RAISECOM

www.raisecom.com

Gazelle S1000i-LI (A) Configuration Guide (Web) (Rel_01)

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

Website: http://www.raisecom.com

Tel: 8610-82883305

Fax: 8610-82883056

Email: export@raisecom.com

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

Postal code: 100094

Notice

Preface

Objectives

This document describes features supported by the Gazelle S1000i-LI, and related configurations, including basic principles and configuration procedure of basic configurations, Ethernet, route, security, system.

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

By reading this document, you can master principles and configurations of the Gazelle S1000i-LI, and how to network with the Gazelle S1000i-LI.

Versions

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

Product name	Product version	Software version	Hardware version
Gazelle S1000i-2GF-4FE-LI	P100R001	V3.50	A.00 or later
Gazelle S1000i-2GF-8FE-LI (A)	P100R001	V3.50	A.00 or later
Gazelle S1000i-2GF-8FE-LI (H)	P100R001	V3.50	A.00 or later
Gazelle S1000i-4GF-16FE-LI	P100R001	V3.50	A.00 or later
Gazelle S1000i-4GX-16FE-LI	P100R001	V3.50	A.00 or later

Conventions

Symbol conventions

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

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

General conventions

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

GUI conventions

Convention	Description
Boldface	Buttons, menus, parameters, tabs, windows, and dialog titles are in **boldface**. For example, click **OK**.
>	Multi-level menus are in boldface and separated by the ">" signs. For example, choose **File** > **Create** > **Folder**.

Keyboard operation

Format	Description
Key	Press the key. For example, press **Enter** and press **Tab**.

Format	Description
Key 1+**Key 2**	Press the keys concurrently. For example, pressing **Ctrl+C** means the two keys should be pressed concurrently.
Key 1, **Key 2**	Press the keys in turn. For example, pressing **Alt**, **A** means the two keys should be pressed in turn.

Mouse operation

Action	Description
Click	Select and release the primary mouse button without moving the pointer.
Double-click	Press the primary mouse button twice continuously and quickly without moving the pointer.
Right-click	Press the right mouse button to pop up a menu for later selection.
Drag	Press and hold the primary mouse button and move the pointer to a certain position.

Change history

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

Issue 01 (2017-11-24)

Initial commercial release

Contents

Figures

Tables

1 Preparing for configurations

This chapter describes how to prepare for configurations on the Web configuration interface and basic information about the Web configuration interface, including the following sections:

- Establishing configuration environment
- Logging in to Web configuration interface
- Learning Web configuration interface
- Saving configurations
- Exiting Web configuration interface

1.1 Establishing configuration environment

To remotely manage and maintain the Gazelle S1000i-LI through Web login, configure it first.

For the Gazelle S1000i-LI, the default IP address is 192.168.0.1, and the subnet mask is 255.255.255.0. To modify the IP address, you can log in to the Gazelle S1000i-LI through the Console interface, and configure the Gazelle S1000i-LI as below:

Step 1 Use the cable to connect the network interface on the PC to the Ethernet interface on the Gazelle S1000i-LI.

Step 2 After login, enter the Command Line Interface (CLI) configuration mode. In CLI, both the default user name and password for login are raisecom.

```
Login:raisecom
Password:********
Raisecom#config
Raisecom(config)#
```

Step 3 Configure the IP address so that the Gazelle S1000i-LI can ping through the PC.

For example, the IP address of the PC is 192.168.18.100, the IP address of the Gazelle S1000i-LI is 192.168.18.111, the subnet mask is 255.255.255.0, and the management VLAN is VLAN 1, which keeps the PC and Gazelle S1000i-LI on the same segment.

```
Raisecom(config)#interface vlan 1
Raisecom(config-vlan1)#ip address 192.168.18.111 255.255.255.0
Raisecom(config-vlan1)#exit
```

Step 4 Enable HTTP.

```
Raisecom(config)#ip http server enable
```

Note

By default, HTTP is enabled on the Gazelle S1000i-LI.

1.2 Logging in to Web configuration interface

Scenario

To manage the Gazelle S1000i-LI through Web, connect it with a PC.

Configuration steps

Log in to the Web configuration interface as below:

Step 1 Start the Internet Explorer (IE) on a PC.

Step 2 Enter the IP address in the address bar, such as "http://192.168.0.1/", and then press **Enter**. The Web login page appears, as shown in Figure 1-1.

