by BPDU Guard.

Note

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

2.6.16 Configuring STP/RSTP/MSTP mode switching

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

- STP compatible mode: the ISCOM2600G series switch does not implement fast switching from the replacement interface to the root interface and fast forwarding by a specified interface; instead it sends STP configuration BPDU and STP Topology Change Notification (TCN) BPDU. After receiving MST BPDU, it discards unidentifiable part.
- RSTP mode: the ISCOM2600G series switch implements fast switching from the replacement interface to the root interface and fast forwarding by a specified interface. It sends RST BPDUs. After receiving MST BPDUs, it discards unidentifiable part. If the peer device runs STP, the local interface is switched to STP compatible mode. If the peer device runs MSTP, the local interface remains in RSTP mode.
- MSTP mode: the ISCOM2600G series switch 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 ISCOM2600G series switch as below.

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

2.6.17 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 configuring 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 ISCOM2600G series switch 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-gigaethernet1/1/1)#`**`spanning-tree link-type`** `{` **`auto`** `|` **`point-to-point`** `|` **`shared`** `}`	Configure link type for interface.

2.6.18 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 BPDUs with higher priority, the network may become unstable due to 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 ISCOM2600G series switch 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-gigaethernet1/1/1)#`**`spanning-tree rootguard enable`**	Enable/Disable root interface protection.

2.6.19 Configuring interface loopguard

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

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

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

Note

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

Configure interface loop protection for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**spanning-tree loopguard enable**	Configure interface loopguard attributes.

2.6.20 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*] *interface-type interface-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.

2.6.21 Maintenance

Maintain the ISCOM2600G series switch as below.

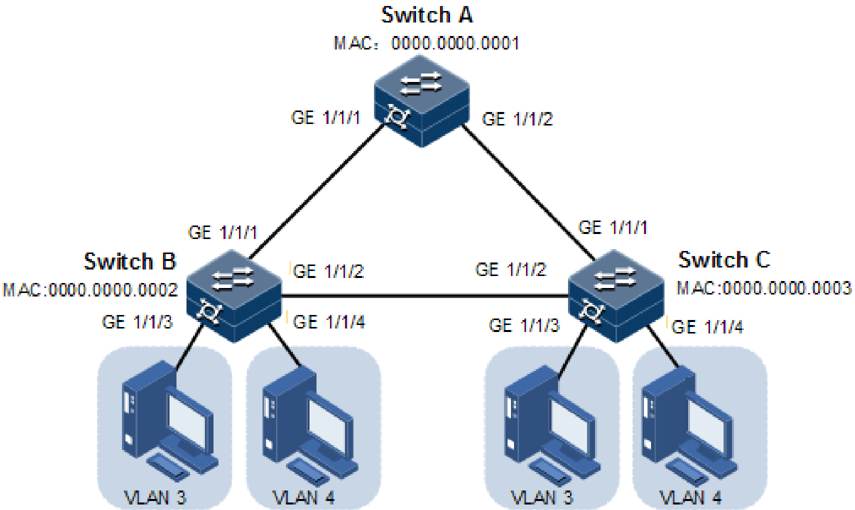
Command	Description
Raisecom(config-gigaethernet1/1/1)#**spanning-tree clear statistics**	Clear statistics of spanning tree on the interface.

2.6.22 Example for configuring MSTP

Networking requirements

As shown in Figure 2-17, three ISCOM2600G series switch 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 associated with VLAN 3. Instant 4 is associated with 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 loops and implements load balancing.

Figure 2-17 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#name SwitchA
SwitchA#config
SwitchA(config)#create vlan 3,4 active
```

Configure Switch B.

```
Raisecom#name SwitchB
SwitchB#config
SwitchB(config)#create vlan 3,4 active
```

Configure Switch C.

```
Raisecom#name SwitchC
SwitchC#config
SwitchC(config)#create vlan 3,4 active
```

Step 2 Configure GE 1/1/1 and GE 1/1/2 on Switch A to allow packets of all VLAN to pass in Trunk mode. Configure GE 1/1/1 and GE 1/1/2 on Switch B to allow packets of all VLANs to pass in Trunk mode. Configure GE 1/1/1 and GE 1/1/2 on Switch C to allow packets of all VLANs to pass in Trunk mode. Configure GE 1/1/3 and GE 1/3/4 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 gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#exit
SwitchA(config)#interface gigaethernet 1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
SwitchA(config-gigaethernet1/1/2)#exit
```

Configure Switch B.

```
SwitchB(config)#interface gigaethernet 1/1/1
SwitchB(config-gigaethernet1/1/1)#switchport mode trunk
SwitchB(config-gigaethernet1/1/1)#exit
SwitchB(config)#interface gigaethernet t 1/1/2
SwitchB(config-gigaethernet1/1/2)#switchport mode trunk
SwitchB(config-gigaethernet1/1/2)#exit
SwitchB(config)#interface gigaethernet 1/1/3
SwitchB(config-gigaethernet1/1/3)#switchport access vlan 3
SwitchB(config-gigaethernet1/1/3)#exit
SwitchB(config)#interface gigaethernet 1/1/4
SwitchB(config-gigaethernet1/1/4)#switchport access vlan 4
SwitchB(config-gigaethernet1/1/4)#exit
```

Configure Switch C.

```
SwitchC(config)#interface gigaethernet 1/1/1
SwitchC(config-gigaethernet1/1/1)#switchport mode trunk
SwitchC(config-gigaethernet1/1/1)#exit
SwitchC(config)#interface gigaethernet 1/1/2
SwitchC(config-gigaethernet1/1/2)#switchport mode trunk
SwitchC(config-gigaethernet1/1/2)#exit
SwitchC(config)#interface gigaethernet 1/1/3
SwitchC(config-gigaethernet1/1/3)#switchport access vlan 3
SwitchC(config-gigaethernet1/1/3)#exit
SwitchC(config)#interface gigaethernet 1/1/4
SwitchC(config-gigaethernet1/1/4)#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 internal path cost of GE 1/1/1 of spanning tree instance 3 to 500000 on Switch B.

```
SwitchB(config)#interface gigaethernet 1/3/1
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.

Take Switch A for example.

```
SwitchA#show spanning-tree region-operation
Operational Information:
-----------------------------------------------
Name: aaa
Revision level: 0
Instances running: 3
Digest: 0X024E1CF7E14D5DBBD9F8E059D2C683AA
Instance  Vlans Mapped
--------  ------------------------------
0        1-2,5-4094
3        3
4        4
```

Use the **show spanning-tree instance 3** command to show basic information about spanning tree instance 3.

Take Switch A for example.

```
SwitchA#show spanning-tree instance 3
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP

MST ID: 3
-----------------------------------------------------------
BridgeId:    Mac 000E.5E11.2233  Priority 32768
RegionalRoot: Mac 000E.5E11.2233  Priority 32768  InternalRootCost 0
Port     PortState   PortRole   PathCost  PortPriority  LinkType
------------------------------------------------------------------
```

Use the **show spanning-tree instance 4** command to show basic information about spanning tree instance 4.

Take Switch A for example.

```
SwitchA#show spanning-tree instance 4
Spanning-tree admin state: enable
Spanning-tree protocol mode: MSTP

MST ID: 4
```

```
-----------------------------------------------------------------
BridgeId:    Mac 000E.5E11.2233  Priority 32768
RegionalRoot: Mac 000E.5E11.2233  Priority 32768  InternalRootCost 0
Port     PortState   PortRole   PathCost  PortPriority  LinkType
-------------------------------------------------------------------------
```

2.7 Loop detection

2.7.1 Introduction

Loop detection can address the influence on network caused by a loop, providing the self-detection, fault-tolerance, and robustness.

During loop detection, an interface enabled with loop detection periodically sends loop detection packets (Hello packets). Under normal conditions, the edge interface should not receive any loop detection packets because loop detection is applied to the edge interface. However, if the edge interface receives a loop detection packet, it is believed that a loop occurs on the network. There are two conditions that an edge interface receives a loop detection packet: receiving a loop detection packet from itself or receiving a loop detection packet from other devices, which can be told by comparing the MAC address of the device and the MAC address carried in the packet.

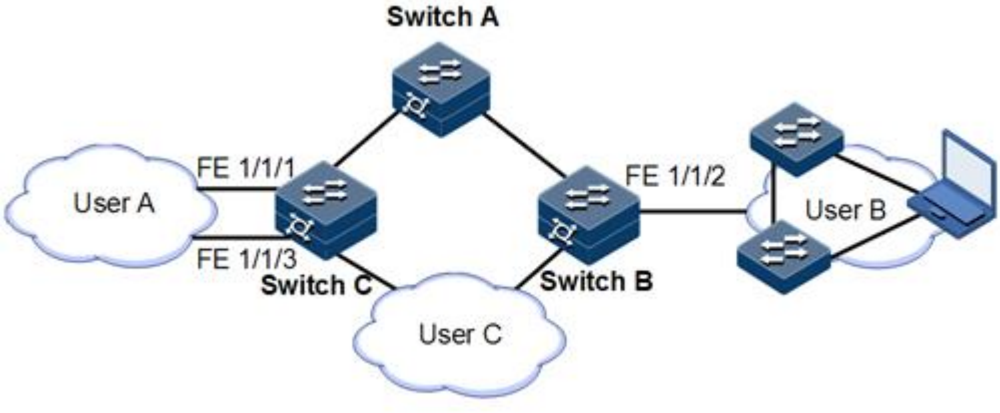
Loop types

Common loop types include self-loop, inner loop, and outer loop.

As shown in Figure 2-18, Switch B and Switch C are connected to the user network.

- Self-loop: a user loop on the same Ethernet interface of the same device. User network B has a loop, which forms self-loop on FE 1/1/2 on Switch B.
- Inner loop: a loop forming on different Ethernet interfaces of the same device. FE 1/1/1 and FE 1/1/3 on Switch C forms an inner loop with the user network A.
- Outer loop: a loop forming between Ethernet interfaces on different devices. For example, Switch A, Switch B, Switch C, and User C network form an outer loop.

Figure 2-18 Loop detection networking



Principle for processing loops

The ISCOM2600G series switch processes loops as below:

- If the device sending the loop detection packet is not the one receiving the packet, process the device with the larger MAC address to eliminate the loop (outer loop).
- If the device sending the loop detection packet is the one receiving the packet but the interface sending the packet and the interface receiving the packet are different, process the interface with the larger interface ID to eliminate the loop (inner loop).
- If the interface sending the packet and the interface receiving the packet are the same, process the interface to eliminate the loop (self-loop).

In Figure 2-18, assume that both Switch B and Switch C connect user network interfaces enabled with loop detection. The system processes loops for the three loop types as below:

- Self-loop: the interface sending the packet and the interface receiving the packet on Switch B are the same, the configured loop detection action will be taken to eliminate the loop on FE 1/1/2.
- Inner loop: Switch C receives the loop detection packets sent by it and the interface sending the packet and the interface receiving the packet are the same, the configured loop detection action will be taken to eliminate the loop on the interface with a bigger interface number, namely, FE 1/1/3.
- Outer loop: Switch B and Switch C receive the loop detection packets from each other, and the configured loop detection action will be taken to eliminate the loop on the switch with a bigger MAC address.

Action for processing loops

The action for processing loops is the method for the ISCOM2600G series switch to use upon loop detection. You can define different actions on the specified interface according to actual situations, including:

- Discarding: block the interface and send Trap.
- Trap-only: send Trap only.
- Shutdown: shut down the interface and send Trap.

Loop detection modes

The loop detection modes consist of port mode and VLAN mode:

- Port mode: when a loop occurs, the system blocks the interface and sends Trap in the loopback processing mode of discarding, or shuts down the physical interface and sends Trap information in the loopback processing mode of shutdown.
- VLAN mode: when a loop occurs,
  - In loopback processing mode of discarding, when a loop occurs on one or more of VLANs to which the interface belongs, the system blocks the VLANs with loop and leaves other VLANs to normally receive or send packets.
  - In loopback processing mode of shutdown, the system shuts down the physical interface and sends Trap information.

If the loop detection processing mode is Trap-only in the previous two modes, the ISCOM2600G series switch sends Trap only.

Loop restoration

After an interface is blocked or shut down, you can configure it, such as no automatic restoration and automatic restoration after a specified period.

- If an interface is configured as automatic restoration after a specified period, the system will start loop detection after the period. If the loop disappears, the interface will be restored; otherwise, it will be kept in blocking or shutdown status.
- If an interface is configured as no automatic restoration, namely, the automatic restoration time is infinite; it will not be automatically restored. However, you can use the **no loopback-detection discarding** command to manually restore the interface blocked or shut down upon loop detection.

2.7.2 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 on all access devices to avoid the network congestion generated by unlimited copies of data traffic. Once a loopback is detected on an interface, the interface will be blocked.

Prerequisite

Loopback interface, interface backup, STP, G.8032, and RRPS interfere with each other. We do not recommend configuring two or more of them concurrently.

2.7.3 Default configurations of loop detection

Default configurations of loop detection are as below.

Function	Default value
Loop detection status	Disable
Automatic recovery time for the blocked interface	Infinite, namely, no automatic recovery
Mode for processing detected loops	trap-only
Loop detection period	4s
Loop detection mode	VLAN

2.7.4 Configuring loop detection

Note

- Loop detection and STP are exclusive, so only one can be enabled at a time.
- Loop detection cannot be concurrently enabled on both two directly-connected devices.

Configure loop detection based on interface+VLAN for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#**loopback-detection** [[**detect-vlanlist** *vlanlist*] [**pkt-vlan** { **untag** | *vlan-id* }] [**hello-time** *second*] [**restore-time** *second*] [**action** { **block** | **trap-only** | **shutdown** }] [**log-interval** *log-interval time*]	Enable loop detection on the interface. Configure the VLAN for sending loop detection packets. (Optional) configure the period for sending Hello packets. (Optional) configure the time for automatically restoring the blocked interface due to loop detection and the action for processing loops.
4	Raisecom(config-gigaethernet1/1/1)#**loopback-detection manual restore**	Manually restore the interface blocked due to loop detection.

2.7.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show loopback-detection** [**statistics**] [*interface-type interface-number*] [**details**]	Show configurations and status of loop detection.

2.7.6 Maintenance

Maintain the ISCOM2600G series switch by below commands.

Command	Description
Raisecom(config)#**clear loopback-detection statistic**	Clear statistics of loop detection.

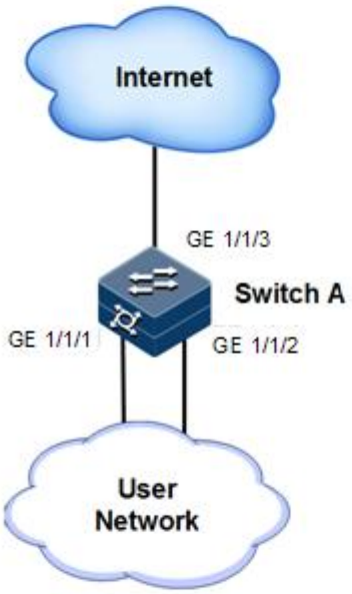
2.7.7 Example for configuring inner loop detection

Networking requirements

As shown in Figure 2-19, GE 1/1/2 and GE 1/1/3 on Switch A are connected to the user network. To avoid loops on the user network, enable loop detection on Switch A to detect loops on user network, and then take actions accordingly. Detailed requirements are as below:

- Enable loop detection on GE 1/1/2 and GE 1/1/3.
- Configure the interval for sending loop detection packets to 3s.
- Configure the VLAN for sending loop detection packets to VLAN 3.
- Configure the loop detection processing action to discarding, namely, sending Trap and blocking the interface.

Figure 2-19 Loop detection networking



Configuration steps

Step 1 Create VLAN 3, and add interfaces to VLAN 3.

```
Raisecom#config
Raisecom(config)#create vlan 3 active
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport access vlan 3
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport access vlan 3
Raisecom(config-gigaethernet1/1/2)#exit
```

Step 2 Configure the VLAN for sending loop detection packets.

```
Raisecom(config-gigaethernet1/1/1)#loopback-detection pkt-vlan 3
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#loopback-detection pkt-vlan 3
```

Step 3 Configure the action taken for processing detected loops.

```
Raisecom(config-gigaethernet1/1/1)#loopback-detection action block
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#loopback-detection action block
Raisecom(config-gigaethernet1/1/2)#exit
```

Step 4 Configure the interval for sending loop detection packets.

```
Raisecom(config-)#loopback-detection hello-time 3
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#loopback-detection hello-time 3
Raisecom(config-gigaethernet1/1/2)#exit
```

Checking results

Use the **show loopback-detection** command to show loop detection status. GE 1/1/2 is already blocked because of its greater interface ID, so the loop is eliminated.

```
Raisecom#show loopback-detection
Interface  pktVlan  detect-vlanlist    hellotime  restoretime  loop-act
log-interval  Status   loop-srcMAC      loop-srcPort   loop-Duration  loop-
vlanlist
-----------------------------------------------------------------------------
-----------------------------------------------------------------------------
-----------------
GE1/1/1    3      --               1        5         block      0
no      --              --           --          --

GE1/1/2    3      --               1        5         block      0
no      --              --           --          --
```

2.7.8 Example for configuring outer loop detection

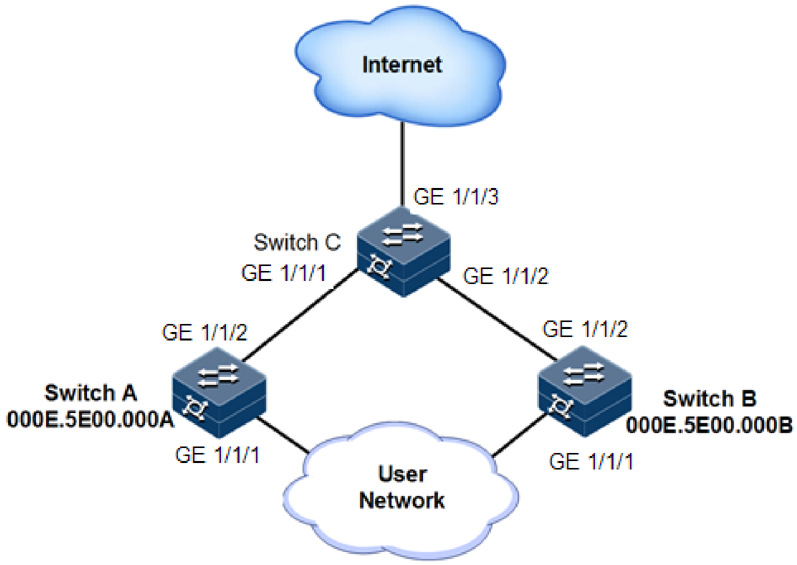
Networking requirements

As shown in Figure 2-20, Switch A, Switch B, and Switch C are connected to the user network (VLAN 3). To avoid loops on the user network, enable loop detection on Switch A and Switch B to detect loops on the user network, and then take actions accordingly. Detailed requirements are as below:

- Enable loop detection on GE 1/1/1 on both Switch A and Switch B.
- Configure the interval for sending loop detection packets to 3s.

- Configure loop detection mode to Port.
- Configure the loop detection processing action to shutdown, namely, shutting down the interface.

Figure 2-20 Networking with outer loop detection



Configuration steps

Step 1 Create VLAN 3, and add interfaces to VLAN 3.

Configure Switch A.

```
Raisecom#name SwitchA
SwitchA#config
SwitchA(config)#create vlan 3 active
SwitchA(config)#interface gigaethernet1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode access
SwitchA(config-gigaethernet1/1/1)#switchport access vlan 3
SwitchA(config-gigaethernet1/1/1)#exit
SwitchA(config)#interface gigaethernet1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
SwitchA(config-gigaethernet1/1/2)#exit
```

Configure Switch B.

```
Raisecom#name SwitchB
SwitchB#config
SwitchB(config)#create vlan 3 active
SwitchB(config)#interface gigaethernet1/1/1
SwitchB(config-gigaethernet1/1/1)#switchport mode access
SwitchB(config-gigaethernet1/1/1)#switchport access vlan 3
SwitchB(config-gigaethernet1/1/1)#exit
SwitchB(config)#interface gigaethernet1/1/2
SwitchB(config-gigaethernet1/1/2)#switchport mode trunk
SwitchB(config-gigaethernet1/1/2)#exit
```

Configure Switch C.

```
Raisecom#name SwitchC
SwitchC#config
SwitchB(config)#interface gigaethernet1/1/1
SwitchB(config-gigaethernet1/1/1)#switchport mode trunk
SwitchB(config-gigaethernet1/1/1)#exit
SwitchB(config)#interface gigaethernet1/1/2
SwitchB(config-gigaethernet1/1/2)#switchport mode trunk
SwitchB(config-gigaethernet1/1/2)#exit
```

Step 2 Enable loop detection.

Configure Switch A.

```
SwitchA(config)#loopback-detection enable gigaethernet1/1/1
SwitchA(config)#loopback-detection mode port-based
SwitchA(config)#loopback-detection loop shutdown gigaethernet1/1/1
SwitchA(config)#loopback-detection hello-time 3
```

Configure Switch B.

```
SwitchB(config)#loopback-detection enable gigaethernet 1/1/1
SwitchB(config)#loopback-detection mode port-based
SwitchB(config)#loopback-detection loop shutdown gigaethernet 1/1/1
SwitchB(config)#loopback-detection hello-time 3
```

Checking results

Use the **show loopback-detection** command on Switch A and Switch B to show loop detection status. GE 1/1/1 on Switch B will be shut down to eliminate the loop because the MAC address of Switch B is greater than that of Switch A.

```
SwitchA#show loopback-detection gigaethernet 1/1/1
Destination address: FFFF.FFFF.FFFF
Mode:Port-based
Period of loopback-detection:3s
Restore time:infinite
Port                PortState      State    Status     loop-act
vlanlist
```

```
-----------------------------------------------------------------
gigaethernet 1/1/1   Down           Ena      no        shutdown

SwitchB#show loopback-detection gigaethernet 1/1/1
Destination address: FFFF.FFFF.FFFF
Mode:Port-based
Period of loopback-detection:3s
Restore time:infinite
Port              PortState      State    Status     loop-act
vlanlist
-----------------------------------------------------------------
gigaethernet1/1/1   Down           Ena      yes      shutdown
```

2.8 Interface protection

2.8.1 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.

2.8.2 Preparing for configurations

Scenario

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

Prerequisite

N/A

2.8.3 Default configurations of interface protection

Default configurations of interface protection are as below.

Function	Default value
Interface protection status of each interface	Disable

2.8.4 Configuring interface protection

Caution

Interface protection is unrelated with the VLAN to which the interface belongs.

Configure interface protection for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**switchport protect**	Enable interface protection.

2.8.5 Checking configurations

Use the following commands to check configuration results.

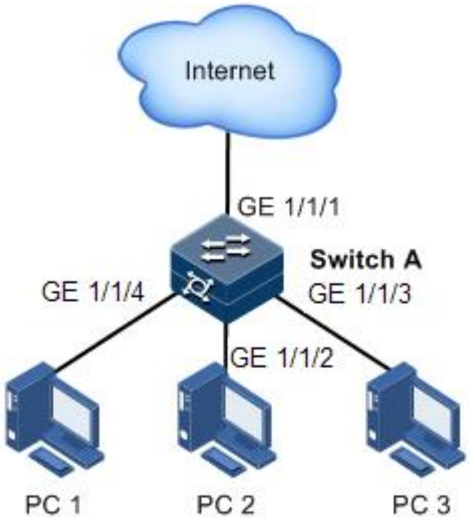
No.	Command	Description
1	Raisecom#**show switchport protect**	Show configurations of interface protection.

2.8.6 Example for configuring interface protection

Networking requirements

As shown in Figure 2-21, to prevent PC 1 and PC 2 from interconnecting with each other and to enable them to interconnect with PC 3 respectively, enable interface protection on GE 1/1/1 and GE 1/1/2 on Switch A.

Figure 2-21 Interface protection networking



Configuration steps

Step 1 Enable interface protection on the GE 1/1/1.

```
Raisecom#config
Raisecom(config)#interface gigaethernet1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport protect
Raisecom(config-gigaethernet1/1/1)#exit
```

Step 2 Enable interface protection on the GE 1/1/2.

```
Raisecom(config)#interface gigaethernet1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport protect
```

Checking results

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

```
Raisecom#show switchport protect
Port             Protected State
--------------------------
gigaethernet1/1/1   enable
gigaethernet1/1/2   enable
gigaethernet1/1/3   disable
gigaethernet1/1/4   disable
gigaethernet1/1/5   disable
gigaethernet1/1/6   disable
```

……

Check whether PC 1 and PC 2 can ping PC 3 successfully.

- PC 1 can ping PC 3 successfully.
- PC 2 can ping PC 3 successfully.

Check whether PC 1 can ping PC 2 successfully.

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

2.9 Port mirroring

2.9.1 Introduction

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

Figure 2-22 Principles of port mirroring

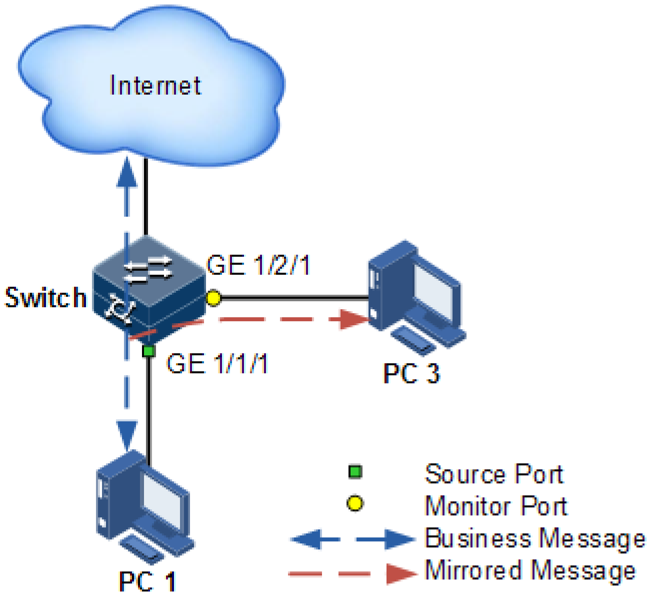


Figure 2-22 shows principles of port mirroring. PC 1 is connected to the external network by the GE 1/1/1; PC 3 is the monitor PC, connecting the external network by GE 1/2/1.

When monitoring packets from the PC 1, you needs to assign GE 1/1/1 to connect to PC 1 as the mirror source port, enable port mirroring on the ingress port and assign GE 1/2/1 as monitor port to mirror packets to destination port.

When service packets from PC 1 enter the ISCOM2600G series switch, the ISCOM2600G series switch will forward and copy them to monitor port (GE 1/2/1). The monitor device connected to mirror the monitor port can receive and analyze these mirrored packets.

The ISCOM2600G series switch supports mirroring data stream 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.

2.9.2 Preparing for configurations

Scenario

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

Port mirroring copies the port flow monitored 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

2.9.3 Default configurations of port mirroring

Default configurations of port mirroring are as below.

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

2.9.4 Configuring port mirroring on local port

Configure local port mirroring for the ISCOM2600G series switch as below.

Step	Configure	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`mirror-group`** *`group-id`*	Create a port mirroring group.
3	`Raisecom(config)#`**`interface`** *`interface-type interface-number`*	Enter physical interface configuration mode.
4	`Raisecom(config-gigaethernet1/1/1)#`**`mirror-group`** *`group-id`* **`monitor-port`**	Configure the monitor port for mirroring.
5	`Raisecom(config-gigaethernet1/1/1)#`**`mirror-group`** *`group-id`* **`source-port`** `{` **`ingress`** `|` **`egress`** `}`	Configure the mirroring port of port mirroring, and designate the mirroring rule for port mirroring. Port mirroring supports mirroring packets in both the ingress and egress directions of the port.

Step	Configure	Description

6	`Raisecom(config-gigaethernet1/1/1)#exit`
	`Raisecom(config)#mirror-group group-id source-cpu [ ingress | egress ]`
		Configure port mirroring to mirror packets to or from the CPU.

2.9.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show mirror-group [ group-id ]`	Show configurations of port mirroring.

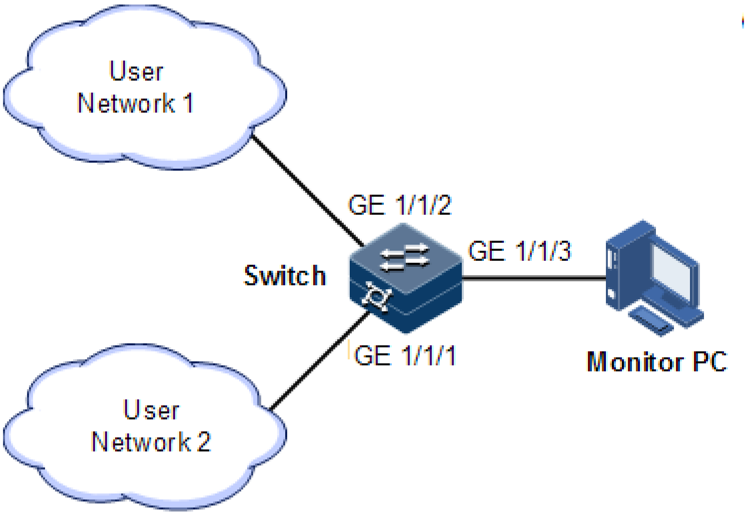
2.9.6 Example for configuring port mirroring

Networking requirements

As shown in Figure 2-23, the network administrator wishes to monitor user network 1 through the monitor device, then to catch the fault or abnormal data flow for analyzing and discovering faults and then solve them in time.

The ISCOM2600G series switch is disabled with storm control and automatic packets sending. User network 1 accesses the ISCOM2600G series switch through GE 1/1/1, user network 2 accesses the ISCOM2600G series switch through GE 1/1/2, and the data monitor device is connected to GE 1/1/3.

Figure 2-23 Port mirroring networking



Configuration steps

Enable port mirroring on the Switch.

```
Raisecom#config
Raisecom(config)#mirror-group 1
Raisecom(config)interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#mirror-group 1 monitor-port
Raisecom(config-gigaethernet1/1/3)#exit
Raisecom(config)interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#mirror-group 1 source-port ingress
```

Checking results

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

```
Raisecom#show mirror-group
Mirror Group 1 :
Monitor Port :
   gigaethernet1/1/3
Source Port :
   gigaethernet1/1/1       : ingress
   gigaethernet1/1/2       : ingress
Remote Vlan: --
```

2.10 L2CP

2.10.1 Introduction

Metro Ethernet Forum (MEF) introduces service concepts, such as EPL, EVPL, EP-LAN, and EVP-LAN. Different service types have different processing modes for Layer 2 Control Protocol (L2CP) packets.

MEF6.1 defines processing modes for L2CP as below.

- Discard: discard the packet, by applying the configured L2CP profile on the ingress interface of the ISCOM2600G series switch, to complete configuring processing mode.
- Peer: send packets to the CPU in the same way as the discard action.
- Tunnel: send packets to the MAN. It is more complex than discard and peer mode, requiring cooperating profile at network side interface and carrier side interface tunnel terminal to allow packets to pass through the carrier network.

2.10.2 Preparing for configurations

Scenario

On the access device of MAN, you can configure profile on user network interface according to services from the carrier to configure L2CP of the user network.

Prerequisite

N/A

2.10.3 Defaul configurations of L2CP

Default configurations of L2CP are as below.

Function	Default value
Global L2CP status	Disable
Applying the profile on the interface	Disable
Specified multicast destination MAC address	0x0100.0ccd.cdd0
Description of the L2CP profile	N/A

2.10.4 Configuring global L2CP

Configure global L2CP for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`l2cp-process tunnel destination-address`** *`mac-address`*	(Optional) configure the destination MAC address for transparently transmitted packets.

2.10.5 Configuring L2CP profile

Configure the L2CP profile for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`l2cp-process profile`** *`profile-number`*	Create and enter the L2CP profile.
3	`Raisecom(config-l2cp-profile)#`**`name`** *`string`*	(Optional) add profile description.

Step	Command	Description
4	Raisecom(config-l2cp-profile)#**l2cp-process protocol { oam | stp | dot1x | lacp | lldp | cdp | vtp | pvst |all } action { tunnel | drop | peer }**	(Optional) configure the mode for processing L2CP packets.
5	Raisecom(config-l2cp-profile)#**tunnel vlan** *vlan-id*	(Optional) configure the specified VLAN for transparent transmission.
6	Raisecom(config-l2cp-profile)#**tunnel** *interface-type interface-number*	(Optional) configure the specified egress interface for transparent transmission.
7	Raisecom(config-l2cp-profile)#**tunnel tunnel-type mac**	(Optional) configure the type of the tunnel for transparent transmission.

2.10.6 Configuring L2CP profile on interface

Configure the L2CP profile on the interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** interface-type interface-number	Enter physical interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#**l2cp profile** *profile-number*	Apply the L2CP profile on the interface.

Note

Applying a profile to an interface takes effect unless global L2CP is enabled. You can configure it but it will not take effect if global L2CP is disabled. The configuration takes effect once global L2CP is enabled.

2.10.7 Checking configurations

Use the following commands check configuration results.

No.	Command	Description
1	Raisecom#**show l2cp-process** profile [*profile-number*]	Show information about the created L2CP profile.
2	Raisecom#**show l2cp-process** [*interface-type interface-number*]	Show configurations of L2CP on the interface.

No.	Command	Description
3	`Raisecom#show l2cp-process [ tunnel statistics ] [ interface-type interface-number]`	Show statistics of L2CP packets on the interface.

2.10.8 Maintenance

Maintain the ISCOM2600G series switch as below.

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

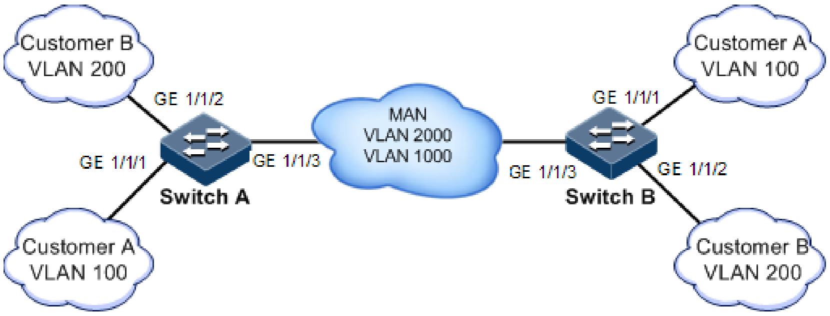
2.10.9 Example for configuring L2CP

Networking requirements

As shown in Figure 2-24, configure L2CP on Switch A and Switch B as below.

- Specify the multicast destination MAC address of them to 0100.1234.1234.
- Configure the STP packets of Customer A to traverse the MAN, and discard other packets.
- Configure the STP and VTP packets of Customer B to traverse the MAN, send elmi packets to the CPU, and discard other packets.

Figure 2-24 L2CP networking



Configuration steps

Configure Switch A and Switch B.

Configurations of Switch A and Switch B are identical. Take Switch A for example.

Step 1 Configure the switch name.

```
Raisecom#name SwitchA
```

Step 2 Configure the specified multicast destination MAC address.

```
Raisecom(config)#l2cp-process tunnel destination-address 0100.1234.1234
```

Step 3 Configure L2CP profile 1, and apply the profile to GE 1/1/1 for Customer A.

```
Raisecom(config)#l2cp-process profile 1
Raisecom(config-l2cp-profile)#name CustomerA
Raisecom(config-l2cp-profile)#l2cp-process protocol all action drop
Raisecom(config-l2cp-profile)#l2cp-process protocol stp action tunnel
Raisecom(config-l2cp-profile)#exit
Raisecom(config)#interface gigaethernet1/1/1
Raisecom(config-gigaethernet1/1/1)#l2cp-process profile 1
Raisecom(config-gigaethernet1/1/1)#exit
```

Step 4 Configure L2CP profile 2, and apply the profile to GE 1/1/2 for Customer B.

```
Raisecom(config)#l2cp-process profile 2
Raisecom(config-l2cp-proflie)#name CustomerB
Raisecom(config-l2cp-proflie)#l2cp-process protocol all action drop
Raisecom(config-l2cp-proflie)#l2cp-process protocol stp action tunnel
Raisecom(config-l2cp-proflie)#l2cp-process protocol vtp action tunnel
Raisecom(config-l2cp-proflie)#l2cp-process protocol elmi action peer
Raisecom(config-l2cp-proflie)#exit
Raisecom(config)#interface gigaethernet1/1/2
Raisecom(config-gigaethernet1/1/2)#l2cp-process profile 2
Raisecom(config-gigaethernet1/1/2)#exit
```

Checking results

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

```
Raisecom#show l2cp-process profile
Destination MAC Address for Encapsulated Packets: 0100.1234.1234
ProfileId: 1
Name: customerA
BpduType   Mac-address     l2cp-process  Mac-vlan  EgressPort  tunneltype
-------------------------------------------------------------------------
-------------
stp       0180.C200.0000   tunnel       --                 none
dot1x      0180.C200.0003   drop        --                 none
lacp      0180.C200.0002   drop        --                 none
```

```
oam       0180.C200.0002   drop        --                 none
cdp       0100.0CCC.CCCC   drop        --                 none
vtp       0100.0CCC.CCCC   drop        --                 none
pvst      0100.0CCC.CCCD   drop        --                 none
lldp      0180.C200.000E   drop        --                 none
elmi      0180.C200.0007   drop        --                 none
udld      0100.0CCC.CCCC   drop        --                 none
pagp      0100.0CCC.CCCC   drop        --                 none
ProfileId: 2
Name: customerB
BpduType   Mac-address     l2cp-process  Mac-vlan  EgressPort  tunneltype
------------------------------------------------------------------------
-------------
stp       0180.C200.0000   tunnel       --                 none
dot1x      0180.C200.0003   drop        --                 none
lacp      0180.C200.0002   drop        --                 none
oam       0180.C200.0002   drop        --                 none
cdp       0100.0CCC.CCCC   drop        --                 none
vtp       0100.0CCC.CCCC   tunnel       --                 none
pvst      0100.0CCC.CCCD   drop        --                 none
lldp      0180.C200.000E   drop        --                 none
elmi      0180.C200.0007   peer        --                 none
udld      0100.0CCC.CCCC   drop        --                 none
pagp      0100.0CCC.CCCC   drop        --                 none
…
```

Use the **show l2cp** command to show interface configurations.

```
Raisecom#show l2cp
L2CP running information
Port     ProfileID   BpduType   mac-address     l2cp-process
------------------------------------------------------------------------
-----
GE1/1/1   1          stp       0180.C200.0000   tunnel
                   dot1x      0180.C200.0003   drop
                   lacp      0180.C200.0002   drop
                   oam       0180.C200.0002   drop
                   cdp       0100.0CCC.CCCC   drop
                   vtp       0100.0CCC.CCCC   drop
                   pvst      0100.0CCC.CCCD   drop
                   lldp      0180.C200.000E   drop
                   elmi      0180.C200.0007   drop
                   udld      0100.0CCC.CCCC   drop
                   pagp      0100.0CCC.CCCC   drop
GE1/1/2   2          stp       0180.C200.0000   tunnel
                   dot1x      0180.C200.0003   drop
                   lacp      0180.C200.0002   drop
                   oam       0180.C200.0002   drop
                   cdp       0100.0CCC.CCCC   drop
                   vtp       0100.0CCC.CCCC   tunnel
                   pvst      0100.0CCC.CCCD   drop
                   lldp      0180.C200.000E   drop
                   elmi      0180.C200.0007   peer
```

```
                    udld      0100.0CCC.CCCC   drop
                    pagp      0100.0CCC.CCCC   drop
GE1/1/3   --          --        --             --
GE1/1/4   --          --        --             --
GE1/1/5   --          --        --             --
…
```

3 Ring network protection

This chapter describes principles and configuration procedures of ring network protection, including the following section:

- G.8032

3.1 G.8032

3.1.1 Introduction

G.8032 Ethernet Ring Protection Switching (ERPS) is an APS protocol based on the ITU-T G.8032 recommendation. It is a link-layer protocol specially used in Ethernet rings. Generally, ERPS can avoid broadcast storm caused by data loopback in Ethernet rings. When a link/device on the Ethernet ring fails, traffic can be quickly switched to the backup link to ensure restoring services quickly.

G.8032 uses the control VLAN on the ring network to transmit ring network control information. Meanwhile, combining with the topology feature of the ring network, it discovers network fault quickly and enable the backup link to restore service fast.

3.1.2 Preparing for configurations

Scenario

With development of Ethernet to Telecom-grade network, voice and video multicast services bring higher requirements on Ethernet redundant protection and fault-recovery time. The fault-recovery time of current STP system is in second level that cannot meet requirements.

By defining different roles for nodes on a ring, G.8032 can block a loopback to avoid broadcast storm in normal condition. Therefore, the traffic can be quickly switched to the protection line when working lines or nodes on the ring fail. This helps eliminate the loop, perform protection switching, and automatically recover from faults. In addition, the switching time is shorter than 50ms.

The ISCOM2600G series switch supports the single ring, intersecting ring, and tangent ring.

G.8032 provides a mode for detecting faults based on physical interface status. The ISCOM2600G series switch learns link fault quickly and switches services immediately, so this mode is suitable for detecting the fault between neighboring devices.

Prerequisite

- Connect the interface.
- Configure its physical parameters to make it Up.
- Create VLANs.
- Add interfaces to VLANs.

3.1.3 Default configurations of G.8032

Default configurations of G.8032 are as below.

Function	Default value
Protocol VLAN	1
Protection ring mode	Revertive
Ring WTR timer	5min
Ring protocol version	2
Guard timer	500ms
Ring HOLDOFF timer	0ms
G.8032 fault reported to NMS	Enable
Tributary ring virtual channel mode in intersecting node	With
Ring Propagate switch in crossing node	Disable

3.1.4 Creating G.8032 ring

Configure G.8032 for the ISCOM2600G series switch as below.

Caution

- Only one device on the protection ring can be configured to the Ring Protection Link (RPL) Owner and one device is configured to RPL Neighbour. Other devices are configured to ring forwarding nodes.
- The tangent ring consists of 2 independent single rings. Configurations on the tangent ring are identical to the ones on the common single ring. The intersecting ring consists of a main ring and a tributary ring. Configurations on the main ring are identical to the ones on the common single ring. For detailed configurations of the tributary ring, see section 3.1.5 (Optional) creating G.8032 tributary ring.

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

Step	Command	Description
2	Raisecom(config)#**ethernet ring-protection** *ring-id* **east** { *interface-type interface-number* | **port-channel** *port-channel-number* } **west** { *interface-type interface-number* | **port-channel** *port-channel-number* } [**node-type rpl-owner rpl** { **east** | **west** }] [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create a protection ring and configure the node as the RPL Owner. **Note** The east and west interfaces cannot be the same one.
	Raisecom(config)#**ethernet ring-protection** *ring-id* **east** { *interface-type interface-number* | **port-channel** *port-channel-number* } **west** { *interface-type interface-number* | **port-channel** *port-channel-number* } **node-type rpl-neighbour rpl** { **east**| **west** } [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create a protection ring, and configure the node as the RPL Neighbour.
	Raisecom(config)#**ethernet ring-protection** *ring-id* **east** { *interface-type interface-number* | **port-channel** *port-channel-number* } **west** { *interface-type interface-number* | **port-channel** *port-channel-number* } [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create a protection line, and configure the node as the protection forwarding node.
3	Raisecom(config)#**ethernet ring-protection** *ring-id* **name** *string*	(Optional) configure a name for the protection ring. Up to 32 bytes are available.
4	Raisecom(config)#**ethernet ring-protection** *ring-id* **version** { **1** | **2** }	(Optional) configure the protocol version. The protocol version of all nodes on a protection ring should be identical. In protocol version 1 protection rings are distinguished based on the protocol VLAN. Therefore, you need to configure different protocol VLANs for protection rings. We recommend configuring different protocol VLANs for protection rings even if protocol version 2 is used.

Step	Command	Description
5	`Raisecom(config)#`**`ethernet ring-protection`** *`ring-id`* **`guard-time`** *`guard-time`*	(Optional) after the ring Guard timer is configured, the failed node does not process APS packets during a period. In a bigger ring network, if the failed node recovers from a fault immediately, it may receive the fault notification sent by the neighbour node on the protection ring. Therefore, the node is in Down status again. You can configure the ring Guard timer to solve this problem.
6	`Raisecom(config)#`**`ethernet ring-protection`** *`ring-id`* **`wtr-time`** *`wtr-time`*	(Optional) configure the ring WTR timer. In revertive mode, when the working line recovers from a fault, traffic is not switched to the working line unless the WTR timer times out.
7	`Raisecom(config)#`**`ethernet ring-protection`** *`ring-id`* **`holdeoff-time`** *`holdoff-time`*	(Optional) configure the ring HOLDOFF timer. After the HOLDOFF timer is configured, when the working line fails, the system will delay processing the fault. It means that traffic is delayed to be switched to the protection line. This helps prevent frequent switching caused by working line vibration. Note If the ring HOLDOFF timer value is too great, it may influence 50ms switching performance. Therefore, we recommend configuring the ring HOLDOFF timer value to 0.