Step 3 Enter the user name and password.

Step 4 Click the **English** radio button, and then input the random verification code. If you fail to identify the current PIN, click **Unclear** to obtain a new code.

Step 5 Click **Login** to enter the Web configuration interface.

Figure 1-1 Web login interface

Note

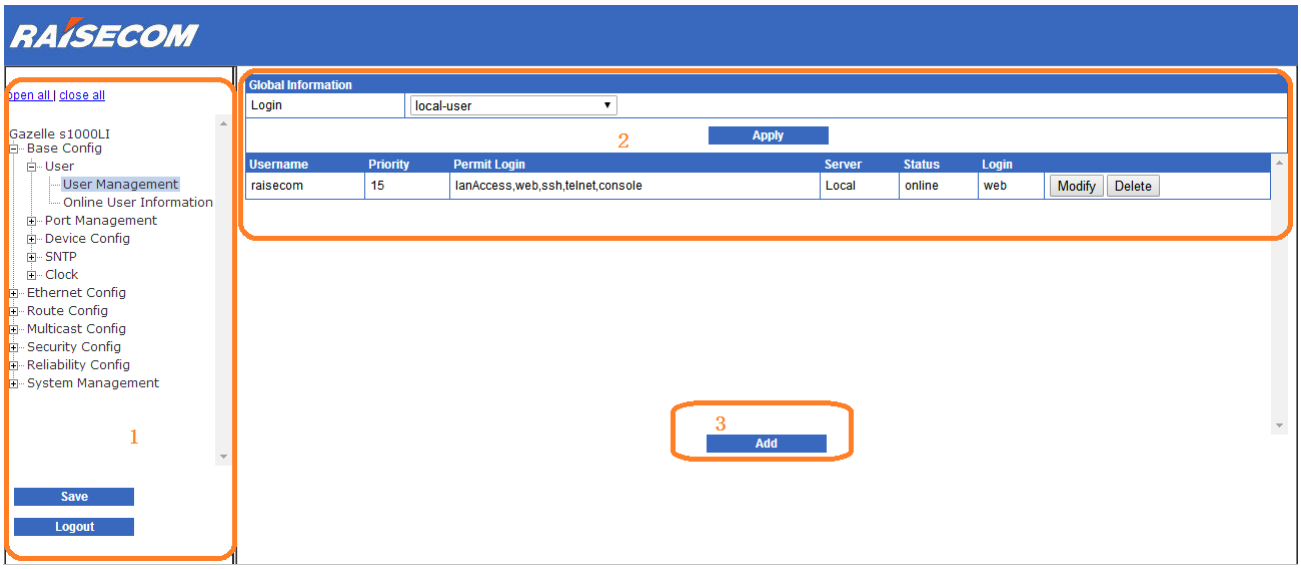
- When you log in for the first time, use the default user name (raisecom) and password (raisecom).
- After you successfully log in, you can choose **Base Config** > **User** > **User Management** from the navigation bar to modify the password.

1.3 Learning Web configuration interface

1.3.1 Structure of Web configuration interface

The Web configuration interface of the client is of uniform style and easy to use, as shown in Figure 1-2.

Figure 1-2 Typical Web configuration interface

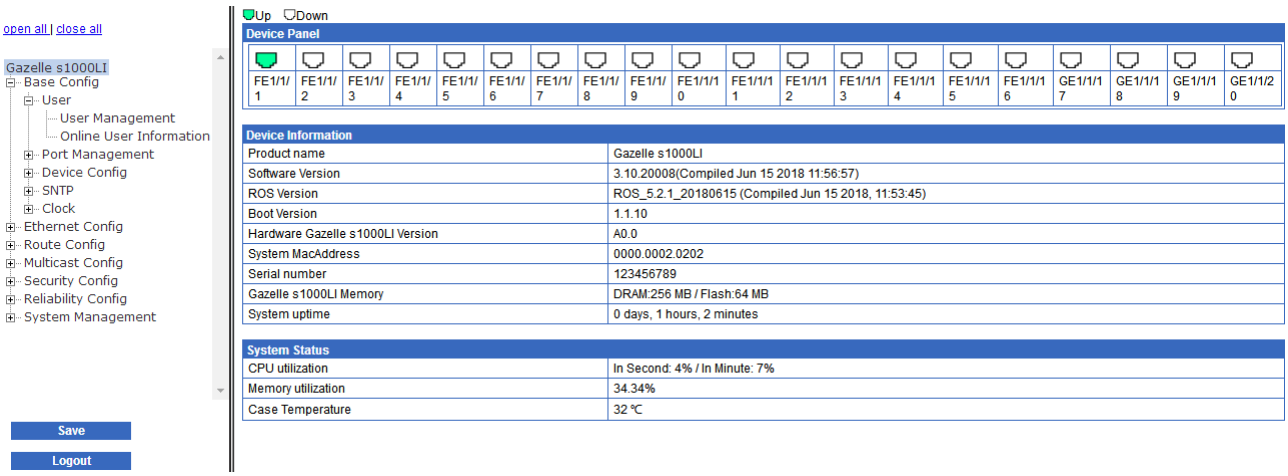


1	Navigation bar	2	Current configuration page
3	Common buttons		

1.3.2 Device overview

When you log in to the Web configuration interface through Web, you will enter the device overview page by default. This page shows the device panel, device information, system status, as shown in Figure 1-3.

Figure 1-3 Device overview



When you want to return to the interface from other interfaces, click the name in the upper area of the navigation bar, as shown in Figure 1-2.

You can view the connection status of each interface on the device panel. When the status is Green, it indicates that the interface is connected.

Note

When the cursor hovers over an interface, its interface ID will be displayed.

Device Information

The Device information area shows the following information:

- Software version and hardware version
- System MAC address
- Serial number
- Memory
- System uptime

By viewing basic information about the Gazelle S1000i-LI, you can learn its information and operation status.

System Status

The System Status area shows the following information:

- Chassis temperature
- CPU utilization
- Memory utilization

By viewing system status about the Gazelle S1000i-LI, you can learn its operation status.

1.3.3 Common buttons

Table 1-1 lists common buttons on the Web configuration interface.

Table 1-1 Common buttons

Button	Description
open all	Expanding button, used to expand the navigation bar in all levels
close all	Collapsing button, used to collapse the navigation bar to level 1
Add	Adding button, used to create an item on the current interface
Cancel	Cancelling button, used to cancel the current configurations
Modify	Modifying button, used to modify a selected item on the current interface
Delete	Deleting button, used to delete a selected item on the current interface
Refresh	Refreshing button, used to refresh the current interface
Apply	Applying button, used to apply current configurations to the system

Button	Description
Logout	Logout button, used to exit the current interface
Save	Saving button, used to save system configurations

1.4 Saving configurations

Caution

- After configurations on the current interface are complete, click **Apply** to save them to the memory. However, saving them in memory does not equal to saving them to the configuration file. If the Gazelle S1000i-LI encounters power failure or is reset, configurations since the last saving of configurations will be lost.
- After all configurations are complete, click **Save** to save them to the configuration file. In this case, though the Gazelle S1000i-LI is powered off or reset, configurations will not be lost.

The Web configuration interface provides the following methods to save configurations:

- Click **Apply** in any Web configuration interface to save configurations of the current interface to the memory.
- Click **Save** in the lower left corner of the navigation bar to save configurations to the configuration file.

1.5 Exiting Web configuration interface

After all configurations are complete, exit the Web configuration interface to ensure system security.

Caution

Before exiting the Web configuration interface, save all configurations to avoid losing them.

You can exit the Web configuration interface in the following two methods:

- Click the icon of the current page on the IE to close the IE.
- Click **Logout** in the lower left corner of the navigation bar.

2 Base Config

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

- User
- Port Management
- Device Config
- SNTP
- Clock

2.1 User

2.1.1 Introduction

Users can log in to and manage the Gazelle S1000i-LI. To prevent risks due to login by malicious users through Telnet or other methods, you must manage users effectively.

Note

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

2.1.2 User Management

Scenario

When a user logs in to the Web network management client for the first time, the Gazelle S1000i-LI provides a default user name with the password. To better maintain information about users, the Web network management client provides functions, such as adding users, modifying the password, and deleting users.

Users can access the device only after being authenticated and authorized with rights for the network and network resources. Authentication and authorization information is saved on the remote RADIUS server, remote TACACS+ server, or local device. You can configure the authentication mode for user login on this interface.