3.1.5 (Optional) creating G.8032 tributary ring

Caution

- Only the intersecting ring consists of a main ring and a tributary ring.
- Configurations of the main ring are identical to those of the single/tangent ring. For details, see section 3.1.4 Creating G.8032 ring.
- For the intersecting ring, configure its main ring and then the tributary ring; otherwise, the tributary ring will fail to find the interface of the main ring, thus failing to establish the virtual channel of the tributary ring.
- The ID of the tributary ring must be greater than that of the main ring.
- Configurations of non-intersecting nodes of the intersecting ring are identical to those of the single/tangent ring. For details, see section 3.1.4 Creating G.8032 ring.

Configure G.8032 intersecting rings for ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } { *interface-type interface-number* | **port-channel** *port-channel-number* } **node-type rpl-owner** [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create the tributary ring on the intersecting node and configure the intersecting node as the RPL Owner. The protection ring is in non-revertive mode if you configure the non-revertive parameter. ● In revertive mode, when the working line recovers from a fault, traffic is switched from the protection line to the working line. ● In non-revertive mode, when the working line recovers from a fault, traffic is not switched from the protection line to the working line. By default, the protection ring is in revertive mode. Note The links between 2 intersecting nodes belong to the main ring. Therefore, when you configure the tributary ring on the intersecting node, you can only configure the west or east interface.
	Raisecom(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } { *interface-type interface-number* | **port-channel** *port-channel-number* } **node-type rpl-neighbour** [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create the tributary ring on the intersecting node and configure the intersecting node as the RPL Neighbour.
	Raisecom(config)#**ethernet ring-protection** *ring-id* { **east** | **west** } { *interface-type interface-number* | **port-channel** *port-channel-number* } [**not-revertive**] [**protocol-vlan** *vlan-id*] [**block-vlanlist** *vlan-list*]	Create the tributary ring on the intersecting node and configure the intersecting node as the protection forwarding node.

Step	Command	Description
3	Raisecom(config)#**ethernet ring-protection** *ring-id* **raps-vc** { **with** | **without** }	(Optional) configure the tributary ring virtual channel mode on the intersecting node. Because the intersecting node belongs to the main ring, transmission modes of protocol packets in the tributary ring are different from the ones of the main ring. In the tributary ring, transmission modes are divided into with and without modes. • with: the main ring provides channels for APS packets of the tributary ring; the tributary ring intersecting node transmits APS packets of the tributary ring to the main ring to use the main ring to complete communications among intersecting nodes of the tributary ring. • without: APS packets of the tributary ring on intersecting nodes need to be ended and cannot be transmitted to the main ring. This mode requires the tributary ring not to block the protocol VLAN of the tributary ring (to ensure tributary ring packets to traverse Owner). By default, the virtual channel of the tributary ring adopts the with mode. Transmission modes on 2 intersecting nodes must be identical.
4	Raisecom(config)#**ethernet ring-protection** *ring-id* **propagate enable**	Enable the ring Propagate switch on the intersecting node. Because data of the tributary ring needs to be transmitted through the main ring, there is a MAC address table of the tributary ring on the main ring. When the tributary ring fails, it needs to use the Propagate switch to inform the main ring of refreshing the MAC address table to avoid traffic loss.

3.1.6 (Optional) configuring G.8032 switching control

Configure G.8032 switching control for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ethernet ring-protection** *ring-id* **force-switch** { **east** | **west** }	Switch the traffic on the protection ring to the west/east interface forcedly. FS can be configured on multiple interfaces of multiple ring nodes.

Step	Command	Description
3	`Raisecom(config)#ethernet ring-protection ring-id manual-switch { east | west }`	Switch the traffic on the protection ring to the west/east interface manually. Its priority is lower than the one of FS and APS. MS can be configured on one interface of a ring node.
4	`Raisecom(config)#clear ethernet ring-protection ring-id { command | statistics }`	Clear switching control commands, including force-switch, manual-switch, WTR timer, and WTB timer.

Note

By default, traffic is automatically switched to the protection line when the working line fails. Therefore, you need to configure G.8032 control in some special cases.

3.1.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show ethernet ring-protection`	Show configurations of the G.8032 ring.
2	`Raisecom#show ethernet ring-protection status`	Show G.8032 ring status.
3	`Raisecom#show ethernet ring-protection statistics`	Show G.8032 ring statistics.

3.1.8 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description
`Raisecom(config)#clear ethernet ring-protection ring-id statistics`	Clear statistics of the protection ring.

4 IP services

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

- IP basis
- Loopback interface
- ARP
- NDP
- Static route

4.1 IP basis

4.1.1 Introduction

The IP interface is the virtual interface based on VLAN. Configuring Layer 3 interface is generally used for network management or routing link connection of multiple devices.

4.1.2 Preparing for configurations

Scenario

Configure the IP address of each VLAN interface and loopback interface.

Prerequisite

- Create VLANs.
- Activate them.

4.1.3 Default configurations of Layer 3 interface

Default configurations of the Layer 3 interface are as below.

Function	Default value
Management VLAN TPID	0x8100

Function	Default value
Management VLAN inner VLAN	1
Management VLAN CoS	0
IP address of IP interface 0	192.168.0.1

4.1.4 Configuring IPv4 adress of VLAN interface

Configure the IPv4 address of the VLAN interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface vlan`** *`vlan-id`*	Enter VLAN interface configuration mode.
3	`Raisecom(config-vlan)#`**`ip address`** *`ip-address`* `[` *`ip-mask`* `] [` **`sub`** `]`	Configure the IP address of the VLAN interface. Use the **no ip address** *ip-address* command to delete configuration of the IP address.

4.1.5 Configuring IPv6 address of VLAN interface

Configure the IPv6 address of the VLAN interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface vlan`** *`vlan-id`*	Enter Layer 3 interface configuration mode.
3	`Raisecom(config-ip)#` **`ipv6 address`** *`ipv6-address/prefix-length`* `[` **`sub`** `]`	Configure the IPv6 address of the VLAN interface.

4.1.6 Checking configurations

Use the following commands to check configuration results.

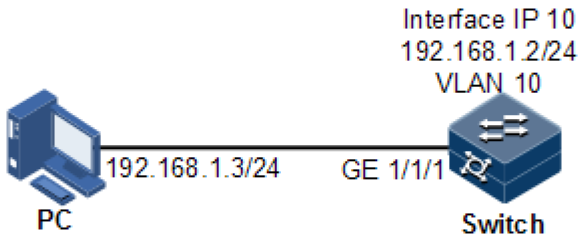
No.	Command	Description
1	`Raisecom#`**`show ip interface brief`**	Show configurations of the IP address of the IP interface.
2	`Raisecom#`**`show ipv6 interface brief`**	Show configurations of the IPv6 address of the IP interface.

4.1.7 Example for configuring VLAN interface to interconnect with host

Networking requirements

As shown in Figure 4-1, configure the VLAN interface to the switch so that the host and the ISCOM2600G series switch can ping each other.

Figure 4-1 VLAN interface networking



Configuration steps

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

```
Raisecom#config
Raisecom(config)#create vlan 10 active
```

Step 2 Configure Layer 3 interface on the ISCOM2600G series switch, configure its IP address, and associate the interface with the VLAN.

```
Raisecom(config)#interface VLAN 10
Raisecom(config-VLAN10)#ip address 192.168.1.2 255.255.255.0
```

Checking results

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

```
Raisecom#show vlan 10
VLAN Name                             State   Status  Priority Member-Ports
-------------------------------------------------------------------------
---------------------------------------
10   VLAN0010                         active  static  --
```

Use the **show ip interface brief** to show configurations of the Layer 3 interface.

```
Raisecom#show ip interface brief
VRF                 IF                         Address       NetMask
Catagory
-------------------------------------------------------------------------
------------------------------
Default-IP-Routing-Table  fastethernet1/0/1          192.168.0.1
255.255.255.0   primary
Default-IP-Routing-Table  vlan10                   192.168.1.2
255.255.255.0   primary
```

Use the **ping** command to check whether the ISCOM2600G series switch 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.
```

4.2 Loopback interface

4.2.1 Introduction

The loopback interface is a virtual interface and can be classified into two types:

- Loopback interface automatically created by the system: the IP address is fixed to 127.0.0.1. This type of interfaces receives packets sent to the device. It does not broadcast packets through routing protocols.
- Loopback interface created by users: without affecting physical interface configurations, configure a local interface with a specified IP address, and make the interface Up permanently so that packets can be broadcasted through routing protocols.

Loopback interface status is free from physical interface status (Up/Down). As long as the ISCOM2600G series switch is working normally, the loopback interface will not become Down. Thus, it is used to identify the physical device as a management address.

4.2.2 Preparing for configurations

Scenario

Use the IP address of the loopback interface to log in through Telnet so that the Telnet operation does not become Down due to change of physical status. The loopback interface ID is also used as the router ID of dynamic routing protocols, such as OSPF, to uniquely identify a device.

Prerequisite

N/A

4.2.3 Default configurations of loopback interface

N/A

4.2.4 Configuring IP address of loopback interface

Configure the IP address of the loopback interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface loopback`** *`lb-number`*	Enter loopback interface configuration mode.
3	`Raisecom(config-loopback)#`**`ip address`** *`ip-address`* `[` *`ip-mask`* `]`	Configure the IP address of the loopback interface.
4	`Raisecom(config-loopback)#`**`ipv6 address`** *`ipv6-address/prefix-length`* `[` **`sub`** `]`	Configure the IPv6 address of the loopback interface.

4.2.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show interface loopback`**	Show configurations of the loopback interface.

4.3 ARP

4.3.1 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 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 packet to the destination host correctly. Then Address Resolution Protocol (ARP) is applied to resolve IP address to MAC address and configure mapping relationship between IP address and MAC address.

ARP address mapping 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.
  - Static ARP addresses are not aged.
- 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 ISCOM2600G series switch supports the following two modes of dynamically learning ARP address entries:

- Learn-all: in this mode, the ISCOM2600G series switch 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 ISCOM2600G series switch learns ARP response packets with corresponding ARP request only sent by itself. 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.

4.3.2 Preparing for configurations

Scenario

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

Generally, ARP address mapping table is dynamically maintained by the ISCOM2600G series switch. The ISCOM2600G series switch searches for the mapping between IP address and MAC address automatically according to ARP. You just need to configure the ISCOM2600G series switch manually for preventing ARP dynamic learning from cheating and adding static ARP address entries.

Prerequisite

N/A

4.3.3 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-all

4.3.4 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 ISCOM2600G series switch as below.

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

4.3.5 Configuring dynamic ARP entries

Configure dynamic ARP entries for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**arp mode** { **learn-all** | **learn-reply-only** }	Configure the aging time of dynamic ARP entries.
3	Raisecom(config)#**arp aging-time** *time*	Enter Layer 3 interface configuration mode.
4	Raisecom(config)#**arp max-learning-num** *number*	(Optional) configure the maximum number of dynamic ARP entries allowed to learn on the Layer 3 interface.

4.3.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show arp** [*ip-address* | **interface** *interface-type* *interface-number* | **static**]	Show information about entries in the ARP address table.

4.3.7 Maintenance

Maintain the ISCOM2600G series switch as below.

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

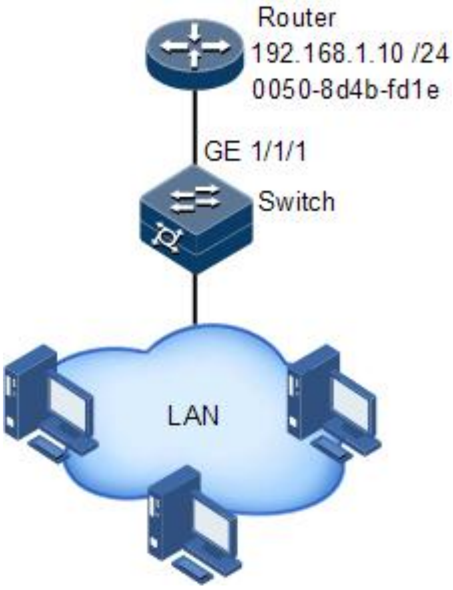
4.3.8 Example for configuring ARP

Networking requirements

As shown in Figure 4-2, the ISCOM2600G series switch is connected to the host, and is also connected to the upstream Router through GE 1/1/1. For the Router, the IP address and submask are 192.168.1.10/24, and the MAC address is 0050-8d4b-fd1e.

To improve communication security between the Switch and Router, you need to configure related static ARP entry on the ISCOM2600G series switch.

Figure 4-2 Configuring ARP networking



Configuration steps

Add a static ARP entry.

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

Checking results

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

```
Raisecom#show arp
ARP aging-time: 1200 seconds(default: 1200s)
ARP mode: Learn all
ARP table:
Total: 1    Static: 1    Dynamic: 0
IP Address       Mac Address      Interface                        Type
Age(s)    status
-------------------------------------------------------------------------
---------------------------
192.168.1.10     0050.8D4B.FD1E    vlan10                         static    --
PERMANENT
```

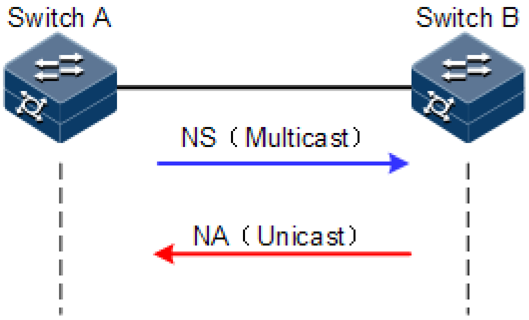
4.4 NDP

4.4.1 Introduction

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

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

Figure 4-3 Principles of NDP address resolution



As shown in Figure 4-3, take Switch A for example. Switch A obtains the data link layer address of Switch B as below:

Step 1 Switch A sends a NS message in multicast mode. The source address of the NS message is the IPv6 address of Layer 3 interface on Switch A, and the destination address of the NS message is the multicast address of the requested node of the Switch B. The NS message even contains the data link layer address of Switch A.

Step 2 After receiving the NS message, Switch B judges whether the destination address of the NS message is the multicast address of the request node corresponding to the IPv6 address of Switch B. If yes, Switch B can obtain the data link layer address of Switch A, and sends a NA message which contains its data link layer address in unicast mode.

Step 3 After receiving the NA message from Switch B, Switch A obtains the data link layer address of Switch B.

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

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

4.4.2 Preparing for configurations

Scenario

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

Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.
- Configure the IPv6 address of the Layer 3 interface.

4.4.3 Default configurations of NDP

Default configurations of NDP are as below.

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

4.4.4 Configuring static neighbor entries

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

Configure static neighbor entries for the ISCOM2600G series switch as below.

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

Step	Command	Description
2	Raisecom(config)#**ipv6 neighbor** *ipv6-address mac-address*	configure static neighbor entries

4.4.5 Configuring times of sending NS messages for detecting duplicated addresses

Configure times of sending NS messages for detecting duplicated addresses for the ISCOM2600G series switch as below.

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

Note

When the ISCOM2600G series switch obtains an IPv6 address, it uses the duplicated address detection function to determine whether the IPv6 address is already used by another device. After sending NS messages for a specified times and receiving no response, it determines that the IPv6 address is not duplicated and thus can be used.

4.4.6 Configuring maximum number of NDPs allowed to be learnt on Layer 3 interface

Configure the maximum number of NDPs allowed to be learnt on the Layer 3 interface for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface vlan** *vlan-id*	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)#**ipv6 neighbors max-learning-num** *number*	Configure the maximum number of NDPs allowed to be learnt on the Layer 3 interface.

4.4.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show ipv6 neighbors`**	Show all NDP neighbor information.
2	`Raisecom#`**`show ipv6 neighbors`** *`ipv6-address`*	Show neighbor information about a specified IPv6 address.
3	`Raisecom#`**`show ipv6 neighbors vlan`** *`vlan-id`*	Show neighbor information about a specified layer 3 interface.
4	`Raisecom#`**`show ipv6 neighbors static`**	Show information about IPv6 static neighbor.
5	`Raisecom#`**`show ipv6 interface prefix`** `[` **`ip`** *`if-number`* `]`	Show prefix information about the IPv6 address.
6	`Raisecom#`**`show ipv6 interface nd`** `[` **`ip`** *`if-number`* `]`	Show ND information configured on the interface.

4.4.8 Maintenance

Maintain the ISCOM2600G series switch as below.

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

4.5 Static route

4.5.1 Introduction

A route is required for communication among different devices in one VLAN, or different VLANs. The route is to transmit packets through network to destination, which adopts routing table for forwarding packets.

The ISCOM2600G series switch supports default route and static route only but dynamic route.

Default route

The default route is a special route that can be used only when there is no matched item in the routing table. The default route appears as a route to network 0.0.0.0 (with mask 0.0.0.0) in the routing table. You can show configurations of the default route by using the **show ip route** command. If the ISCOM2600G series switch has not been configured with default route and the destination IP of the packet is not in the routing table, the ISCOM2600G series switch will discard the packet and return an ICMP packet to the Tx end to inform that the destination address or network is unavailable.

Static route

The static route is the route configured manually, thus bringing low requirements on the system. It is available to simple, small, and stable network. The disadvantage is that it cannot adapt to network topology changes automatically and needs manual intervention.

4.5.2 Preparing for configurations

Scenario

Configure the static route for simple network topology manually to establish an intercommunication network.

Prerequisite

Configure the IP address of the VLAN interface correctly.

4.5.3 Configuring static route

Configure static route for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip route** *ip-address* { *masklength* | *ip-mask* } *next-hop-ip-address*	Configure the static route.
3	Raisecom(config)#**ip route static distance** *value*	(Optional) configure the default IPv4 management distance.

4.5.4 Checking configurations

Use the following commands to check configuration results.

No.	Item	Description
1	Raisecom#**show ip route** [**detail**]	Show information about IPv4 routes.

5 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 power supply

Note

This chapter is supported by PoE switches only.

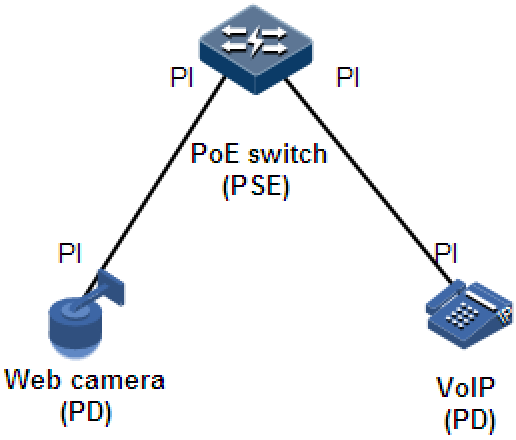
5.1 Introduction

5.1.1 Principles of PoE

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 Power Interface (PI).

Figure 5-1 shows principles of PoE.

Figure 5-1 Principles of PoE



5.1.2 PoE modules

The PoE system consists of the following modules:

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

5.1.3 PoE advantages

PoE has the following advantages:

- Reliability: a centralized PSE supplies power with convenient backup, uniform management of power modules, and high security.
- Convenient connection: the network terminal does not need an external power supply; instead, it needs only one 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.

5.1.4 PoE concepts

- Maximum output power of PoE

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

- Priority of PoE

There are three levels of priorities for power supply: critical, high, and low. The PSE supplies power to the PD connected to the PI with critical priority preferentially, the PD connected to the PI with the high priority, and finally the PD connected to the PI with the low priority.

- 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 current PSE power utilization rate exceeds the threshold, or the status of PoE changes, the ISCOM2600G series switch sends Trap to the NMS.

- PSE power utilization rate threshold

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

5.2 Configuring PoE

5.2.1 Preparing for configurations

Scenario

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

Prerequisite

N/A

5.2.2 Default configurations of PoE

Default configurations of PoE are as below.

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

5.2.3 Enabling interface PoE

Enable interface PoE for the ISCOM2600G series switch 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-gigaethernet1/1/1)#`**`poe enable`**	Enable interface PoE.

5.2.4 Configuring maximum output power of PoE

Configure the maximum output power of PoE for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**poe max-power** *max-power-value*	Configure the maximum output power of PoE.

5.2.5 Configuring priority of PoE

Configure priority of PoE for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**poe priority** { **critical** | **high** | **low** }	Configure priority of PoE.

5.2.6 Configuring PSE power utilization rate threshold

Configure the PSE power utilization rate threshold for the ISCOM2600G series switch 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 rate threshold.

5.2.7 Configuring identification of non-standard PDs

Caution

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 too high output power.

Configure identification of non-standard PDs for the ISCOM2600G series switch as below.

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

Step	Command	Description
2	`Raisecom(config)#poe legacy enable`	Enable the PSE to identify non-standard PDs.

5.2.8 Enabling forcible power supply on interface

Caution

When using the ISCOM2600G series switch to supply power for a remote PD, we recommend using a standard PD, pre-standard PD, or Cisco-primate standard PD. To use other non-standard PD in forcible power supply mode, confirm its power consumption, voltage, and current in advance to properly set the maximum output power on the PSE and to avoid damaging the PD due to too high output power.

Enable forcible power supply on interfaces for the ISCOM2600G series switch 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-gigaethernet1/1/1)#poe force-power`	Enable forcible PoE power supply on the interface.

5.2.9 Enabling overtemperature protection

Enable overtemperature protection for the ISCOM2600G series switch as below.

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

5.2.10 Enabling global Trap

Enable global Trap for the ISCOM2600G series switch as below.

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

5.2.11 Checking configurations

Use the following commands to check configuration results.

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

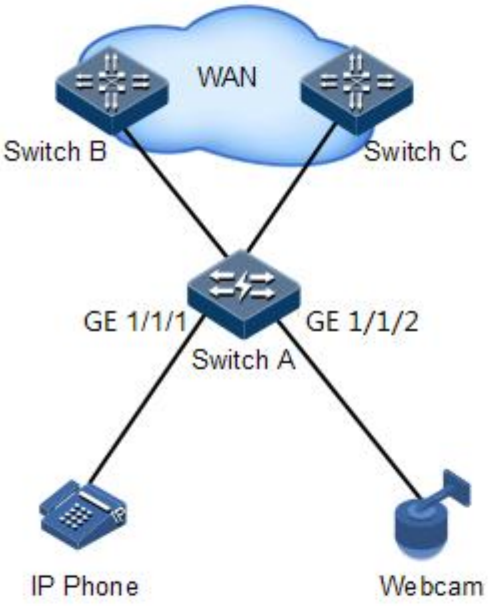
5.3 Example for configuring PoE power supply

Networking requirements

As shown in Figure 5-1, both Switch B and Switch C connect Switch A to the WAN, and PoE-supportive Switch A is used to supply power to an IP phone and a monitor camera. Switch A is required to supply power to the monitor camera preferentially when it runs at full load. Detailed requirements are as below:

- Configure the maximum output power of GE 1/1/1 and GE 1/1/2 to 30000 mW.
- Enable overtemperature protection on Switch A.
- Enable Trap for power supply on Switch A.
- Configure the priorities of GE 1/1/2 and GE 1/1/1 to high and low respectively.

Figure 5-1 PoE switch power supply networking



Configuration steps

Step 1 Enable PoE on GE 1/1/1 and GE 1/1/2.

```
Raisecom#config
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#poe enable
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#poe enable
Raisecom(config-gigaethernet1/1/2)#exit
```

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

```
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#poe max-power 30000
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#poe max-power 30000
Raisecom(config-gigaethernet1/1/2)#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 GE 1/1/2 and GE 1/1/1 to high and low respectively.

```
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#poe priority high
Raisecom(config-gigaethernet1/1/2)#exit
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#poe priority low
```

Checking results

Use the **show poe gigaethernet 1/1/1 detail** and **show poe gigaethernet 1/1/2 detail** commands to show PoE configurations on GE 1/1/2 and GE 1/1/1.

```
Raisecom#show poe gigaethernet 1/1/1 detail
Port: gigaethernet 1/1/1
-------------------------------------------------
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)

Raisecom#show poe gigaethernet 1/1/2 detail
Port: gigaethernet 1/1/1
-------------------------------------------------
POE administrator status: Enable
POE operation status: Enable
Power detection status:Searching
POE Power Pairs mode:Signal
PD power classification:Class0
POE power Priority: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)
```

6 DHCP

This chapter describes basic principles and configurations procedures of DHCP, and providing related configuration examples, including the following sections:

- DHCP Client
- DHCP Snooping
- DHCP Options
- DHCP Server
- DHCP Relay

6.1 DHCP Client

6.1.1 Introduction

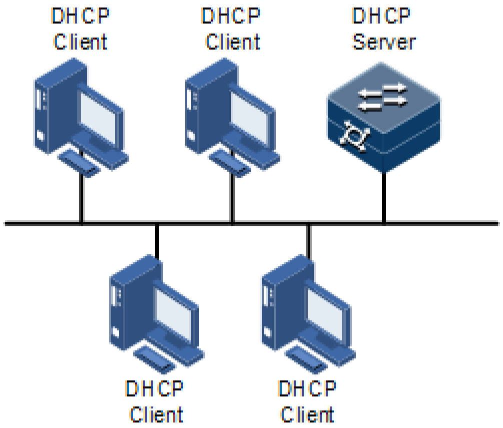
Dynamic Host Configuration Protocol (DHCP) refers to the protocol which assigns configurations, such as the IP address, to users on the TCP/IP network. Based on BOOTP (Bootstrap Protocol) protocol, it has additional features, such as automatically assigning available network addresses, reusing network addresses, and other extended configuration features.

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 changes of locations 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 configuration to the server (including IP address, subnet mask, and default gateway), and the server replies with IP address for the client and other related configurations to implement dynamic configurations of IP address.

Typical applications of DHCP usually include a set of DHCP server and multiple clients (for example PC or Notebook), as shown in Figure 6-1.

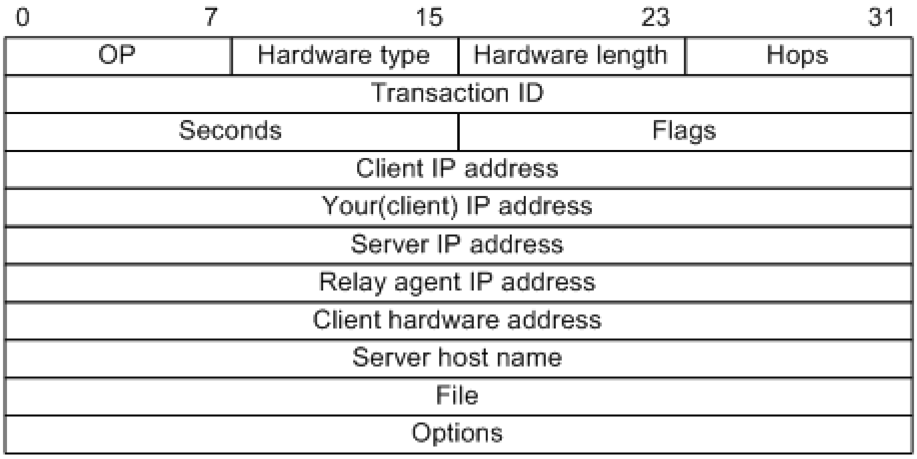
Figure 6-1 DHCP typical networking



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

Figure 6-2 shows structure of a DHCP packet. The DHCP packet is encapsulated in a UDP data packet.

Figure 6-2 Structure of 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 6-1 describes fields of DHCP packets.

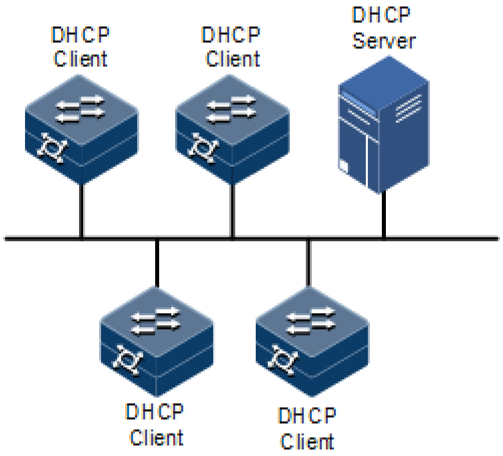
Table 6-1 Fields of DHCP packet

Field	Length	Description
OP	1	Packet type • 1: a request packet • 2: a reply packet
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 a DHCP packet This field increases by 1 every time the DHCP request packet passes a DHCP hop.

Field	Length	Description
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, IP address of the DNS server, and IP address of the WINS server

The ISCOM2600G series switch can be used as a DHCP client to obtain the IP address from the DHCP server for future management, as shown in Figure 6-3.

Figure 6-3 DHCP Client networking



6.1.2 Preparing for configurations

Scenario

As a DHCP client, the ISCOM2600G series switch obtains the IP address from the DHCP server.

The IP address assigned by the DHCP client is limited with a certain leased 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 VLANs
- Add the Layer 3 interface to the VLANs.
- DHCP Snooping is disabled.

6.1.3 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

6.1.4 Configuring DHCP Client

Before a DHCP client applies for an IP address, you must create a VLAN, and add the interface with the IP address to the VLAN. Meanwhile you must configure the DHCP server; otherwise the interface will fail to obtain the IP address through DHCP.

For interface IP 0, the IP addresses obtained through DHCP and configured manually can overwrite each other.

Note

- If the ISCOM2600G series switch is enabled with DHCP Server or DHCP Relay, DHCP Client cannot be enabled. If it is enabled with DHCP Client, DHCP Server or DHCP Relay cannot be enabled.
- By default, the ISCOM2600G series switch is enabled with DHCP Client. Use the **no ip address dhcp** command to disable DHCP Client.
- If the ISCOM2600G series switch obtains the 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.

Configure DHCP Client for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface vlan 1**	Enter Layer 3 interface configuration mode.
3	Raisecom(config-vlan)#**ip dhcp client** { **class-id** *class-id* | **client-id** *client-id* | **hostname** *hostname* }	(Optional) configure DHCP client information, including the type identifier, client identifier, and host name. Caution After the IP address is obtained by a DHCP client, client information cannot be modified.
4	Raisecom(config-vlan)#**ip address dhcp** [**server-ip** *ip-address*]	Configure the DHCP client to obtain IP address through DHCP.
5	Raisecom(config-vlan)#**ip dhcp client renew**	(Optional) renew the IP address. If the Layer 3 interface of the DHCP client has obtained an IP address through DHCP, the IP address will automatically be renewed when the leased period expires.
6	Raisecom(config-ip)#**no ip address dhcp**	(Optional) release the IP address.

6.1.5 Configuring DHCPv6 Client

Configure the DHCPv6 client for the ISCOM2600 series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface vlan** *vlan-id*	Enter VLAN interface configuration mode.
3	Raisecom(config-vlan1)#**ipv6 address dhcp** [**server-ip** *ipv6-address*]	Configure applying for IPv6 address through DHCPv6. If the ISCOM2600G series switch has obtained an IP address from the DHCP server through DHCPv6 before, it will restart the application process for the IP address if you use the command to modify the IPv6 address of the DHCP server.
4	Raisecom(config-vlan1)#**ipv6 dhcp client renew**	(Optional) renew the IPv6 address. If the Layer 3 interface on the ISCOM2600G series switch has obtained an IP address through DHCP, the IPv6 address will automatically be renewed when the leased period expires.
5	Raisecom(config-vlan1)#**ipv6 dhcp client rapid-commit**	(Optional) enable DHCPv6 Client to apply for rapid interaction.

6.1.6 Checking configurations

Use the following commands to check configuration results.

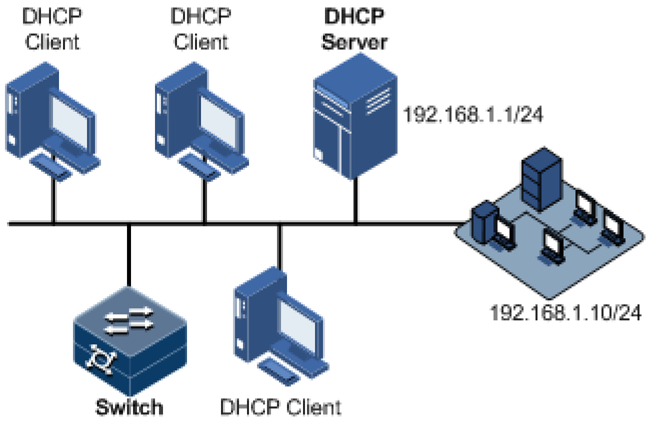
No.	Command	Description
1	Raisecom#**show ip dhcp client**	Show configurations of DHCP Client.
2	Raisecom#**show ipv6 dhcp client**	Show configurations of DHCPv6 Client.

6.1.7 Example for configuring DHCP Client

Networking requirements

As shown in Figure 6-4, the Switch is used as a DHCP client, and the host name is raisecom. The Switch is connected to the DHCP server and NMS. The DHCP server should assign IP addresses to the SNMP interface on the Switch and make NMS manage the Switch.

Figure 6-4 DHCP Client networking



Configuration steps

Step 1 Configure the DHCP client.

```
Raisecom#config
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip dhcp client hostname raisecom
```

Step 2 Configure applying for IP address through DHCP.

```
Raisecom(config-vlan1)#ip address dhcp 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
DHCP Client Mode:               Normal Mode
  Interface :                    vlan1
  Hostname:                     Raisecom
  Class-ID:                     Raisecom-ROS_5.2.1
  Client-ID:                    Raisecom-000e5e112233-IF0
  DHCP Client Is Requesting For A Lease.
  Assigned IP Addr:               0.0.0.0
  Subnet Mask:                  0.0.0.0
  Default Gateway:                --
  Client Lease Starts:            Jan-01-1970 08:00:00
  Client Lease Ends:             Jan-01-1970 08:00:00
  Client Lease Duration:          0(sec)
  DHCP Server:                  0.0.0.0
  TFTP Server Name:               --
  TFTP Server IP Addr:             --
```

```
Bootfile Filename:            --
NTP Server IP Addr:            --
Root Path:                   --

DHCP Client Mode:             Normal Mode
Interface :                  vlan10
Hostname:                    Raisecom
Class-ID:                    Raisecom-ROS_5.2.1
Client-ID:                   Raisecom-000e5e112233-IF0
DHCP Client Is Disabled.
Assigned IP Addr:             0.0.0.0
Subnet Mask:                 0.0.0.0
Default Gateway:             --
Client Lease Starts:           Jan-01-1970 08:00:00
Client Lease Ends:            Jan-01-1970 08:00:00
Client Lease Duration:         0(sec)
DHCP Server:                 0.0.0.0
TFTP Server Name:             --
TFTP Server IP Addr:           --
Bootfile Filename:            --
NTP Server IP Addr:            --
Root Path:                   --
```

6.2 DHCP Snooping

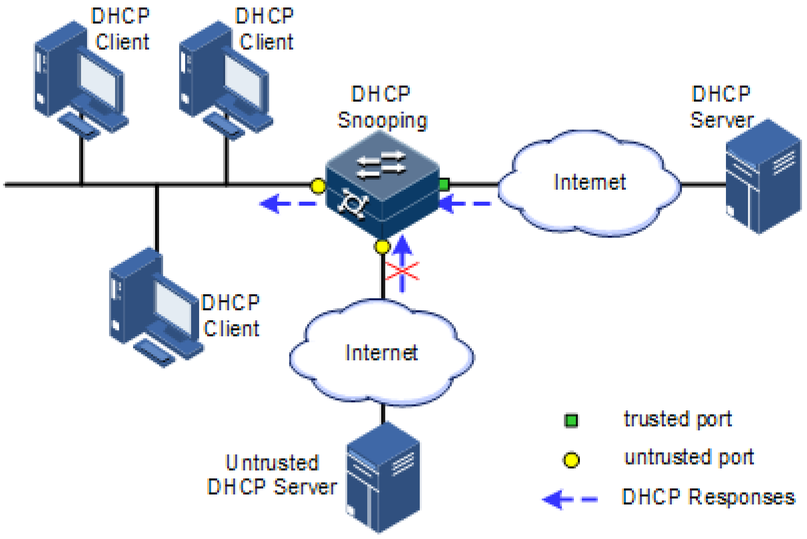
6.2.1 Introduction

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, but cannot communicate normally. As shown in Figure 6-5, to make DHCP client obtain the IP address from ta legal DHCP server, the DHCP Snooping security system permits to configure an interface as the trusted interface or untrusted interface: the trusted interface forwards DHCP packets normally; the untrusted interface discards the reply packets from the DHCP server.

Figure 6-5 DHCP Snooping



- 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. Then implement following by the record 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 ISCOM2600G series switch is configured with DHCP Snooping to support Option function:

- When the ISCOM2600G series switch receives a DHCP request packet, it processes packets according to Option field included or not, filling mode, and processing policy configured by user, then forwards the processed packet to DHCP server.
- When the ISCOM2600G series switch 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.

6.2.2 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

N/A

6.2.3 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 trusted/untrusted status	Untrust
DHCP Snooping in support of Option 82	Disable

6.2.4 Configuring DHCP Snooping

Generally, you must ensure that the ISCOM2600G series switch interface connected to DHCP server is in trusted status while the interface connected to the user is in untrusted status.

If enabled with DHCP Snooping but without the feature of DHCP Snooping supporting DHCP Option, the ISCOM2600G series switch will do nothing to Option fields in packets. For packets without Option fields, the ISCOM2600G series switch does not conduct the insertion operation.

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

Configure DHCP Snooping for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`ip dhcp snooping`**	Enable global DHCP Snooping.
3	`Raisecom(config)#`**`interface`** *`interface-type interface-number`*	Enter physical layer interface configuration mode.
4	`Raisecom(config-gigaethernet1/1/1)#`**`ip dhcp snooping`**	(Optional) enable interface DHCP Snooping.
5	`Raisecom(config-gigaethernet1/1/1)#`**`ip dhcp snooping trust`**	Configure the trusted interface of DHCP Snooping.

Step	Command	Description
6	Raisecom(config-gigaethernet1/1/1)#**ip dhcp snooping information option vlan-list** *vlan-list*	(Optional) configure the lists of VLANs that support Option 82 through DHCP Relay.
7	Raisecom(config-gigaethernet1/1/1)#**exit** Raisecom(config)#**ip dhcp snooping option** *option-id*	(Optional) configure DHCP Snooping to support user-defined Option fields.
8	Raisecom(config)#**ip dhcp snooping option client-id**	(Optional) configure DHCP Snooping to support Option 61 field.
9	Raisecom(config)#**ip dhcp snooping information option**	(Optional) configure DHCP Snooping to support Option 82 field.

6.2.5 Configuring DHCPv6 Snooping

Configure DHCPv6 Snooping for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ipv6 dhcp snooping**	Enable global DHCPv6 Snooping.
3	Raisecom(config)#**ipv6 dhcp snooping** *interface-type interface-number*	(Optional) enable interface DHCPv6 Snooping.
4	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
5	Raisecom(config-gigaethernet1/1/1)#**ipv6 dhcp snooping trust**	Configure the trusted interface of DHCPv6 Snooping.
6	Raisecom(config-gigaethernet1/1/1)#**exit** Raisecom(config)#**ipv6 dhcp snooping option** *number*	(Optional) configure DHCPv6 Snooping to support customized Options.
7	Raisecom(config)#**ipv6 dhcp snooping option interface-id**	(Optional) configure DHCP Snooping to support Option 18.

6.2.6 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	Raisecom#**show ip dhcp snooping**	Show configurations of DHCP Snooping.

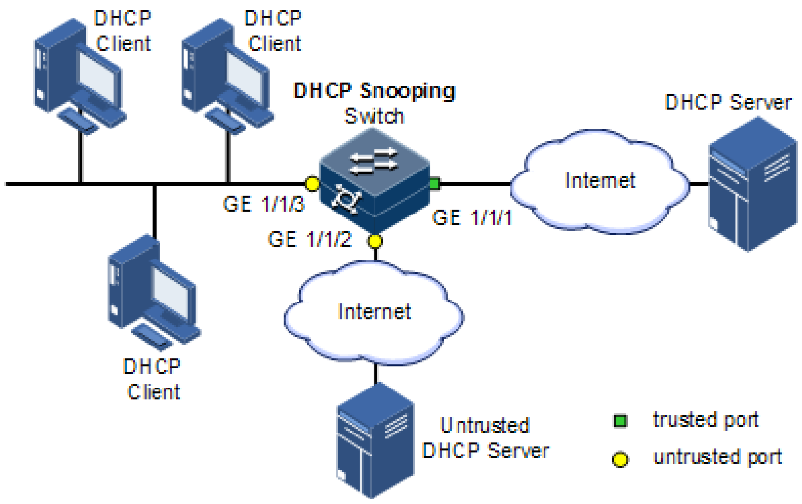
Step	Command	Description
2	`Raisecom#show ip dhcp snooping binding`	Show configurations of the DHCP Snooping binding table.
3	`Raisecom#show ipv6 dhcp snooping`	Show configurations of DHCPv6 Snooping.
4	`Raisecom#show ipv6 dhcp snooping binding`	Show configurations of the DHCPv6 Snooping binding table.

6.2.7 Example for configuring DHCP Snooping

Networking requirements

As shown in Figure 6-6, 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 to facilitate client management. You can configure padding information of about circuit ID sub-option to raisecom on GE 1/1/3, and padding information about remote ID sub-option to user01.

Figure 6-6 DHCP Snooping networking



Configuration steps

Step 1 Configure global DHCP Snooping.

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

Step 2 Configure the trusted interface.

```
Raisecom(config)#interface gigaethernet1/1/1
Raisecom(config-gigaethernet1/1/1)#ip dhcp snooping
Raisecom(config-gigaethernet1/1/1)#ip dhcp snooping trust
Raisecom(config-gigaethernet1/1/1)#quit
```

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

```
Raisecom(config)#ip dhcp snooping information option
Raisecom(config)#ip dhcp information option remote-id string user01
Raisecom(config)#interface gigaethernet1/1/3
Raisecom(config-gigaethernet1/1/3)#ip dhcp information option circuit-id
raisecom
```

Checking results

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

```
Raisecom#show ip dhcp snooping
DHCP Snooping: Enabled
DHCP Option 82: Enabled
Port                        vlan         Enabled Status  Trusted Status
Option82 Vlanlist
-------------------------------------------------------------------------
------------------------
gigaethernet1/1/1             --           enabled       yes           1-
4094
gigaethernet1/1/2             --           enabled       no            1-
4094
gigaethernet1/1/3             --           enabled       no            1-
4094
gigaethernet1/1/4             --           enabled       no            1-
4094
gigaethernet1/1/5             --           enabled       no            1-
4094
gigaethernet1/1/6             --           enabled       no            1-
4094
……
```

6.3 DHCP Options

6.3.1 Introduction

DHCP transmits control information and network configuration parameters through Option field in packet to dynamically assign addresses to provide abundant network configurations for clients. DHCP has 255 types of options, with the final option as Option 255. Table 6-2 lists frequently used DHCP options.

Table 6-2 Common DHCP options

Options	Description
3	Router option, used to assign the gateway address of DHCP clients
6	DNS server option, used to specify the IP address of the DNS server assigned for DHCP clients
18	IPv6 DHCP client flag option, used to specify interface information about DHCP clients
51	IP address lease option
53	DHCP packet type option, used to mark the type of DHCP packets
55	Request parameter list option, used to indicate network configuration parameters to be obtained from the server, containing values of these parameters
61	DHCP client flag option, used to assign device information for DHCP clients
66	TFTP server name option, used to specify the domain name of the TFTP server assigned for DHCP clients
67	Startup file name option, used to specify the name of the startup file assigned for DHCP clients
82	DHCP client flag option, customized, used to mark the position of DHCP clients, including Circuit ID and remote ID
150	TFTP server address option, used to specify the IP address of the TFTP server assigned for DHCP clients
184	DHCP reserved option. At present Option 184 is used to carry information required by voice calling. Through Option 184, the DHCP server can distribute IP addresses for DHCP clients with voice function and meanwhile provide information about voice calling.
255	Complete option

Options 18, 61, and 82 in DHCP Option are relay information options in DHCP packets. When a DHCP client sends request packets to the DHCP server by passing a DHCP Relay or DHCP Snooping device, the DHCP Relay or DHCP Snooping device will add Option fields to the request packets.

Options 18, 61, and 82 implement recording of information about DHCP clients on the DHCP server. By cooperating with other software, it can implement functions, such as limit on IP address distribution and accounting. For example, by cooperating with IP Source Guard, Options 18, 61, 82 can defend deceiving through IP address+MAC address.