Caution

To guarantee security of the Web network management client, modify the password for login periodically.

Configuration steps

Step 1 In the navigation bar, choose **Base Config** > **User** > **User Management**. The User Management page appears.

Step 2 In the Global Information area, choose the login mode. Click **Apply** to complete configurations.

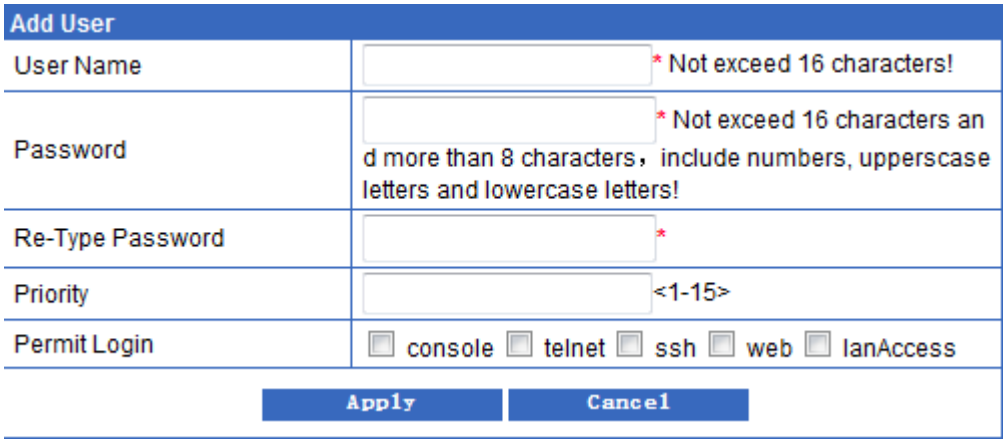
Figure 2-1 Global Information page

Step 3 You can view user configurations on the page.

- To add an item, click **Add** to enter the adding interface. Configure related items, and click **Apply**.
- To modify a configured item, click **Modify** to enter the modification interface. Configure related items, and click **Apply**.
- To delete an item, click **Delete** in the corresponding row.

Step 4 After configurations are complete, click **Save** to save configurations.

Figure 2-2 Add User page



Note

For a logged user, you cannot modify its information or delete its account.

Configuration items

Table 2-1 Configuration items on User Management page

Configuration item	Description
Login	Authentication mode for login, including: • local-user: local authentication • radius-user: RADIUS authentication • local-radius: when local authentication and RADIUS authentication coexist, the system uses local authentication preferentially. • radius-local: when local authentication and RADIUS authentication coexist, the system uses RADIUS authentication preferentially. • tacacs-user: TACACS+ authentication • local-tacacs: when local authentication and TACACS+ authentication coexist, the system uses local authentication preferentially. • tacacs-local: when local authentication and TACACS+ authentication coexist, the system uses TACACS+ authentication preferentially. • radius-local server-no-response: when the RADIUS server stops responding, the system uses local authentication. • tacacs-local server-no-response: when the TACACS+ server stops responding, the system uses local authentication.

Table 2-2 Configuration items on Add User page

Configuration item	Description
User Name	Name of the user to be added, a string, a string of 1 to 16 characters
Password	Password of the user to be added, a string of 8–16 characters (must contain all of numbers, upper-case letter, lower-case letters, and special characters)
Re-Type Password	Confirmation password
Priority	User priority, an integer, ranging from 1 to 15, being 15 by default when this field is blank
Permit Login	Permitted login mode, including: • Console: users accessing from the Console interface • telnet: users accessing through Telnet • ssh: users accessing through SSH • web: users accessing through Web • lanAccess: users accessing through LANs

Table 2-3 Configuration items on Modify page

Configuration item	Description
User Name	User name to be modified, read-only
Old password	Password to log in to the Web configuration interface
New Password	New password, a string of 8–16 characters (must contain all of numbers, upper-case letter, lower-case letters, and special characters)
Re-Type Password	Confirmation new password
Priority	User priority, an integer, ranging from 1 to 15
Permit Login	Permitted login mode, including: • Console: users accessing from the Console interface • telnet: users accessing through Telnet • ssh: users accessing through SSH • web: users accessing through Web • lanAccess: users accessing through LANs

2.1.3 Online User Information

Scenario

You can show information about online users, including the user name, priority, IP address of the authentication server, IP address of the login terminal, login type, and login time.