Option 82 can include up to 255 sub-options. If the Option 82 field is defined, at least one sub-option must be defined. The ISCOM2600G series switch supports the following two sub-options:

- Sub-Option 1 (Circuit ID): it contains the interface ID, interface VLAN, and additional information about request packets of the DHCP client.
- Sub-Option 2 (Remote ID): it contains interface MAC address (DHCP Relay), or bridge MAC address (DHCP Snooping device) of the ISCOM2600G series switch, or user-defined string in request packets of the DHCP client.

6.3.2 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 are used to 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

6.3.3 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

6.3.4 Configuring DHCP Option field

Configure DHCP Option field for the ISCOM2600G series switch 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 additional information for Option 82 field.

Step	Command	Description
	Raisecom(config)#**interface** *interface-type interface-number* Raisecom(config-gigaethernet1/1/1)#**ip dhcp information option circuit-id** *circuit-id* [**prefix-mode**]	(Optional) configure circuit ID sub-option information for Option 82 field on the interface.
	Raisecom(config)#**ip dhcp information option** { **attach-string** | **circuit-id format** | **circuit-id hex** } *string*	(Optional) configure the attached string in Option 82 of DHCP packets.
	Raisecom(config)#**ip dhcp information option circuit-id mac-format** *string*	(Optional) configure the format of the MAC address in the variable of Circuit ID in Option 82 of DHCP packets.
	Raisecom(config-gigaethernet1/1/1)#**exit** Raisecom(config)#**ip dhcp information option remote-id** { **client-mac** | **client-mac-string** | **hostname** | **string** *string* | **switch-mac** | **switch-mac-string** }	(Optional) configure remote ID sub-option information for Option 82 field.
3	Raisecom(config)#**ipv4 dhcp option** *option-id* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }	(Optional) create user-defined Option based on IPv4.
	Raisecom(config)#**interface gigaethernet1/1/1** Raisecom(config-gigaethernet1/1/1)#**ipv4 dhcp option** *option-id* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }	(Optional) create user-defined Option field information on the interface.
4	Raisecom(config-gigaethernet1/1/1)#**exit** Raisecom(config)#**ipv4 dhcp option client-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }	(Optional) configure Option 61 field information.
	Raisecom(config-gigaethernet1/1/1)#**ipv4 dhcp option client-id** { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }	(Optional) configure Option61 field information on the interface.

6.3.5 Configuring DHCP Option 18 over IPv6

Configure DHCP Option 18 over IPv6 for the ISCOM2600G series switch as below.

Option 18 over IPv6 should be configured on the device that is enabled with DHCP Snooping.

All the following steps are optional and in any sequence.

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

Step	Command	Description
2	`Raisecom(config)#ipv6 dhcp option interface-id { ascii ascii-string | hex hex-string | ipv6-address ipv6-address }`	(Optional) configure information about Option 18.

3	`Raisecom(config)#interface interface-type interface-number`
	`Raisecom(config-gigaethernet1/1/1)#ipv6 dhcp option interface-id { ascii ascii-string | hex hex-string | ipv6-address ipv6-address }`
		(Optional) configure information about Option 18 on the interface.

6.3.6 Configuring DHCP Option 37 over IPv6

Configure DHCP Option 37 over IPv6 for the ISCOM2600G series switch as below.

Option 37 over IPv6 should be configured on the device that is enabled with DHCP Snooping.

All the following steps are optional and in any sequence.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ipv6 dhcp option remote-id { ascii | hex } string`	(Optional) configure information about Option 37.

3	`Raisecom(config)#interface interface-type interface-number`
	`Raisecom(config-gigaethernet1/1/1)#ipv6 dhcp option remote-id mac-format string`
		(Optional) configure the format of the MAC address of the Circuit ID variable in Option 37 in DHCPv6 packets.

6.3.7 Configuring customized DHCP Option over IPv6

Configure customized DHCP Option over IPv6 for the ISCOM2600G series switch as below.

Customized Option over IPv6 should be configured on the device that is enabled with DHCP Snooping.

All the following steps are optional and in any sequence.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#ipv6 dhcp option number { ascii ascii-string | hex hex-string | ipv6-address ipv6-address }`	(Optional) create customized Option information over IPv6.

Step	Command	Description

3	`Raisecom(config)#interface interface-type interface-number`
	`Raisecom(config-gigaethernet1/1/1)#ipv6 dhcp option number { ascii ascii-string | hex hex-string | ipv6-address ipv6-address }`
		(Optional) create customized Option information over IPv6 on the interface.

6.3.8 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.

6.4 DHCP Server

6.4.1 Introduction

Dynamic Host Configuration Protocol (DHCP) refers to assigning IP address configurations dynamically for users on the 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 notebooks 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 configuration to the server (including IP address, subnet mask, and default gateway), and the server replies with an IP address for the client and other related configurations to implement dynamic configurations of IP address.

In DHCP Client/Server communication mode, a specific host is configured to assign IP addresses, and send network configurations to related hosts. The host is called the DHCP server.

DHCP application

Under normal circumstances, use the DHCP server to assign IP addresses in following situations:

- The network scale is large. It requires much workload for manual configurations, and is difficult to manage the entire network intensively.
- The number of hosts on the network is greater than the number of IP addresses, which make it unable to assign a fixed IP address for each host, and restrict the number of users connected to network simultaneously.

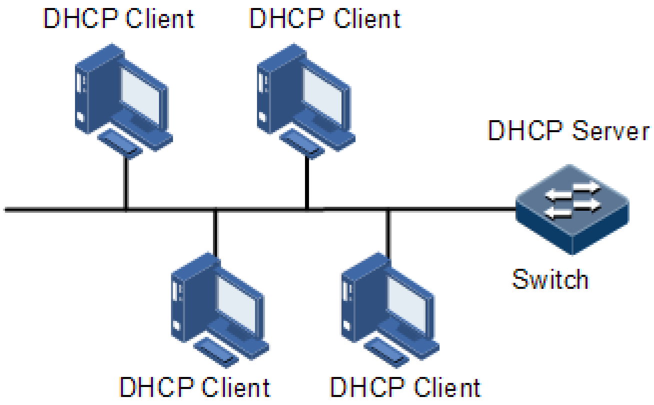
- Only the minority of hosts on the network need fixed IP addresses, most of hosts have no requirement for fixed IP address.

After a DHCP client obtains the IP address from the DHCP server, it cannot use the IP address permanently but in a fixed period, which is called the leased period. You can specify the duration of the leased period.

The DHCP technology ensures rational allocation, avoids waste of IP addresses, and improves the utilization rate of IP addresses on the entire network.

The ISCOM2600G series switch, as the DHCP server, assigns dynamic IP addresses to clients, as shown in Figure 6-7.

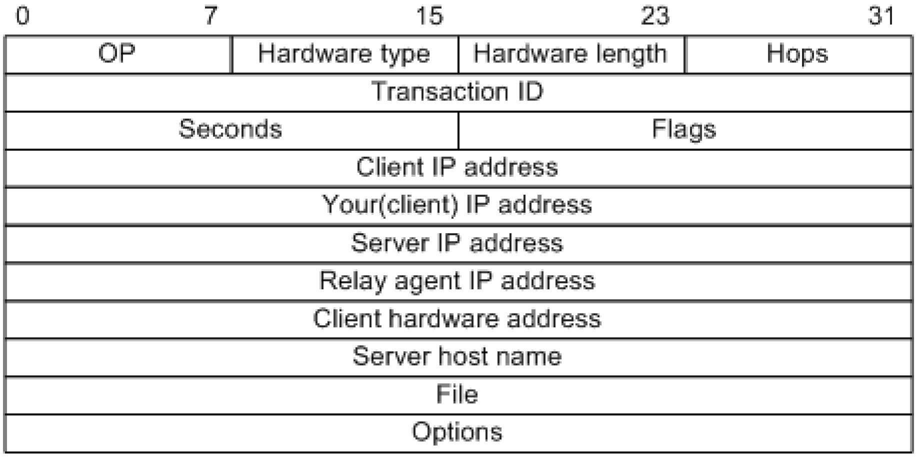
Figure 6-7 DHCP Server and Client networking



DHCP packets

Figure 6-8 shows the structure of a DHCP packet. The DHCP packet is encapsulated in a UDP data packet.

Figure 6-8 Structure of a DHCP packet



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 6-3 describes fields of a DHCP packet.

Table 6-3 Fields of a DHCP packet

Field	Length	Description
OP	1	Packet type ● 1: a request packet ● 2: a reply packet
Hardware type	1	Hardware address type of a DHCP client
Hardware length	1	Hardware address length of a DHCP client
Hops	1	Number of DHCP hops passing by the DHCP packet This field increases 1 every time the DHCP request packet passes a DHCP relay.
Transaction ID	4	A random number selected by the client to initiate a request, used to identify an address request process
Seconds	2	Duration after the DHCP request for the DHCP client, fixed to 0, being idle currently
Flags	2	Bit 1 is the broadcast reply flag, used to mark that the DHCP server response packet is transmitted in unicast or broadcast mode. ● 0: unicast ● 1: broadcast Other bits are reserved.
Client IP address	4	IP address of the DHCP client, only filled when the client is in bound, updated or re-bound status, used to respond to ARP request
Your (client) IP address	4	IP address of the DHCP client assigned 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 relay passing by the request packet sent by the DHCP client
Client hardware address	16	Hardware address of the DHCP client
Server host name	64	Name of the DHCP server
File	128	Startup configuration file name and path assigned by the DHCP server to the DHCP client
Options	Modifiable	A modifiable option field, including packet type, available leased period, IP address of the DNS server, IP address of the WINS

6.4.2 Preparing for configurations

Scenario

When working as the DHCPv4 server, the ISCOM2600G series switch can assign IP addresses to DHCPv4 clients.

Prerequisite

- Disable DHCPv4 Client on the ISCOM2600G series switch.
- The DHCP server is a common one.

6.4.3 Creating and configuring IPv4 address pool

Configure the IPv4 address pool for the ISCOM2600G series switch as below.

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

6.4.4 Enabling interface DHCPv4 Server

Enable interface DHCPv6 Server for the ISCOM2600G series switch as below.

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

Step	Command	Description
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
3	Raisecom(config-port)#**ip dhcp server**	Enable interface DHCPv4 Server.

6.4.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom(config)#**show ip dhcp server**	Show configurations of DHCP Server.
2	Raisecom(config)#**show ip dhcp server lease**	Show assigned IP addresses and clients information.
3	Raisecom(config)#**show ip dhcp server statistics**	Show packet statistics on the DHCP Server.
4	Raisecom(config)#**show ip dhcp static-bind**	Show DHCPv4 static binding.
5	Raisecom(config)#**show ip server pool**	Show configurations of the address pool of DHCP Server.

6.5 DHCP Relay

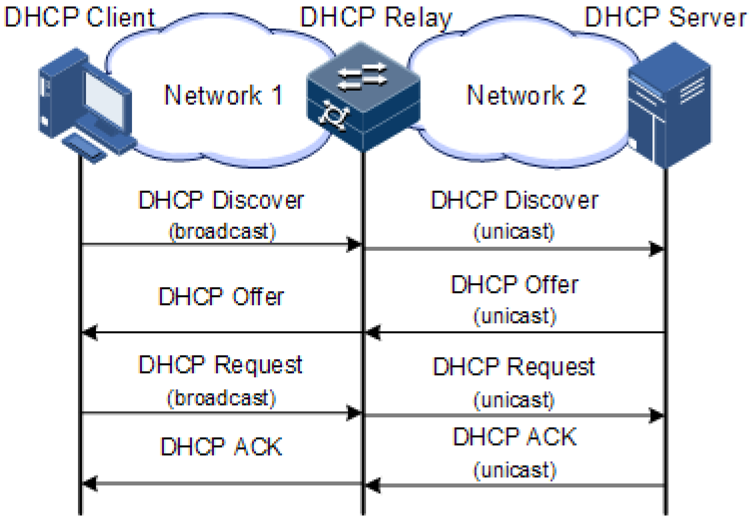
6.5.1 Introduction

At the beginning, DHCP requires the DHCP server and clients to be in the same segment, instead of different segments. As a result, a DHCP server is configured for all 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 the DHCP server that are in different segments. It relays packets across segments to the DHCP server or clients.

Figure 6-9 shows typical application of DHCP Relay.

Figure 6-9 Typical application of DHCP Relay



When a DHCP client sends a request packet to the DHCP server through a DHCP relay, the DHCP relay processes the request packet and sends it to the DHCP server in the specified segment. The DHCP server sends required information to the DHCP client through the DHCP relay according to the request packet, thus implementing dynamic configuration of the DHCP client.

6.5.2 Preparing for configurations

Scenario

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

Prerequisite

DHCP Relay is mutually exclusive with DHCP Server, DHCP Client, and DHCP Snooping. Namely, disable DHCP Server, DHCP Client, and DHCP Snooping on the device to be configured with DHCP Relay.

6.5.3 Default configurations of DHCP Relay

Default configurations of DHCP Relay are as below.

Function	Default value
Global DHCP Relay	Disable
Interface DHCP Relay	Disable

6.5.4 Configuring global DHCP Relay

Configure global DHCP Relay for the ISCOM2600G series switch as below.

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

6.5.5 Configuring destination IP address for forwarding packets

Configure the destination IP address for forwarding packets for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface vlan vlan-id`	Enter VLAN interface configuration mode.
3	`Raisecom(config-vlan1)#ip dhcp relay target-ip ip-address`	Configure the destination IP address for forwarding packets.

6.5.6 Configuring IP address of DHCP relay

Configure the IP address of the DHCP relay for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#interface vlan vlan-id`	Enter VLAN interface configuration mode.
3	`Raisecom(config-vlan1)#ip dhcp realy relay-ip ip-address`	Configure the IP address of the DHCP relay.

6.5.7 (Optional) configuring DHCP Relay to support Option 82

Configure DHCP Relay to support Option 82 for the ISCOM2600G series switch 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

Step	Command	Description
4	`Raisecom(config)#`**`interface`** *`interface-type interface-number`*	Enter physical layer interface configuration mode.
5	`Raisecom(config-gigaethernet1/1/1)#`**`ip dhcp relay information trust`**	Configure the trusted interface of DHCP Relay.
6	`Raisecom(config-gigaethernet1/1/1)#`**`ip dhcp relay information option vlan-list`** *`vlan-list`*	Configure the VLAN list of DHCP Relay to support Option 82.

6.5.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show ip dhcp relay`**	Show configurations of DHCP Relay.
2	`Raisecom#`**`show ip dhcp relay information`**	Show information about Option 82 supported by DHCP Relay.

7 QoS

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

- Introduction
- Configuring priority
- Configuring congestion management
- Configuring congestion avoidance
- Configuring traffic classification and traffic policy
- Configuring rate limiting

7.1 Introduction

When network applications become more and more versatile, users bring forward different Quality of Service (QoS) requirements on them. In this case, the network should distribute and schedule resources for different network applications as required. When network is overloaded or congested, QoS can ensure service timeliness and integrity and make the entire network run efficiently.

QoS is composed of a group of flow management technologies:

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

7.1.1 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 the Best-effort service, the network will send packets as possible as it can, but it does not guarantee the delay and reliability.

Best-effort is the default Internet service model now, suitable to most network applications, such as FTP and E-mail. It 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 preconfigured packet 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 CAR can not only control the flows, but also mark and remark the packets.
- Queuing technology: the queuing technologies of SP, WRR, DRR, SP+WRR, and SP+DRR cache and schedule the congestion packets to implement congestion management.

7.1.2 Priority trust

Priority trust means that the ISCOM2600G series switch uses priority of packets for classification and performs QoS management.

The ISCOM2600G series switch supports packet priority trust based on interface, including:

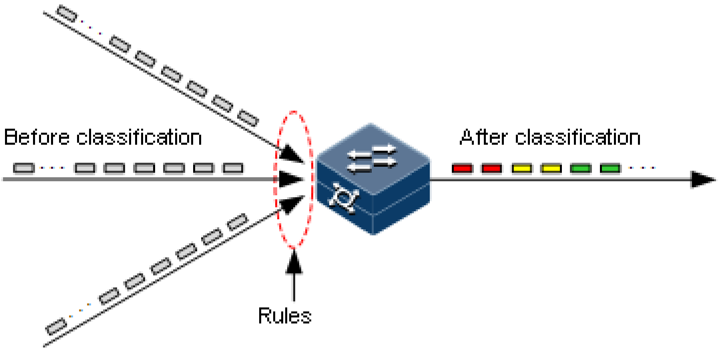
- Differentiated Services Code Point (DSCP) priority
- Class of Service (CoS) priority
- ToS priority

7.1.3 Traffic classification

Traffic classification refers to identifying certain packets according to specified rules and performing different QoS policies on packets matched with different rules. Traffic classification is the premise and basis for differentiated services.

The ISCOM2600G series switch supports traffic classification based on ToS priority, DSCP priority, and CoS priority over IP packets, and classification based on Access Control List (ACL) rules and VLAN ID. The traffic classification procedure is shown in Figure 7-1.

Figure 7-1 Traffic classification



IP priority and DSCP priority

Figure 7-2 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 7-3 shows the structures of ToS and DSCP priorities.

Figure 7-2 Structure of IP packet header

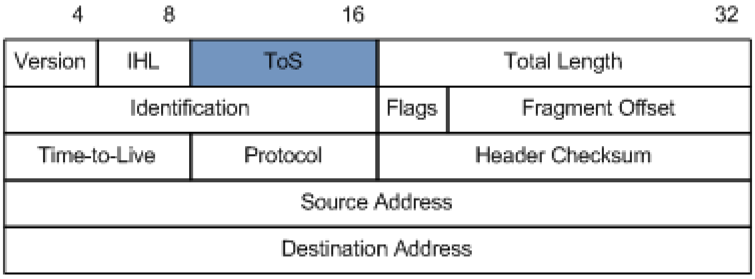
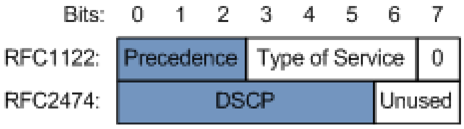


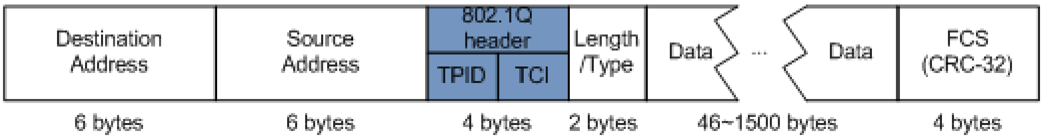
Figure 7-3 Structures of ToS priority and DSCP priority



CoS priority

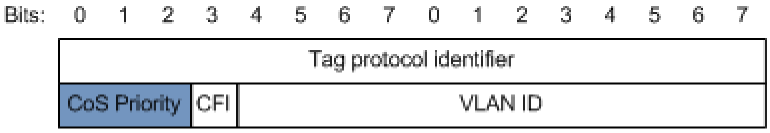
IEEE802.1Q-based VLAN packets are modifications of Ethernet packets. A 4-byte 802.1Q header is added between the source MAC address and protocol type, as shown in Figure 7-4. The 802.1Q header consists of a 2-byte Tag Protocol Identifier (TPID, valuing 0x8100) filed and a 2-byte Tag Control Information (TCI) field.

Figure 7-4 Structure of VLAN packet



The first 3 bits of the TCI field represent the CoS priority, which ranges from 0 to 7, as shown in Figure 7-5. CoS priority is used to guarantee QoS on the Layer 2 network.

Figure 7-5 Structure of CoS priority



7.1.4 Traffic policy

After performing traffic classification on packets, you need to perform different operations on packets of different categories. A traffic policy is formed when traffic classifiers are bound to traffic behaviours.

Rate limiting based on traffic policy

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 ISCOM2600G series switch supports rate limiting based on traffic policy in the ingress direction on the interface.

The ISCOM2600G series switch 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 ISCOM2600G series switch supports redirecting packets to the specified interface for forwarding in the ingress direction of the interface.

Remarking

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

The ISCOM2600G series switch supports remarking packets by the following priority fields:

- IP priority
- 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.

7.1.5 Priority mapping

Priority mapping refers to sending packets to different queues with different local priorities according to pre-configured mapping between external priority and local priority. Therefore, packets in different queues can be scheduled on the egress interface.

The ISCOM2600G series switch supports performing priority mapping based on the DSCP priority of IP packets or the CoS priority of VLAN packets. The Traffic-Class field of IPv6 packets corresponds to the DSCP priority of IPv4 packets. The mapping from DSCP priority to local priority is applicable to IPv6 packets. Take the first 6 bits of the Traffic-Class field for use.

By default, the mapping between the local priority and DSCP, CoS priorities of the ISCOM2600G series switch is listed in Table 7-1 and Table 7-2.

Table 7-1 Mapping between local priority and DSCP priority

Local	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 meaning assigned by the ISCOM2600G series switch and is the priority corresponding to queue in QoS queue scheduling.

Local priority ranges from 0 to 7. Each interface of the ISCOM2600G series switch supports 8 queues. Local priority and interface queue are 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 7-2.

Table 7-2 Mapping between local priority and queue

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

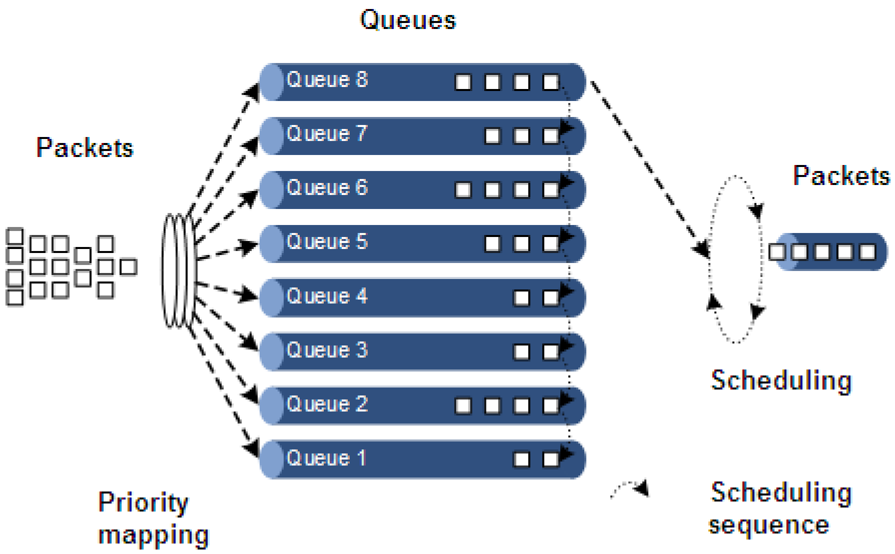
7.1.6 Queue scheduling

The ISCOM2600G series switch needs to perform queue scheduling when delay-sensitive services need better QoS services than non-delay-sensitive services and when the network is congested once in a while.

Queue scheduling adopts different scheduling algorithms to send packets in a queue. Scheduling algorithms supported by the ISCOM2600G series switch include Strict-Priority (SP), Weight Round Robin (WRR), Deficit Round Robin (DRR), SP+WRR, and SP+DRR. All scheduling algorithms are designed for addressing specified traffic problems. And they have different effects on bandwidth distribution, delay, and jitter.

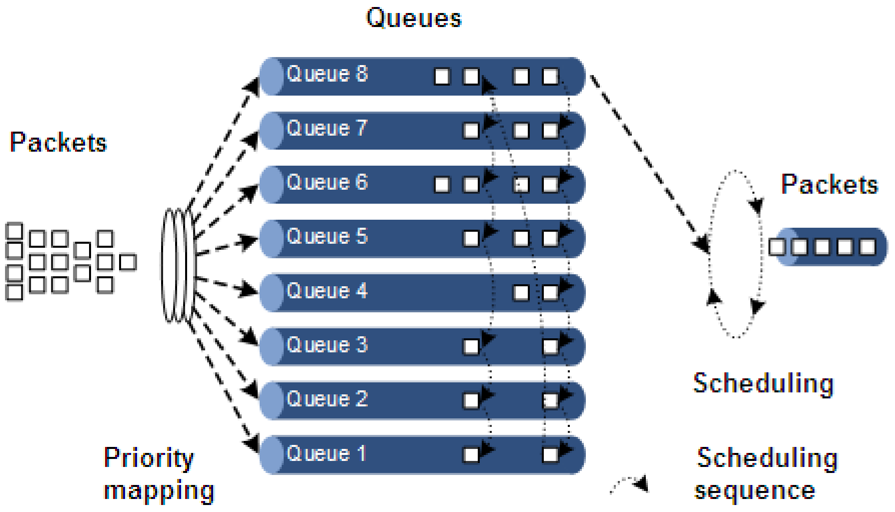
- SP: the ISCOM2600G series switch strictly schedules packets in a descending order of priority. Packets with lower priority cannot be scheduled until packets with higher priority are scheduled, as shown in Figure 7-6.

Figure 7-6 SP scheduling



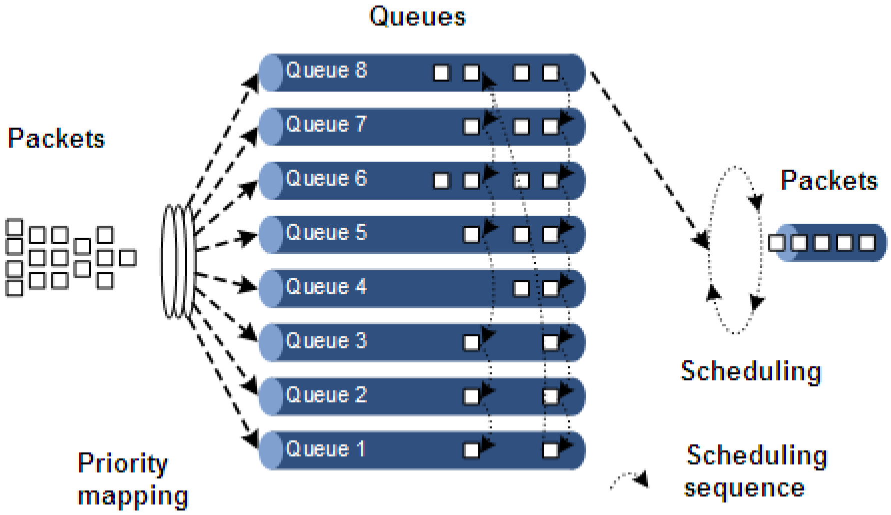
- WRR: on the basis of scheduling packets in a polling manner according to the priority, the ISCOM2600G series switch schedules packets according to the weight (based on bytes) of the queue, as shown in Figure 7-7.

Figure 7-7 WRR scheduling



- DRR: similar with WRR, on the basis of scheduling packets in a polling manner according to the scheduling sequence, the ISCOM2600G series switch schedules packets according to the weight of the queue (based on packet), as shown in DRR scheduling

Figure 7-8 DRR scheduling



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

7.1.7 Congestion avoidance

By monitoring utilization of network resources (queues/memory buffer), congestion avoidance can discard packets actively when congestion occurs or network traffic increases. It is a traffic control mechanism that is used to resolve network overload by adjusting network traffic.

The traditional packet loss policy uses the Tail-Drop mode to process all packets equally without differentiating class of services. When congestion occurs, packets at the end of a queue are discarded until congestion is resolved.

This Tail-Drop policy may cause TCP global synchronization, making network traffic change between heavy and low and affecting link utilization.

RED

The Random Early Detection (RED) technology discards packets randomly and makes multiple TCP connection not reduce transport speed simultaneously to avoid TCP global synchronization.

The RED algorithm configures a minimum threshold and maximum threshold for length of each queue. In addition:

- Packets are not discarded when the queue length is smaller than the minimum threshold.
- All received packets are discarded when the queue length is greater than the maximum threshold.
- Packets to be received are discarded randomly when the queue length is between the minimum and maximum thresholds. The greater the queue size is, the higher the packet drop probability is.

7.1.8 Rate limiting based on interface and VLAN

The ISCOM2600G series switch supports rate limiting both based on traffic policy and based on interface or VLAN ID. Similar to rate limiting based on traffic policy, the ISCOM2600G series switch discards the exceeding traffic.

7.1.9 QoS enhancement

QoS enhancement is a sub-function of QoS and is more flexible than basic QoS. It is widely used on the switches.

QoS enhancement has the following functions:

- Ingress interface
  - Bandwidth guarantee: QoS enhancement implements the bandwidth service based on interface or flow. It also supports hierarchical bandwidth guarantee and refining bandwidth of different service flows.
  - Awaring: this function determines whether to conduct color-aware of packets when a flow enters the bandwidth-guaranteed interface.
- Egress interface
  - Bandwidth guarantee: bandwidth service based on interface or flow is implemented. QoS enhancement does not support hierarchical bandwidth guarantee.
  - Marking: this function determines whether to mark a packet with color when a flow leaves the bandwidth-guaranteed interface.

Bandwidth guarantee

The bandwidth guarantee function guarantees that the traffic entering the network is within the defined range, and it discards or schedules packets. Bandwidth guarantee can meet users' requirements on service bandwidth, and also protect network resources and carriers' benefits.

By configuring the bandwidth guarantee profile and applying it to an interface, you can mark different flows green, yellow, and red. The ISCOM2600G series switch takes different actions over flows of different colors: forward green flows, schedule yellow flows, and discard red flows.

Hierarchical bandwidth guarantee

Hierarchical bandwidth guarantee is a more flexible bandwidth guarantee. You can configure guaranteed bandwidth for each flow independently and even configure guaranteed bandwidth for sum of multiple flows through hierarchical bandwidth guarantee.

Color-aware and marking

If enabled with color-aware, the ISCOM2600G series switch is in color-aware status, in which it can identify whether the ingress flow is marked with color. If disabled with color-aware, the ISCOM2600G series switch is in color-blind status, in which it can neglect whether the ingress flow is marked with color, but identify the flow color again.

The function of color marking judges the color of a flow according to Committed Information Rate (CIR), Committed Burst Size (CBS), Excess Information Rate (EIR), and Excess Burst Size (EBS) configured in the bandwidth guarantee profile, and modifies the flag bit to mark it with color according to the packet format defined in IEEE 802.1ad.

7.2 Configuring priority

7.2.1 Preparing for configurations

Scenario

You can choose to trust the priority carried by packets from an upstream device, or process packets with untrusted priority through traffic classification and traffic policy. After being configured to priority trust mode, the ISCOM2600G series switch processes packets according to their priorities and provides services accordingly.

To specify local priority for packets is the prerequisite for queue scheduling. For packets from the upstream device, you can not only map the external priority carried by packets to different local priorities, but also configure local priority for packets based on interface. Then the ISCOM2600G series switch will conduct queue scheduling according to local priority of packets. Generally, IP packets need to be configured with mapping relationship between IP priority/DSCP priority and local priority; while VLAN packets need to be configured with mapping relationship between CoS priority and local priority.

Prerequisite

N/A

7.2.2 Default configurations of basic QoS

Default configurations of basic QoS are as below.

Function	Default value
Global QoS status	Enable
Interface trust priority type	Trust CoS priority
Mapping from CoS to local priority	See Table 7-3.
Mapping from DSCP to local priority	See Table 7-4.
Mapping from ToS to local priority and color	See Table 7-5.
Interface priority	0

Table 7-3 Default mapping from CoS to local priority

CoS	0	1	2	3	4	5	6	7
Local	0 (green)	1 (green)	2 (green)	3 (green)	4 (green)	5 (green)	6 (green)	7 (green)

Table 7-4 Default mapping from DSCP to local priority

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

Table 7-5 Default mapping from ToS to local priority and color

DSCP	0	1	2	3	4	5	6	7
Local	0 (green)	1 (green)	2 (green)	3 (green)	4 (green)	5 (green)	6 (green)	7 (green)

7.2.3 Configuring types of priorities trusted by interface

Configure types of priorities trusted by interface for the ISCOM2600G series switch 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-gigaethernet1/1/1)#`**`mls qos trust`** `{` **`cos`** `|` **`dscp`** `|` **`port-priority`** `}`	Configure types of priorities trusted by interface. CoS priority exists in the head of 802.1q packets. When you use it, the interface type must be Trunk Tunnel.
4	`Raisecom(config-gigaethernet1/1/1)#`**`mls qos priority`** *`portpri-value`*	Configure the interface priority.

7.2.4 Configuring mapping from CoS to local priority

Configure mapping from CoS to local priority and color for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`mls qos mapping cos-to-local-priority`** *`profile-id`*	Create a profile of mapping from CoS to local priority and color, and enter cos-to-pri configuration mode.
3	`Raisecom(cos-to-pri)#`**`cos`** *`cos-value`* **`to local-priority`** *`localpri-value`* `[` **`color`** `{` **`green`** `|` **`red`** `|` **`yellow`** `} ]`	(Optional) modify the profile of mapping from CoS to local priority and color.

Step	Command	Description
4	Raisecom(cos-to-pri)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
5	Raisecom(config-gigaethernet1/1/1)#**mls qos cos-to-local-priority** *profile-id*	Apply the profile of mapping from CoS to local priority and color on the interface.

7.2.5 Configuring mapping from DSCP to local priority and color

Configure mapping from DSCP to local priority and color for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos mapping dscp-to-local-priority** *profile-id*	Create a profile of mapping from DSCP to local priority and color, and enter dscp-to-pri configuration mode.
3	Raisecom(dscp-to-pri)#**dscp** *dscp-value* **to local-priority** *localpri-value* [**color** { **green** | **red** | **yellow** }]	(Optional) modify the profile of mapping from DSCP to local priority and color.
4	Raisecom(dscp-to-pri)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
5	Raisecom(config-gigaethernet1/1/1)#**mls qos dscp-to-local-priority** *profile-id*	Apply the profile of mapping from DSCP to local priority and color on the interface.

7.2.6 Configuring DSCP mutation

Configure DSCP mutation for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos mapping dscp-mutation** *profile-id*	Create a DSCP mutation mapping profile, and enter dscp mutation configuration mode.
3	Raisecom(dscp-mutation)#**dscp** *dscp-value* **to new-dscp** *newdscp-value*	(Optional) modify the DSCP mutation profile.
4	Raisecom(dscp-mutation)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.

Step	Command	Description
5	Raisecom(config-gigaethernet1/1/1)#**mls qos dscp-mutation** *profile-id*	Apply the DSCP mutation profile on the interface.

7.2.7 Configuring CoS remarking

Configure CoS remarking for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos mapping cos-remark** *profile-id*	Create a CoS remarking profile, and enter cos-remark configuration mode.
3	Raisecom(cos-remark)#**local-priority** *localpri-value* **to cos** *newcos-value*	Modify the CoS remarking profile.
4	Raisecom(dscp-remark)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
5	Raisecom(config-gigaethernet1/1/1)#**mls qos cos-remark** *profile-id*	Apply the DSCP remarking profile on the interface.

7.2.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#show mls qos[*interface-type interface-number*]	Show QoS priority, trust mode, and scheduling mode on the interface.
2	Raisecom#**show mls qos mapping cos-to-local-priority** [**default** | *profile-id*]	Show information about mapping from CoS to local priority and color profile.
3	Raisecom#**show mls qos mapping dscp-to-local-priority** [**default** | *profile-id*]	Show information about mapping from DSCP to local priority and color profile.
4	Raisecom#**show mls qos mapping dscp-mutation** [*profile-id*]	Show mapping information about the DHCP mutation profile
5	Raisecom#show mls qos mapping cos-remark [**default** | *profile-id*]	Show information about the CoS remarking profile.

7.3 Configuring congestion management

7.3.1 Preparing for configurations

Scenario

When the network is congested, you can configure queue scheduling if you wish to:

- Balance delay and delay jitter of various packets, preferentially process packets of key services (such as video and voice).
- Fairly process packets of secondary services (such as Email) with identical priority.
- Process packets of different priorities according to respective weight values.

The scheduling algorithm to be chosen depends on the current service condition and customer requirements.

Prerequisite

Enable global QoS.

7.3.2 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. • DRR weight for scheduling 8 queues is 81.

7.3.3 Configuring SP queue scheduling

Configure SP queue scheduling for the ISCOM2600G series switch 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-gigaethernet1/1/1)#`**`mls qos queue scheduler sp`**	Configure queue scheduling mode as SP on the interface.

7.3.4 Configuring WRR or SP+WRR queue scheduling

Configure WRR or SP+WRR for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**mls qos queue scheduler wrr** *weigh1 weight2 weight3…weight8*	Configure queue scheduling mode as WRR on the interface and the weight for each queue.

7.3.5 Configuring DRR or SP+DRR queue scheduling

Configure DRR or SP+DRR for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**mls qos queue scheduler drr** *weigh1 weight2 weight3…weight8*	Configure queue scheduling mode as DRR, and configure weight for various queues. Conduct SP scheduling when priority of a queue is 0.

7.3.6 Configuring queue bandwidth guarantee

Configure queue bandwidth guarantee for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**mls qos queue** *queue-id* **shaping cir** *cir* pir *pir*	(Optional) configure queue bandwidth guarantee on the interface and configure burst size.

7.3.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show mls qos queue interface`** *`interface-type interface-number`*	Show the weight of queues on the interface.
2	`Raisecom#`**`show mls qos queue statistics interface`** *`interface-type interface-number`*	Show statistics of queues on the interface.
3	`Raisecom#`**`show mls qos queue shaping interface`** *`interface-type interface-list`*	Show queue shaping on the interface.

7.4 Configuring congestion avoidance

7.4.1 Preparing for configurations

Scenario

To avoid network congestion and solve the problem of TCP global synchronization, you can configure congestion avoidance to adjust network flow and relieve network overload.

The ISCOM2600G series switch conducts congestion avoidance based on WRED.

Prerequisite

Enable global QoS.

7.4.2 Default configurations of congestion avoidance

Default configurations of congestion avoidance are as below.

Function	Default value
Global WRED status	Enable

7.4.3 Configuring SRED

Configure SRED for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`mls qos sred profile`** *`profile-id`*	Create a SRED profile, and enter SRED configuration mode.
3	`Raisecom(sred)#`**`sred [ color { red | yellow } ] start-drop-threshold`** *`start-drop value`* **`drop-probability`** *`drop probability value`*	Modify the SRED profile.

Step	Command	Description
4	Raisecom(sred)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.

7.4.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom# **show mls qos sred profile** [*profile-list*]	Show information about the WRED profile.

7.5 Configuring traffic classification and traffic policy

7.5.1 Preparing for configurations

Scenario

Traffic classification is the basis of QoS. You can classify packets from the upstream device according to the priorities and ACL rules. After classification, the ISCOM2600G series switch can perform corresponding operations on packets in different categories and provide corresponding services.

A traffic classification rule will not take effect until it is bound to a traffic policy. You should apply traffic policy according to current network loading conditions and period. Usually, the ISCOM2600G series switch limits the rate for transmitting packets according to CIR when packets enter the network, and remarks priority according to service feature of packets.

Prerequisite

Enable global QoS.

7.5.2 Default configurations of traffic classification and traffic policy

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

Function	Default value
Traffic policy status	Disable
Traffic policy statistics status	Disable

7.5.3 Creating traffic classification

Create traffic classification for the ISCOM2600G series switch 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) configure the description of traffic classification.

7.5.4 Configuring traffic classification rules

Configure traffic classification rules for the ISCOM2600G series switch 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)#`**`match access-list`**`{` *`access-list`* `|` *`name`*`}`
	`Raisecom(config-cmap)#`**`exit`**
		(Optional) configure traffic classification over ACL rule. The ACL rule must be defined firstly and the type must be **permit**.

4	`Raisecom(config)#`**`policy-map`** *`policy-map-name`*
	`Raisecom(config-pmap)#`**`class-map`** *`class-map-name`*
		(Optional) configure traffic classification based on traffic classification rule.
		The traffic classification must have been created, and the matching type of its rule must be consistent with the

5	`Raisecom(config-cmap)#`**`match cos`** *`cos-value`*	(Optional) configure traffic classification based on CoS priority of packets.
6	`Raisecom(config-cmap)#`**`match inner-vlan`** *`inner-vlan-value`*	(Optional) configure traffic classification based on inner VLAN of packets.
7	`Raisecom(config-cmap)#`**`match vlan`** *`vlan-value`*	(Optional) configure traffic classification based on VLANs of packets.
8	`Raisecom(config-cmap)#`**`match dscp`** *`dscp-value`*	(Optional) configure traffic classification based on DSCP priority rule.

Note

- 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.

7.5.5 Creating rate limit rule and shapping rule

When you need to limit rate of packets based on traffic policy, create a token bucket, configure rate limit and shaping rules on the token bucket, quote these rules to traffic classification bound to the traffic policy.

Create rate limiting rules and shaping rule for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**mls qos policer-profile** *policer-name* [**single** | **hierarchy** | **aggregate**]	Create a traffic policer profile, and enter traffic-policer configuration mode.
3	Raisecom(traffic-policer)#**cir** *cir* **cbs** *cbs*	(Optional) configure flow mode token bucket parameters. Note Flow mode token bucket is single token bucket, only supporting to configure red and green packets operation.
4	Raisecom(traffic-policer)#**cir** *cir* **cbs** *cbs* **ebs** *ebs*	(Optional) configure RFC2697 mode token bucket parameters.
5	Raisecom(traffic-policer)#**cir** *cir* **cbs** *cbs* **pir** *pir* **pbs** *pbs*	(Optional) configure RFC2698 mode token bucket parameters.
6	Raisecom(traffic-policer)#**cir** *cir* **cbs** *cbs* **eir** *eir* **ebs** *ebs* [**coupling**]	(Optional) configure RFC4115 mode or MEF token bucket parameters.
7	Raisecom(traffic-policer)# **drop-color red**	(Optional) configure the token bucket to discard red packets.
8	Raisecom(traffic-policer)#**recolor** { **green-recolor red** | **red-recolor green** }	(Optional) configure packet recoloring.
9	Raisecom(traffic-policer)#**set-cos** { **green** *cos* | **red** *cos* }	(Optional) configure the mapping from packets color to CoS.
10	Raisecom(traffic-policer)#**set-dscp** { **green** *green-value* | **red** *red-value* }	(Optional) configure the mapping from packets color to DSCP.
11	Raisecom(traffic-policer)#**set-pri** { **green** *green-value* | **red** *red-value* }	(Optional) configure the mapping from packets color to local priority.

7.5.6 Creating traffic policy

Create traffic policy for the ISCOM2600G series switch 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 description of traffic policy.

7.5.7 Defining traffic policy mapping

Note

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

Define traffic policy mapping for the ISCOM2600G series switch 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 a traffic policy. The traffic policy is applied to the packets matching traffic classification. **Note** At least one rule is required for traffic classification to bind traffic policy, otherwise the binding will fail.

7.5.8 Defining traffic policy operation

Note

Define different operations to different flows in policy.

Define a traffic policy operation for the ISCOM2600G series switch 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 a traffic policy. The traffic policy is applied to the packets matching traffic classification. **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 the token bucket on traffic policy and conduct rate limiting and shaping. **Note** The token bucket needs to be created in advance and be configured with rate limiting and shaping rules; otherwise, the operation will fail.
6	Raisecom(config-pmap-c)#**redirect-to port** *port-id*	(Optional) configure redirection rules under traffic classification, forwarding classified packets from assigned interface.
7	Raisecom(config-pmap-c)#**set** { **cos** *cos-value* | **dscp** *dscp-value* | **local-priority** *value* }	(Optional) configure remarking rules under traffic classification, modify packet CoS priority, local priority, inner VLAN, DSCP priority, IP priority, and VLAN ID.
8	Raisecom(config-pmap-c)#**copy-to-mirror**	(Optional) configure traffic mirroring to the monitor interface.
9	Raisecom(config-pmap-c)#**statistics enable**	(Optional) configure traffic statistic rules under traffic classification, statistic packets for matched traffic classification.

7.5.9 Applying traffic policy to interfaces

Apply traffic policy to the interface for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**service-policy ingress** *policy-map-name*	Apply the configured traffic policy to the ingress direction of the interface.

7.5.10 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show service-policy statistics interface** *interface-type interface-number* **ingress policy-map** *policy-map-name* [**class-map** *class-map-name*]	Show statistics of applied traffic policy.
2	Raisecom#**show service-policy interface** [*interface-type interface-number*] [**ingress**]	Show information about the applied traffic policy.
3	Raisecom#**show class-map** [*class-map-name*]	Show information about traffic classification.
4	Raisecom#**show policy-map** [*policy-map-name*]	Show information about traffic policy.
5	Raisecom#**show policy-map** [*policy-map-name*] [**class** *class-map-name*]	Show information about traffic classification in traffic policy.
6	Raisecom#**show mls qos policer** [*policer-name*]	Show information about the assigned token bucket (rate limiting and shaping).