Configuration steps

Step 1 In the navigation bar, choose **Base Config** > **User** > **Online User Information**. The Online User Information page appears.

Step 2 View information about online users.

Figure 2-3 Online User Information page

Username	Priority	ServerIp	TerminalIp	Login	LoginTime
raisecom	15	--	172.16.70.146	web-1	1970-01-01,09:58:43

Step 3 3 Click **Refresh** to view current information about online users.

Configuration items

Table 2-4 Configuration items on Online User Information page

Configuration item	Description
Username	User name

Configuration item	Description
Priority	User priority
ServerIp	IP address of the server If the user is a local user, "--" will be displayed; otherwise, the IP address of the server will be displayed.
TerminalIp	IP address of the terminal If the login mode is Console, "--" will be displayed; otherwise, the IP address of the terminal will be displayed.
Login	Login mode • console: log in through Console. • telnet: log in through Telnet. Up to 5 Telnet connections can be established. • ssh: log in through SSH. Up to 5 SSH connections can be established. • web: log in through Web. Up to 20 Web connections can be established. When multiple users log in in the same mode, the displayed name is related to the sequence in which users log in. For example, if there is only one Telnet user, "telnet-1" will be displayed in the Login area; for the second Telnet user, "telnet-2" will be displayed.
LoginTime	Login time

2.2 Port Management

2.2.1 Introduction

Ethernet interface

The Ethernet is of high flexibility and easy implementation, so it becomes a key Local Area Network (LAN) networking technology. The Gazelle S1000i-LI supports the Ethernet electrical interface and Ethernet optical interface.

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. Auto-negotiation parameters include duplex mode and interface rate. Once successful in negotiation, the devices at both ends of the link can work in the same duplex mode and interface rate.

2.2.2 Port configuration

Scenario

You can configure parameters on the interface, such as the interface status, duplex mode, interface rate, and flow control.

The Gazelle S1000i-LI supports Ethernet electrical interfaces and Ethernet optical interfaces. You can choose the proper type as required.

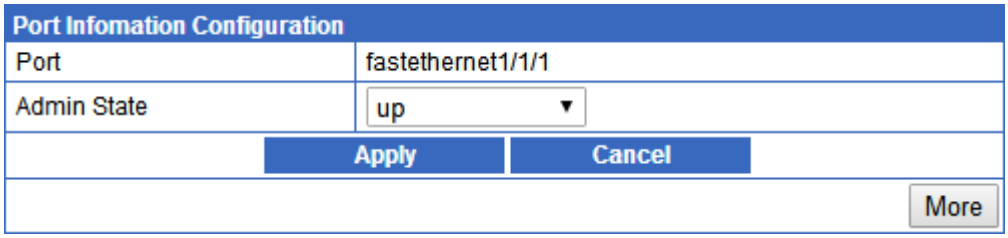
Configuration steps

Step 1 In the navigation bar, choose **Base Config** > **Port Management** > **Port Config**. The Port Config page appears.

Step 2 You can view related configuration of each interface.

To modify configurations of an interface, click **Modify** to enter the Port Information Configuration page.

Figure 2-4 Port Information Configuration page



- Configure related items, and click **Apply**.
- Click **More** to configure more items. Configure related items, and click **Apply**.
- Click **Back** to return to the basic configuration page.

Step 3 Click **Refresh** to show current configurations of interfaces.

Step 4 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 2-5 Configuration items on Port Config page

Configuration item	Description
Port	Port name
Operate State	Current operation status of the interface
Admin State	Current configuration status of the interface, which can be modified from the drop-down list, including: • Up • Down

Configuration item	Description
Speed	Current configuration rate of the interface, which can be modified from the drop-down list, including: • 10M: 10 Mbit/s • 100M: 100 Mbit/s • 1000M: 1000 Mbit/s
Duplex	Current duplex mode of the interface, which can be modified from the drop-down list, including: • Auto-negotiate • half duplex • full duplex
FlowControl(Tx)	Current flow control mode in the Tx direction of the interface, including: • On • Off By default, it is disabled.
FlowControl(Rx)	Current flow control mode in the Rx of the interface, including: • On • Off By default, it is disabled.
MDI	MDI of the electrical interface • Auto: automatic mode • Normal: straight-through mode • Xover: crossover mode