7.6 Configuring rate limiting

7.6.1 Preparing for configurations

Scenario

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

Prerequisite

N/A

7.6.2 Configuring rate limiting based on interface

Configure rate limiting based on interface for the ISCOM2600G series switch as below.

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

Step	Command	Description
3	Raisecom(config-gigaethernet1/1/1)#**rate-limit ingress cir** *cir-value* **cbs** *cbs-value*	Configure rate limiting based on interface.

Note

- By default, no interface-based rate limiting is configured.
- Adopt the drop processing mode for packets on the ingress interface if they exceed the configured rate limit.
- When you configure the rate limit and burst for an interface, the burst value should not be much greater if the configured rate limit is smaller than 256 kbit/s. Otherwise, packets may be inconsecutive.
- When the rate limit is too small, we recommend that the burst value is 4 times greater than then rate limit. If packets are inconsecutive, reduce the burst value or increase the rate limit.
- Packets discarded due to rate limiting on the egress interface are included in statistics of packet loss of the ingress interface.

7.6.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show rate-limit interface**	Show configurations of rate limiting on interfaces.
	Raisecom#**show rate-limit interface** *interface-type interface-number*	

7.7 Configuring examples

7.7.1 Example for configuring congestion management

Networking requirements

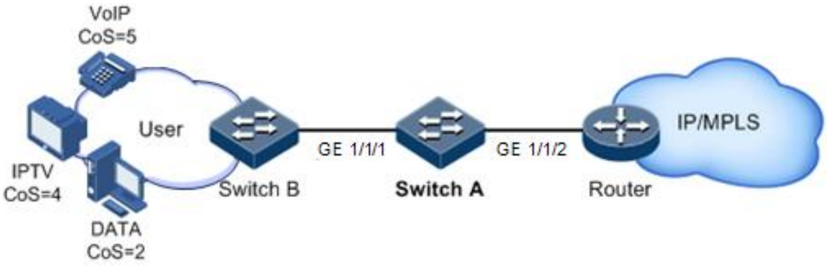
As shown in Figure 7-9, the user use voice, video and data services.

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

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

- For voice service, perform SP schedule to grant high priority.
- For video service, perform WRR schedule, with weight value of 50.
- For data service, perform WRR schedule, with weight value of 20.

Figure 7-9 Queue scheduling networking



Configuration steps

Step 1 Configure interface priority trust mode.

```
Raisecom#name SwitchA
SwitchA#config
SwitchA(config)#interface gigaethernet1/1/2
SwitchA(config-gigaethernet1/1/2)#mls qos trust cos
SwitchA(config-gigaethernet1/1/2)#quit
```

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

```
SwitchA(config)#mls qos mapping cos-to-local-priority 1
SwitchA(cos-to-pri)#cos 5 to local-priority 6
SwitchA(cos-to-pri)#cos 4 to local-priority 5
SwitchA(cos-to-pri)#cos 2 to local-priority 2
SwitchA(cos-to-pri)#quit
```

Step 3 Apply the profile for mapping between CoS priority and local priority on GE 1/1/2.

```
SwitchA(config)#interface gigaethernet1/1/2
SwitchA(config-gigaethernet1/1/2)#mls qos cos-to-local-priority 1
SwitchA(config-gigaethernet1/1/2)#quit
```

Step 4 Conduct SP+WRR queue scheduling in the egress direction of GE 1/1/1.

```
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#mls qos queue scheduler wrr 1 1 20 1 1
50 0 0
SwitchA(config-gigaethernet1/1/1)#quit
```

Checking results

Show priority trust mode on the interface.

```
Raisecom#show mls qos interface
Interface            TrustMode  Priority       Cos-PriProfile Dscp-
PriProfile Dscp-Mutation Cos-Remark
-------------------------------------------------------------------------
-------------------------------------
gigaethernet1/1/1      cos      0              0            0             0
0
gigaethernet1/1/2      cos      0              1            0             0
0
…
```

Show configurations of mapping between CoS priority and local priority

```
Raisecom#show mls qos mapping cos-to-local-priority
G:GREEN
Y:YELLOW
R:RED
cos-to-localpriority(color)
Index Description    Ref   CoS:          0      1      2      3      4
5      6      7
-------------------------------------------------------------------------
--------------------------------
1                   1    localpri(color) :0(G)   1(G)   2(G)   3(G)   5(G)
6(G)   6(G)   7(G)
```

Show configurations of queue scheduling on the interface.

```
Raisecom#show mls qos queue interface gigaethernet 1/1/1
gigaethernet1/1/1
Queue    Weight(WRR)
-------------------------
  1       1
  2       1
  3       20
  4       1
  5       1
  6       50
  7       0
  8       0
```

7.7.2 Example for configuring rate limiting based on traffic policy

Networking requirements

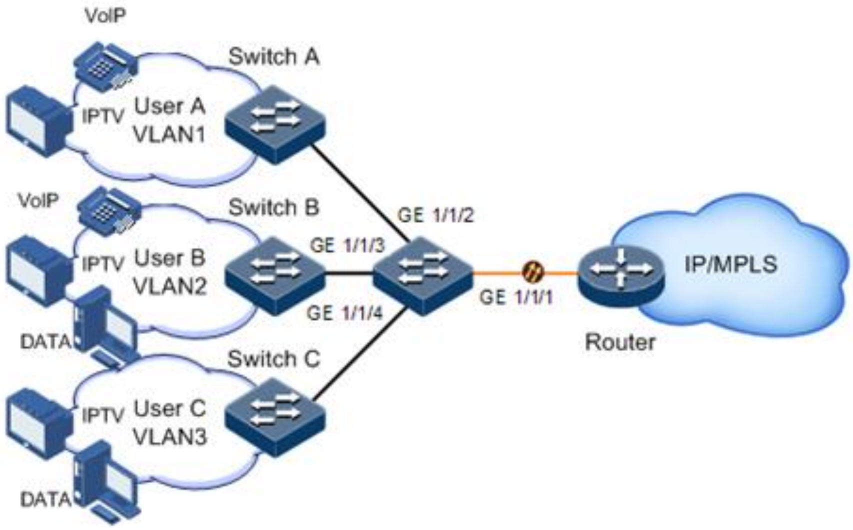
As show in Figure 7-10, User A, User B, and User C respectively belong to VLAN 1, VLAN 2, VLAN 3, and are connected to the Switch through Switch A, Switch B, Switch C.

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

According to service requirements, user needs to make rules as below.

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

Figure 7-10 Rate limiting based on traffic policy



Configuration steps

Step 1 Create and configure traffic classification, and classify users by VLAN ID.

```
Raisecom#config
Raisecom(config)#class-map usera match-any
Raisecom(config-cmap)#match vlan 1
Raisecom(config-cmap)#quit
Raisecom(config)#class-map userb match-any
Raisecom(config-cmap)#match vlan 2
Raisecom(config-cmap)#quit
Raisecom(config)#class-map userc match-any
Raisecom(config-cmap)#match vlan 3
Raisecom(config-cmap)#quit
```

Step 2 Create rate limiting rules.

```
Raisecom(config)#mls qos policer-profile usera single
Raisecom(traffic-policer)#cir 25000 cbs 100
Raisecom(traffic-policer)##quit
Raisecom(config)#mls qos policer-profile userb single
Raisecom(traffic-policer)#cir 35000 cbs 100
Raisecom(traffic-policer)##quit
Raisecom(config)#mls qos policer-profile userc single
Raisecom(traffic-policer)#cir 30000 cbs 100
Raisecom(traffic-policer)##quit
```

Step 3 Create and configure the traffic policy.

```
Raisecom(config)#policy-map usera
Raisecom(config-pmap)#class-map usera
Raisecom(config-pmap-c)#police usera
Raisecom(config-pmap-c)#quit
Raisecom(config-pmap)#quit
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#service-policy ingress usera
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#policy-map userb
Raisecom(config-pmap)#class-map userb
Raisecom(config-pmap-c)#police userb
Raisecom(config-pmap-c)#quit
Raisecom(config-pmap)#quit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#service-policy ingress userb
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#policy-map userc
Raisecom(config-pmap)#class-map userc
Raisecom(config-pmap-c)#police userc
Raisecom(config-pmap-c)#quit
Raisecom(config-pmap)#quit
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#service-policy userc ingress 4
Raisecom(config-gigaethernet1/1/1)#exit
```

Checking results

Use the **show class-map** command to show configurations of traffic classification.

```
Raisecom#show class-map usera
Class Map match-any usera (id 0)(ref 1)
    Match vlan 1
Raisecom#show class-map userb
 Class Map match-any userb (id 1)(ref 1)
```

```
    Match vlan 2
Raisecom#show class-map userc
 Class Map match-any userb (id 2)(ref 1)
    Match vlan 3
```

Use the **show mls qos policer** command to show configurations of rate limiting rules.

```
Raisecom(config)#show mls qos policer
single-policer: USERC        mode:flow   color:blind
cir: 30000 kbps  cbs: 100 kB

single-policer: usera        mode:flow   color:blind
cir: 25000 kbps  cbs: 100 kB

single-policer: userb        mode:flow   color:blind
cir: 35000 kbps  cbs: 100 kB
```

Use the **show policy-map** command to show configurations of traffic policy.

```
Raisecom(config)#show policy-map
  Policy Map usera
    Class usera
        police usera

  Policy Map userb
    Class userb
        police userb

  Policy Map userc
    Class userc
        police userc
```

7.7.3 Example for configuring rate limiting based on interface

Networking requirements

As shown in Figure 7-11, User A, User B, and User C are respectively connected to Switch A, Switch B, Switch C, and the ISCOM2600G series switch.

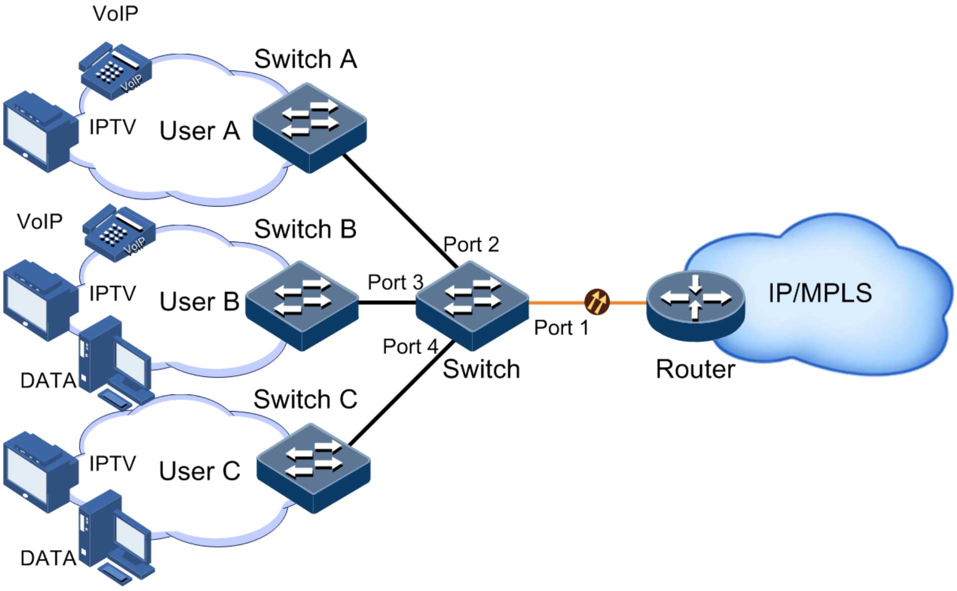
User A uses voice and video services. User B uses voice, video and data services. User C uses video and data services.

According to service requirements, make rules as below.

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

- For User C, provide 30 Mbit/s guaranteed bandwidth, permitting burst flow of 100 Kbytes and discarding redundant flow.

Figure 7-11 Rate limiting based on interface



Configuration steps

Configure rate limiting based on interface.

```
Raisecom#config
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#rate-limit ingress cir 25000 cbs 100
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#rate-limit ingress cir 35000 cbs 100
Raisecom(config-gigaethernet1/1/2)#exit
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#rate-limit ingress cir 30000 cbs 100
Raisecom(config-gigaethernet1/1/3)#exit
```

Checking results

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

```
Raisecom(config)#show rate-limit interface
Interface           Direction Cir(kbps)        Cbs(kb)
CirOper(kbps)        CbsOper(kb)
--------------------------------------------------------------------------
---------------------------------------
```

```
gigaethernet1/1/1     ingress  25000           100            25024
101
gigaethernet1/1/2     ingress  30000           100            30016
101
gigaethernet1/1/3     ingress  30000           100            30016
101
```

8 Multicast

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

- Introduction
- Basic functions of Layer 2 multicast
- IGMP Snooping
- IGMP MVR
- IGMP filtering

8.1 Introduction

8.1.1 Multicast

With the continuous development of Internet, more and more interactive data, voice, and video of various types 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 bring higher requirements on network bandwidth, information security, and paid feature. Traditional unicast and broadcast cannot meet these requirements well, while multicast has met them timely.

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

Comparison among unicast, broadcast, and multicast

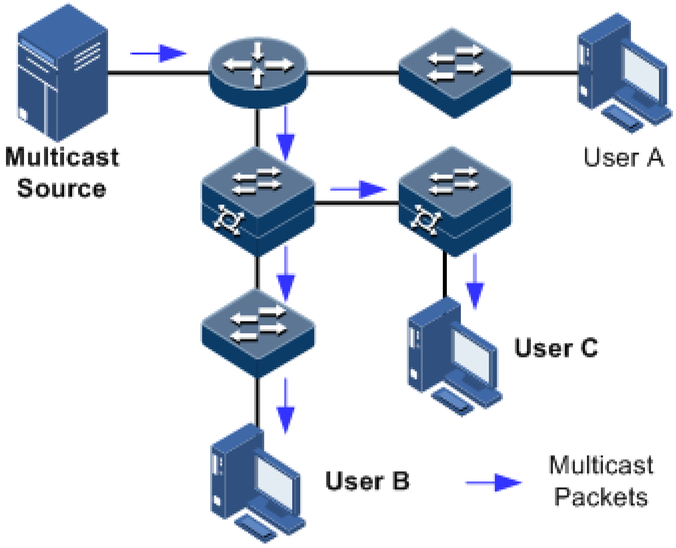
Multicast is a kind of packets transmission method which is parallel with unicast and broadcast.

- Unicast: the system establishes a data transmission path for each user who needs the information, and sends separate copy information about them. Through unicast, the amount of information transmitted over the network is proportional to the number of users, so when the number of users becomes huge, there will be more identical information on the network. In this case, bandwidth will become an bottleneck, and unicast will not be conducive to large-scale information transmission.

- Broadcast: the system sends information to all users regardless of whether they need or not, so any user will receive it. Through broadcast, the information source delivers information to all users in the segment, which fails to guarantee information security and paid service. In addition, when the number of users who require this kind of information decreases, the utilization of network resources will be very low, and the bandwidth will be wasted seriously.
- Multicast: when some users in the network need specific information, the sender only sends one piece of information, then the transmitted information can be reproduced and distributed in fork junction as far as possible.

As shown in Figure 8-1, assume that User B and User C need information, you can use multicast transmission to combine User B and User C to a receiver set, then the information source just needs to send one piece of information. Each switch on the network will establish their multicast forwarding table according to IGMP packets, and finally transmits the information to the actual receiver User B and User C.

Figure 8-1 Multicast transmission networking



In summary, the unicast is for a network with sparse users and broadcast is for a network with dense users. When the number of users in the network is uncertain, unicast and broadcast will present low efficiency. When the number of users are doubled and redoubled, the multicast mode does not need to increase backbone bandwidth, but sends information to the user in need. These advantages of multicast make itself become a hotspot in study of the current network technology.

Advantages and application of multicast

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

- Improve efficiency: reduce network traffic, relieve server and CPU load.
- Optimize performance: reduce redundant traffic and guarantee information security.
- Support distributed applications: solve the problem of point-point data transmission.

The multicast technology is used in the following aspects:

- Multimedia and streaming media, such as, network television, network radio, and realtime video/audio conferencing

- Training, cooperative operations communications, such as: distance education, telemedicine
- Data warehousing, financial applications (stock)
- Any other "point-to-multipoint" applications

Basic concepts in multicast

- Multicast group

A multicast group refers to the recipient set using the same IP multicast address identification. Any user host (or other receiving device) will become a member of the group after joining the multicast group. They can identify and receive multicast data with the destination address as IP multicast address.

- Multicast group members

Each host joining a multicast group will become a member of the multicast group. Multicast group members are dynamic, and hosts can join or leave multicast group at any time. Group members may be widely distributed in any part of the network.

- Multicast source

A multicast source refers to a server which regards multicast group address as the destination address to send IP packet. A multicast source can send data to multiple multicast groups; multiple multicast sources can send to a multicast group.

- Multicast router

A multicast router is a router that supports Layer 3 multicast. The multicast router can achieve multicast routing and guide multicast packet forwarding, and provide multicast group member management to distal segment connecting with users.

- Routed interface

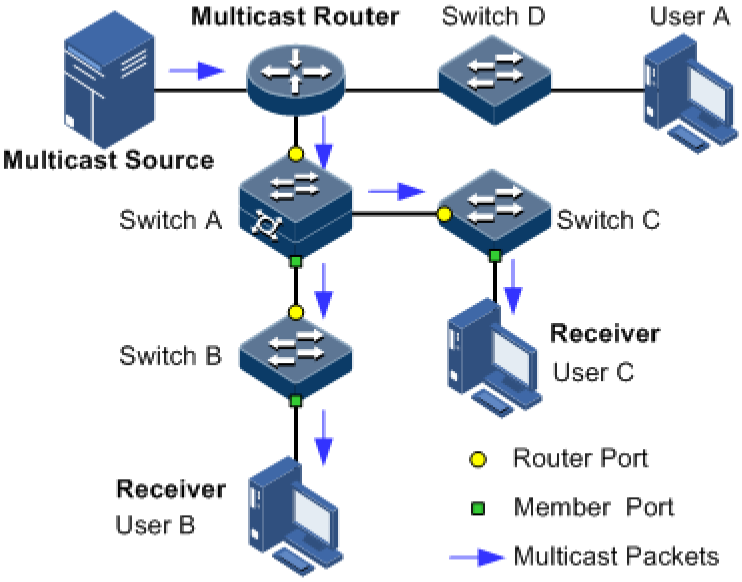
A routed interface refers to the interface towards the multicast router between a multicast router and a host. The ISCOM2600G series switch receives multicast packets from this interface.

- Member interface

Known as the Rx interface, a member interface is the interface towards the host between multicast router and the host. The ISCOM2600G series switch sends multicast packets from this interface.

Figure 8-2 shows basic concepts in multicast.

Figure 8-2 Basic concepts in multicast



Multicast address

To make multicast source and multicast group members communicate across the Internet, you need to provide network layer multicast address and link layer multicast address, namely, the IP multicast address and multicast MAC address.

- IP multicast address

Internet Assigned Numbers Authority (IANA) assigns Class D address space to IPv4 multicast; the IPv4 multicast address ranges from 224.0.0.0 to 239.255.255.255.

- Multicast MAC address

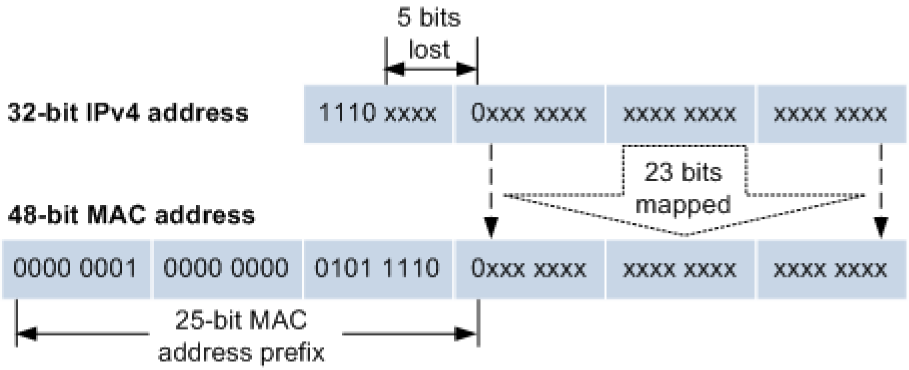
When the Ethernet transmits unicast IP packets, it uses the MAC address of the receiver as the destination MAC address. However, when multicast packets are transmitted, the destination is no longer a specific receiver, but a group with an uncertain number of members, so the Ethernet needs to use the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

The multicast MAC address identifies receivers of the same multicast group on the link layer.

According to IANA, high bit 24 of the multicast MAC address are 0x01005E, bit 25 is fixed to 0, and the low bit 23 corresponds to low bit 23 of the IPv4 multicast address.

Figure 8-3 shows mapping between the IPv4 multicast address and MAC address.

Figure 8-3 Mapping between IPv4 multicast address and multicast MAC address



The first 4 bits of IP multicast address are 1110, indicating multicast identification. In the last 28 bits, only 23 bits are mapped to the multicast MAC address, and the missing of 5 bits makes 32 IP multicast addresses mapped to the same multicast MAC address. Therefore, in Layer 2, the ISCOM2600G series switch may receive extra data besides IPv4 multicast group, and these extra multicast data needs to be filtered by the upper layer on the ISCOM2600G series switch.

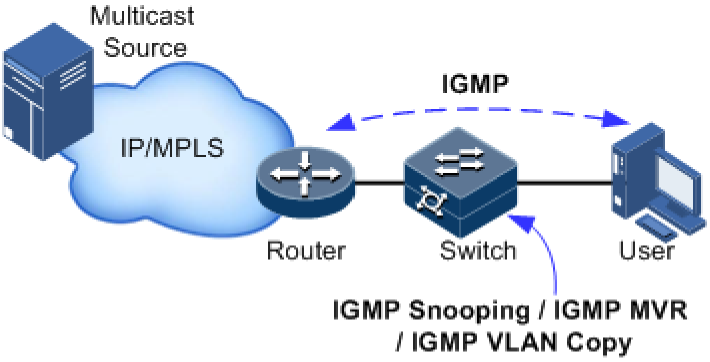
Basis of multicast protocol

To implement complete set of multicast services, you need to deploy a variety of multicast protocols in various positions of network and make them cooperate with each other.

Typically, IP multicast working at network layer is called Layer 3 multicast, so the corresponding multicast protocol is called Layer 3 multicast protocol, including Internet Group Management Protocol (IGMP). IP multicast working at data link layer is called Layer 2 multicast, so the corresponding multicast protocol is called Layer 2 multicast protocol, including Internet Group Management Protocol (IGMP) Snooping.

Figure 8-4 shows operating of IGMP and Layer 2 multicast features.

Figure 8-4 Operating of IGMP and Layer 2 multicast features



IGMP, a protocol in TCP/IP protocol suite, is responsible for managing IPv4 multicast members. IGMP runs between the multicast router and host, defines the establishment and maintenance mechanism of multicast group membership between hosts and the multicast router. IGMP is not involved in transmission and maintenance of group membership between multicast routers, which is completed by the multicast routing protocol.

IGMP manages group members through interaction of IGMP packets between the host and multicast router. IGMP packets are encapsulated in IP packets, including Query packets, Report packets, and Leave packets. Basic functions of IGMP are as below:

- The host sends Report packets to join the multicast group, sends Leave packets to leave the multicast group, and automatically determines which multicast group packets to receive.
- The multicast router sends Query packets periodically, and receives Report packets and Leave packets from hosts to understand the multicast group members in connected segment. The multicast data will be forwarded to the segment if there are multicast group members, and not forward if there are no multicast group members.

Up to now, IGMP has three versions: IGMPv1, IGMPv2, and IGMPv3. The newer version is fully compatible with the older version. Currently the most widely used version is IGMPv2, while IGMPv1 does not support the Leave packet.

Layer 2 multicast runs on Layer 2 devices between the host and multicast router.

Layer 2 multicast manages and controls multicast groups by monitoring and analyzing IGMP packets exchanged between hosts and multicast routers to implement forwarding multicast data at Layer 2 and suppress multicast data diffusion at Layer 2.

Supported multicast features

The ISCOM2600G series switch supports the following multicast features:

- Basic functions of IGMP
- IGMP Snooping
- IGMP Multicast VLAN Registration (MVR)
- IGMP filtering

Note

- IGMP Snooping and IGMP MVR can be enabled concurrently. Multicast VLAN copy and IGMP Snooping, or Multicast VLAN copy and IGMP MVR cannot be enabled concurrently.
- The ISCOM2600G series switch supports both IGMPv1 and IGMPv2.

8.2 Basic functions of Layer 2 multicast

8.2.1 Introduction

Basic IGMP functions are as below:

- Assign the multicast router interface.
- Enable immediate leave.
- Configure multicast forwarding entries and the aging time of router interfaces.
- Enable IGMP ring network forwarding.

Basic functions of Layer 2 multicast provide Layer 2 multicast common features, which must be used on the ISCOM2600G series switch enabled with IGMP Snooping or IGMP MVR.

Note

Configurations of basic function take effect on IGMP Snooping or IGMP MVR concurrently.

The concepts related to IGMP basic functions are as below.

Multicast router interface

The router interface can be learnt dynamically (learnt through IGMP query packets, on the condition that the multicast routing protocol is enabled on multicast routers) on Layer 2 multicast switch, or configured manually to forward downstream multicast report and leave packets to the router interface.

The router interface learnt dynamically has an aging time, while the router interface configured manually will not be aged.

Aging time

The configured aging time takes effect on both multicast forwarding entries and the router interface.

On Layer 2 switch running multicast function, each router interface learnt dynamically starts a timer, of which the expiration time is the aging time of IGMP Snooping. The router interface will be deleted if no IGMP Query packets are received in the aging time. The timer of the router interface will be updated when an IGMP Query packet is received.

Each multicast forwarding entry starts a timer, namely, the aging time of a multicast member. The expiration time is IGMP Snooping aging time. The multicast member will be deleted if no IGMP Report packets are received in the aging time. Update timeout for multicast forwarding entry when receiving IGMP Report packets. The timer of the multicast forwarding entry will be updated when an IGMP Report packet is received.

Immediate leave

On Layer 2 switch running multicast function, the system will not delete the corresponding multicast forwarding entry immediately, but wait until the entry is aged after sending Leave packets. You can enable this function to delete the corresponding multicast forwarding entry quickly when there are a large number of downstream users and adding or leaving is more frequently required.

Note

Only IGMPv2/v3 version supports immediate leave.

IGMP ring network forwarding

On Layer 2 switch running multicast function, IGMP ring network forwarding can be enabled on any type of interfaces.

Enabling IGMP ring network forwarding can implement multicast backup protection on the ring network, make multicast services more stable, and prevent link failure from causing multicast service failure.

IGMP ring network forwarding can be applied to the RRPS ring, STP/RSTP/MSTP ring, and G.8032 ring.

8.2.2 Preparing for configurations

Scenario

Basic functions of Layer 2 multicast provide common features of Layer 2 multicast, and must be used on the ISCOM2600G series switch enabled with IGMP Snooping or IGMP MVR.

Prerequisite

- Create VLANs.
- Add related interfaces to VLANs.

8.2.3 Default configurations of Layer 2 multicast basic functions

Default configurations of Layer 2 multicast basic functions are as below.

Function	Default value
IGMP immediate leave status	Disable
Multicast forwarding entry aging time	300s
Interface IGMP ring network forwarding status	Disable

8.2.4 Configuring basic functions of Layer 2 multicast

Configure basic functions of Layer 2 multicast for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`igmp mrouter vlan`** *`vlan-id interface-type interface-number`*	(Optional) configure multicast route interface.
3	`Raisecom(config)#`**`igmp immediate-leave`** *`interface-type interface-number`* **`vlan`** *`vlan-list`*	(Optional) configure immediate leave.
4	`Raisecom(config)#`**`igmp ring`** *`interface-type interface-number-list`*	(Optional) enable IGMP ring network forwarding on the interface.

8.2.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show igmp mrouter`**	Show configurations of the multicast route interface.
2	`Raisecom#`**`show igmp immediate-leave`** `[` *`interface-type interface-number`* `]`	Show configuration of immediate leave on Layer 2 multicast.
3	`Raisecom#`**`show igmp statistics`** `[` *`interface-type interface-number`* `]`	Show Layer 2 multicast statistics.

8.2.6 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description
`Raisecom(config)#`**`clear igmp statistics`** `[` *`interface-type interface-number`* `]`	Clear statistics of Layer 2 multicast IGMP.
`Raisecom(config)#`**`no igmp member`** *`interface-type interface-number`*	Delete a specified multicast forwarding entry.

8.3 IGMP Snooping

8.3.1 Introduction

IGMP Snooping is a multicast constraining mechanism running on Layer 2 devices, used for managing and controlling multicast groups, and implementing Layer 2 multicast.

IGMP Snooping allows the ISCOM2600G series switch to monitor IGMP sessions between the host and multicast router. When monitoring a group of IGMP Report from host, the ISCOM2600G series switch will add host-related interface to the forwarding entry of this group. Similarly, when a forwarding entry reaches the aging time, the ISCOM2600G series switch will delete host-related interface from the forwarding table.

IGMP Snooping forwards multicast data through Layer 2 multicast forwarding entry. When receiving multicast data, the ISCOM2600G series switch 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 ISCOM2600G series switch effectively.

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

Note

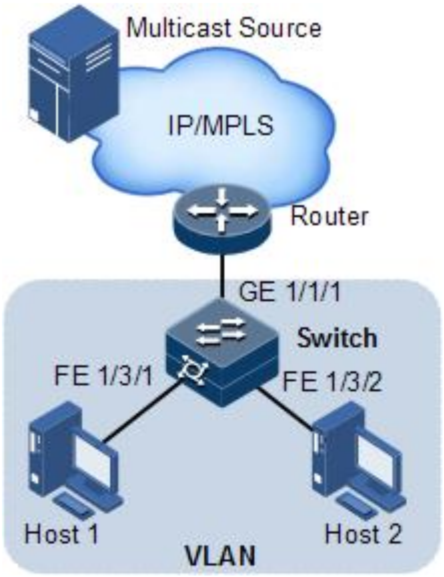
Currently, the ISCOM2600G series switch supports up to 1024 Layer 2 multicast entries.

8.3.2 Preparing for configurations

Scenario

As shown in Figure 8-5, multiple hosts belonging to a VLAN receive data from the multicast source. You can enable IGMP Snooping on the Switch that connects the multicast router and hosts. By listening IGMP packets transmitted between the multicast router and hosts, creating and maintaining the multicast forwarding table, you can implement Layer 2 multicast.

Figure 8-5 IGMP Snooping networking



Prerequisite

- Disable multicast VLAN copy on the ISCOM2600G series switch.
- Create VLANs.
- Add related interfaces to the VLANs.

8.3.3 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

8.3.4 Configuring IGMP Snooping

Configure IGMP Snooping for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`igmp snooping`**	Enable global IGMP Snooping.
3	`Raisecom(config)#`**`igmp snooping member time-out`** `{` *`seconds`* `|` **`infinite`** `}`	(Optional) configure the aging time of IGMP members.

8.3.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show igmp snooping`** `[` **`vlan`** *`vlan-list`* `]`	Show configurations of IGMP Snooping.
2	`Raisecom#`**`show igmp snooping member`** `[` *`interface-type interface-number`* `|` **`vlan`** *`vlan-id`* `]`	Show information about multicast group members of IGMP Snooping.
3	`Raisecom#`**`show igmp snooping vlan`** *`vlan-id`*	Show configurations of IGMP Snooping in the specified VLAN.

8.3.6 Example for applying multicast on ring network

Networking requirements

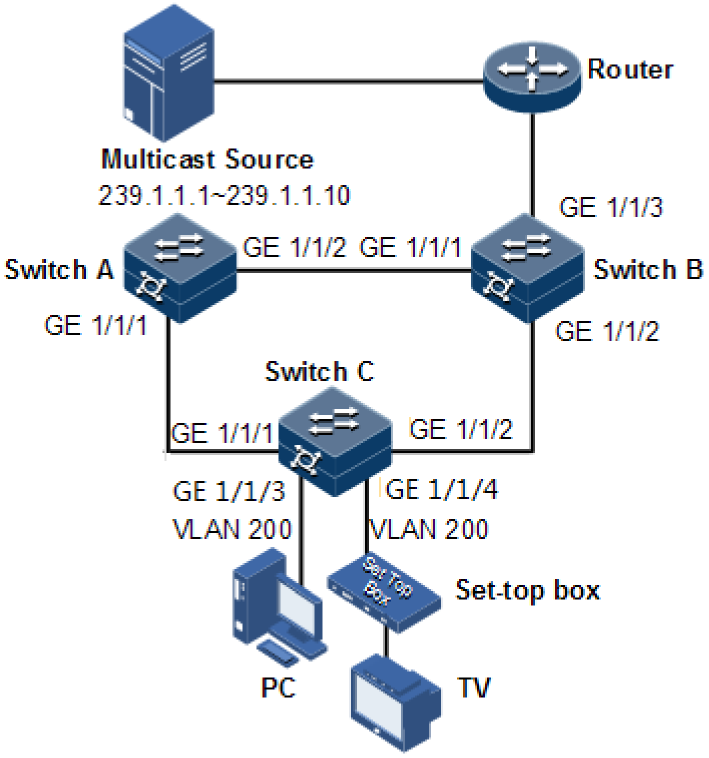
Configure IGMP ring forwarding on single Ethernet ring to make multicast service more stable and prevent multicast service from being disrupted by link failure.

As shown in Figure 8-6, GE 1/1/1 and GE 1/1/2 on Switch A, GE 1/1/1 and GE 1/1/2 on Switch B, GE 1/1/1 and GE 1/1/2 on Switch C form a physical ring. Multicast traffic is input from GE 1/1/1 on Switch B. The customer demands multicast traffic through GE 1/1/3 and GE 1/1/4 on Switch C. By doing this, it will not affect user's on-demand multicast stream whichever link fails in the Switch.

When using single Ethernet ring to provide multicast services, you can adopt IGMP MVR or IGMP Snooping to receive the multicast traffic.

The following example shows that STP provides ring network detection and IGMP Snooping provides multicast function.

Figure 8-6 Ring network multicast networking



Configuration steps

Step 1 Enable STP, create a VLAN, and add interfaces to the VLAN.

Configure Switch A.

```
SwitchA#config
SwitchA(config)#spanning-tree enable
SwitchA(config)#spanning-tree mode stp
SwitchA(config)#interface gigaethernet1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport mode trunk
SwitchA(config-gigaethernet1/1/1)#switchport trunk native vlan 200
SwitchA(config-gigaethernet1/1/1)#exit
SwitchA(config)#interface gigaethernet1/1/2
SwitchA(config-gigaethernet1/1/2)#switchport mode trunk
SwitchA(config-gigaethernet1/1/2)#switchport trunk native vlan 200
```

Configure Switch B.

```
SwitchB#config
SwitchB(config)#spanning-tree enable
SwitchB(config)#spanning-tree mode stp
SwitchB(config)#interface gigaethernet1/1/1
SwitchB(config-gigaethernet1/1/1)switchport mode trunk
SwitchB(config-gigaethernet1/1/1)#switchport trunk native vlan 200
SwitchB(config-gigaethernet1/1/1)#exit
SwitchB(config)#interface gigaethernet1/1/2
SwitchB(config-gigaethernet1/1/2)#switchport mode trunk
SwitchB(config-gigaethernet1/1/2)#switchport trunk native vlan 200
```

Configure Switch C.

```
SwitchC#config
SwitchC(config)#spanning-tree enable
SwitchC(config)#spanning-tree mode stp
SwitchC(config)#interface gigaethernet1/1/1
SwitchC(config-gigaethernet1/1/1)#switchport mode trunk
SwitchC(config-gigaethernet1/1/1)#switchport trunk native vlan 200
SwitchC(config-gigaethernet1/1/1)#exit
SwitchC(config)#interface gigaethernet1/1/2
SwitchC(config-gigaethernet1/1/2)#switchport mode trunk
SwitchC(config-gigaethernet1/1/2)#switchport trunk native vlan 200
```

Step 2 Enable IGMP Snooping and IGMP ring network forwarding on the interface.

Configure Switch A.

```
SwitchA(config)#igmp ring gigaethernet1/1/1
SwitchA(config)#igmp ring gigaethernet1/1/2
SwitchA(config)#igmp snooping
```

Configure Switch B.

```
SwitchB(config)#igmp ring gigaethernet1/1/1
SwitchB(config)#igmp ring gigaethernet1/1/2
SwitchB(config)#igmp snooping
```

Configure Switch C.

```
SwitchC(config)#igmp ring gigaethernet1/1/1
SwitchB(config)#igmp ring gigaethernet1/1/2
SwitchC(config)#igmp snooping
```

Checking results

Disconnect any link in the ring, and check whether the multicast flow can be received normally.

8.4 IGMP MVR

8.4.1 Introduction

IGMP 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.

IGMP MVR adds member interfaces belonging to different user VLAN in switch 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 IGMP 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 IGMP MVR can be different with user VLAN.

Note

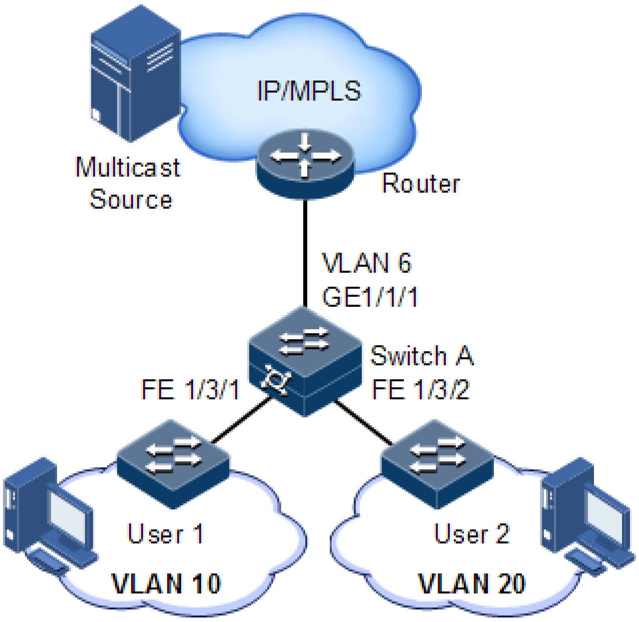
One switch can configure up to 10 multicast VLAN, at least one multicast VLAN and group addresses. The supported maximum number of multicast groups is 1024.

8.4.2 Preparing for configurations

Scenario

As shown in Figure 8-7, multiple users receive data from the multicast source. These users and the multicast router belong to different VLAN. Enable IGMP MVR on Switch A, and configure multicast VLAN. In this way, users in different VLAN can share a multicast VLAN to receive the same multicast data, and bandwidth waste is reduced.

Figure 8-7 IGMP MVR networking



Prerequisite

- Disable multicast VLAN copy.
- Create VLANs.
- Add related interfaces to the VLANs.

8.4.3 Default configurations of IGMP MVR

Default configurations of MVR are as below.

Function	Default value
Global IGMP MVR status	Disable
Interface IGMP MVR status	Disable
Multicast VLAN and group address set	N/A

8.4.4 Configuring IGMP MVR

Configure IGMP MVR for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#igmp mvr`	Enable global IGMP MVR.

Step	Command	Description
3	Raisecom(config)#**igmp mvr mcast-vlan** *vlan-id* **group** { *start-ip-address* [*end-ip-address*] | **any** }	Configure the group address set for multicast VLAN. Note After IGMP MVR is enabled, you need to configure multicast VLAN and bind group address set. If the received IGMP Report packet does not belong to a group address set of any VLAN, it is not processed and the user cannot make multicast traffic on demand.

8.4.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show igmp mvr**[*interface-type interface-number*]	Show configurations of IGMP MVR.
2	Raisecom#**show igmp mvr members** [*interface-type interface-number* | **user-vlan** *vlan-id*]	Show information about multicast group members of IGMP MVR.
3	Raisecom#**show igmp mvr vlan-group** [**mcast-vlan** *vlan-id*]	Show multicast VLAN and its group address set.

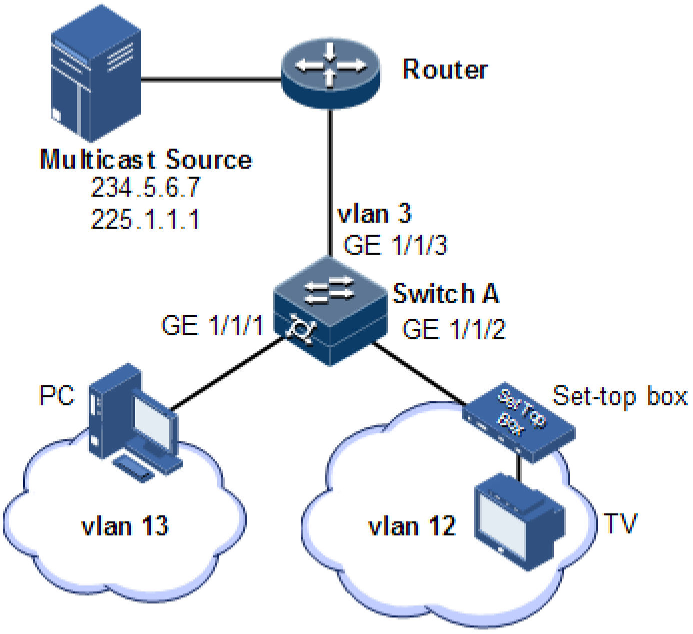
8.4.6 Example for configuring IGMP MVR

Networking requirements

As shown in Figure 8-8, GE 1/1/1 on Switch A connects with the multicast router, and GE 1/1/2 and GE 1/1/3 connect with users in different VLANs to receive data from multicast addresses 234.5.6.7 and 225.1.1.1.

Configure IGMP MVR on Switch A to specify VLAN 3 as a multicast VLAN, and then the multicast data needs to be duplicated with one copy in the multicast VLAN instead of copying for each customer VLAN, thus saving bandwidth.

Figure 8-8 MVR networking



Configuration steps

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

```
Raisecom(config)#config
Raisecom(config)#creat vlan 3,12,13 active
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport mode trunk
Raisecom(config-gigaethernet1/1/1)#switchport trunk native vlan 3
Raisecom(config-gigaethernet1/1/1)#switchport trunk untagged vlan 12,13
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet1/1/2
Raisecom(config-gigaethernet1/1/1)#switchport mode trunk
Raisecom(config-gigaethernet1/1/1)#switchport trunk native vlan 12
Raisecom(config-gigaethernet1/1/1)#switchport trunk untagged vlan 3
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet1/1/3
Raisecom(config-gigaethernet1/1/3)#switchport mode trunk
Raisecom(config-gigaethernet1/1/3)#switchport trunk native vlan 13
Raisecom(config-gigaethernet1/1/3)#switchport trunk untagged vlan 3
Raisecom(config-gigaethernet1/1/3)#exit
```

Step 2 Configure IGMP MVR on Switch A.

```
Raisecom(config)#igmp mvr
Raisecom(config)#interface gigaethernet1/1/1
Raisecom(config-gigaethernet1/1/1)#igmp mvr
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet1/1/2
Raisecom(config-gigaethernet1/1/2)#igmp mvr
Raisecom(config-gigaethernet1/1/2)#exit
Raisecom(config)#igmp mvr mcast-vlan 3 group 234.5.6.7
Raisecom(config)#igmp mvr mcast-vlan 3 group 225.1.1.1
```

Checking results

Use the following command to show IGMP MVR configurations on Switch A.

```
Raisecom#show igmp mvr
igmp mvr running              :Enable
igmp mvr port                 :GE1/1/1 GE1/1/2
igmp mvr multicast vlan(ref)    :3(2)
igmp aging time(s)            :300
igmp ring                   :--
```

Use the following command to show information about the multicast VLAN and group address.

```
Raisecom#show igmp mvr vlan-group
vlan      Port               Age        Type
-----------------------------------------------------
Raisecom(config)#show igmp mvr vlan-group
Mcast-vlan     Start-group    End-group
-------------------------------------------
3            225.1.1.1     225.1.1.1
3            234.5.6.7     234.5.6.7
```

8.5 IGMP filtering

8.5.1 Introduction

To control user access, you can configure IGMP filtering. IGMP filtering includes limiting the range of accessible multicast groups by using the filtering profile and limiting the maximum number of multicast groups.

- IGMP filter profile

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.

You can configure IGMP Profile filter profile 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 disallow the interface to receive this group of multicast data.

IGMP filter profile can be configured on an interface or interface+VLAN.

IGMP Profile only applies to dynamic multicast groups, but not static ones.

- Limit to the maximum number of multicast groups

You can configure the maximum number of multicast groups allowed to join based on interface or interface+VLAN and the rules to restrict the maximum number.

The maximum group number rule defines the actions to be taken for reaching the maximum number of multicast groups jointed by users, namely, disallowing new users to join the multicast group or overriding a joined group.

Note

IGMP filtering is generally used with IGMP Snooping/IGMP MVR/multicast VLAN copy.

8.5.2 Preparing for configurations

Scenario

Different users in the same multicast group receive different multicast requirements and permissions. You can configure filtering rules on the switch which connects the multicast router and user host to restrict multicast users. You also can configure the maximum number of multicast groups jointed by users. IGMP Proxy is generally used with IGMP Snooping or IGMP MVR.

Prerequisite

- Create VLANs.
- Add related interfaces to the VLANs.

8.5.3 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, no application filter profile
IGMP filtering under interface+VLAN	No maximum group limit, the largest group action is drop, no application filter profile

8.5.4 Enabling global IGMP filtering

Enable global IGMP filtering for the ISCOM2600G series switch as below.

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

Note

When configuring IGMP filter profile or the maximum group number, use the **igmp filter** command to enable global IGMP filtering.

8.5.5 Configuring IGMP filter profile

IGMP filter profile can be used to interface or interface+VLAN.

Configure IGMP filter profile for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode
2	Raisecom(config)#**igmp filter profile** *profile-number*	Create IGMP Profile and enter Profile configuration mode.
3	Raisecom(config-igmp-profile)#{ **permit** | **deny** }	Configure IGMP Profile action.
4	Raisecom(config-igmp-profile)#**range** *range-id start-ip-address* [*end-ip-address*]	Configure to control IP multicast address access and range.
5	Raisecom(config-igmp-profile)#**exit** Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode or LAG configuration mode.
6	Raisecom(config-gigaethernet1/1/1)#**igmp filter profile** *profile-number* [**vlan** *vlan-list*]	Configure IGMP Profile filter profile to physical interface or interface+VLAN.
	Raisecom(config-aggregator)#**igmp filter profile** *profile-number* [**vlan** *vlan-list*]	Configure IGMP Profile filter profile to LAG interface or interface+VLAN.

Note

Perform the command of **igmp filter profile** *profile-number* in interface configuration mode to make the created IGMP profile apply to the specified interface. One IGMP profile can be applied to multiple interfaces, but each interface can have only one IGMP profile.

8.5.6 Configuring maximum number of multicast groups

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

Configure the maximum number of multicast groups for the ISCOM2600G series switch 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 or LAG configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#**igmp filter max-groups** *group-number* [**vlan** *vlan-list*]	Configure the maximum number of multicast groups to physical interface or interface+VLAN.
	Raisecom(config-aggregator)#**igmp filter max-groups** *group-number* [**vlan** *vlan-list*]	Configure the maximum number of multicast groups to LAG interface or interface+VLAN.
4	Raisecom(config-gigaethernet1/1/1)#**igmp filter max-groups action** { **drop** | **replace** } [**vlan** *vlan-list*]	(Optional) configure the action over maximum number of multicast groups in physical interface or interface+VLAN.
	Raisecom(config-aggregator)#**igmp filter max-groups action** { **drop** | **replace** } [**vlan** *vlan-list*]	(Optional) configure the action over maximum number of multicast groups in LAG interface or interface+VLAN.

8.5.7 Checking configurations

Use the following commands to check configuration results.

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

8.5.8 Example for applying IGMP filtering on interface

Networking requirements

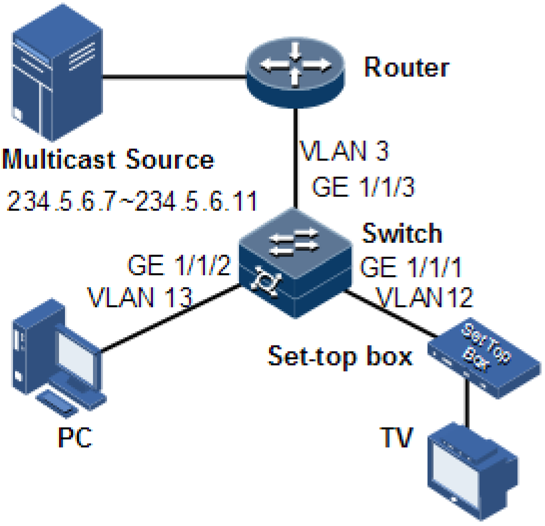
Enable IGMP filtering on the switch. Add filtering rules on the interface to filter multicast users.

As shown in Figure 8-9,

- Create an IGMP filtering rule Profile 1, and configure the action to pass for the multicast group ranging from 234.5.6.7 to 234.5.6.10.
- Apply filtering rule on GE 1/1/1, allow the STB to join the 234.5.6.7 multicast group, forbid it to join the 234.5.6.11 multicast group.
- Apply no filtering rule on Port 3, and allow PCs to join the 234.5.6.11 multicast group.

Configure the maximum number of multicast groups on GE 1/1/1. After the STB is added to the 234.5.6.7 multicast group, add it to the 234.5.6.8 multicast group while it quits the 234.5.6.7 multicast group.

Figure 8-9 Applying IGMP filtering on interface



Configuration steps

Step 1 Create VLANs, and add interfaces to VLANs.

```
Raisecom#config
Raisecom(config)#creat vlan 3,12,13 active
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport mode trunk
Raisecom(config-gigaethernet1/1/1)#switchport trunk native vlan 3
Raisecom(config-gigaethernet1/1/1)#switchport trunk untagged vlan 12,13
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport mode trunk
Raisecom(config-gigaethernet1/1/2)#switchport trunk native vlan 12
Raisecom(config-gigaethernet1/1/2)#switchport trunk untagged vlan 3
Raisecom(config-gigaethernet1/1/2)#exit
Raisecom(config)#interface gigaethernet1/1/3
Raisecom(config-gigaethernet1/1/3)#switchport mode trunk
Raisecom(config-gigaethernet1/1/3)#switchport trunk native vlan 13
Raisecom(config-gigaethernet1/1/3)#switchport trunk untagged vlan 3
Raisecom(config-gigaethernet1/1/3)#exit
```

Step 2 Enable IGMP MVR.

```
Raisecom(config)#igmp mvr
Raisecom(config)#interface gigaethernet1/1/1
Raisecom(config-gigaethernet1/1/1)#igmp mvr
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet1/1/2
Raisecom(config-gigaethernet1/1/2)#igmp mvr
Raisecom(config-gigaethernet1/1/2)#exit
Raisecom(config)#igmp mvr mcast-vlan 3 group any
```

Step 3 Configure the IGMP filtering profile.

```
Raisecom(config)#igmp filter profile 1
Raisecom(config-igmp-profile)#permit
Raisecom(config-igmp-profile)#range 1 234.5.6.7 234.5.6.10
Raisecom(config-igmp-profile)#exit
```

Step 4 Configure the STB to apply the IGMP filter profile.

```
Raisecom(config)#igmp filter
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#igmp filter profile 1
```

Step 5 Configure the maximum number of multicast groups on the STB interface.

```
Raisecom(config-gigaethernet1/1/1)#igmp filter max-groups 1
Raisecom(config-gigaethernet1/1/1)#igmp filter max-groups action replace
```

Checking results

Use the following command to show configurations of IGMP filtering on the interface.

```
Raisecom#show igmp filter gigaethernet 1/1/1
igmp profile:  1
max group:      1
current group:  0
action:       replace
```

9 Security

This chapter describes principles and configuration procedures of security, and provides related configuration examples, including the following sections.

- ACL
- Port security MAC
- Dynamic ARP inspection
- RADIUS
- TACACS+
- Storm control
- 802.1x
- IP Source Guard
- PPPoE+

9.1 ACL

9.1.1 Introduction

Access Control List (ACL) is a set of ordered rules, which can control the ISCOM2600G series switch to receive or refuse some data packets.

You need to configure rules on the network to prevent illegal packets from affecting network performance and determine the packets allowed to pass. These rules are defined by ACL.

ACL is a series of rule composed of permit | deny sentences. The rules are described according to source address, destination address, and port ID of data packets. The ISCOM2600G series switch judges receiving or rejecting packets according to the rules.

9.1.2 Preparing for configurations

Scenario

ACL can help a network device recognize filter data packets. The device recognizes special objects and then permits/denies packets to pass according to the configured policy.

ACL is divided into the following types:

- IP ACL: define classification rules according to source or destination address taken by packets IP head, port ID used by TCP or UDP (being 0 by default) attributes.
- MAC ACL: define classification rules according to source MAC address, destination MAC address, Layer 2 protocol type taken by packets Layer 2 frame head attributes.
- MAP ACL: MAP ACL can define more protocols and more detailed protocol fields than IP ACL and MAC ACL, also can match any bytes from byte 0 to byte 127 of Layer 2 data frame according to user's definition (the offset starts from 0).

There are 4 ACL modes according to difference of application environment:

- ACL based on device
- ACL based on interface
- ACL based on flow from ingress interface to egress interface
- ACL based on VLAN

Prerequisite

N/A

9.1.3 Configuring MAC ACL

Configure MAC ACL for the ISCOM2600G series switch as below.

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

Step	Command	Description
2	Raisecom(config)#**access-list** *acl-number* [**name** *acl-name*]	Create an ACL, and enter ACL configuration mode. ● When the ACL number is 1000–1999, this configuration enters basic IP ACL configuration mode. ● When the ACL number is 2000–2999, this configuration enters extended IP ACL configuration mode. ● When the ACL number is 3000–3999, this configuration enters MAC ACL configuration mode. ● When the ACL number is 5000–5999, this configuration enters User ACL configuration mode. ● When the ACL number is 6000–6999, this configuration enters IPv6 ACL configuration mode. ● When the ACL number is 7000–7999, this configuration enters advanced ACL configuration mode.
3	Raisecom(config-acl-ip-std)#**rule** [*rule-id*] { **deny** | **permit** } { *source-ip-address source-ip-mask* | **any** }	(Optional) configure the matching rule for basic IP ACL.
4	Raisecom(config-acl-ipv4-ext)# **rule** [*rule-id*] { **deny** | **permit** } { *protocol-id* | **icmp** | **igmp** | **ip** } { *source-ip-address source-ip-mask* | **any** } { *destination-ip-address destination-ip-mask* | **any** } [**dscp** *dscp-value*] [**ttl** *ttl-value*] [**fragment**] [**icmp-type** *icmp-type-value*] [**precedence** *precedence-value*] [**tos** *tos-value*]	(Optional) configure the matching rule for extended IP ACL.

Step	Command	Description
	Raisecom(config-acl-ipv4-advanced)# **rule** [*rule-id*] { **deny** | **permit** } { **tcp** | **udp** } { *source-ip-address source-ip-mask* | **any** } [*source-port*] [**range** *minimum source port maximum source port*] { *destination-ip-address destination-ip-mask* | **any** } [*destination-port*] [**ack** *ack-value*] [**dscp** *dscp-value*] [**fin** *fin-value*] [**fragment**] [**precedence** *precedence-value*] [**psh** *psh-valu*e] [**range** *minimum source port maximum source port*] [**rst** *rst-value*] [**syn** *syn-value*] [**tos** *tos-value*] [**urg** *urg-value*] [**ttl** *ttl-value*]	
5	Raisecom(config-acl-mac)#**rule** [*rule-id*] { **deny** | **permit** } { *source-mac-address source-mac-mask* | **any** } { *destination-mac-address destination-mac-mask* | **any** } [**ethertype** { *ethertype* [*ethertype-mask*] | **ip** | **arp** }] [**svlan** *svlanid*] [**cos** *cos-value*] [**cvlan** *cvlanid*] [**inner-cos** *inner-cos*]	(Optional) configure the matching rule for MAC ACL.
6	Raisecom(config-acl-udf)#**rule** [*rule-id*] { **deny** | **permit** } { **ipv4** | **layer2** } *rule-string rule-mask offset*	(Optional) configure the matching rule for User ACL.
7	Raisecom(config-acl-ipv6)#**rule** [*rule-id*] { **deny** | **permit** } { *protocol-id* | **ipv6** | **icmpv6** } { *source-ipv6-address/prefix* | **any** } { *destination- ipv6-address/prefix* | **any** } [**dscp** *dscp-value*] [**fragment**] [**flow-label** *flow label-value*] Raisecom(config-acl-ipv6)#**rule** [*rule-id*] { **deny** | **permit** } { **tcp** | **udp** } { *source-ipv6-address/prefix source-ip-mask* | **any** } { *destination-ipv6-address/prefix* | **any** } [*destination-port*] [**ack** *ack-value*] [**dscp** *dscp-value*] [**fin** *fin-value*] [**fragment**] [**flow-label** *flow label-value*] [**psh** *psh-valu*e] [**rst** *rst-value*] [**syn** *syn-value*] [**urg** *urg-value*]	(Optional) configure the matching rule for MAP ACL.

Step	Command	Description
8	Raisecom(config-acl-advanced)#**rule** [*rule-id*] { **deny** | **permit** } { *source-mac-address source-mac-mask* | **any** } { *destination-mac-address destination-mac-mask* | **any** } [**svlan** *svlanid*] [**cos** *cos-value*] [**cvlan** *cvlanid*] [**inner-cos** *inner-cos*] { *source-ip-address source-ip-mask* | **any** } { *destination-ip-address destination-ip-mask* | **any** }[**dscp** *dscp-value*] [**ttl** *ttl-value*] [**fragment**] [**precedence** *precedence-value*] [**tos** *tos-value*]	(Optional) configure the matching rule for advanced ACL.

9.1.4 Configuring filter

Configure the filter for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#**filter ingress access-list** *acl-number* [**statistics**]	Apply ACL on the interface.

9.1.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show access-list** [*acl-number*]	Show ACL configurations.
2	Raisecom#**show acl resource** { **egress** | **ingress** } *interface-type interface-number*	Show resources used by ACL.
3	Raisecom#**show filter interface**	Show filter configurations.
	Raisecom#**show filter interface** *interface-type interface-number* [**ingress**]	
	Raisecom#**show filter interface** *interface-type interface-number* [**ingress** | **egress**]	

9.2 Port security MAC

9.2.1 Introduction

Port security MAC is used for the switching device on the edge of the network user side, which can ensure security of accessed data on an interface, and control the incoming packets according to the source MAC address.

You can enable port security MAC to limit and distinguish which users can access the network through secure interfaces. Only secure MAC addresses can access the network, unsecure MAC addresses will be dealt with as configured interface access violation mode.

Secure MAC address classification

Secure MAC addresses supported by the device are divided into the following three categories:

- Static secure MAC address

The 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.

The dynamic secure MAC address can be converted to Sticky secure MAC address if necessary, so as not to be aged and supports auto-loading.

- Sticky secure MAC address

Sticky secure MAC address is generated from the manual configuration of user 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.
- 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, inputting of packets from a strange source MAC address will be regarded as a violation operation. For the illegal user access, there are different processing modes for configuring 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 an alarm to the NMS.
- Shutdown mode: for illegal access users, the secure interface will discard the user's packets, and the console will print Syslog information, send an alarm to the NMS, and then shut down the secure interface.

⚠ Caution

When the MAC address is flapping, namely, secure interface A is accessed by a user corresponding to a secure MAC address that is already on secure interface B, secure interface A will process the access as violation.

9.2.2 Preparing for configurations

Scenario

To ensure the security of data accessed by the interface of the switch, you can control the incoming 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

9.2.3 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	300s
Aging type of dynamic secure MAC address	Absolute
Restoration time of port security MAC	Disable, namely, no restoration
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

9.2.4 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.
- When the 802.1x interface adopts a MAC address-based authentication mode, port security MAC and 802.1x are mutually exclusive. We do not recommend co-configuring them concurrently.
- Port security MAC and interface-/interface VLAN-based MAC number limit are mutually exclusive, which cannot be configured concurrently.

Configure basic functions of secure MAC address for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**switchport port-security**	Enable port security MAC.
4	Raisecom(config-gigaethernet1/1/1)#**switchport port-security maximum** *maximum*	(Optional) configure the maximum number of secure MAC addresses.
5	Raisecom(config-gigaethernet1/1/1)#**switchport port-security violation** { **protect** | **restrict** | **shutdown** }	(Optional) configure secure MAC violation mode.
6	Raisecom(config-gigaethernet1/1/1)#**no port-security shutdown** Raisecom(config-gigaethernet1/1/1)#**exit**	(Optional) re-enable the interface which is shut down due to violating the secure MAC address.
7	Raisecom(config)#**port-security recovery-time** *second*	(Optional) configure the restoration time of port security MAC.

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.

9.2.5 Configuring static secure MAC address

Configure static secure MAC address for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**switchport port-security**	Enable port security MAC.
4	Raisecom(config-gigaethernet1/1/1)#**switchport port-security mac-address** *mac-address* **vlan** *vlan-id*	Configure static secure MAC address.

9.2.6 Configuring dynamic secure MAC address

Configure dynamic secure MAC address for the ISCOM2600G series switch 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.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-gigaethernet1/1/1)#**switchport port-security aging-type** { **absolute** | **inactivity** }	(Optional) configure the aging type of port security MAC addresses.
5	Raisecom(config-gigaethernet1/1/1)#**switchport port-security**	(Optional) enable port dynamic security MAC learning.
6	Raisecom(config-gigaethernet1/1/1)#**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.

9.2.7 Configuring Sticky secure MAC address

Caution

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

Configure Sticky secure MAC address for the ISCOM2600G series switch 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-portgigaethernet1/1/1)#**switchport port-security**	Enable port security MAC.
4	Raisecom(config-gigaethernet1/1/1)#**switchport port-security mac-address sticky**	Enable Sticky secure MAC learning.
5	Raisecom(config-gigaethernet1/1/1)#**switchport port-security mac-address sticky** *mac-address* **vlan** *vlan-id*	(Optional) manually configure Sticky secure MAC addresses.

Note

After Sticky secure MAC address learning is enabled, dynamic secure MAC address will be converted to Sticky secure MAC address; the manually configured Sticky secure MAC address will take effect.

9.2.8 Checking configurations

Use the following commands to check configuration results.

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

9.2.9 Maintenance

Maintain the ISCOM2600G series switch as below.

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

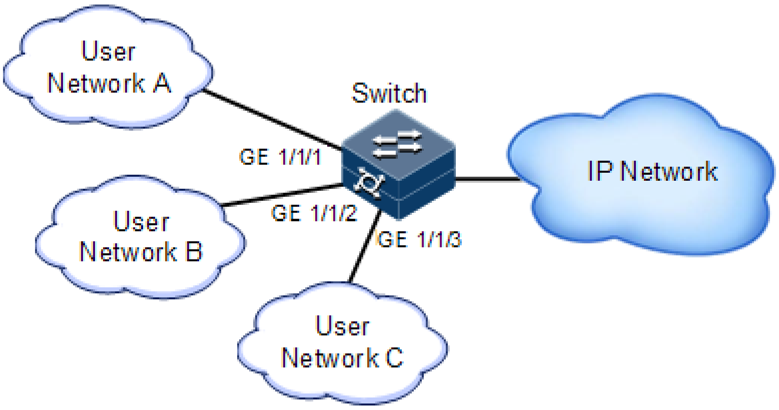
9.2.10 Example for configuring port security MAC

Networking requirements

As shown in Figure 9-1, the Switch connects 3 user networks. To ensure security of data accessing on the interface, configure the Switch as below.

- GE 1/1/1 allows up to 3 users to access the network. One of specified user MAC addresses is 0000.0000.0001. The other two users are in dynamic learning mode. The NMS can receive Trap information once the user learns a MAC address. The violation mode is Protect mode and the aging time of the two learning user MAC addresses is 10min.
- GE 1/1/2 allows up to 2 users to access the network. MAC addresses of the 2 users are determined through learning; once they are learnt, they will not be aged. The violation mode is Restrict mode.
- GE 1/1/3 allows up to 1 user to access the network. The specified user MAC address is 0000.0000.0002. Whether MAC addresses are aged can be controlled. The violation mode is Shutdown mode.

Figure 9-1 Port security MAC networking



Configuration steps

Step 1 Configure secure MAC address on GE 1/1/1.

```
Raisecom#config
Raisecom(config)#interface gigaethernet1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport port-security
Raisecom(config-gigaethernet1/1/1)#switchport port-security maximum 3
Raisecom(config-gigaethernet1/1/1)#switchport port-security mac-address
0000.0000.0001 vlan 1
Raisecom(config-gigaethernet1/1/1)#switchport port-security violation
protect
Raisecom(config-gigaethernet1/1/1)#switchport port-security trap enable
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#port-security aging-time 10
```

Step 2 Configure secure MAC address on GE 1/1/2.

```
Raisecom(config)#interface gigaethernet1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport port-security
Raisecom(config-gigaethernet1/1/2)#switchport port-security maximum 2
Raisecom(config-gigaethernet1/1/2)#switchport port-security mac-address
sticky
Raisecom(config-gigaethernet1/1/2)#switchport port-security violation
restrict
Raisecom(config-gigaethernet1/1/2)#exit
```

Step 3 Configure secure MAC address for GE 1/1/3.

```
Raisecom(config)#interface gigaethernet1/1/3
Raisecom(config-gigaethernet1/1/3)#switchport port-security
Raisecom(config-gigaethernet1/1/3)#switchport port-security maximum 1
Raisecom(config-gigaethernet1/1/3)#switchport port-security mac-address
sticky 0000.0000.0002 vlan 1
Raisecom(config-gigaethernet1/1/3)#switchport port-security mac-address
sticky
Raisecom(config-gigaethernet1/1/3)#switchport port-security violation
shutdown
```

Checking results

Use the **show port-security** command to show configurations of port security MAC.

```
Raisecom#show port-security
Port security aging time:10 (mins)
Port security recovery time:Disable (s)
port                  status    Max-Num   Cur-Num  His-MaxNum   vio-Count
vio-action Dynamic-Trap Aging-Type
-------------------------------------------------------------------------
-----------------------------------------
gigaethernet1/1/1       Enable    3        1       1          0
protect   Enable      Absolute
gigaethernet1/1/2       Enable    2        0       0          0
restrict  Disable     Absolute
gigaethernet1/1/3       Enable    1        1       1          0
shutdown  Disable     Absolute
gigaethernet1/1/4       Disable   1024      0       0          0
protect   Disable     Absolute
gigaethernet1/1/5       Disable   1024      0       0          0
…
```

Use the **show port-security mac-address** command to show configurations and learning of secure MAC address.

```
Raisecom#show port-security mac-address
VLAN  Security-MAC-Address  Flag            Port                  Age(min)
---------------------------------------------------------------------------
1     0000.0000.0001      Security-static   gigaethernet1/1/1       --
1     0000.0000.0002      sticky            gigaethernet1/1/3       --
```

9.3 Dynamic ARP inspection

9.3.1 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 9-2 Principles of dynamic ARP inspection

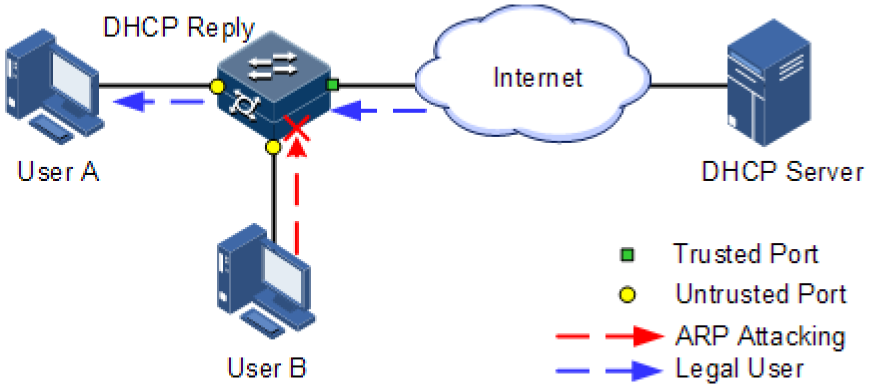


Figure 9-2 shows principles of dynamic ARP inspection. When the ISCOM2600G series switch receives an ARP packet, it compares the source IP address, source MAC address, interface number, and VLAN information of the ARP packet with the DHCP Snooping entry information. If matched, it indicates that it is 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 ISCOM2600G series switch by sending a large number of ARP packets to the ISCOM2600G series switch.

- When the number of ARP packets received by an interface per second exceeds the threshold, the system will determine that the interface encounters ARP attacks, and then discard all received ARP packets to avoid ARP attacks.
- 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.

9.3.2 Preparing for configurations

Scenario

Dynamic ARP inspection is used to prevent common ARP spoofing attacks on the network, which isolates ARP packets from unsafe sources. Whether to trust ARP packets depend on the trusting status of an interface while ARP packets meet requirements depends on the ARP binding table.

Prerequisite

Enable DHCP Snooping if there is a DHCP user.

9.3.3 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
Dynamic ARP inspection dynamic binding	Disable
Dynamic ARP inspection static binding table	N/A
Dynamic ARP inspection protection VLAN	All VLANs
Interface rate limiting on ARP packets	Disable
Interface rate limiting on ARP packets	60 pps
Auto-recovery rate limiting on ARP packets	Disable
Auto-recovery time for rate limiting on ARP packets	30s

9.3.4 Configuring trusted interfaces of dynamic ARP inspection

Configure trusted interfaces of dynamic ARP inspection for the ISCOM2600G series switch 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-gigaethernet1/1/1)#`**`ip arp-inspection trust`**	Configure the interface as a trusted interface. Use the **no ip arp-inspection trust** command to configure the interface to an untrusted interface, namely, the interface does not trust the ARP packet.

9.3.5 Configuring static binding of dynamic ARP inspection

Configure static binding of dynamic ARP inspection for the ISCOM2600G series switch 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.
3	`Raisecom(config)#`**`ip arp-inspection binding`** *`ip-address`* `[` *`mac-address`* `] [` **`vlan`** *`vlan-id`* `]` *`interface-type interface-number`*	Configure the static binding.

9.3.6 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 ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip arp-inspection dhcp-snooping**	Enable global dynamic ARP binding.

9.3.7 Configuring protection VLAN of dynamic ARP inspection

Configure protection VLAN of dynamic ARP inspection for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip arp-inspection dhcp-snooping**	Enable global dynamic ARP binding.
3	Raisecom(config)#**ip arp-inspection vlan** *vlan-list*	Configure protection VLAN of dynamic ARP inspection.

9.3.8 Configuring rate limiting on ARP packets on interface

Configure rate limiting on ARP packets on the interface for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**ip arp-rate-limit enable**	Enable interface ARP packet rate limiting.
4	Raisecom(config-gigaethernet1/1/1)#**ip arp-rate-limit rate** *rate-value*	Configure rate limiting on ARP packets on the interface.

9.3.9 Configuring auto-recovery time for rate limiting on ARP packets

Configure the auto-recovery time for rate limiting on ARP packets for the ISCOM2600G series switch 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.

9.3.10 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 [ interface-type interface-number ]`	Show information about the dynamic ARP inspection binding table.
3	`Raisecom#show ip arp-rate-limit`	Show configurations of rate limiting on ARP packets.

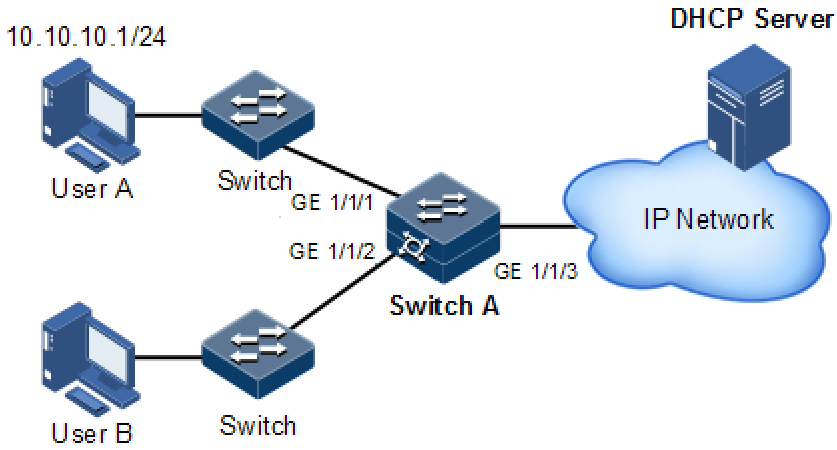
9.3.11 Example for configuring dynamic ARP inspection

Networking requirements

To prevent ARP attacks, configure dynamic ARP inspection on Switch A, as shown in Figure 9-3.

- Uplink GE 1/1/3 allows all ARP packets to pass.
- Downlink GE 1/1/1 allows ARP packets with specified IP address 10.10.10.1 to pass.
- Other interfaces allow ARP packets complying with dynamic binding learnt by DHCP Snooping to pass.
- Configure rate limiting on ARP packets on downlink GE 1/1/2. The rate threshold is configured to 20 pps and recovery time for rate limiting is configured to 15s.

Figure 9-3 Configuring dynamic ARP inspection



Configuration steps

Step 1 Configure GE 1/1/3 to the trusted interface.

```
Raisecom#config
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/3)#ip arp-inspection trust
Raisecom(config-gigaethernet1/1/3)#exit
```

Step 2 Configure static binding.

```
Raisecom(config)#ip arp-inspection static-config
Raisecom(config)#ip arp-inspection binding 10.10.10.1 gigaethernet 1/1/1
```

Step 3 Enable dynamic ARP inspection binding.

```
Raisecom(config)#ip dhcp snooping
Raisecom(config)#ip arp-inspection dhcp-snooping
```

Step 4 Configure rate limiting on ARP packets on the interface.

```
Raisecom(config)#interface gigaethernet1/1/2
Raisecom(config-gigaethernet1/1/2)#ip arp-rate-limit rate 20
Raisecom(config-gigaethernet1/1/2)#ip arp-rate-limit enable
Raisecom(config-gigaethernet1/1/2)#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
Static Config ARP Inspection: Enable
DHCP Snooping ARP Inspection: Disable
ARP Inspection Protect Vlan : 1-4094
Bind Rule Num             : 1
Vlan Rule Num             : 0
Bind Acl Num              : 1
Vlan Acl Num              : 0
Remained Acl Num           : 511

Port                        Trust
----------------------------------------
gigaethernet1/1/1              no
gigaethernet1/1/2              no
gigaethernet1/1/3              yes
gigaethernet1/1/4              no
gigaethernet1/1/5              no
gigaethernet1/1/6              no
gigaethernet1/1/7              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       --          --      gigaethernet1/1/1             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
-------------------------------------------------------------------------
--
gigaethernet1/1/1             Disabled       100           No
gigaethernet1/1/2             Enabled        20            No
gigaethernet1/1/3             Disabled       100           No
gigaethernet1/1/4             Disabled       100           No
gigaethernet1/1/5             Disabled       100           No
gigaethernet1/1/6             Disabled       100           No
……
```

9.4 RADIUS

9.4.1 Introduction

Remote Authentication Dial In User Service (RADIUS) is a standard communication protocol that provides centralized authentication of remote access users. RADIUS uses UDP as the transmission protocol (port 1812 and port 1813) which has a good instantaneity; at the same time, RADIUS features good reliability by supporting retransmission mechanism and standby server mechanism.

RADIUS authentication

RADIUS adopts client/server mode. The network access device is used as client of RADIUS server. The RADIUS server receives user connection requests, authenticates users, and replies them with configurations for providing services. In this way, RADIUS can control user to access devices and network, thus improving network security.

Communication between clients and RADIUS server is authenticated by the shared key, which will not be transmitted on the network. Besides, any user password to be transmitted between clients and RADIUS server must be encrypted to prevent it from being intercepted through sniffing through any insecure network.

RADIUS accounting

RADIUS accounting is used on users that have passed RADIUS authentication. When a user logs in, the device sends an Account-Start packet to the RADIUS accounting server. During user login, the device sends Account-Update packets to the RADIUS accounting server according to the accounting policy. When the user logs off, the device sends an Accounting-Stop packet, which contains user online time, to the RADIUS accounting server. The RADIUS accounting server can record the access time and operations of each user through these packets.

9.4.2 Preparing for configurations

Scenario

You can deploy the RADIUS server on the network to conduct authentication and accounting to control users to access to the ISCOM2600G series switch and network. The ISCOM2600G series switch can be used as agent of the RADIUS server, which authorizes user to access according to feedback from RADIUS.

Prerequisite

N/A

9.4.3 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
Port ID of RADIUS authentication server	1812
Port ID of RADIUS accounting server	1813
Shared key used for communication with RADIUS accounting server	N/A
Accounting failure processing policy	Online
Period for sending update packet	0

9.4.4 Configuring RADIUS authentication

Configure RADIUS authentication for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`radius [ backup ]`** *`ip-address`* `[` **`auth-port`** *`port-id`* `] [` **`vpn-instance`** *`vrf-name`* `] [` **`sourceip`** *`ip-address`* `]`	Assign the IP address and port ID for RADIUS authentication server. Configure the **backup** parameter to assign the backup RADIUS authentication server.
2	`Raisecom#`**`radius-key`** *`string`*	Configure the shared key for RADIUS authentication.

Step	Command	Description
3	Raisecom#**user login** { **local-radius** | **local-user** | **radius-local** [**server-no-response**] | **radius-user** | **local-tacacs** | **tacacs-local** [**server-no-response**] | **tacacs-user** }	Configure users to perform login authentication through RADIUS.

9.4.5 Configuring RADIUS accounting

Configure RADIUS accounting for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**aaa accounting login enable**	Enable RADIUS accounting.
2	Raisecom#**radius** [**backup**] **accounting-server** *ip-address* [*account-port*] [**sourceip** *ip-address*]	Assign IP address and UDP port ID for RADIUS accounting server. Configure the **backup** parameter to assign the backup RADIUS accounting server.
3	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.
4	Raisecom#**aaa accounting fail** { **offline** | **online** }	Configure the processing policy for accounting failure.
5	Raisecom#**aaa accounting update** *minute*	Configure the period for sending accounting update packets. If it is configured to 0, no Account-Update packet will be 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.

9.4.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show radius-server**	Show configurations of the RADIUS server.

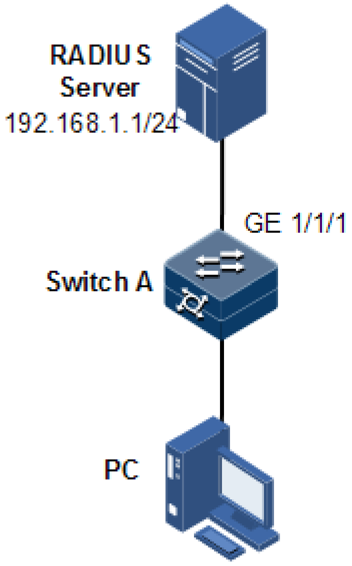
No.	Command	Description
2	`Raisecom#show aaa`	Show configurations of RADIUS accounting.

9.4.7 Example for configuring RADIUS

Networking requirements

As shown in Figure 9-4, to control a user from accessing the Switch, you need to configure RADIUS authentication and accounting on Switch A to authenticate login users on Switch A and record the operations. The period for sending update packets is 2 minutes. The user will be logged out if accounting fails.

Figure 9-4 RADIUS networking



Configuration steps

Step 1 Configure authentication for login user through RADIUS.

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

Step 2 Configure accounting for login user 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** to show RADIUS configurations.

```
Raisecom#show radius-server
Authentication server IP:      192.168.1.1 port:1812
Backup authentication server IP: port:1812
Authentication server key:     I+NNa9uluaix
Backup authentication server Key:      --
Accounting server IP:         192.168.1.1 port:1813
Backup accounting server IP:    port:1813
Accounting server key:        orMCKszV2X38
Backup Accounting server Key:         --
Accounting login:            enable
Update interval(minute):      2
Accounting fail policy:       offline
Auth vpn instance name:
Backup auth vpn instance name:
Accounting vpn instance name:
Backup accounting vpn instance name:
Authentation source ip:
Authentation backup source ip:
Accounting source ip:
Accounting backup source ip:
```

Use the **show aaa** command to show RADIUS accounting.

```
Raisecom#show aaa
Accounting login:            enable
Update interval(minute):      2
Accounting fail policy:       offline
```

9.5 TACACS+

9.5.1 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.

9.5.2 Preparing for configurations

Scenario

You can authenticate and account on users by deploying a TACACS+ server on the network to control users to access the ISCOM2600G series switch and network. TACACS+ is safer and more reliable than RADIUS. The ISCOM2600G series switch can be used as an agent of the TACACS+ server, and authorize users access according to feedback result from the TACACS+ server.

Prerequisite

N/A

9.5.3 Default configurations of TACACS+

Default configurations of TACACS+ are as below.

Function	Default value
TACACS+ function	Disable
Login mode	local-user
IP address of the TACACS+ authentication server	0.0.0.0, shown as "--"
IP address of the TACACS+ accounting server	0.0.0.0, shown as "--"
Shared key for communicating with the TACACS+ accounting server	N/A
Accounting failure processing policy	Online
Period for sending update packet	0

9.5.4 Configuring TACACS+ authentication

Configure TACACS+ authentication for the ISCOM2600G series switch as below.

Step	Command	Description

1	`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.

Step	Command	Description
2	Raisecom#**tacacs-server key** *string*	Configure the shared key for TACACS+ authentication.
3	Raisecom#**user login** { **local-tacacs** | **tacacs-local** [**server-no-response**] | **tacacs-user** }	Configure users to perform login authentication through TACACS+.
4	Raisecom#**enable login** { **local-tacacs** | **tacacs-local** [**server-no-response**] | **tacacs-user** }	Configure the authentication mode for users to enter privileged EXEC mode to TACACS+.

9.5.5 Configuring TACACS+ accounting

Configure TACACS+ accounting for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**aaa accounting login enable**	Enable TACACS+ accounting.
2	Raisecom#**tacacs** [**backup**] **accounting-server** *ip-address*	Assign the IP address and UDP port ID for the TACACS+ accounting server. Configure the **backup** parameter to assign the backup TACACS+ accounting server.
3	Raisecom#**tacacs-server key** *string*	Configure the shared key to communicate with the TACACS+ accounting server.
4	Raisecom#**aaa accounting fail** { **offline** | **online** }	Configure the processing policy for accounting failure.
5	Raisecom#**aaa accounting update** *period*	Configure the period for sending accounting update packets. If it is configured to 0, no Account-Update packet will be sent.

9.5.6 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.
2	Raisecom#**show aaa**	Show configurations of TACACS+ accounting.

9.5.7 Maintenance

Maintain the ISCOM2600G series switch as below.

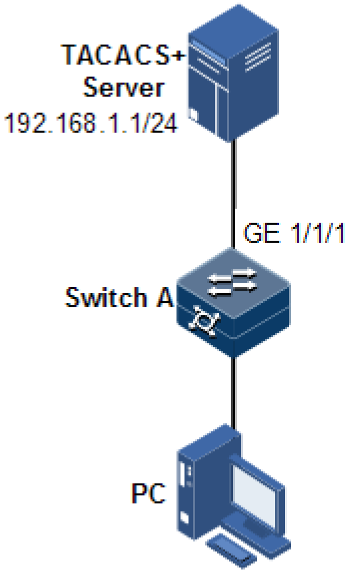
Command	Description
`Raisecom#clear tacacs statistics`	Clear TACACS+ statistics.

9.5.8 Example for configuring TACACS+

Networking requirements

As shown in Figure 9-5, configure TACACS+ authentication on Switch A to authenticate login user and control users from accessing the ISCOM2600G series switch.

Figure 9-5 TACACS+ networking



Configuration steps

Configure user login authentication 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
```

```
Port:  --
Backup Server Address         : --
Port:  --
Server Shared Key            : oLMCKszV2X38
Backup Authentication server Shared Key:       --
Accounting server Address      : --
port:  --
Backup Accounting server Address: --
Port:  --
Accounting server Shared Key:                --
Backup Accounting server Shared Key:          --
Total Packet Sent               : 0
Total Packet Recv               : 0
Num of Error Packets             : 0
Auth vpn instance name           : --
Backup auth vpn instance name     : --
Accounting vpn instance name      : --
Backup accounting vpn instance name: --
Authentication source ip         : --
Authentication backup source ip   : --
Accounting source ip             : --
Accounting backup source ip       : --
```

9.6 Storm control

9.6.1 Introduction

The Layer 2 network is a broadcast domain. When an interface receives excessive broadcast, unknown multicast, and unknown unicast packets, broadcast storm occurs. If you do not control broadcast packets, broadcast storm may occur and occupies much network bandwidth. Broadcast storm can degrade network performance and impact forwarding of unicast packets or even lead to communication halt.

Restricting broadcast flow generated from network on Layer 2 device can suppress broadcast storm and ensure common unicast forwarding normally.

Occurrence of broadcast storm

The following flows may cause broadcast flow:

- Unknown unicast packets: unicast packets of which the destination MAC is not in the MAC address table, namely, the Destination Lookup Failure (DLF) packets. If these packets are excessive in a period, the system floods them and broadcast storm may occur.
- Unknown multicast packets: the ISCOM2600G series switch neither supports multicast nor has a multicast MAC address table, so it processes received multicast packets as unknown multicast packets.
- Broadcast packets: packets of which the destination MAC is a broadcast address. If these packets are excessive in a period, broadcast storm may occur.

Principles of storm control

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.

Types of storm control

Storm controls is performed in the following forms:

- Radio (bandwidth ratio): the allowed percentage of broadcast, unknown multicast, or unknown unicast traffic to total bandwidth
- Bits Per Second (BPS): the number of bits allowed to pass per second
- Packet Per Second (PPS): the number of packets allowed to pass per second

The ISCOM2600G series switch supports BPS and PPS storm control.

9.6.2 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, normal packets can be properly forwarded.

Prerequisite

N/A

9.6.3 Default configurations of storm control

Default configurations of storm control are as below.

Function	Default value
Broadcast storm control	Enable
Multicast and unknown unicast storm control	Disable
Bytes of frame gap and preamble	20 bytes
Storm control mode	bps
Bytes per second	64 kbit/s
Number of allowed storm packets per second	1024 pps
DLF packet forwarding	Enable

9.6.4 Configuring storm control

Caution

Storm control and VLAN-based rate limiting are exclusive. We do not recommend enabling them on the same interface concurrently.

Configure storm control for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**storm-control** { **broadcast** | **unknown-multicast** | **dlf** | **all** } { **kbps** *value* | **pps** *value* }	Enable storm control, and configure the storm control threshold.

Caution

The ISCOM2600G series switch does not support configuring multiple control modes on the same interface regardless whether storm control is enabled. To change the control mode and control threshold of some packet on the interface, perform one of the following operations:

- If the value is configured to the default one, the control modes and control thresholds of all packets on an interface are identical.
- If the value is not configured to the default one, configurations fail. In addition, the system asks you to delete configurations on the interface in advance. In this case, you should configure the control threshold of all packets in a control mode to the default value. In addition, you should configure control modes of all packets and then configure other control thresholds.

9.6.5 Configuring DLF packet forwarding

Configure DLF packet forwarding for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**dlf-forwarding enable**	Enable DLF packet forwarding on an interface.

9.6.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show storm-control [ interface-type interface-number ]`	Show configurations of storm control.
2	`Raisecom#show dlf-forwarding`	Show DLF packet forwarding status.

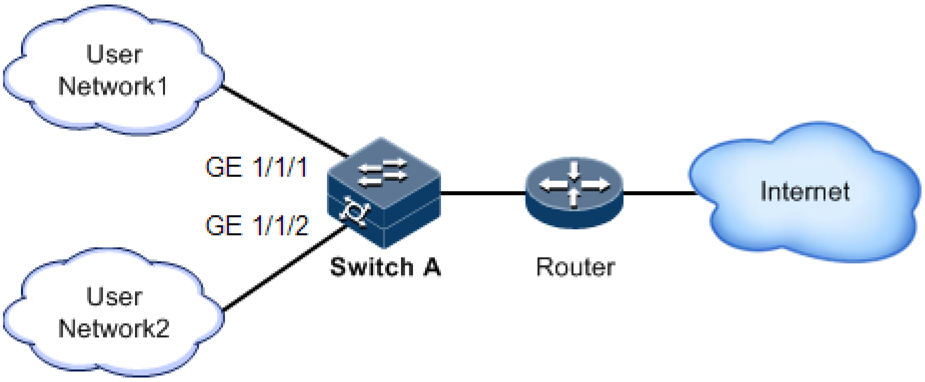
9.6.7 Example for configuring storm control

Networking requirements

As shown in Figure 9-6, when GE 1/1/1 and GE 1/1/2 on the Switch receive excessive unknown unicast packets or broadcast packets, the Switch forwards these packets to all interfaces except the Rx interface, which may cause broadcast storm and lower forwarding performance of the Switch.

To restrict impacts on Switch A caused by broadcast storm, you need to configure storm control on Switch A to control broadcast packets from user networks 1 and 2, with the threshold of 640 pps.

Figure 9-6 Storm control networking



Configuration steps

Step 1 Enable storm control, and configure the threshold for storm control.

```
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#storm-control broadcast kbps 640
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#storm-control broadcast kbps 640
```

Checking results

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

```
Raisecom#show storm-control
Interface               Packet-Type   Threshold    Unit
--------------------------------------------------------------
gigaethernet1/1/1        Broadcast     640          kbps
                      Multicast     0           --
                      Unicast       640         kbps
--------------------------------------------------------------
gigaethernet1/1/2        Broadcast     640          kbps
                      Multicast     0           --
                      Unicast       640         kbps
--------------------------------------------------------------
gigaethernet1/1/3        Broadcast     64           kbps
                      Multicast     0           --
                      Unicast       0           --
--------------------------------------------------------------
gigaethernet1/1/4        Broadcast     64           kbps
                      Multicast     0           --
                      Unicast       0           --
--------------------------------------------------------------
gigaethernet1/1/5        Broadcast     64           kbps
                      Multicast     0           --
                      Unicast       0           --
…
```

9.7 802.1x

9.7.1 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.

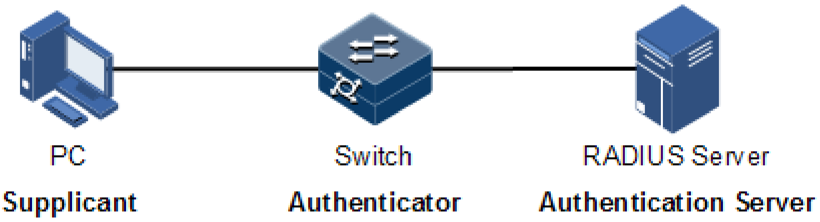
It is used to authenticate and control access devices at the physical later of the network device. It defines a point-to-point connection mode between the device interface and user devices. User devices, connected to the interface, can access resources in the LAN if they are authenticated. Otherwise, they cannot access resources in the LAN through the switch.

802.1x structure

As shown in Figure 9-7, 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 9-7 802.1x 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, namely, users are disallowed to be authenticated.

802.1x authentication procedure

The 802.1x system supports finishing authentication procedure between the RADIUS server through EAP relay and EAP termination.

- EAP relay

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) packets. 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. This procedure is call EAP relay.

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 the received user name with the one in the database, finds the password for the user, and encrypts the password with a randomly-generated encryption word. Meanwhile it sends the encryption word to the authenticator who then sends the encryption word to the suppliant.

Step 6 The suppliant encrypts the password with the received encryption password, and sends the encrypted password to the authentication server.

Step 7 The authentication server compares with received encrypted password with the one generated by itself. 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.

- EAP termination

Terminate the EAP packet at the device and map it to the RADIUS packet. Use standard RADIUS protocol to finish the authorization, authentication, and accounting procedure. The device and RADIUS server adopt Password Authentication Protocol (PAP)/Challenge Handshake Authentication Protocol (CHAP) to perform authentication.

In the EAP termination mode, the random encryption character, used for encrypting the password, is generated by the device. And then the device sends the user name, random encryption character, and encrypted password to the RADIUS server for authentication.

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 ISCOM2600G series switch re-initiates authorization.
- Quiet-period: quiet timer. When user authorization fails, the ISCOM2600G series switch needs to keep quiet for a period. After the period is exceeded, the ISCOM2600G series switch re-initiates authorization. During the quiet time, the ISCOM2600G series switch does not process authorization packets.
- Tx-period: transmission timeout timer. When the ISCOM2600G series switch sends a Request/Identity packet to users, the ISCOM2600G series switch will initiate the timer. If users do not send an authorization response packet during the tx-period, the ISCOM2600G series switch will re-send an authorization request packet. The ISCOM2600G series switch sends this packet three times in total.
- Supp-timeout: Supplicant authorization timeout timer. When the ISCOM2600G series switch sends a Request/Challenge packet to users, the ISCOM2600G series switch will initiate supp-timeout timer. If users do not send an authorization response packet during the supp-timeout, the ISCOM2600G series switch will re-send the Request/Challenge packet. The ISCOM2600G series switch 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 the RADIUS server and start a new authorization process.

9.7.2 Preparing for configiruations

Scenario

To realize access authentication on LAN users and ensure access user security, you need to configure 802.1x authentication on the ISCOM2600G series switch.

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 ISCOM2600G series switch can ping through the RADIUS server successfully.

9.7.3 Default configurations of 802.1x

Default configurations of 802.1x are as below.

Function	Default value
Global 802.1x	Disable
Interface 802.1x	Disable
Global authentication mode	Chap
Interface access control mode	Auto
Authentication method	Portbased
Re-authentication	Disable
802.1x re-authentication timer	3600s
802.1x quiet timer	60s
transmission timeout timer	30s
Supplicant authorization timeout timer	30s

9.7.4 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 ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**dot1x enable**	Enable global 802.1x.
3	Raisecom(config)#**dot1x authentication-method** { **chap** | **pap** | **eap** }	Configure global authentication mode.
4	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
5	Raisecom(config-gigaethernet1/1/1)#**dot1x enable**	Enable interface 802.1x.
6	Raisecom(config-gigaethernet1/1/1)#**dot1x auth-control** { **auto** | **authorized-force** | **unauthorized-force** }	Configure access control mode on the interface.
7	Raisecom(config-gigaethernet1/1/1)#**dot1x auth-method** { **portbased** | **macbased** }	Configure access control mode of 802.1x authentication on the interface.

Note

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.

9.7.5 Configuring 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.

Configure 802.1x re-authentication for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**dot1x reauthentication enable**	Enable 802.1x re-authentication.

9.7.6 Configuring 802.1x timers

Configure 802.1x timers for the ISCOM2600G series switch 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-gigaethernet1/1/1)#`**`dot1x timer reauth-period`** *`reauth-period`*	Configure the time of the re-authentication timer.
4	`Raisecom(config-gigaethernet1/1/1)#`**`dot1x timer quiet-period`** *`second`*	Configure the time of the quiet timer.
5	`Raisecom(config-gigaethernet1/1/1)#`**`dot1x timer supp-timeout`** *`supp-timeout`*	Configure the time of the supplicant authorization timeout timer.
6	`Raisecom(config-gigaethernet1/1/1)#`**`dot1x timer server-timeout`** *`server-timeout`*	Configure the time of the authentication server timeout timer.

9.7.7 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show dot1x`** *`interface-type interface-list`*	Show 802.1x configurations on the interface.
2	`Raisecom#`**`show dot1x`** *`interface-type interface-list`* **`statistics`**	Show 802.1x statistics on the interface.
3	`Raisecom#`**`show dot1x`** *`interface-type interface-list`* **`user`**	Show user information of 802.1x authentication on the interface.

9.7.8 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description
`Raisecom(config)#`**`clear dot1x`** *`interface-type interface-list`* **`statistics`**	Clear interface 802.1x statistics.

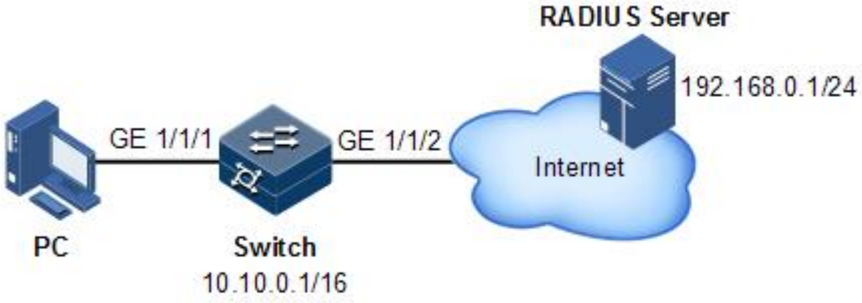
9.7.9 Example for configuring 802.1x

Networking requirements

As shown in Figure 9-8, the network administrator configures 802.1x to control the PC to access the Internet.

- For the switch: the IP address is 10.10.0.1, the mask is 255.255.0.0, and default gateway is 10.10.0.2.
- The RADIUS server works to authenticate and authorize PCs. Its IP address is 192.168.0.1, and the password is raisecom.
- The interface control mode is auto.
- After the PC passes authentication, the Switch will start reauthentication every 600s.

Figure 9-8 Dot1x networking



Configuration steps

Step 1 Configure the IP addresses of the Switch and RADIUS server.

```
Raisecom#config
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip address 10.10.0.1 255.255.0.0
Raisecom(config-vlan1)#exit
Raisecom(config)#ip route 0.0.0.0 0.0.0.0 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 gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#dot1x enable
```

Step 3 Configure interface authorization mode to auto.

```
Raisecom(config-gigaethernet1/1/1)#dot1x auth-control auto
```

Step 4 Enable reauthentication, and configure the timer to 600s.

```
Raisecom(config-gigaethernet1/1/1)#dot1x reauthentication enable
Raisecom(config-gigaethernet1/1/1)#dot1x timer reauth-period 600
```

Checking results

Use the **show dot1x** command to show 802.1x configurations on the interface.

```
Raisecom#show dot1x gigaethernet 1/1/1
802.1x Global Admin State: enable
802.1x Authentication Method: chap
Port gigaethernet1/1/1
--------------------------------------------------------
802.1X Port Admin State: Enable
PAE: Authenticator
PortMethod: Portbased
PortControl: Auto
PortStatus: Authorized
Authenticator PAE State: Initialize
Backend Authenticator State: Initialize
ReAuthentication: Enable
QuietPeriod: 60(s)
ServerTimeout: 100(s)
SuppTimeout: 30(s)
ReAuthPeriod: 600(s)
TxPeriod: 30(s)
```

9.8 IP Source Guard

9.8.1 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 be combined 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:

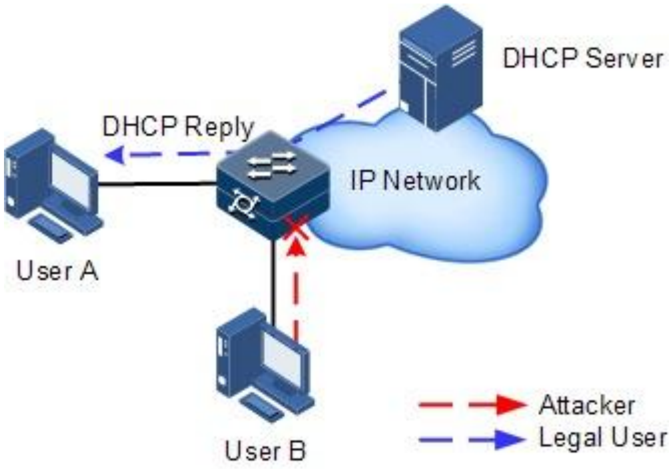
- Static binding: configure binding information manually and generate binding entry to complete the interface control, which fits for the case where the number of hosts is small or where you need to perform separate binding on a single host.
- Dynamic binding: obtain binding information automatically from DHCP Snooping to complete the interface control, which fits for the case where there are many hosts and you need to adopt DHCP to perform dynamic host configurations. Dynamic binding can effectively prevent IP address conflict and embezzlement.

Principles of IP Source Guard

The principle of IP Source Guard is to create an IP source binding table within the ISCOM2600G series switch. The IP source binding table is taken as the basis for each interface to test received data packets. Figure 9-9 shows principles 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 9-9 Principles of IP Source Guard



Before forwarding IP packets, the ISCOM2600G series switch compares the source IP address, source MAC address, interface ID, and VLAN ID of the IP packets with the binding table. If the information matches, it indicates that the user is legal and the packets are permitted to forward normally. Otherwise, the user is an attacker and the IP packets are discarded.

9.8.2 Preparing for configurations

Scenario

There are often some IP source spoofing attacks on the network. For example, the attacker forges legal users to send IP packets to the server, or the attacker forges the source IP address of another user to communicate. This makes the legitimate users cannot get network services normally.

With IP Source Guard binding, you can filter and control packets forwarded by the interface, prevent the illegal packets from passing through the interface, thus to restrict the illegal use of network resources and improve the interface security.

Prerequisite

Enable DHCP Snooping if there are DHCP users.

9.8.3 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

9.8.4 Configuring interface trust status of IP Source Guard

Configure interface trust status of IP Source Guard for the ISCOM2600G series switch 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-gigaethernet1/1/1)#`**`ip verify source trust`**	(Optional) configure the interface to a trusted interface. Use the **no ip verify source trust** command to configure the interface to an untrusted interface. In this case, all packets, except DHCP packets and IP packets that meet binding relation, are not forwarded. When the interface is in trusted status, all packets are forwarded normally.

9.8.5 Configuring IP Source Guide binding

Configuring IP Source Guide static binding

Configure IP Source Guide static binding for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip verify source**	Enable IP Source Guide static binding.
3	Raisecom(config)#**ip source binding** *ip-address* [*mac-address*] [**vlan** *vlan-id*] *interface-type interface-number*	Configure static binding.

Note

- The configured static binding does not take effect when global static binding is disabled. Only when global static binding is enabled can the static binding take effect.
- For an identical IP address, the manually configured static binding will cover the dynamic binding. However, it cannot cover the existing static binding. When the static binding is deleted, the system will recover the covered dynamic binding automatically.

Configuring IP Source Guide dynamic binding

Configure IP Source Guide dynamic binding for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip verify source dhcp-snooping**	Enable IP Source Guide dynamic binding.

Note

- The dynamic binding learnt through DHCP Snooping does not take effect when global dynamic binding is disabled. Only when global dynamic binding is enabled can the dynamic binding take effect.
- If an IP address exists in the static binding table, the dynamic binding does not take effect. In addition, it cannot cover the existing static binding.

Configuring binding translation

Configure binding translation for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**ip verify source dhcp-snooping**	Enable IP Source Guide dynamic binding.
3	Raisecom(config)#**ip source binding dhcp-snooping static**	Translate the dynamic binding to the static binding.
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.

9.8.6 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** [*interface-type interface-number*]	Show configurations of IP Source Guard binding, interface trusted status, and binding table.

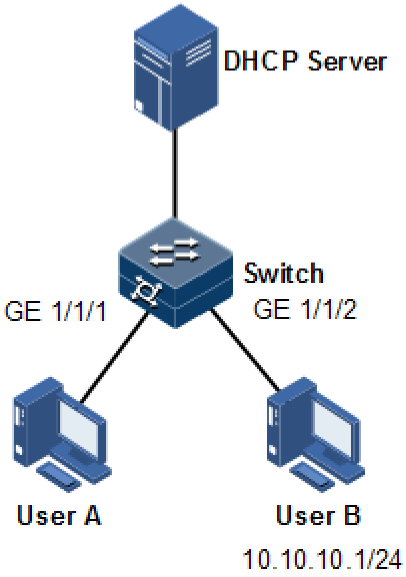
9.8.7 Example for configuring IP Source Guard

Networking requirements

As shown in Figure 9-10, to prevent IP address embezzlement, you need to configure IP Source Guard on the Switch.

- The Switch permits all IP packets on GE 1/1/1 to pass.
- GE 1/1/2 permits those IP packets to pass, of which the IP address is 10.10.10.1, the subnet mask is 255.255.255.0, and the status meets the dynamic binding learnt by DHCP Snooping.
- Other interfaces only permit the packets meeting DHCP Snooping learnt dynamic binding to pass.

Figure 9-10 Configuring IP Source Guard



Configuration steps

Step 1 Configure GE 1/1/1 to the trusted interface.

```
Raisecom#config
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#ip verify source trust
Raisecom(config-gigaethernet1/1/1)#exit
```

Step 2 Configure static binding.

```
Raisecom(config)#ip verify source
Raisecom(config)#ip source binding 10.10.10.1 gigaethernet 1/1/2
```

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                        --            --    gigaethernet1/1/2
static        yes
```

Use the **show ip verify source** command to show interface trusting status and configurations of IP Source Guard static/dynamic binding.

```
Raisecom#show ip verify source
Static Bind: Enable
Dhcp-Snooping Bind: Enable
Port                        Trust
----------------------------------------
gigaethernet1/1/1             yes
gigaethernet1/1/2             no
gigaethernet1/1/3             no
gigaethernet1/1/4             no
gigaethernet1/1/5             no
gigaethernet1/1/6             no
gigaethernet1/1/7             no
……
```

9.9 PPPoE+

9.9.1 Introduction

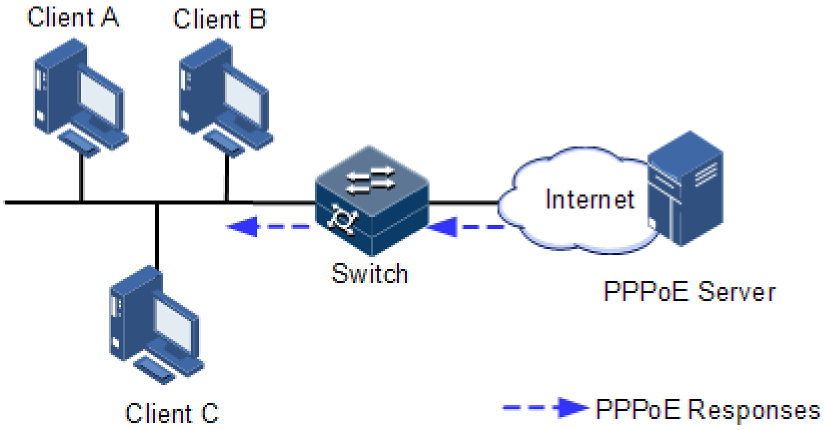
PPPoE Intermediate Agent (PPPoE+) is used to process authentication packets. PPPoE+ adds more information about access devices into the authentication packet to bind account and access device so that the account is not shared and stolen, and the carrier's and users' interests are protected. This provides the server with enough information to identify users, avoiding account sharing and theft and ensuring the network security.

In PPPoE dial-up mode, you can access the network through various interfaces on the device as long as authentication by the authentication server is successful.

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 9-11. 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 9-11 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 authentication 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.

9.9.2 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

9.9.3 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, the PPPoE packet is forwarded without being attached with any information.

9.9.4 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; namely, an interface enabled with PPPoE+ cannot be configured as a trusted interface.

Enabling PPPoE+

After global PPPoE+ and 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 ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`pppoeagent enable`**	Enable global PPPoE+.
3	`Raisecom(config)#`**`interface`** *`interface-type interface-number`*	Enter physical layer interface configuration mode.
4	`Raisecom(config-gigaethernet1/1/1)#`**`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 to 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 ISCOM2600G series switch 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-gigaethernet1/1/1)#**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.

9.9.5 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 number, 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 number, 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 ID string.

Configure Circuit ID for the ISCOM2600G series switch 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)#interface interface-type interface-number`	Enter physical layer interface configuration mode.
4	`Raisecom(config-gigaethernet1/1/1)#pppoeagent circuit-id string`	(Optional) configure the Circuit ID to the customized string.

In default mode, the Circuit ID contains an attached string. By default, the attached string is configured to the hostname of the switch. You can configure it to a customized string.

Configure the attached string of the Circuit ID for the ISCOM2600G series switch as below.

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. If the Circuit ID is in default mode, attached string configured by this command will be added to the Circuit ID.

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 ISCOM2600G series switch 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-gigaethernet1/1/1)#pppoeagent remote-id { client-mac | switch-mac }`	(Optional) configure PPPoE+ Remote ID to be padded with the MAC address.
4	`Raisecom(config-gigaethernet1/1/1)#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 ISCOM2600G series switch 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-gigaethernet1/1/1)#`**`pppoeagent vendor-specific-tag overwrite enable`**	Enable Tag overriding.

9.9.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show pppoeagent`**	Show PPPoE+ configurations.
2	`Raisecom#`**`show pppoeagent statistic`**	Show PPPoE+ statistics.

9.9.7 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description
`Raisecom(config)#`**`clear pppoeagent statistic`**	Clear PPPoE+ statistics.

9.9.8 Example for configuring PPPoE+

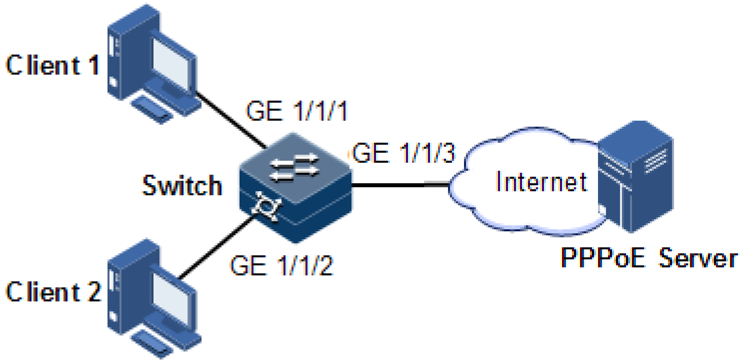
Networking requirements

As shown in Figure 9-12, to prevent illegal clients from accessing and managing legal users, you can configure PPPoE+ on the Switch.

- GE 1/1/1 and GE 1/1/2 are connected to Client 1 and Client 2 respectively. GE 1/1/3 is connected to the PPPoE server.
- Enable global PPPoE+, and PPPoE on GE 1/1/1 and GE 1/1/2. Configure GE 1/1/3 as the trusted interface.

- Configure the attached string of Circuit ID to raisecom, padding information about Circuit ID on GE 1/1/1 to user01, padding information about Circuit ID on GE 1/1/2 to the MAC address of Client 2, in ASCII format.
- Enable Tag overwriting on GE 1/1/1 and GE 1/1/2.

Figure 9-12 PPPoE+ networking



Configuration steps

Step 1 Configure GE 1/1/3 as the trusted interface.

```
Raisecom#config
Raisecom(config)#interface gigaethernet 1/1/3
Raisecom(config-gigaethernet1/1/1)#pppoenagent trust
Raisecom(config-gigaethernet1/1/1)#exit
```

Step 2 Configure packet information about GE 1/1/1 and GE 1/1/2.

```
Raisecom(config)#pppoeagent circuit-id attach-string raisecom
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#pppoeagent circuit-id user01
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet1/1/2
Raisecom(config-gigaethernet1/1/2)#pppoeagent remote-id client-mac
Raisecom(config-gigaethernet1/1/2)#pppoeagent remote-id format ascii
Raisecom(config-gigaethernet1/1/2)#exit
```

Step 3 Enable Tag overwriting on GE 1/1/1 and GE 1/1/2.

```
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#pppoeagent vendor-specific-tag
overwrite enable
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet1/1/2
Raisecom(config-gigaethernet1/1/2)#pppoeagent vendor-specific-tag
overwrite enable
Raisecom(config-gigaethernet1/1/2)#exit
```

Step 4 Enable global PPPoE+, and PPPoE on GE 1/1/1 and GE 1/1/2.

```
Raisecom(config)#pppoeagent enable
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#pppoeagent enable
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#pppoeagent enable
```

Checking results

Use the **show pppoeagent** command to show PPPoE+ configurations.

```
Raisecom#show pppoeagent
Mac-format: hhhhhhhhhhhh
Global PPPoE+ status: enable
Attach-string: raisecom
Circuit ID padding mode: switch
       Port            State   Overwrite  Remote-ID   Format-rules
Circuit-ID
-------------------------------------------------------------------------
-----------
gigaethernet1/1/1        enable   enable    switch-mac   binary
user01
gigaethernet1/1/2        enable   enable    client-mac
ASCII       %default%
gigaethernet1/1/3        trust   disable    switch-mac
binary      %default%
gigaethernet1/1/4        disable  disable   switch-mac
binary      %default%
gigaethernet1/1/5        disable  disable   switch-mac
binary      %default%
gigaethernet1/1/6        disable  disable   switch-mac
binary      %default%
```

9.10 Configuring CPU protection

9.10.1 Preparing for configurations

Scenario

When the ISCOM2600G series switch receives massive attacking packets in a short period, the CPU will run with full load and the CPU utilization rate will reach 100%. This will cause device malfunction. CPU CAR helps efficiently limit the speed of packets which enters the CPU.

Prerequisite

N/A

9.10.2 Configuring global CPU CAR

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`cpu-protect car`** `{` **`arp`** `|` **`dhcp`** `|` **`global`** `|` **`icmp`** `|` **`igmp`** `}` **`kbps cir`** *`cir`* **`cbs`** *`cbs`*	Configure the protocol type, CIR, and CBS of global CPU packet protection.

9.10.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show cpu-protect car statistics`**	Show CPU CAR statistics.

9.10.4 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description
`Raisecom#`**`show cpu-protect car statistics`**	Show CPU CAR statistics.

10 Reliability

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

- Link aggregation
- Interface backup
- Link-state tracking

10.1 Link aggregation

10.1.1 Introduction

Link aggregation refers to aggregating multiple physical Ethernet interfaces to a Link Aggregation Group (LAG) and taking multiple physical links in the same LAG as one logical link. Link aggregation helps share traffic among members in the LAG. Besides effectively improving reliability on links between two 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 aggregating multiple physical interfaces to one logical interface so that they can balance load.

- 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 number, and operation Key.

After receiving the LACPDU, the peer compares its information with the one received from other interfaces to select an interface able to be in Selected status, on which both sides can agree. 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.

10.1.2 Preparing for configurations

Scenario

To provide higher bandwidth and reliability for a link between two devices, configure link aggregation.

Prerequisite

- Configure physical parameters of interfaces and make them Up.
- In the same LAG, member interfaces that share loads must be identically configured. Otherwise, data cannot be forwarded properly. These configurations include QoS, QinQ, VLAN, interface properties, and MAC address learning.
  - QoS: traffic policing, traffic shaping, congestion avoidance, 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 MAC address learning is enabled and whether the interface is configured with MAC address limit.

10.1.3 Configuring manual link aggregation

Configure manual link aggregation for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface port-channel`** *`channel-number`*	Enter LAG configuration mode.
3	`Raisecom(config-port-channel1)#`**`mode manual`**	Configure manual link aggregation mode.

Step	Command	Description
4	Raisecom(config-port-channel1)#**{ max-active | min-active } links** *value threshold*	(Optional) configure the maximum or minimum number of active links in LACP LAG. By default, the maximum number is 8 while the minimum is 1.
5	Raisecom(config-port-channel1)#**load-sharing mode { dst-ip | dst-mac | label | src-dst-ip | src-dst-mac | src-ip | src-mac }**	(Optional) configure a load balancing mode for link aggregation. By default, the load balancing algorithm is configured to sxordmac. In this mode, select a forwarding interface based on the OR result of the source and destination MAC addresses.
6	Raisecom(config-port-channel1)#**exit**	Return to global configuration mode.

10.1.4 Configuring static LACP link aggregation

Configure static LACP link aggregation for the ISCOM2600G series switch 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. By default, system LACP priority is 32768.
3	Raisecom(config)#**lacp timeout { fast | slow }**	(Optional) configure LACP timeout mode. By default, it is slow.
4	Raisecom(config)#**interface port-channel** *channel-number*	Enter LAG configuration mode.
5	Raisecom(config-port-channel1)#**mode lacp**	Configure the working mode of the LAG to static LACP LAG.
6	Raisecom(config-port-channel1)#**{ max-active | min-active } links** *value threshold*	(Optional) configure maximum or minimum number of active links in LACP LAG. By default, the maximum number is 8 while the minimum number is 1.
7	Raisecom(config-port-channel1)#**exit**	Return to global configuration mode.

Step	Command	Description
8	Raisecom(config)#**interface** *interface-type interface-number*	Enter Layer 2 or Layer 3 physical interface configuration mode.
9	Raisecom(config-gigaethernet1/1/1)#**port-channel** *channel-number*	Add the Layer 2 or Layer 3 interface to the LAG.
10	Raisecom(config-port-channel1)#**lacp mode** { **active** | **passive** }	(Optional) configure LACP mode for member interface. LACP connection will fail when both ends of a link are in passive mode. By default, it is in active mode.
11	Raisecom(config-port-channel1)#**lacp port-priority** *port-priority*	(Optional) configure interface LACP priority. The priority affects election for the default interface for LACP. The smaller the value is, the higher the priority is. By default, it is 32768.
12	Raisecom(config-port-channel1)#**exit**	Return to global configuration mode.

Note

- In a static LACP LAG, a member interface can be an active/standby one. Both the active interface and standby interface can receive and send LACPDU. However, the standby interface cannot forward user packets.
- The system 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.

10.1.5 Configuring manual master/slave link aggregation

Configure manual master/slave link aggregation for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface port-channel** *channel-number*	Enter LAG configuration mode.
3	Raisecom(config-port-channel1)#**mode manual backup**	Configure the working mode of the LAG to manual backup LAG.
4	Raisecom(config-port-channel1)#**master-port** *interface-type interface-number*	Configure the active interface of the LAG.

Step	Command	Description
5	`Raisecom(config-port-channel1)#restore-mode { non-revertive | revertive [ restore-delay second ] }`	Configure the restoration mode and wait-to-restore time of the LAG. By default, the restoration mode is non-revertive.
6	`Raisecom(config-port-channel1)#exit`	Return to global configuration mode.
7	`Raisecom(config)#interface interface-type interface-number`	Enter physical layer interface configuration mode.
8	`Raisecom(config-gigaethernet1/1/1)#port-channel channel-number`	Add member interfaces to the LAG.
9	`Raisecom(config-gigaethernet1/1/1)#exit`	Return to global configuration mode.

10.1.6 Checking configurations

Use the following commands to check configuration results.

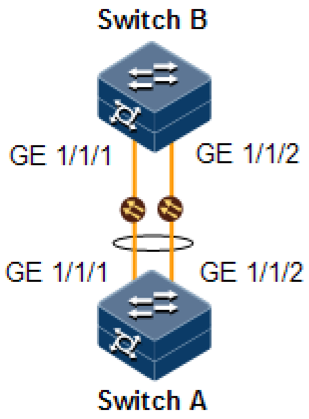
No.	Command	Description
1	`Raisecom#show lacp internal`	Show local system LACP interface status, flag, interface priority, administration key, operation key, and interface status machine status.
2	`Raisecom#show lacp neighbor`	Show information about LACP neighbors, including tag, interface priority, device ID, Age, operation key value, interface ID, and interface status machine status.
3	`Raisecom#show lacp statistics`	Show statistics of interface LACP, including the total number of received/sent LACP packets, the number of received/sent Marker packets, the number of received/sent Marker Response packets, and the number of errored Marker Response packets,
4	`Raisecom#show lacp sys-id`	Show global LACP status of the local system, device ID, including system LACP priority and system MAC address.
5	`Raisecom#show port-channel`	Show link aggregation status of the current system, load balancing mode of link aggregation, all LAG member interfaces, and active member interfaces. **Note** The active member interface refers to the one whose interface status is Up.

10.1.7 Example for configuring static LACP link aggregation

Networking requirements

As shown in Figure 10-1, to improve link reliability between Switch A and Switch B, you can configure static LACP link aggregation. That is to add GE 1/1/1 and GE 1/1/2 into one LAG; wherein GE 1/1/1 is used as the active interface and GE 1/1/2 as the standby interface.

Figure 10-1 Static LACP mode Link aggregation networking



Configuration steps

Step 1 Create static LACP link aggregation on Switch A. Configure Switch A as the active end.

```
Raisecom#name SwitchA
SwitchA#config
SwitchA(config)#lacp system-priority 1000
SwitchA(config)#interface port-channel 1
SwitchA(config-port-channel1)#mode lacp
SwitchA(config-port-channel1)#max-active links 1
SwitchA(config-port-channel1)#exit
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#port-channel 1
SwitchA(config-gigaethernet1/1/1)#lacp port-priority 1000
SwitchA(config-gigaethernet1/1/1)#exit
SwitchA(config)#interface gigaethernet1/1/2
SwitchA(config-gigaethernet1/1/2)#port-channel 1
SwitchA(config-gigaethernet1/1/2)#exit
```

Step 2 Create static LACP link aggregation on Switch B.

```
Raisecom#hostname SwitchB
SwitchB#config
SwitchB(config)#interface port-channel 1
SwitchB(config-aggregator)#mode lacp-static
SwitchB(config-aggregator)#exit
SwitchB(config)#interface gigaethernet1/1/1
SwitchB(config-gigaethernet1/1/1)#port-channel 1
SwitchB(config-gigaethernet1/1/1)#exit
SwitchB(config)#interface gigaethernet1/1/2
SwitchB(config-gigaethernet1/1/2)#port-channel 1
SwitchB(config-gigaethernet1/1/2)#exit
```

Checking results

Use the **show port-channel** command to show global configurations of the static LACP link aggregation on Switch A.

```
SwitchA#show port-channel
Group 1 information:
Mode   :  Lacp                  Load-sharing mode  : src-dst-mac
MinLinks:  1                    Max-links        : 1
UpLinks :  0                    Priority-Preemptive: Disable
Member Port: gigaethernet1/1/1 gigaethernet1/1/2
Efficient Port:
```

Use the **show lacp internal** command to show configurations of local LACP interface status, flag, interface priority, administration key, operation key, and interface state machine on Switch A.

```
SwitchA#show lacp internal
Flags:
  S - Device is requesting Slow LACPDUs  F - Device is requesting Fast
LACPDUs
  A - Device in Active mode  P - Device in Passive mode   MP - MLACP Peer
Port
Interface          State      Flag   Port-Priority   Admin-key  Oper-key
Port-State
---------------------------------------------------------------------------
-----------------
gigaethernet1/1/1   Down       SA     1000          1        1
0x45
gigaethernet1/1/2   Down       SA     32768         1        1
0x45
```

Use the **show lacp neighbor** command to show configurations of LACP interface status, flag, interface priority, administration key, operation key, and interface state machine of the peer system on Switch A.

10.2 Interface backup

10.2.1 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, 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 core of the carrier-grade network.

Interface backup, targeted for dual uplink networking, implements redundancy backup and quick switching through working and protection links. It ensures performance and simplifies configurations.

Interface backup is another STP solution. 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.

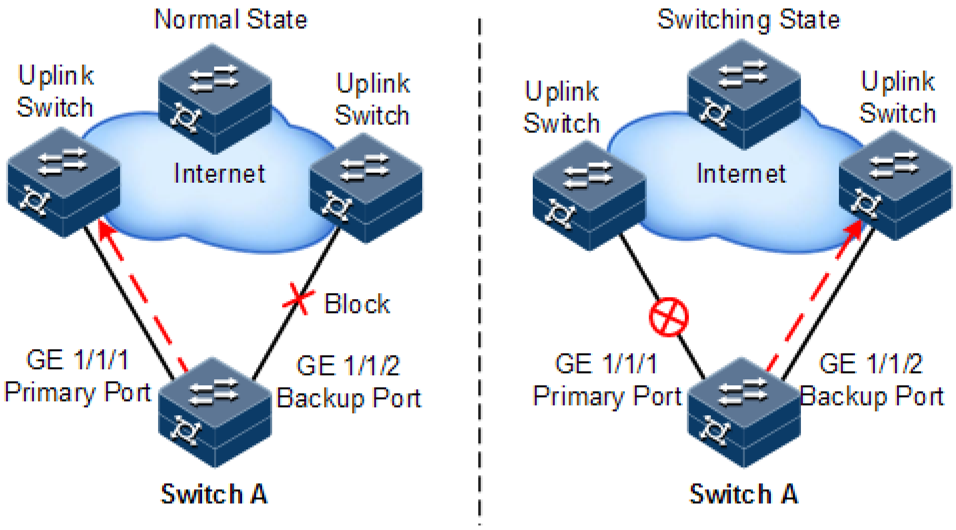
When the primary link fails, traffic is switched to the backup link. In this way, not only 50ms fast switching is ensured, but also configurations are simplified.

Principles of interface backup

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 10-2 Principles of interface backup



As shown in Figure 10-2, GE 1/1/1 and GE 1/1/2 on Switch A are connected to their uplink devices respectively. The interface forwarding states are shown as below:

- Under normal conditions, GE 1/1/1 is the primary interface while GE 1/1/2 is the backup interface. GE 1/1/1 and the uplink device forward packet while GE 1/1/2 and the uplink device do not forward packets.
- When the link between GE 1/1/1 and its uplink device fails, the backup GE 1/1/2 and its uplink device forward packets.
- When GE 1/1/1 restores normally and keeps Up for a period (restore-delay), GE 1/1/1 restores to forward packets and GE 1/1/2 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 10-3.

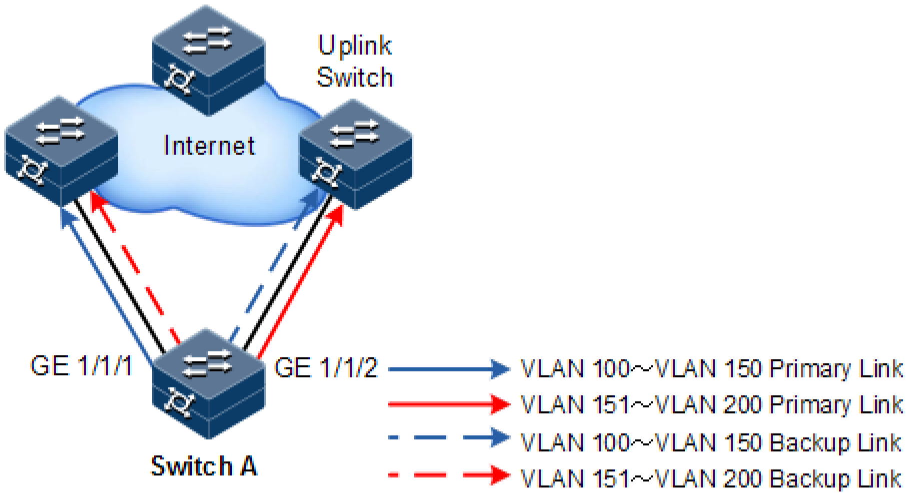

Uplink
Switch
Internet
GE 1/1/1
GE 1/1/2
Switch A
VLAN 100~VLAN 150 Primary Link
VLAN 151~VLAN 200 Primary Link
VLAN 100~VLAN 150 Backup Link
VLAN 151~VLAN 200 Backup Link

Figure 10-3 Networking with interface backup in different VLANs

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

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

10.2.2 Preparing for configurations

Scenario

By configuring interface backup in a dual uplink network, you can realize redundancy backup and fast switching of the primary/backup link, and load balancing between different interfaces.

Compared with STP, interface backup not only ensures millisecond-level switching, also simplifies configurations.

Prerequisite

N/A

10.2.3 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)

10.2.4 Configuring basic functions of interface backup

Configure basic functions of interface backup for the ISCOM2600G series switch as below.

Caution

Interface backup may interfere with STP, loop detection, Ethernet ring, and G.8032. We do not recommend configuring them concurrently on the same interface.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type primary-interface-number*	Enter physical layer interface configuration mode or LAG configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#**switchport backup** *interface-type backup-interface-number* **vlanlist** *vlan-list* Raisecom(config-port-channel1)#**switchport backup** *interface-type backup-interface-number* [**vlanlist** *vlan-list*]	Configure the interface backup group. In the VLAN list, configure the interface *backup-interface-number* to the backup interface and configure the interface *primary-interface-number* to the primary interface. If no VLAN list is specified, the VLAN ranges from 1 to 4094.
4	Raisecom(config-gigaethernet1/1/1)#**exit**	Return to global configuration mode.

Step	Command	Description
	Raisecom(config-port-channel1)#**exit**	
5	Raisecom(config)#**switchport backup restore-delay** *period*	(Optional) configure the restore-delay period.
6	Raisecom(config)#**switchport backup restore-mode { disable | 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.

10.2.5 (Optional) configuring FS on interfaces

Caution

- After FS is successfully configured, the primary/backup link will be switched; namely, the current link is switched to the backup link (without considering Up/Down status of the primary/backup interface).
- In the FS command, the backup interface number is optional. If different VLANs of the primary interface are configured with multiple interface backup groups, you should enter the backup interface ID.

Configure FS on interfaces for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type primary-interface-number*	Enter physical layer interface configuration mode or LAG configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#**switchport backup** [*interface-type backup-interface-number*] **force-switch** Raisecom(config-port-channel1)#**switchport backup** [*interface-type backup-interface-number*] **force-switch**	Configure FS on the interface. Use the **no switchport backup** [*interface-type backup-interface-number*] **force-switch** command to cancel FS. Then, the principles of selecting the current link according to link status are as below: • If the Up/Down statuses of the two interfaces are the same, the primary interface is of high priority. • If the Up/Down statuses of the two interfaces are different, the Up interface is of high priority.

10.2.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show switchport backup`	Show status information about interface backup.

10.2.7 Example for configuring interface backup

Networking requirements

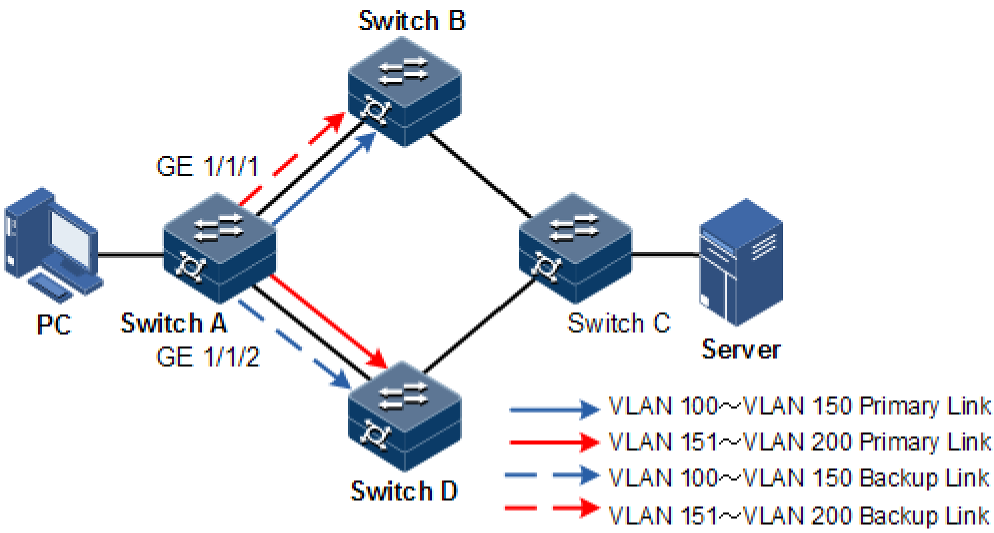
As shown in Figure 10-4, the PC accesses the server through the Switch. To implement a reliable remote access from the PC to the server, configure an interface backup group on Switch A and specify the VLAN list so that the two interfaces concurrently forward services in different VLANs and balance load. Configure Switch A as below:

- Add GE 1/1/1 to VLANs 100–150 as the primary interface and GE 1/1/2 as the backup interface.
- Add GE 1/1/2 to VLANs 151–200 as the primary interface and GE 1/1/1 as the backup interface.

When GE 1/1/1 or its link fails, the system switches traffic to the backup interface GE 1/1/2 to resume the link.

Switch A is required to support interface backup while other switches are not.

Figure 10-4 Interface backup networking


Switch B
GE 1/1/1
PC
Switch A
GE 1/1/2
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 100–400, and add GE 1/1/1 and GE 1/1/2 to these VLANs.

```
Raisecom#config
```

```
Raisecom(config)#create vlan 100-200 active
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport mode trunk
Raisecom(config-gigaethernet1/1/1)#switchport trunk allowed vlan 100-200
confirm
Raisecom(config-gigaethernet1/1/1)#exit
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport mode trunk
Raisecom(config-gigaethernet1/1/2)#switchport trunk allowed vlan 100-200
confirm
Raisecom(config-gigaethernet1/1/2)#exit
```

Step 2 Configure GE 1/1/1 as the primary interface of VLANs 100–150 and GE 1/1/2 as the backup interface.

```
Raisecom(config)#interface gigaethernet 1/1/1
Raisecom(config-gigaethernet1/1/1)#switchport backup gigaethernet 1/1/2
vlanlist 100-150
Raisecom(config-gigaethernet1/1/1)#exit
```

Step 3 Configure GE 1/1/2 as the primary interface of VLANs 151–200 and GE 1/1/1 as the backup interface.

```
Raisecom(config)#interface gigaethernet 1/1/2
Raisecom(config-gigaethernet1/1/2)#switchport backup gigaethernet 1/1/1
vlanlist 151-200
```

Checking results

Use the **show switchport backup** command to show status of interface backup under normal or faulty conditions.

When both GE 1/1/1 and GE 1/1/2 are Up, GE 1/1/1 forwards traffic of VLANs 100–150, and GE 1/1/2 forwards traffic of VLANs 151–200.

```
Raisecom#show switchport backup
Restore delay: 15s.
Restore mode: port-up.
Active Port(State)    Backup Port(State)    Vlanlist
--------------------------------------------------------
gigaethernet1/1/1(Up)  gigaethernet1/1/2(Standby)    100-150
gigaethernet1/1/2(Up)  gigaethernet1/1/1(Standby)    151-200
```

Manually disconnect the link between Switch A and Switch B to emulate a fault. Then, GE 1/1/1 becomes Down, and GE 1/1/2 forwards traffic of VLANs 100–200.

```
Raisecom#show switchport backup
Restore delay: 15s
Restore mode: port-up
Active Port(State)   Backup Port(State)   Vlanlist
-----------------------------------------------------------------
gigaethernet1/1/1(Down)   gigaethernet1/1/2(Up)           100-150
gigaethernet1/1/2(Up)      gigaethernet1/1/1(Down)         151-200
```

When GE 1/1/1 resumes and keeps Up for 15s (restore-delay), it forwards traffic of VLANs 100–150 while GE 1/1/2 forwards traffic of VLANs 151–200.

10.3 Link-state tracking

10.3.1 Introduction

Link-state tracking is used to provide interface linkage scheme for specific application and it can extend range of link backup. By monitoring uplinks and synchronizing downlinks, add uplink and downlink interfaces to a link-state group. Therefore, the fault of the upstream device can be informed to the downstream device to trigger switching. Link-state tracking can be used to prevent traffic loss due to failure in sensing the uplink fault by the downstream device.

When all uplink interfaces fail, down link interfaces are configured to Down status. When at least one uplink interface recovers, the downlink interface recovers to Up status. Therefore, the fault of the upstream device can be informed to the downlink device immediately. Uplink interfaces are not influenced when the downlink interface fail.

10.3.2 Preparing for configurations

Scenario

When uplink fails, traffic cannot be switched to the standby link if the downlink device fails to be notified in time. Then traffic will be disrupted.

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, the fault of the upstream device can be informed to the downstream device to trigger switching.

Prerequisite

N/A

10.3.3 Default configurations of link-state tracking

Default configurations of link-state tracking are as below.

Function	Default value
Link-state group	N/A

10.3.4 Configuring link-state tracking

Note

Link-state tracking supports being configured on the physical interface and LAG interface.

Configure link-state tracking for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**link-state-tracking group** *group-number*	Create the link-state group and enable link-state tracking.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-gigaethernet1/1/1)#**link-state-tracking group** *group-number* { **downstream** | **upstream** }	Configure the link-state group of the interface and interface type. One interface can belong to only one link-state group and be configured as an either uplink or downlink interface.
5	Raisecom(config-gigaethernet1/1/1)#**link-state-tracking processing mode** { **shutdown** | **trap-only** }	Configure the mode for processing the fault on the link-state interface.

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 will link-state tracking occur.
- In global configuration mode, when you use the **no link-state-tracking group** *group-number* command to disable link-state tracking, the link-state group without interfaces will be deleted.
- In physical layer interface configuration mode, use the **no link-state-tracking group** *group-number* command to delete an interface. During the execution of this command, if the link-state group contains no other interfaces and is disabled, it will also be deleted.

10.3.5 Checking configurations

Use the following commands to check configuration results.

Step	Command	Description
1	Raisecom#**show link-state-tracking group** *group-number* [**detail**]	Show configurations and status of the link-state group.

11 OAM

This chapter describes principles and configuration procedures of OAM and provide related configuration examples, including following sections:

- Introduction
- Configuring EFM

11.1 Introduction

Initially, Ethernet is designed for LAN. Operation, Administration and Maintenance (OAM) is weak because of its small size 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 size of Telecom network is bigger and bigger. The lack of effective management and maintenance mechanism has seriously obstructed Ethernet technology applying to the Telecom network.

To confirm connectivity of Ethernet virtual connection, effectively detect, confirm, and locate faults on network, balance network utilization, measure network performance, and provide service according Service Level Agreement (SLA), implementing OAM on Ethernet has becoming an inevitable developing trend.

11.1.1 EFM

Complying with IEEE 802.3ah protocol, Ethernet in the First Mile (EFM) is a link-level Ethernet OAM technology. It provides link connectivity detection, link fault monitoring, and remote fault notification for a link between two directly connected devices. EFM is mainly used for Ethernet links on edges of the network accessed by users.

OAM mode and OAM discovery

The Ethernet OAM connection process is the OAM discovery phase, where an OAM entity discovers a remote OAM entity and establishes a session with it.

In the discovery phase, a connected Ethernet OAM entity (interface enabled with OAM) informs others of its Ethernet OAM configurations and Ethernet OAM capabilities supported by the local node by exchanging information OAM PDU. After the OAM entity receives parameters of the peer, it determines whether to establish OAM connection. If both ends agree on establishment of the OAM connection, Ethernet OAM protocol will work on the link layer.

The ISCOM2600G series switch can choose one of the following 2 modes to establish Ethernet OAM connection:

- Active mode
- Passive mode

Only the OAM entity in active mode can initiate OAM connection while the OAM entity in passive mode just waits for connection request of the active OAM entity.

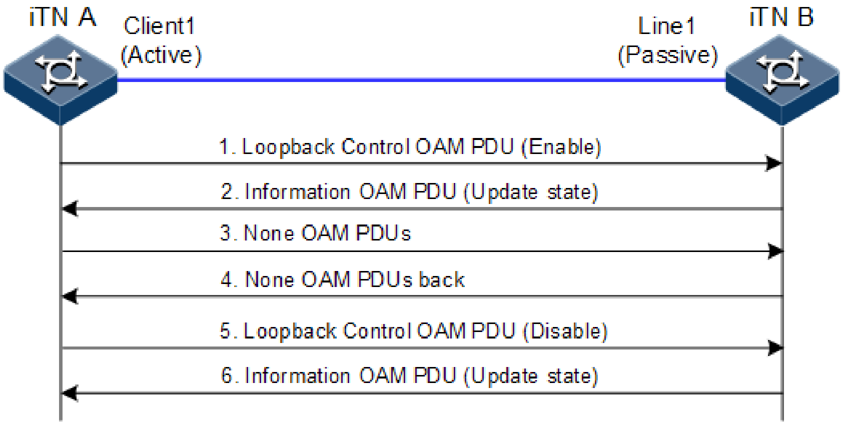
After the OAM connection is established, both ends keep connected by exchanging information OAM PDU. If an OAM entity does not receive information OAM PDU within 5s, it believes that connection expires and connection re-establishment is required.

OAM loopback

OAM loopback occurs only after the Ethernet OAM connection is established. When connected, the active OAM entity initiates OAM loopback command, and the peer OAM entity responds to the command.

When the remote OAM entity is in loopback mode, all packets but OAM PDU packets are sent back. By observing the returned PAMPDU packets, the network administrator can judge the link performance (including packet loss ratio, delay, and jitter).

Figure 11-1 OAM loopback


iTN A
Client1
(Active)
Line1
(Passive)
iTN B
1. Loopback Control OAM PDU (Enable)
2. Information OAM PDU (Update state)
3. None OAM PDUs
4. None OAM PDUs back
5. Loopback Control OAM PDU (Disable)
6. Information OAM PDU (Update state)

As shown in Figure 11-1, Port 1 on iTN A works in active mode. After the 802.3ah OAM connection between iTN A and iTN B is established, enable remote loopback on Client 1.

Start OAM loopback as below:

Step 1 iTN A sends a Loopback Control OAM PDU packet with the Enable information to iTN B, and waits for response.

Step 2 After receiving the Loopback Control OAM PDU packet with the Enable information, iTN B replies the Information OAM PDU packet to iTN A, and enters the loopback state.

Step 3 After receiving the response, iTN A sends a non-OAM PDU test packet to iTN B.

Step 4 After receiving a non-OAM PDU test packet, iTN B sends it back to iTN A.

Stop OAM loopback as below:

Step 1 If iTN A needs to stop remote loopback, it sends a Loopback Control OAM PDU packet with the Disable information to iTN B.

Step 2 After receiving the Loopback Control OAM PDU packet with the Disable information, iTN B exits loopback state and sends an Information OAM PDU packet to iTN A.

You can troubleshoot the fault through loop detection in different phases.

OAM events

It is difficult to detect Ethernet failures, especially when the physical communication works properly while the network performance deteriorates slowly. A flag is defined in OAM PDU packet to allow an OAM entity to transmit fault information to the peer. The flag may stand for the following threshold events:

- Link fault: signals from the peer are lost.
- Dying gasp: an unpredictable event occurs, such as power failure.
- Critical event: an uncertain critical event occurs.

In the OAM connection, an OAM entity keeps sending Information OAM PDUs. The local OAM entity can inform the peer OAM entity of threshold events through Information OAM PDUs. In this way, the network administrator can learn the link state and take actions accordingly.

The network administrator monitors Ethernet OAM through the Event Notification OAM PDU. When a link fails, the passive OAM entity detects the failure, and actively sends Event Notification OAM PDU to the peer active OAM entity to inform the following threshold events. Therefore, the network administrator can dynamically master the network status through the link monitoring process.

- Error frame event: the number of error frames exceeds the threshold in a time unit.
- Error frame period event: the number of error frames exceeds the threshold in a period (specified N frames).
- Error frame second event: the number of error frames in M seconds exceeds the threshold. The second when an errored frame is generated is called the errored frame second.
- Error symbol period event: the number of error symbols received in a period (monitor window) exceeds the threshold.

Note

If an errored frame occurs in a second, the second is called the errored frame second.

Acquiring OAM MIB

The ISCOM2600G series switch learns the status and parameters of the peer link by acquiring link configurations/statistics of the peer through OAM.

11.2 Configuring EFM

11.2.1 Preparing for configurations

Scenario

Deploying EFM feature between directly connected devices can efficiently improve Ethernet link management and maintenance capability and ensure stable network operation.

Prerequisite

- Connect interfaces.
- Configure physical parameters to make interfaces Up at the physical layer.

11.2.2 Configuring basic functions of EFM

Configure basic functions of EFM for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`interface gigaethernet`** *`interface-number`*	Enter Layer 2 or Layer 3 interface configuration mode.
3	`Raisecom(config-gigaethernet1/1/1)#`**`oam`** `{` **`active`** `|` **`passive`** `}`	Configure a working mode of EFM. By default, the ISCOM2600G series switch is in passive mode.
4	`Raisecom(config-gigaethernet1/1/1)#`**`oam send-period`** *`period-number`* **`timeout`** *`time`*	(Optional) Configure the period for sending OAM PDUs and the OAM link timeout. By default, the period is configured to 1s (namely, *period*-number is 10, 10 ×100ms = 1s), and timeout is 5s.
5	`Raisecom(config-gigaethernet1/1/1)#`**`oam enable`**	Enable interface OAM. By default, OAM is disabled on the interface.

11.2.3 Configuring EFM active function

Note

The EFM active function can be configured only when the ISCOM2600G series switch is in active mode.

(Optional) enabling EFM remote loop

Note

- Perform loopback detection periodically can discover network fault in time. Loopback detection in network sections can locate exact fault area and help users clear fault.
- In link loopback status, the ISCOM2600G series switch sends back all packets except OAM packets received by the link to the peer device. Disable this function in time if no loopback detection is needed.

Enable EFM remote loop for the ISCOM2600G series switchISCOM2600G (A) Series as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#**oam remote-loopback**	Configure the interface to start EFM remote loopback.
4	Raisecom(config-gigaethernet1/1/1)#**oam loopback timeout** *time*	(Optional) Configure the timeout for remote loopback on the physical interface. By default, it is 3s.
5	Raisecom(config-gigaethernet1/1/1)#**oam loopback retry** *times*	(Optional) Configure the retry times for remote loopback on the physical interface. By default, it is 3.

(Optional) showing current variable information about peer device

Note

By obtaining the current variable of the peer, you can learn status of current link. 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 ISCOM2600G series switch supports obtaining OAM information and interface statistics.
Peer variable cannot be obtained until EFM is connected.

Show current variable information about the peer device for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**show oam peer oam-info** [**gigaethernet** *interface-number*] Raisecom#**show oam peer** [**gigaethernet** *interface-number*]	Obtain basic OAM information about the peer device.

11.2.4 Configuring EFM passive function

Note

The EFM passive function can be configured regardless the ISCOM2600G series switch is in active or passive mode.

(Optional) configuring device to respond with EFM remote loop

Configure the ISCOM2600G series switch to respond with EFM remote loop as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gigaethernet** *interface-number*	Enter Layer 2 or Layer 3 interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#**oam loopback** { **ignore** | **process** }	Configure the Layer 2 physical interface to ignore or process EFM remote loopback. By default, the Layer 2 physical interface responds to EFM remote loopback.

11.2.5 Configuring link monitoring and fault indication

(Optional) configuring OAM link monitoring

Note

OAM link monitor is used to detect and report link error in different conditions. When the detection link has a fault, the ISCOM2600G series switch notifies the peer of the error generated time, window and threshold by OAM event, the peer receives event notification and reports the NView NNM system through SNMP Trap. Besides, the local device can directly report events to the NView NNM system center through SNMP Trap.

By default, the system has default values for error generated time, window and threshold.

Configure OAM link monitoring for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gigaethernet** *interface-number*	Enter Layer 2 physical interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#**oam errored-frame window** *framewindow* **threshold** *framethreshold*	Configure errored frame monitor window and threshold. By default, the monitor window is 1s, and the threshold is 1 errored frame.
4	Raisecom(config-gigaethernet1/1/1)#**oam errored-frame-period window** *frameperiodwindow* **threshold** *frameperiodthreshold*	Configure errored frame period event monitor window and threshold. By default, the monitor window is 1000ms, and the threshold is 1 errored frame.

Step	Command	Description
5	Raisecom(config-gigaethernet1/1/1)#**oam errored-frame-seconds window** *framesecswindow* **threshold** *framesecsthreshold*	Configure link errored frame second window and threshold. By default, the monitor window is 60s, and the threshold is 1s.
6	Raisecom(config-gigaethernet1/1/1)#**oam errored-symbol-period window** *symperiodwindow* **threshold** *symperiodthreshold*	Configure errored code window and threshold. By default, the monitor window is 1s, and the threshold is 1s.

(Optional) configuring OAM fault indication

Configure OAM fault indication for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**interface gigaethernet** *interface-number*	Enter Layer 2 physical interface configuration mode.
3	Raisecom(config-gigaethernet1/1/1)#**oam notify** { **critical-event** | **dying-gasp** | **errored-frame** | **errored-frame-period** | **errored-frame-seconds** | **errored-symbol-period** } **enable**	Configure the OAM link event notification. By default, OAM link event notification is enabled.
4	Raisecom(config-gigaethernet1/1/1)#**oam event trap enable**	Enable local OAM event Trap to report link monitoring events to the NView NNM system immediately. By default, local OAM event Trap is disabled.
5	Raisecom(config-gigaethernet1/1/1)#**oam peer event trap** { **enable** | **disable** }	Enable peer OAM event Trap to report link monitoring events to the NView NNM system immediately. By default, peer OAM event Trap is disabled.

11.2.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show oam** [**gigaethernet** *interface-number*]	Show basic configurations of EFM.
2	Raisecom#**show oam event** [**gigaethernet** *interface-number*] [**critical**]	Show local OAM link events.
3	Raisecom#**show oam loopback** [**gigaethernet** *interface-number*]	Show configurations of OAM remote loopback.
4	Raisecom#**show oam notify** [**gigaethernet** *interface-number*]	Show configurations of OAM event notification.
5	Raisecom#**show oam peer event** [**gigaethernet** *interface-number*] [**critical**]	Show configurations of OAM peer events.
6	Raisecom#**show oam peer link-statistic** [**gigaethernet** *interface-number*]	Show statistics of peer OAM links.
7	Raisecom#**show oam statistics** [**gigaethernet** *interface-number*]	Show OAM statistics.
8	Raisecom#**show oam trap** [**gigaethernet** *interface-number*]	Show OAM Trap.

12 System management

This chapter describes principles and configuration procedures of system management and maintenance, and provides related configuration examples, including the following sections:

- SNMP
- KeepAlive
- RMON
- LLDP
- Optical module DDM
- System log
- Alarm management
- Hardware environment monitoring
- CPU monitoring
- Cable diagnosis
- Memory monitoring
- Ping
- Traceroute
- Performance statistics

12.1 SNMP

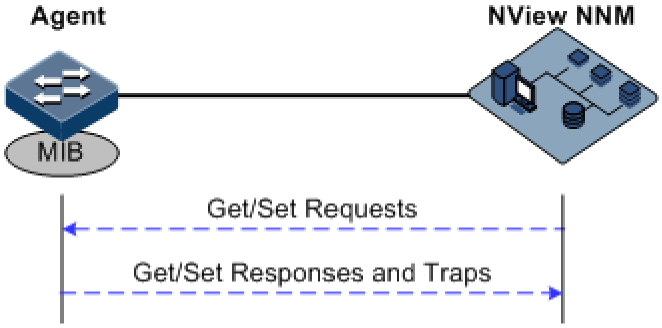
12.1.1 Introduction

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 that 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.

Principles

A SNMP system consists of two parts: Agent and the NView NNM system. The Agent and the NView NNM system communicate through SNMP packets sent through UDP. Figure 12-1 shows the SNMP principle.

Figure 12-1 Principles of SNMP



The 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 on the managed device, implementing the following functions:

- Receive/Reply request packets from the NView NNM system
- To read/write packets and generate replay packets according to the packets type, then return the result to the NView NNM system
- Define trigger condition according to protocol modules, enter/exit system or restart the ISCOM2600G series switch when conditions are satisfied; replying module sends Trap packets to the NView NNM system through agent to report current status of the ISCOM2600G series switch.

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.

Version of protocol

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 ISCOM2600G series switch, the packet will be discarded.
- 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 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 ISCOM2600G series switch supports v1, v2c, and v3 of SNMP.

MIB

Management Information Base (MIB) is the collection of all objects managed by the 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 ISCOM2600G series switch.

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 ISCOM2600G series switch supports standard MIB and Raisecom-customized MIB.

12.1.2 Preparing for configurations

Scenario

When you need to log in to the ISCOM2600G series switch through NMS, configure SNMP basic functions for the ISCOM2600G series switch in advance.

Prerequisite

Configure the routing protocol and ensure that the route between the ISCOM2600G series switch and NMS is reachable.

12.1.3 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)

Function	Default value
SNMP user	none, md5nopriv, shapriv, md5priv, and shanopriv users (default)
Mapping relationship between SNMP user and access group	Index GroupName UserName SecModel --- 0 initialnone none usm 1 initial md5priv usm 2 initial shapriv usm 3 initial md5nopriv usm 4 initial shanopriv usm
Logo and the contact method of the administrator	support@Raisecom.com
Device physical location	world china raisecom
Trap	Enable
SNMP target host address	N/A
SNMP engine ID	800022B603000E5E000016

12.1.4 Configuring basic functions of SNMPv1/SNMPv2c

To protect itself and prevent its MIB from unauthorized access, the SNMP Agent proposes the concept of community. Management stations in the same community must use the community name in all Agent operations, or their requests will not be accepted.

The community name is used by different SNMP strings to identify different groups. Different communities can have read-only or read-write access permission. Groups with read-only permission can only query the device information, while groups with read-write access permission can configure the ISCOM2600G series switch in addition to querying the device information.

SNMPv1/SNMPv2c uses the community name authentication scheme, and the SNMP packets of which the names are inconsistent to the community name will be discarded.

Configure basic functions of SNMPv1/SNMPv2c for the ISCOM2600G series switch 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.

Step	Command	Description
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.

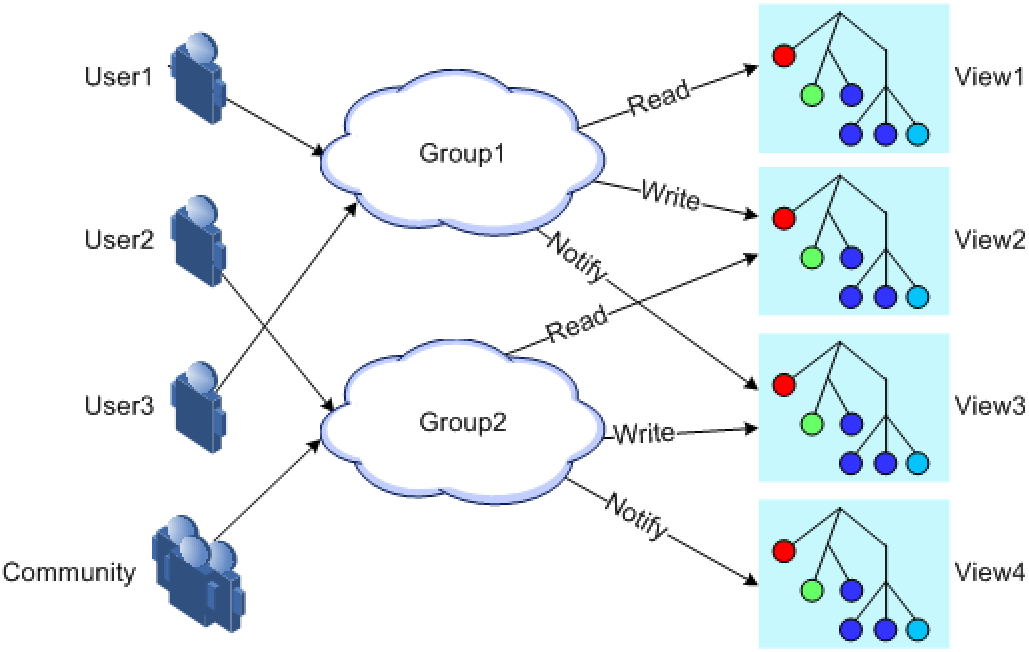
12.1.5 Configuring basic functions of SNMPv3

SNMPv3 uses USM over user authentication 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 announce view; users in access group have access permission in this view. The user access group to send Get and Set request must have permission corresponding to the request; otherwise the request will not be accepted.

As shown in Figure 12-2, the network management station uses the normal access from SNMPv3 to switch and the configuration is as below.

- Configure users.
- Check the access group to which the user belongs.
- Configure view permission for access groups.
- Create views.

Figure 12-2 SNMPv3 authentication mechanism



Configure basic functions of SNMPv3 for the ISCOM2600G series switch as below.

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

Step	Command	Description
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* [**privkey** *privkeypassword*]	Create users and configure authentication modes.
4	Raisecom(config)#**snmp-server user** *user-name* [**remote** *engine-id*] **authkey** { **md5** | **sha** } *keyword* [**privkey** *privkeypassword*]	(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** | **authpriv** | **noauthnopriv** }	Create and configure the SNMPv3 access group.
6	Raisecom(config)#**snmp-server group** *group-name* **user** *user-name* **usm**	Configure the mapping relationship between users and the access group.

12.1.6 Configuring IP address authentication by SNMP server

Configure IP address authentication by SNMP server for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server server-auth enable**	Enable IP address authentication by the SNMP server.
3	Raisecom(config)#**snmp-server server-auth** *ip-address*	Configure the IP address of the SNMP server for authentication.

12.1.7 Configuring other information about SNMP

Other information about SNMP includes:

- 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 about SNMP for the ISCOM2600G series switch 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 E-mail to the logo and contact method of the administrator.
3	Raisecom(config)#**snmp-server location** *location*	(Optional) specify the physical location of the device.

12.1.8 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 ISCOM2600G series switch 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. SNMPv1 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 ISCOM2600G series switch and NMS is reachable.

Configure Trap of SNMP for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server host** *ip-address* **version 3** { **authnopriv** | **authpriv** | **noauthnopriv** } *user-name* [**udpport** *udpport*]	(Optional) configure the SNMPv3 Trap target host.
3	Raisecom(config)#**snmp-server host** *ip-address* **version** { **1** | **2c** } *com-name* [**udpport** *udpport*]	(Optional) configure the SNMPv1/SNMPv2c Trap target host.
4	Raisecom(config)#**snmp-server enable traps**	Enable Trap.

12.1.9 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 the local SNMP engine ID, logo and contact method of the administrator, physical location of the device, and Trap status.
4	`Raisecom#show snmp group`	Show the mapping relationship 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.
9	`Raisecom#show snmp server-auth`	Show SNMP server authentication configurations.

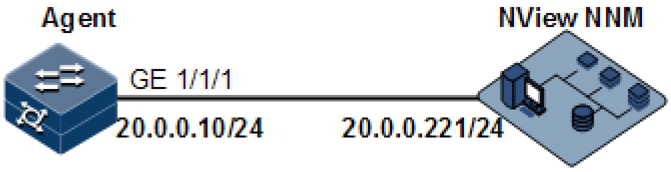
12.1.10 Example for configuring SNMPv1/SNMPv2c and Trap

Networking requirements

As shown in Figure 12-3, the route between the NView NNM system and the ISCOM2600G series switch is available. The Nview NNM system can check the MIB under view corresponding to the remote Switch by SNMPv1/SNMPv2c, and the ISCOM2600G series switch can send Trap automatically to the Nview NNM system in emergency.

By default, there is VLAN 1 on the ISCOM2600G series switch and all physical interfaces belong to VLAN 1.

Figure 12-3 SNMPv1/SNMPv2c networking



Configuration steps

Step 1 Configure the IP address of the ISCOM2600G series switch.

```
Raisecom#config
```

```
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip address 20.0.0.10 255.255.255.0
Raisecom(config-vlan1)#exit
```

Step 2 Configure SNMPv1/SNMPv2c views.

```
Raisecom(config)#snmp-server view mib2 1.3.6.1.2.1 included
```

Step 3 Configure SNMPv1/SNMPv2c community.

```
Raisecom(config)#snmp-server community raisecom view mib2 ro
```

Step 4 Configure Trap sending.

```
Raisecom(config)#snmp-server enable traps
Raisecom(config)#snmp-server host 20.0.0.221 version 2c raisecom
```

Checking results

Use the **show ip interface brief** command to show configurations of the IP address.

```
Raisecom#show ip interface brief
VRF                   IF                         Address        NetMask
Catagory
-------------------------------------------------------------------------
------------------------------
Default-IP-Routing-Table  fastethernet1/0/1            192.168.0.1
255.255.255.0   primary
Default-IP-Routing-Table  vlan1                      20.0.0.10
255.255.255.0   primary
```

Use the **show snmp view** command to show view configurations.

```
Raisecom#show snmp view
Index:    0
View Name: mib2
OID Tree:  1.3.6.1.2.1
Mask:     --
Type:     include
…
```

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

```
Raisecom#show snmp community
Index   Community Name       View Name          Permission
------------------------------------------------------------
1      private              internet           rw
2      public               internet           ro
3      raisecom             mib2               ro
```

Use the **show snmp host** command to show configurations of the target host.

```
Raisecom#show snmp host
Index:         0
IP family:      IPv4
IP address:     20.0.0.221
Port:          162
User Name:      raisecom
SNMP Version:   v2c
Security Level: noauthnopriv
TagList:       bridge config interface rmon snmp ospf
```

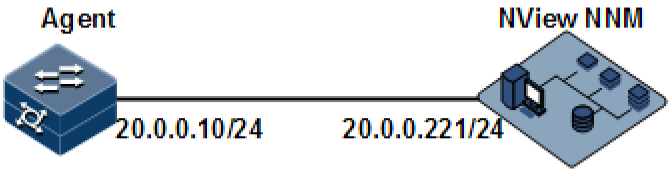
12.1.11 Example for configuring SNMPv3 and Trap

Networking requirements

As shown in Figure 12-4, the route between the NView NNM system and ISCOM2600G series switch is available, the NView NNM system monitors the Agent through SNMPv3, and the ISCOM2600G series switch can send Trap automatically to the Nview NNM system when the Agent is in emergency.

By default, there is VLAN 1 on the ISCOM2600G series switch and all physical interfaces belong to VLAN 1.

Figure 12-4 SNMPv3 and Trap networking



Configuration steps

Step 1 Configure the IP address of the ISCOM2600G series switch.

```
Raisecom#config
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip address 20.0.0.10 255.255.255.0
Raisecom(config-vlan1)#exit
```

Step 2 Configure SNMPv3 access.

Create access view mib2, including all MIB variables under 1.3.6.1.x.1.

```
Raisecom(config)#snmp-server view mib2 1.3.6.1.2.1 1.1.1.1.0.1 included
```

Create user guestuser1, and use md5 authentication algorithm. The password is raisecom.

```
Raisecom(config)#snmp-server user guestuser1 authentication md5 raisecom
```

Create a guest group access group. The security mode is usm, security level is authentication without encryption, and readable view name is mib2.

```
Raisecom(config)#snmp-server access guestgroup read mib2 usm authnopriv
```

Configure the guestuser1 user to be mapped to the access group guestgroup.

```
Raisecom(config)#snmp-server group guestgroup user guestuser1 usm
```

Step 3 Configure Trap sending.

```
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.

```
Raisecom#show snmp access
…
  Index:        1
  Group:        guestgroup
  Security Model: usm
  Security Level: authnopriv
  Context Prefix: --
  Context Match:  exact
  Read View:     mib2
  Write View:    --
  Notify View:   internet
…
```

Use the **show snmp group** command to show mapping between users and access groups.

```
Raisecom#show snmp group
Index   GroupName         UserName          SecModel
-----------------------------------------------------------
0      initialnone       none              usm
1      initial           md5priv            usm
2      initial           shapriv            usm
3      initial           md5nopriv          usm
4      initial           shanopriv          usm
5      guestgroup        guestuser1         usm
```

Use the **show snmp host** command to show configurations of the Trap target host.

```
Raisecom#show snmp host
Index:        0
IP family:     IPv4
IP address:    20.0.0.221
Port:          162
User Name:     guestuser1
SNMP Version:   v3
Security Level: authnopriv
TagList:      bridge config interface rmon snmp ospf
```

12.2 KeepAlive

12.2.1 Introduction

The KeepAlive packet is a kind of KeepAlive mechanism running in High-level Data Link Control (HDLC) link layer protocol. The ISCOM2600G series switch will send a KeepAlive packet to confirm whether the peer is online periodically to implement the neighbor detection mechanism.

Trap is the unrequested information sent by the ISCOM2600G series switch actively to the NView NNM system, used to report some urgent and important events.

The Switch sends KeepAlive Trap actively which includes the basic information about RC551E (device name, device OID, MAC address and IP address) to the NView NNM system. Network management synchronizes device information by IP to make the NView NNM system discover fault in a short time, improve working efficiency and reduce working load of administrators.

12.2.2 Preparing for configurations

Scenario

The ISCOM2600G series switch sends KeepAlive packet to make network management discover segment in a short time, improve working efficiency, and reduce the working load of administrators. You can configure the switch to enable or disable the KeepAlive transmission and its period. When enabled with KeepAlive Trap switch, configure with snmp enable traps and Layer 3 IP address, the Switch will send a KeepAlive Trap alarm message to all target hosts with Bridge Trap every KeepAlive Trap Interval.

Prerequisite

- Configure basic functions of SNMP. SNMPv1 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 ISCOM2600G series switch and NMS is reachable.

12.2.3 Default configurations of KeepAlive

Default configurations of KeepAlive are as below.

Function	Default value
KeepAlive Trap	Disable
KeepAlive Trap period	300s

12.2.4 Configuring KeepAlive

Configure KeepAlive for the ISCOM2600G series switch 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, configure the real transmission period for sending KeepAlive Trap in random transmission of period+5s period.

12.2.5 Checking configurations

Use the following commands to check configuration results.

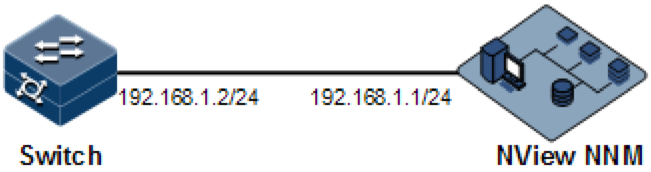
No.	Command	Description
1	`Raisecom#show keepalive`	Show KeepAlive configurations.

12.2.6 Example for configuring KeepAlive

Networking requirements

As shown in Figure 12-5, the IP address of the Switch is 192.168.1.2, the IP address of the SNMPv2c Trap target host is 192.168.1.1, the name of the read-write community is public, and the SNMP version is v2c. Configure the interval for sending KeepAlive Trap from the Switch to SNMP network management station as 120s, and enable sending KeepAlive Trap.

Figure 12-5 KeepAlive networking



Configuration steps

Step 1 Configure the IP address of the Switch.

```
Raisecom#config
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip address 192.168.1.2 255.255.255.0
Raisecom(config-vlan1)#exit
```

Step 2 Configure the IP address of the Trap target host for SNMP.

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

Step 3 Configure sending 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:2
```

12.3 RMON

12.3.1 Introduction

Remote Network Monitoring (RMON) is a standard stipulated by Internet Engineering Task Force (IETF) for network data monitoring through different network Agents and NMS.

RMON is achieved based on SNMP architecture, including the NView NNM system 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 segment and the whole network, while SNMP only can monitor the partial information about a single device and it is difficult for it to monitor one segment.

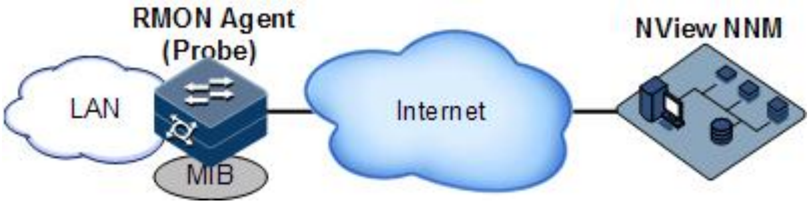
The RMON Agent is commonly referred to as the probe program. The RMON Probe can take the communication subnet statistics and performance analysis. Whenever it finds network failure, RMON Probe can report the NView NNM system, and describes the capture information under unusual circumstances so that the NView NNM system 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, segment or device malfunction more quickly. This method reduces the data flows between the NView NNM system 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 collects data in the following modes:

- 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 about RMON Agent.

The Raisecom ISCOM2600G series switch is embedded with RMON. As shown in Figure 12-6, the ISCOM2600G series switch implements RMON Agent function. Through this function, the management station can obtain the overall flow, error statistics and performance statistics of this segment connected to the managed network device interface so as to achieve the monitoring to one segment.

Figure 12-6 RMON networking



RMON MIB can be divided into nine groups according to function. Currently, there are four function groups achieved: statistics group, history group, alarm group, and event group.

- Statistic group: collect statistics on each interface, including receiving packets accounts and size distribution statistics.
- History group: similar with statistic group, it only collects statistics in an assigned detection period.
- Alarm group: monitor an assigned MIB object and configure upper threshold and lower threshold in assigned time interval, trigger an event if the monitor object receives threshold value.
- Event group: cooperating with alarm group, when an alarm triggers an event, it records the event, such as sending Trap, write into log.

12.3.2 Preparing for configurations

Scenario

RMON helps monitor and account network traffics.

Compared with SNMP, RMON is a more high-efficient monitoring method. After you specifying the alarm threshold, the ISCOM2600G series switch 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 ISCOM2600G series switch and the NView NNM system is reachable.

12.3.3 Default configurations of RMON

Default configurations of RMON are as below.

Function	Default value
Statistics group	Enable on all interfaces
History group	Disable
Alarm group	N/A
Event group	N/A

12.3.4 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, multicast packets, and received packet size.

Configure RMON statistics for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**rmon statistics** *interface-type interface-list* [**owner** *owner-name*]	Enable RMON statistics on an interface and configure related parameters.

Note

When using the **no rmon statistics** *interface-type interface-list* command to disable RMON statistics on an interface, you cannot continue to obtain the interface statistics, but the interface can still count data.

12.3.5 Configuring RMON historical statistics

Configure RMON historical statistics for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**rmon history** *interface-type interface-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** *interface-type interface-list* command to disable RMON historical statistics on an interface, the interface will not count data and clear all historical data collected previously.

12.3.6 Configuring RMON alarm group

Configure one RMON alarm group instance (alarm-id) to monitor one MIB variable (mibvar). When the value of monitoring data exceeds the defined threshold, an alarm event will generate. Record the log to send Trap to network management station according to the definition of alarm event.

The monitored MIB variable must be real, and the data value type is correct. If the set variable does not exist or value type variable is incorrect, return error. In the successfully configured alarm, if the variable cannot be collected later, close the alarm; reconfigure the alarm if you wish to monitor the variable again.

By default, the triggered event number is 0; namely, no event will be triggered. If the number is not zero, and there is no corresponding configuration in event group, when the control variable is abnormal, it cannot trigger the event successfully until the event is established.

An alarm will be triggered as long as matching the condition when the upper or lower limit for one of the events is configured in the event table. If there is no configuration for the upper and lower limits related alarm event (rising-event-id, falling-event-id) in the event table, no alarm will not be generated even alarm conditions are met.

Configure the RMON alarm group for the ISCOM2600G series switch 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.

12.3.7 Configuring RMON event group

Configure the RMON event group for the ISCOM2600G series switch 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.

12.3.8 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.
3	`Raisecom#`**`show rmon events`**	Show information about the RMON event group.

No.	Command	Description
4	Raisecom#**show rmon statistics** [*interface-type interface-list*]	Show information about the RMON statistics group.
5	Raisecom#**show rmon history** *interface-type interface-list*	Show information about the RMON history group.

12.3.9 Maintenance

Maintain the ISCOM2600G series switch as below.

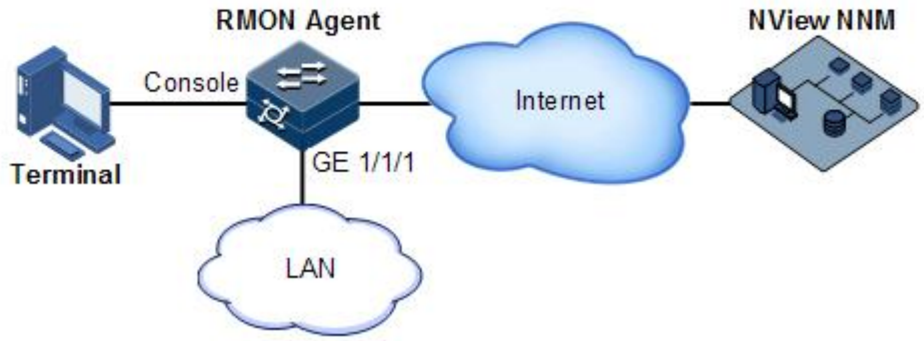
Command	Description
Raisecom(config)#**clear rmon**	Clear all RMON configurations.

12.3.10 Example for configuring RMON alarm group

Networking requirements

As shown in Figure 12-7, the ISCOM2600G series switch is the Agent, connected to terminal through the Console interface, connected to remote NView NNM system through Internet. Enable RMON statistics and gather performance statistic on Port 3. When packets received on Port 3 exceeds the threshold in a period, logs are recorded and Trap is sent.

Figure 12-7 RMON networking



Configuration steps

Step 1 Create an event with index ID 1, used to record and send logs with description string High-ifOutErrors. The owner of logs is system.

```
Raisecom#config
```

```
Raisecom(config)#rmon event 1 log description High-ifOutErrors owner
system
```

Step 2 Create an alarm item with index ID 10, used to monitor MIB variables 1.3.6.1.2.1.2.2.1.20.1 every 20s. If the variable increases by more than 15, the Trap alarm will be triggered. The owner of alarm message is also 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 check whether there is information about event group events on the ISCOM2600G series switch.

```
Raisecom#show rmon alarms
Alarm group information:
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 event**s command to check whether there is information about alarm group on the ISCOM2600G series switch.

```
Raisecom#show rmon events
Event group information:
Event 1 is active, owned by system
Event description:  high.
Event generated at 0:0:0
Register log information when event is fired.
```

When an alarm event is triggered, you can also check related information in the alarm management part of the NView NNM system.

12.4 LLDP

12.4.1 Introduction

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

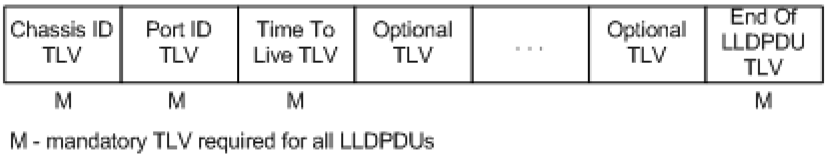
LLDP packet

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

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

As shown in Figure 12-8, LLDPDU is made by several TLV, including 4 mandatory TLV and several optional TLV.

Figure 12-8 Structure of a LLDPDU



As shown in Figure 12-9, each TLV denotes a piece of information at local, such as device ID, interface number related Chassis ID TLV, Port ID TLV, and fixed TLV.

Figure 12-9 Structure of a TLV packet

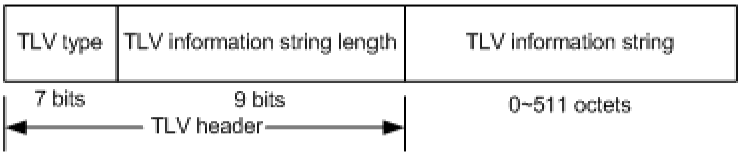


Table 12-1 lists TLV types. At present only types 0–8 are used.

Table 12-1 TLV types

TLV type	Description	Optional/Required
0	End Of LLDPDU	Required
1	Chassis ID	Required
2	Interface number	Required
3	Time To Live	Required
4	Interface description	Optional

TLV type	Description	Optional/Required
5	System name	Optional
6	System description	Optional
7	System capabilities	Optional
8	Management address	Optional

Principles

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

The procedure of packet exchange:

- When the local device transmits packet, it gets system information required by TLV from NView NNM (Network Node Management) and gets configurations from LLDP MIB to generate TLV and form LLDPDU to transmit to peer.
- The peer receives LLDPDU and analyzes TLV information. If there is any change, the information will be updated in neighbor MIB table of LLDP and notifies the NView NNM system.

When the device status is changed, the ISCOM2600G series switch sends a LLDP packet to the peer. To avoid sending LLDP packet continuously because of device status changes frequently, you can configure a delay timer for sending the LLDP packet.

The aging time of Time To Live (TTL) of 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 indicates the time period to send LLDP packets from neighbor node.
- Hold-multiplier refers to the aging coefficient of device information in neighbor node.

12.4.2 Preparing for configurations

Scenario

When you obtain connection information between devices through NView NNM system for topology discovery, the ISCOM2600G series switch 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

12.4.3 Default configurations of LLDP

Default configurations of LLDP are as below.

Function	Default value
Global LLDP	Disable
LLDP interface status	Enable
Delay timer	2s
Period timer	30s
Aging coefficient	4
Restart timer	2s
Alarm function	Enable
Alarm notification timer	5s
Destination MAC address of LLDP packet	0180.c200.000e

12.4.4 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 ISCOM2600G series switch 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 ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**lldp enable**	Enable global LLDP.

12.4.5 Enabling interface LLDP

Enable interface LLDP for the ISCOM2600G series switch 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-gigaethernet1/1/1)#**lldp enable**	Enable LLDP on an interface.

12.4.6 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 ISCOM2600G series switch 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.

12.4.7 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 ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`lldp trap-interval`** *`period`*	(Optional) configure the period of the timer for sending LLDP alarm Traps.

12.4.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#`**`show lldp local config`**	Show LLDP local configurations.

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

12.4.9 Maintenance

Maintain the ISCOM2600G series switch as below.

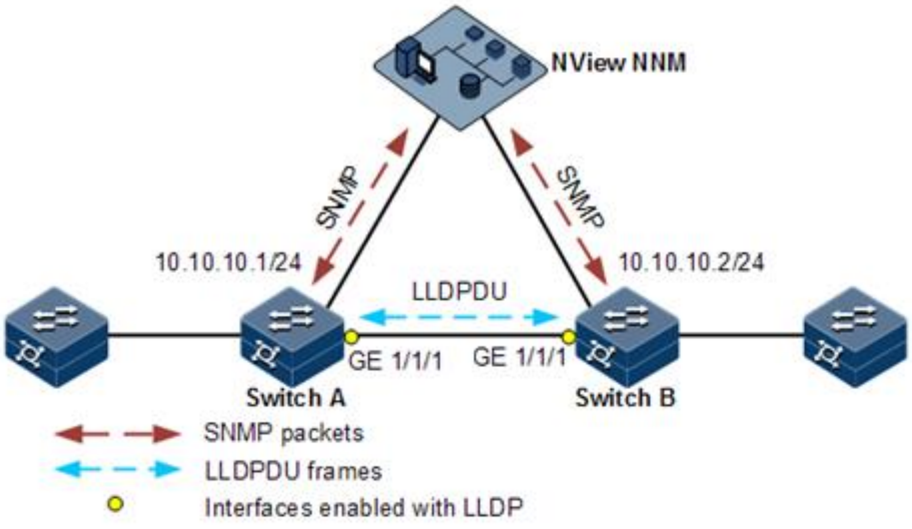
Command	Description
Raisecom(config)#**clear lldp statistic** *interface-type interface-number*	Clear LLDP statistics.
Raisecom(config)#**clear lldp remote-table** [*interface-type interface-number*]	Clear LLDP neighbor information.
Raisecom(config)#**clear lldp global statistic**	Clear global LLDP statistics.

12.4.10 Example for configuring LLDP

Networking requirements

As shown in Figure 12-10, the Switch is connected to the Nview NNM system; enable LLDP between Switch A and Switch B, query Layer 2 link change through the Nview NNM system. The neighbor aging, new neighbor and neighbor information changes will be reported as LLDP alarms to the NView NNM system.

Figure 12-10 LLDP networking



Configuration steps

Step 1 Enable global LLDP and LLDP alarm.

Configure Switch A.

```
Raisecom#name SwitchA
SwitchA#config
SwitchA(config)#lldp enable
```

Configure Switch B.

```
Raisecom#name SwitchB
SwitchB#config
SwitchB(config)#lldp enable
```

Step 2 Configure the management IP address.

Configure Switch A.

```
SwitchA(config)#create vlan 1024 active
SwitchA(config)#interface gigaethernet 1/1/1
SwitchA(config-gigaethernet1/1/1)#switchport access vlan 1024
SwitchA(config-gigaethernet1/1/1)#exit
SwitchA(config)#interface vlan 1
SwitchA(config-vlan1)#ip address 10.10.10.1 255.255.255.0
SwitchA(config-vlan1)#exit
```

Configure Switch B.

```
SwitchB(config)#create vlan 1024 active
SwitchB(config)#interface gigaethernet1/1/1
SwitchB(config-gigaethernet1/1/1)#switchport access vlan 1024
SwitchB(config)#interface vlan 1
SwitchB(config-vlan1)#ip address 10.10.10.2 255.255.255.0
SwitchB(config-vlan1)#exit
```

Step 3 Configure LLDP attributes.

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 configurations.

```
SwitchA#show lldp local config
System configuration:
-------------------------------------------------------------------
LLDP enable status:              enable (default is disabled)
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)
-------------------------------------------------------------------
Port           Status       Packet destination-mac
---------------------------------------------------------
GE1/1/1        enable       0180.C200.000E
GE1/1/2        enable       0180.C200.000E
GE1/1/3        enable       0180.C200.000E
GE1/1/4        enable       0180.C200.000E
GE1/1/5        enable       0180.C200.000E
GE1/1/6        enable       0180.C200.000E
```

```
……
SwitchB#show lldp local config
System configuration:
-----------------------------------------------------------------
LLDP enable status:               enable (default is disabled)
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)
-----------------------------------------------------------------
Port           Status       Packet destination-mac
-------------------------------------------------------
GE1/1/1         enable       0180.C200.000E
GE1/1/2         enable       0180.C200.000E
GE1/1/3         enable       0180.C200.000E
GE1/1/4         enable       0180.C200.000E
GE1/1/5         enable       0180.C200.000E
GE1/1/6         enable       0180.C200.000E
……
```

Use the **show lldp remote** command to show neighbor information.

```
SwitchA#show lldp remote
Port  ChassisId         PortId       SysName   MgtAddress    ExpiredTime
-------------------------------------------------------------------------
gigaethernet1/1/1  000E.5E02.B010    gigaethernet1/1/1        SwitchB
10.10.10.2    106
……
SwitchB#show lldp remote
Port          ChassisId    PortId   SysName   MgtAddress    ExpiredTime
-------------------------------------------------------------------------
gigaethernet1/1/1  000E.5E12.F120 gigaethernet1/1/1   SwitchA
 10.10.10.1 106
……
```

12.5 Optical module DDM

12.5.1 Introduction

Optical module Digital Diagnostics Monitoring (DDM) on the ISCOM2600G series switch supports Small Form-factor Pluggable (SFP) and 10GE SFP+ diagnosis.

The fault diagnostics function of SFP provides the system a performance monitor method. The network administrator analysis the monitor data provided by SFP to predict the age of transceiver, isolate system fault and authenticate modules compatibility during installation.

The performance parameters of optical module which are monitored by optical module DDM are as below:

- Modular temperature
- Inner power voltage
- Tx offset current
- Tx optical power
- Rx optical power

When the performance parameters reach alarm threshold or status information changes, the corresponding Trap alarm will be generated.

12.5.2 Preparing for configurations

Scenario

Fault diagnostics f optical modules provide a method for detecting SFP performance parameters. You can predict the service life of optical module, isolate system fault and check its compatibility during installation through analyzing monitoring data.

Prerequisite

N/A

12.5.3 Default configurations of optical module DDM

Default configurations of optical module DDM are as below.

Function	Default value
Global optical module DDM	Disable
Interface optical module DDM	Enable
Global optical DDM Trap	Disable
Interface optical DDM Trap	Disable
Interface optical DDM password check	Disable

12.5.4 Enabling optical module DDM

Enable optical module DDM for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`transceiver ddm enable`**	Enable SFP DDM globally.
3	`Raisecom(config)#`**`interface`** *`interface-type interface-number`*	Enter physical layer interface configuration mode.

Step	Command	Description
4	Raisecom(config-gigaethernet1/1/1)#**transceiver ddm enable**	Enable interface optical module DDM. Only when global optical DDM is enabled, the optical module, where interface optical module DDM is enabled, can the ISCOM2600G series switch perform DDM.

12.5.5 Enabling optical module DDM Trap

Enable optical module DDM Trap for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server trap transceiver enable**	Enable optical module DDM Trap globally.
3	Raisecom(config)#**interface** *interface-type interface-number*	Enter physical layer interface configuration mode.
4	Raisecom(config-gigaethernet1/1/1)#**transceiver trap enable**	Enable interface optical module DDM Trap. Only when global optical DDM Trap is enabled, the optical module, where interface optical module DDM Trap is enabled, can the ISCOM2600G series switch send Traps.

12.5.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show transceiver**	Show global optical module DDM and interface optical module DDM configurations.
2	Raisecom#**show transceiver ddm** *interface-type interface-list* [**detail**]	Show optical module DDM performance parameters.
3	Raisecom#**show transceiver** *interface-type interface-list* **history** [**15m** | **24h**]	Show historical information about optical module DDM.
4	Raisecom#**show transceiver information** *interface-type interface-list*	Show basic information about the optical module.
5	Raisecom#**show transceiver threshold-violations** *interface-type interface-list*	Show the information when the optical module parameters exceed the thresholds.

12.6 System log

12.6.1 Introduction

The system log refers that the ISCOM2600G series switch records the system information and debugging information in a log and sends the log to the specified destination. When the ISCOM2600G series switch 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 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.
- Buffer: send the log message to the buffer.
- SNMP server: convert logs to Trap and then outputs Trap to the SNMP server.

According to the severity level, the log is identified by 8 severity levels, as listed in Table 12-2.

Table 12-2 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, namely, the severity ranges from emergencies to errors, can be sent.

12.6.2 Preparing for configurations

Scenario

The ISCOM2600G series switch 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

12.6.3 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).
Output log information to buffer	Disable, the default level is information (6).
Log Debug level	Low
Output log information to history list	Disable
Log history list size	1
Transfer log to Trap	Disable. The default level is warning (4).
Log buffer size	4 Kbytes
Transmitting rate of system log	No limit
Timestamp of system log information	• Debug: no timestamp to debug level (7) Syslog information. • Log: The timestamp to 0–6 levels Syslog information is absolute time.

12.6.4 Configuring basic information of system log

Configure basic information of system log for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#logging on`	(Optional) enable system log.

Step	Command	Description
3	Raisecom(config)#**logging time-stamp { debug | log } { datetime | none | uptime }**	(Optional) configure timestamp for system log. The optional parameter **debug** is used to assign debug level (7) system log timestamp; by default, this system log does not have timestamp The optional parameter **log** is used to assign debug level 0–6 system log timestamp; by default, this system log adopts date-time as timestamp.
4	Raisecom(config)#**logging rate-limit** *log-num*	(Optional) configure transmitting rate of system log.
5	Raisecom(config)#**logging sequence-number**	(Optional) configure sequence of system log. The sequence number only applies to the console, monitor, log file, and log buffer, but not log host and history list.
6	Raisecom(config)#**logging discriminator** *distriminator-number* { **facility** | **mnemonics** | **msg-body** } { { **drops** | **includes** } *key* | **none** }	(Optional) create and configure system log filter. The filter can filter output log from the console, monitor, log file and log buffer.
7	Raisecom(config)#**logging buginf** [**high** | **normal** | **low** | **none**]	(Optional) configure sending Debug-level logs.

12.6.5 Configuring system log output

Configure system log output for the ISCOM2600G series switch 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** | **distriminator** *distriminator-number*]	(Optional) output system logs to the console.
3	Raisecom(config)#**logging host** *ip-address* [*log-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** | **distriminator** *distriminator-number*]	(Optional) output system logs to the log host. Up to 10 log hosts are supported.

Step	Command	Description
	Raisecom(config)#**logging** [**host** *ip-address*] **facility** { **alert** | **audit** | **auth** | **clock** | **cron** | **daemon** | **ftp** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **ntp** | **sercurity** | **syslog** | **user** | **uucp** }	Configure the facility field of the log to be sent to the log host. Configuration may fail if you do not create the log host. This configuration is available for all log hosts configured on the ISCOM2600G series switch.
4	Raisecom(config)#**logging monitor** [*log-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** | **distriminator** *distriminator-number*]	(Optional) output system logs to the monitor.
5	Raisecom(config)#**logging file** [**discriminator** *discriminateor-number*]	(Optional) output system logs to the Flash of the ISCOM2600G series switch. Only warning-level logs are available.
6	Raisecom(config)#**logging buffered** [*log-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** | **distriminator** *distriminator-number*]	(Optional) output system logs to the buffer.
	Raisecom(config)#**logging buffered size** *size*	(Optional) configure the system log buffer size.
7	Raisecom(config)#**logging history**	(Optional) output system logs to the log history list. The level of the output logs is the one of the translated Trap.
	Raisecom(config)#**logging history size** *size*	(Optional) configure the log history list size.
	Raisecom(config)#**logging trap** [*log-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings** | **distriminator** *distriminator-number*]	(Optional) enable translating specified logs in the history list to Traps. Configurations may fail if the system logs are not output to the log history list.

12.6.6 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 buffer`	Show information about the system log buffer.
3	`Raisecom#show logging discriminator`	Show filter information.
4	`Raisecom#show logging file`	Show contents of system log.
5	`Raisecom#show logging history`	Show information about the system log history list.

12.6.7 Maintenance

Maintain the ISCOM2600G series switch as below.

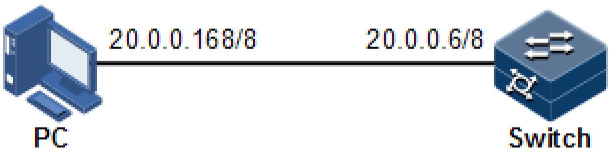
Command	Description
`Raisecom(config)#clear logging buffer`	Clear log information in the buffer.
`Raisecom(config)#clear logging statistics`	Clear log statistics.

12.6.8 Example for configuring outputting system logs to log host

Networking requirements

As shown in Figure 12-11, configure system log, and output device log information to log host for user to check.

Figure 12-11 Networking of outputting system log to log host



Configuration steps

Step 1 Configure the IP address of the ISCOM2600G series switch.

```
Raisecom#config
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip address 20.0.0.6 255.0.0.0
Raisecom(config-vlan1)#exit
```

Step 2 Configure the system log to be output to the log host.

```
Raisecom(config)#logging on
Raisecom(config)#logging time-stamp log datetime
Raisecom(config)#logging rate-limit 2
Raisecom(config)#logging host 20.0.0.168 warnings
```

Checking results

Use the **show logging** command to show configurations of system log.

```
Raisecom#show logging
Syslog logging:         enable
Dropped Log messages:    0
Dropped debug messages:  0
Rate-limited:           2 messages per second
Squence number display:  disable
Debug level time stamp:  none
Log level time stamp:    datetime
Log buffer size:        4kB
Debug level:            low
Syslog history logging:  disable
Syslog history table size:1
Dest     Status   Level           LoggedMsgs  DroppedMsgs  Discriminator
-------------------------------------------------------------------------
---
buffer   enable   informational(6)  10        0          0
console  enable   informational(6)  10        0          0
trap     disable  warnings(4)      0         0          0
file     enable   debugging(7)     17        0          0
Log host information:
Max number of log server:    10
Current log server number:   1
Target Address     Level          Facility      Sent     Drop
Discriminator
-------------------------------------------------------------------------
--------------
20.0.0.168        warnings(4)     local7        0        0        0
```

12.7 Alarm management

12.7.1 Introduction

Alarm means when a fault is generated on the ISCOM2600G series switch or some working condition changes, the system will generate alarm information according to different faults.

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

Alarm information is stored in the alarm buffer. Meanwhile, the alarm information is generated to log information. If a Network Management System (NMS), the alarm information will be sent to network management system through SNMP. The information sent to the NMS is called Trap information.

Alarm classification

There are three kinds of alarm information according to properties of an alarm:

- Fault alarm: refers to alarms for some hardware fault or some abnormal important functions, such as port Down alarm;
- Recovery alarm: refers to alarms that are generated when device failure or abnormal function returns to normal, such as port Up alarm;
- Event alarm: refers to prompted alarms or alarms that are generated because of failure in relating the fault to the recovery, such as alarms generated by failing to Ping.

The alarm information can be divided into five types according to functions:

- Communication alarm: refers to alarms related to the processing of information transmission, including alarms that are generated by communication fault between Network Elements (NE), NEs and NMS, or NMS and NMS.
- Service quality alarm: refers to alarms caused by service quality degradation, including congestion, performance decline, high resource utilization rate, and the bandwidth reducing.
- Processing errored alarm: refers to alarms caused by software or processing errors, including software errors, memory overflow, version mismatching, and the abnormal program aborts.
- Environmental alarm: refers to alarms caused by equipment location-related problems, including the environment temperature, humidity, ventilation and other abnormal working conditions.
- Device alarm: refers to alarms caused by failure of physical resources, including power, fan, processor, clock, Rx/Tx interfaces, and other hardware.

Alarm output

There are three alarm information output modes:

- Alarm buffer: alarm information is recorded in tabular form, including the current alarm table and history alarm table.
  - Current alarm table, recording alarm information which is not cleared, acknowledged or restored.
  - History alarm table, consisting of acknowledged and restored alarm information, recording the cleared, auto-restored or manually acknowledged alarm information.
- Log: alarm information is generated to system log when recorded in the alarm buffer, and stored in the alarm log buffer.
- Trap information: alarm information sent to NMS when the NMS is configured.

Alarm will be broadcasted according to various terminals configured by the ISCOM2600G series switch, including CLI terminal and NMS.

Log output of alarm information starts with the symbol "#", and the output format is: `#Index TimeStamp HostName ModuleName/Severity/name:Arise From Description`.

Table 12-3 lists descriptions about alarm fields.

Table 12-3 Alarm fields

Field	Description
TimeStamp	Time when an alarm is generated
ModuleName	Name for a module where alarms are generated
Severity	Alarm level
Arise From Description	Descriptions about an alarm

Alarm levels

The alarm level is used to identify the severity degree of an alarm. The level is defined in Table 12-4.

Table 12-4 Alarm levels

Level	Description	Syslog
Critical (3)	This alarm has affected system services and requires immediate troubleshooting. Restore the device or source immediately if they are completely unavailable, even it is not during working time.	1 (Alert)
Major (4)	This alarm has affected the service quality and requires immediate troubleshooting. Restore the device or source service quality if they decline; or take measures immediately during working hours to restore all performances.	2 (Critical)
Minor (5)	This alarm has not influenced the existing service yet, which needs further observation and take measures at appropriate time to avoid more serious fault.	3 (Error)
Warning (6)	This alarm will not affect the current service, but maybe the potential error will affect the service, so it can be considered as needing to take measures.	4 (Warning)
Indeterminate (2)	Uncertain alarm level, usually the event alarm.	5 (Notice)
Cleared (1)	This alarm shows to clear one or more reported alarms.	5 (Notice)

Related concepts

Related concepts about alarm management are displayed as below:

- Alarm inhibition

The ISCOM2600G series switch only records root-cause alarms but incidental alarms when enabling alarm inhibition. For example, the generation of alarm A will inevitably produce alarm B which is in the inhibition list of alarm A, then alarm B is inhibited and does not appear in alarm buffer and record the log information when enabling alarm inhibition. By enabling alarm inhibition, the ISCOM2600G series switch can effectively reduce the number of alarms.

Alarm A and alarm B will be recorded on the ISCOM2600G series switch and reported to the NMS when alarm inhibition is disabled.

- Alarm auto-report

Auto-report refers that an alarm will be reported to NMS automatically with its generation and you do not need to initiate inquiries or synchronization.

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

Note

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

- Alarm monitoring

Alarm monitoring is used to process alarms generated by modules:

  - When the alarm monitoring is enabled, the alarm module will receive alarms generated by modules, and process them according to the configurations of the alarm module, such as recording alarm in alarm buffer, or recording system logs.
  - When the alarm monitoring is disabled, the alarm module will discard alarms generated by modules without follow-up treatment. In addition, alarms will not be recorded on the ISCOM2600G series switch.

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

- Alarm reverse mode

Alarm reverse refers to the device will report the information opposite to actual status when recording alarm information, or report the alarm when there is no alarm information. Not report if there is alarm information.

Currently, the device is only in support of reverse mode configuration of the interface. There are three reverse modes to be configure; the specific definitions are as below:

  - Non-reverse mode

The device alarm is reported normally.

  - Manual reverse mode

Configure the alarm reverse mode of an interface as manual reverse mode, then no matter what the current alarm state is, the reported alarm state of the interface will be changed opposite to the actual alarm state immediately, namely, not report when there are alarms, report when there are not alarms actually. The interface will maintain the opposite alarm state regardless of the alarm state changes before the alarm reverse state being restored to non-reverse mode.

  - Auto-reverse mode

Configure the alarm reverse mode as auto-reverse mode. If the interface has not actual reverse alarm currently, the configuration will return fail; if the interface has actual reverse alarm, the configuration is success and enter reverse mode, i.e. the interface reported alarm status is changed opposite to the actual alarm status immediately. After the alarm is finished, the enabling state of interface alarm reverse will ends automatically and changes to non-reverse alarm mode so that the alarm state can be reported normally in next alarm.

- Alarm delay

Alarm delay refers that the ISCOM2600G series switch will record alarms and report them to NMS after a delay but not immediately when alarms generate. Delay for recording and reporting alarms are identical.

By default, the device alarm is reported once generating (0s), which is instant reporting; clear alarm once it ends (0s), which is instant clearing.

- Alarm storage mode

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

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

Use configured storage mode to deal with new generated alarm information when the alarm information in device alarm table is full.

- Clearing alarms

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

- Viewing alarms

The administrator can check alarms and monitor alarm information directly on the ISCOM2600G series switch. If the ISCOM2600G series switch is configured with NView NNM system, the administrator can monitor alarms on the NView NNM system.

12.7.2 Preparing for configurations

Scenario

When the device fails, alarm management module will collect fault information and output alarm occurrence time, alarm name and description information in log format to help users locate problem quickly.

If the device is configured with the NMS, alarm information can be reported directly to the NMS, providing possible alarm causes and treatment recommendations to help users deal with fault.

If the device is configured with hardware monitoring, it will record the hardware monitoring alarm table, generated Syslog, and sent Trap when the operation environment of the device becomes abnormal, and notify the user of taking actions accordingly and prevent faults.

Alarm management makes it easy for the user to take alarm inhibition, alarm auto-reporting, alarm monitoring, alarm reverse, alarm delay, alarm memory mode, alarm clear and alarm view directly on the device.

Prerequisite

Hardware environment monitoring alarm output:

- In Syslog output mode: alarms will be generated into system logs. When you need to send alarm information to the system log host, configure the IP address of the system log host for the device.
- In Trap output mode: configure the IP address of the NMS for the device.

12.7.3 Configuring basic functions of alarm management

Configure basic information of alarm management for the ISCOM2600G series switch as below.

All following steps are optional and no sequence between them.

Step	Command	Description
1	`Raisecom#`**`config`**	Enter global configuration mode.
2	`Raisecom(config)#`**`alarm inhibit enable`**	Enable alarm inhibition. By default, it is enabled.
3	`Raisecom(config)#`**`alarm auto-report all enable`**	Enable alarm auto-reporting.
	`Raisecom(config)#`**`alarm auto-report`** *`alarm-restype alarm-restype-value`* **`enable`**	Enable alarm auto-reporting of a specified alarm source.
	`Raisecom(config)#`**`alarm auto-report type`** *`alarm-type`* **`enable`**	Enable alarm auto-reporting of a specified alarm type.
	`Raisecom(config)#`**`alarm auto-report type`** *`alarm-type alarm-restype alarm-restype-value`* **`enable`**	Enable alarm auto-reporting of a specified alarm source and type.
4	`Raisecom(config)#`**`alarm monitor all enable`**	Enable alarm monitoring.
	`Raisecom(config)#`**`alarm monitor`** *`alarm-restype alarm-restype-value`* **`enable`**	Enable alarm monitoring of a specified alarm source.
	`Raisecom(config)#`**`alarm monitor type`** *`alarm-type`* **`enable`**	Enable alarm monitoring of a specified alarm type.
	`Raisecom(config)#`**`alarm monitor type`** *`alarm-type alarm-restype alarm-restype-value`* **`enable`**	Enable alarm monitoring of a specified alarm source and type.
5	`Raisecom(config)#`**`alarm inverse`** *`interface-type interface-number`* `{` **`none`** `|` **`auto`** `|` **`manual`** `}`	Configure alarm reverse modes. By default, it is none; namely, alarm reverse is disabled.
6	`Raisecom(config)#`**`alarm`** `{` **`active`** `|` **`cleared`** `}` **`delay`** *`second`*	Configure alarm delay. By default, it is 0s.

Step	Command	Description
7	Raisecom(config)#**alarm active storage-mode** { **loop** | **stop**}	Configure alarm storage modes. By default, it is stop.
8	Raisecom(config)#**alarm clear all**	(Optional) clear all current alarms.
	Raisecom(config)#**alarm clear index** *index*	(Optional) clear current alarms of the specified alarm index.
	Raisecom(config)#**alarm clear** *alarm-restype alarm-restype-value*	(Optional) clear current alarms of the specified alarm source.
	Raisecom(config)#**alarm clear type** *alarm-type*	(Optional) clear current alarms of the specified alarm type.
	Raisecom(config)#**alarm clear type** *alarm-type alarm-restype alarm-restype-value*	(Optional) clear current alarms of the specified alarm source and type.
9	Raisecom(config)#**alarm syslog enable**	(Optional) enable alarms to be output to system logs. By default, it is disabled.
10	Raisecom(config)#**exit** Raisecom#**show alarm active** [*module_name* | **severity** *severity*]	(Optional) show information about current alarms.
	Raisecom#**show alarm cleared** [*module_name* | **severity** *severity*]	(Optional) show information about historical alarms.

Note

You can enable/disable alarm monitoring, alarm auto-reporting, and alarm clearing on modules that support alarm management.

12.7.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show alarm management** [*alarm_type*]	Show parameters of current alarms, including status of alarm inhibition, alarm reverse mode, alarm delay, and alarm storage mode, maximum alarm buffer size, and alarm log size.
2	Raisecom#**show alarm log**	Show alarm statistics in the system log.

No.	Command	Description
3	`Raisecom#show alarmmanagement statistics`	Show statistics of alarm management module.
4	`Raisecom#show alarm active`	Show information about current alarms.

12.8 Hardware environment monitoring

12.8.1 Introduction

Hardware environment monitoring mainly refers to monitor the running environment of the ISCOM2600G series switch. The monitoring alarm events include:

- Power supply state alarm
- Temperature beyond threshold alarm
- Voltage beyond threshold alarms
- Abnormal interface status alarm
- Flash monitoring alarm

There are several ways to notify users when an alarm is generated. The alarm event output methods are as below:

- Save to the device hardware environment monitoring alarm buffer;
- Output Syslog system log;
- Send Trap to network management center;
- Output to the relay fault indication LED.

You can take appropriate measures to prevent failure when alarm events happen.

Alarm events

- Power supply monitoring alarms

Power supply state alarms include 2 types.

- Power supply voltage anomaly alarm

An alarm is generated when the power supply voltage is 20% greater than the pre-configured voltage (12 V) or is 20% smaller than the pre-configured voltage (12 V). In addition, an alarm is generated when the voltage value returns to normal state. The ISCOM2600G series switch supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NView NNM system, and outputting to the system log and relay.

- Power supply state change alarms

Power supply state change refers that unplugged power supply is plugged into the device and vice versa. The ISCOM2600G series switch supports dual power supplies. Therefore, power supply state change alarms are divided into the single power supply state change alarm and device dying gasp alarm.

- Dual power supply state change alarm: notify uses that power supply 1/power supply 2 changes. The ISCOM2600G series switch supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NView NNM system, and outputting to the system log and relay.
- Device dying gasp alarm: dual power modules are unplugged, namely, two power modules are out of position. The ISCOM2600G series switch supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NView NNM system, and outputting to the system log and relay.

- Temperature beyond threshold alarm

The device supports temperature beyond threshold alarm event, when the current temperature is lower than low temperature threshold, the low temperature alarm event will generate. The ISCOM2600G series switch supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NView NNM system, and outputting to the system log and relay.

When the device current temperature is higher than high temperature threshold, the high temperature alarm event will generate. The ISCOM2600G series switch supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NView NNM system, and outputting to the system log and relay.

- Voltage beyond threshold alarm

The device supports voltage beyond threshold alarm event, when the current voltage is lower than low voltage threshold, the low voltage alarm event will generate. The ISCOM2600G series switch supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NView NNM system, and outputting to the system log and relay.

When current voltage value of the monitored voltage is greater than the threshold, a high voltage alarm is generated. The ISCOM2600G series switch supports saving to the device hardware environment monitoring alarm buffer, sending Trap to the NView NNM system, and outputting to the system log and relay.

Note

The ISCOM2600G series switch monitors 3.3V master chip voltage only.

- Interface status alarm

Each interface has two alarm events:

- Interface link-fault alarm: link failure alarm refers to the peer link signal loss. The alarm event only aims at optical port, but not power port.
- Interface link-down alarm: interface status Down alarm.

The ISCOM2600G series switch supports saving these two types of alarm events to the device hardware environment monitoring alarm buffer, sending Trap to the NView NNM system, and outputting to the system log and relay.

Alarm output modes

Hardware environment monitoring alarm output modes are as below.

- Hardware environment monitoring alarm buffer output, which is recorded to the hardware environment monitoring alarm table
  - The hardware environment monitoring current alarm table, recording current alarm information which has not been cleared and restored.

- The hardware environment monitoring history alarm table, recording current, restored, and manually cleared alarms.

Hardware environmental monitoring alarm information can be recorded in the current hardware environment monitoring alarm table and hardware environment monitoring history alarm table automatically without configuring manually.

- Trap output

Alarms are output to network management center in Trap mode.

Trap output has global switch and all monitored alarm events still have their own Trap alarm output switches. When enabling the global switch and monitored alarm events switches simultaneously, the alarm will generate Trap output.

Table 12-5 describes Trap information.

Table 12-5 Trap information

Field	Description
Alarm status	● asserted (current alarm) ● cleared (alarm recovery) ● clearall (clear all alarm information)
Alarm source	● device (global alarm) ● Interface number (interface status alarm)
Timestamp	Alarm time, in the form of absolute time
Alarm event type	● dev-power-down (power-down alarm) ● power-abnormal (power-abnormal alarm, one of two powers is power down.) ● high-temperature (high-temperature alarm) ● low-temperature (low-temperature alarm) ● high-volt (high-voltage alarm) ● low-volt (low-voltage alarm) ● link-down (interface LinkDown alarm) ● link-falut (interface LinkFault alarm) ● all-alarm (clear all alarm information)

- Syslog output

Record alarm information to Syslog.

Syslog output has global switch and all monitored alarm events still have their own Syslog alarm output switches. When enabling the global switch and monitored alarm events switches simultaneously, the alarm will generate Syslog output.

Table 12-6 describes Syslog information.

Table 12-6 Syslog information

Field	Description
Facility	The module name generating alarm, the hardware environment monitoring module is fixed as alarm.

Field	Description
Severity	Level, the same as defined in system logs. For details, see Table 12-2.
Mnemonics	Alarm event type. For details, see Table 12-5.
Msg-body	Main body, describing alarm event contents.

- Relay output

"Outputting to relay" or "Outputting from relay" indicates outputting alarms to the relay and fault indication LED simultaneously. The relay and fault indication LED are bound together. Relay output and fault indicate LED output are controlled by the relay alarm output switch. As a public fault output mode for all alarms, the relationship among all alarms is logical "OR".

If any alarm is generated on the ISCOM2600G series switch, the device outputs the alarm from the relay. The relay cannot work properly unless all alarms are cleared.

Relay output cannot be enabled globally. Relay output is enabled for every monitored alarm.

12.8.2 Preparing for configurations

Scenario

Hardware environment monitoring provides environment monitoring for the devices, through which you can monitor the fault. When device operation environment is abnormal, this function will record hardware environment monitoring alarm list, generate system log, or send Trap and other alarms to notify taking corresponding measures and preventing fault.

Prerequisite

Hardware environment monitoring alarm output:

- In Syslog output mode: alarms will be generated into system logs. When you need to send alarm information to the system log host, please configure system log host IP address for the device.
- In Trap output mode: please configure network management center IP address for the device.
- In relay output mode: relay alarm output switch is enabled for every alarm.

12.8.3 Default configurations of hardware environment monitoring

Default configurations of hardware environment monitoring are as below.

Function	Default value
Global hardware environment monitoring alarm Syslog output	Disable
Global hardware environment monitoring alarm Trap output	Disable
Power down event alarm	• Enable Trap output.

Function	Default value
Temperature alarm output	Enable Syslog system log output. Enable relay output.
Voltage alarm output	
Interface link-down event alarm output	Enable Trap output. Enable Syslog system log output. Disable relay output.
Interface link-fault event alarm output	Disable Trap output. Disable Syslog system log output. Disable relay output.
High temperature alarm threshold	102 ℃
Low temperature alarm threshold	-40 ℃
High voltage threshold	3450 mV
Low voltage threshold	3150 mV

12.8.4 Enabling global hardware environment monitoring

Enable global hardware environment monitoring for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#config`	Enter global configuration mode.
2	`Raisecom(config)#logging alarm`	(Optional) enable global hardware environment monitoring alarm Syslog output.
3	`Raisecom(config)#snmp-server alarm-trap enable`	(Optional) enable global hardware environment monitoring alarm Trap.

Note

- When enabling global hardware environment monitoring alarm Syslog output, alarm event can generate Syslog only when Syslog output under alarm event is also enabled.
- When enabling global hardware environment monitoring alarm sending Trap, alarm event can send Trap only when Trap output under alarm event is also enabled.
- When enabling global hardware environment monitoring alarm Relay output, alarm event can generate Relay only when Relay output under alarm event is also enabled.

12.8.5 Configuring temperature monitoring alarm

Configure temperature monitoring alarm for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)# **alarm temperature** { **high** *high-value* | **low** *low-value* | **notifies** | **syslog** }	Enable temperature monitoring alarm output and configure temperature monitoring alarm output modes. • The high temperature threshold (high-value) must be greater than the low temperature threshold (low-value). • The low temperature threshold (low-value) must be smaller than the high temperature threshold (high-value).

12.8.6 Configuring voltage monitoring alarm

Configure voltage monitoring alarm for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)# **alarm voltage** { **high** *high-value* | **low** *low-value* | **notifies** | **syslog** }	Enable voltage alarm output and configure voltage alarm output modes or voltage alarm threshold. **Note** The ISCOM2600G series switch monitors 3.3V master chip voltage only.

12.8.7 Clearing all hardware environment monitoring alarms manually

Clear all hardware environment monitoring alarms manually for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**clear alarm**	Clear alarms manually. **Note** Use this command to clear all alarms in current alarm list and generate an all-alarm alarm in history alarm list. If enabling global sending Trap, the all-alarm alarm will be output in Trap mode; if enabling global Syslog, the all-alarm alarm will be output in Syslog mode.

12.8.8 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show alarm`	Show global hardware environment monitoring alarm configurations.
2	`Raisecom#show alarm currrent`	Show current alarms of hardware environment monitoring.
3	`Raisecom#show alarm history`	Show historic alarms of hardware environment monitoring.
4	`Raisecom#show environment [ temperature | voltage ]`	Show current power supply, temperature, voltage alarms, and current environment information.

12.9 CPU monitoring

12.9.1 Introduction

The ISCOM2600G series switch supports CPU monitoring. It can monitor state, CPU utilization rate, and application of stacking of each task in real time in the system. It helps locate faults.

CPU monitoring can provide the following functions:

- Viewing CPU utilization rate

It can be used to view unitization of CPU in each period (5s, 1minute, 10minutes, 2hours). Total unitization of CPU in each period can be shown dynamically or statically.

It can be used to view the operational status of all tasks and the detailed running status information about assigned tasks.

It can be used to view history utilization of CPU in each period.

It can be used to view information about dead tasks.

- Threshold alarm of CPU unitization

If CPU utilization of the system is more than configured upper threshold or less than preconfigured lower threshold in specified sampling period, Trap will be sent, and Trap will provide serial number of 5 tasks whose unitization rate of CPU is the highest in the latest period (5s, 1minute, 10minutes) and their CPU utilization rate.

12.9.2 Preparing for configurations

Scenario

CPU monitoring can give realtime monitoring to task state, CPU utilization rate and stack usage in the system, provide CPU utilization rate threshold alarm, detect and eliminate hidden dangers, or help administrator for 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.

12.9.3 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	99%
Lower threshold of CPU utilization alarm	1%
Sampling period of CPU utilization	60s

12.9.4 Showing CPU monitoring information

Show CPU monitoring information for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**show cpu-utilization** [**dynamic** | **history** { **10min** | **1min** | **2hour** | **5sec** }]	Show CPU utilization.
2	Raisecom#**show process** [**sorted** { **normal-priority** | **process-name** }]	Show states of all tasks.
3	Raisecom#**show process cpu** [**sorted** [**10min** | **1min** | **5sec** | **invoked**]]	Show CPU utilization of all tasks.

12.9.5 Configuring CPU monitoring alarm

Configure CPU monitoring alarm for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
2	Raisecom(config)#**snmp-server trap enable cpu-threshold**	Enable CPU threshold alarm Trap.

Step	Command	Description
3	`Raisecom(config)#cpu rising-threshold threshold-value`	(Optional) configure the rising threshold for CPU alarms.
4	`Raisecom(config)#cpu falling-threshold value`	(Optional) configure the falling threshold for CPU alarms.

12.9.6 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show cpu-utilization`	Show CPU utilization and related configurations.

12.10 Cable diagnosis

12.10.1 Introduction

The ISCOM2600G series switch supports cable diagnosis, which helps you detect lines.

Cable diagnosis contains the following results:

- Time for last cable diagnosis
- Detection result of the Tx cable
- Errored location of the Tx cable
- Detection result of the Rx cable
- Errored location of the Rx cable

12.10.2 Preparing for configurations

Scenario

After cable diagnosis is enabled, you can learn the running status of cables, locate and clear faults, if any, in time.

Prerequisite

N/A

12.10.3 Configuring cable diagnosis

Configure cable diagnosis for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#test cable-diagnostics` *`interface-type interface-number`*	Enable cable diagnosis.

12.10.4 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show cable-diagnostics` `[` *`interface-type interface-number`* `]`	Show results of cable diagnosis.

12.11 Memory monitoring

12.11.1 Preparing for configurations

Scenario

Memory monitoring enables you to learn the memory utilization in real time, and provides memory utilization threshold alarms, thus facilitating you to locate and clear potential risks and help network administrator to locate faults.

Prerequisite

To output memory utilization threshold alarms as Trap, configure the IP address of the target host, namely, the IP address of the NMS server.

12.11.2 Configuring memory monitoring

Configure memory monitoring for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#memory utilization threshold`*`threshold-value`*	Configure the upper threshold for memory utilization alarms. By default, it is 70, namely, 70%.
2	`Raisecom#memory utilization monitor enable`	Enable memory monitoring. By default, it is enabled.

12.11.3 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	`Raisecom#show memory[utilization threshold ]`	Show the memory utilization.

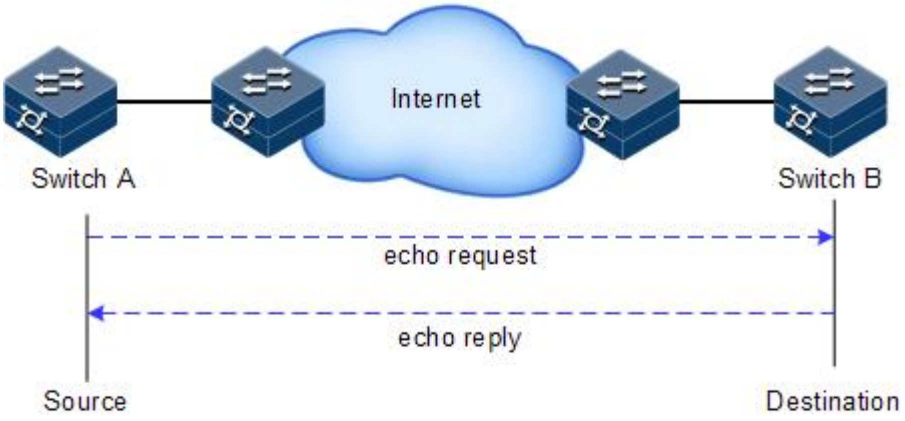
12.12 Ping

12.12.1 Introduction

Packet Internet Groper (PING) derives from the sonar location operation, which is used to detect whether the network is normally connected. Ping is achieved with ICMP echo packets. If an Echo Reply packet is sent back to the source address during a valid period after the Echo Request packet is sent to the destination address, it indicates that the route between source and destination address is reachable. If no Echo Reply packet is received during a valid period and timeout information is displayed on the sender, it indicates that the route between source and destination addresses is unreachable.

Figure 12-12 shows principles of Ping.

Figure 12-12 Principles of Ping



12.12.2 Configuring Ping

Configure Ping for the ISCOM2600G series switch as below.

Step	Command	Description
1	`Raisecom#ping ip-address [ count count ] [ size size ] [ waittime period ]`	(Optional) test the connectivity of the IPv4 network by the **ping** command.
2	`Raisecom#ping ipv6 ipv6-address [ count count ] [ size size ] [ waittime period ]`	(Optional) test the connectivity of the IPv6 network by the **ping** command.

Note

The ISCOM2600G series switch cannot perform other operations in the process of Ping. It can perform other operations only when Ping is finished or break off Ping by pressing **Ctrl**+**C**.

12.13 Traceroute

12.13.1 Introduction

Similar with Ping, Traceroute is a commonly-used maintenance method in network management. Traceroute is often used to test the network nodes of packets from sender to destination, detect whether the network connection is reachable, and analyze network fault

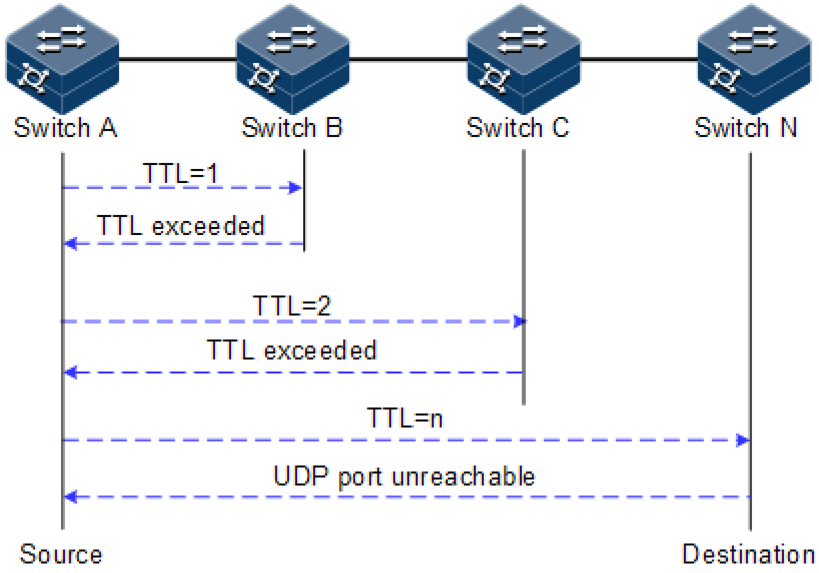
The following shows how Traceroute works:

- First, send a piece of TTL1 sniffer packet (where the UDP port ID of the packet is unavailable to any application programs in destination side).
- TTL deducts 1 when reaching the first hop. Because the TTL value is 0, in the first hop the device returns an ICMP timeout packet, indicating that this packet cannot be sent.
- The sending host adds 1 to TTL and resends this packet.
- Because the TTL value is reduced to 0 in the second hop, the device will return an ICMP timeout packet, indicating that this packet cannot be sent.

The previous steps continue until the packet reaches the destination host, which will not return ICMP timeout packets. Because the port ID of destination host is not be used, the destination host will send the port unreachable packet and finish the test. Thus, the sending host can record the source address of each ICMP TTL timeout packet and analyze the path to the destination according to the response packet.

Figure 12-13 shows principles of traceroute.

Figure 12-13 Principles of Traceroute



12.13.2 Configuring Traceroute

Before using Traceroute, you should configure the IP address and default gateway of the ISCOM2600G series switch.

Configure Traceroute for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**traceroute** *ip-address* [**firstttl** *first-ttl*] [**maxttl** *max-ttl*] [**port** *port-number*] [**waittime** *period*] [**count** *times*] [**size** *size*]	(Optional) test the connectivity of the IPv4 network and view nodes passed by the packet by the **traceroute** command.
2	Raisecom#**traceroute ipv6** *ipv6-address* [**firstttl** *first-ttl*] [**maxttl** *max-ttl*] [**port** *port-id*] [**waittime** *second*] [**count** *times*] [**size** *size*]	(Optional) test the connectivity of the IPv6 network and view nodes passed by the packet by the **traceroute** command.

12.14 Performance statistics

12.14.1 Introduction

Performance statistics is used to gather statistics about service packets on the interface of a monitoring device and enable you to learn network performance. It can be based on interface or service flow in a short or long period. The short period is 15 minutes while the long period is 24 hours. Data in a statistical period is written as data block to the Flash for your review.

- Performance based on interface:
  - Short/Long period performance statistics on the interface: the interfaces include service interfaces and management interfaces.
  - Data saving for short/long period performance statistics on the interface: the interfaces include service interfaces and management interfaces. Data is saved in the Flash in a configured period.
- Performance based on service flow:
  - Short/Long period performance statistics about a service flow: the statistics can be based on the service VLAN or priority.
  - Data saving for short/long period performance statistics about a service flow: the statistics can be based on the service VLAN or priority. Data is saved in the Flash in a configured period.

12.14.2 Preparing for configurations

Scenario

To learn performance of the ISCOM2600G series switch, you can use performance statistics to gather current or historical statistics about packets based on interface or service flow.

Prerequisite

N/A

12.14.3 Default configurations of performance statistics

Default configurations of performance statistics are as below.

Function	Default value
Performance statistics	Enable
Writing global performance statistics to the Flash	Disable
Number of data blocks saved in long period statistics mode	16
Number of data blocks saved in short period statistics mode	3

12.14.4 Configuring performance statistics

Configure performance statistics for the ISCOM2600G series switch as below.

Step	Command	Description
1	Raisecom#**config**	Enter global configuration mode.
5	Raisecom(config)#**performance statistics** { **longinterval** | **shortinterval** } **buckets** *number*	Configure the number of data blocks saved in the Flash for performance statistics in different statistics period mode.

12.14.5 Checking configurations

Use the following commands to check configuration results.

No.	Command	Description
1	Raisecom#**show performance statistics vlan** *vlan-list* { **current** | **history** }	Show performance statistics.

12.14.6 Maintenance

Maintain the ISCOM2600G series switch as below.

Command	Description
Raisecom(config)#**clear performance statistics history**	Clear performance statistics.

13 Appendix

This chapter list terms, acronyms, and abbreviations involved in this document, including the following sections:

- Terms
- Acronyms and abbreviations

13.1 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, and interface ID. The device determines 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 too 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, namely, 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

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 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 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 determine 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	QinQ is (also called Stacked VLAN or Double VLAN) extended from 802.1Q, defined by IEEE 802.1ad recommendation. Basic QinQ is a simple Layer 2 VPN tunnel technology, encapsulating outer VLAN Tag for client private packets at carrier access end, the packets take double VLAN Tag passing through trunk network (public network). In public network, packets only transmit according to outer VLAN Tag, the private VLAN Tag are transmitted as data in packets.
Quality of Service (QoS)	A 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.

13.2 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