2.2.3 Port Statistics

Scenario

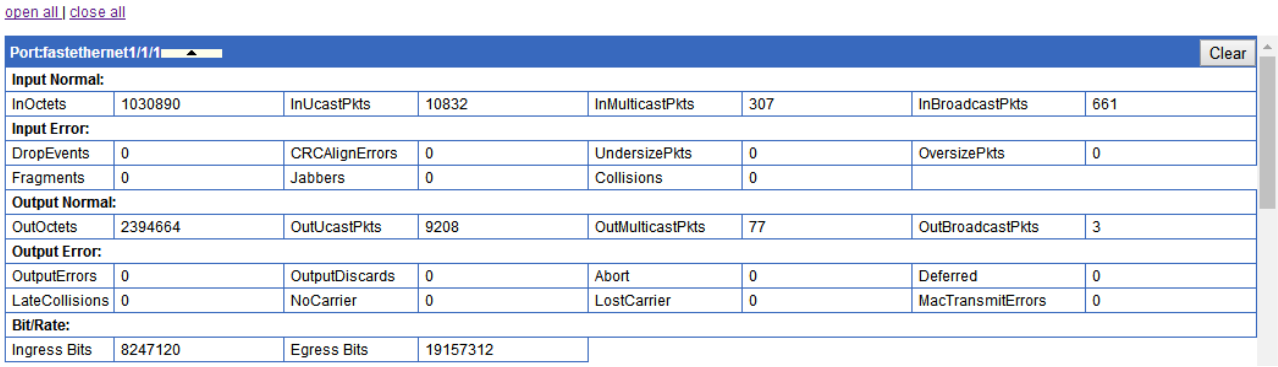
You can show details about traffic on interfaces on the page, or manually refresh or clear statistics of interfaces.

Configuration steps

Step 1 In the navigation bar, choose **Base Config** > **Port Management** > **Port Statistics**. The Port Statistics page appears.

Step 2 You can show details about traffic on interfaces on the page.

Figure 2-5 Port Statistics page



open all | close all

Port:fastethernet1/1/1							Clear
Input Normal:							
InOctets	1030890	InUcastPkts	10832	InMulticastPkts	307	InBroadcastPkts	661
Input Error:							
DropEvents	0	CRCAlignErrors	0	UndersizePkts	0	OversizePkts	0
Fragments	0	Jabbers	0	Collisions	0		
Output Normal:							
OutOctets	2394664	OutUcastPkts	9208	OutMulticastPkts	77	OutBroadcastPkts	3
Output Error:							
OutputErrors	0	OutputDiscards	0	Abort	0	Deferred	0
LateCollisions	0	NoCarrier	0	LostCarrier	0	MacTransmitErrors	0
Bit/Rate:							
Ingress Bits	8247120	Egress Bits	19157312				

- To clear statistics of an interface, click **Clear** in the row of the interface.
- To clear statistics of all interfaces, click **Clear** in the lower part of the page.

Caution

After statistics of an interface or all interfaces is cleared, this operation cannot be rolled back. Do it with care.

Step 3 Click **Refresh** to show current statistics of each interface.

Step 4 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 2-6 Configuration items on Port Statistics page

Configuration item	Description
Port	Port ID information. Click the button on the right part to collapse or expand details. The button will be ▲ for collapse or ▼ for expansion.
Input Normal	Input statistics
InOctets	Total number of input bytes, in units of byte
InUcastPkts	Number of input unicast packets
InMulticastPkts	Number of input multicast packets
InBroadcastPkts	Number of input broadcast packets
Input Error	Statistics of input errored information
DropEvents	Number of discarded packets
CRCAlignErrors	Number of errored frames found by CRC
UndersizePkts	Number of packets of which the size is smaller than the minimum size
OversizePkts	Number of packets of which the size is greater than the maximum size

Configuration item	Description
Fragments	Number of fragment packets
Jabbers	Jabbers packets
Collisions	Number of collision packets
Output Normal	Statistics of output normal packets
OutOctets	Total number of output bytes
OutUcastPkts	Number of output unicast packets
OutMulticastPkts	Number of output multicast packets
OutBroadcast	Number of output broadcast packets
Output Error	Statistics of output errored packets
OutputErrors	Number of output errored packets
OutputDiscards	Number of discarded output packets
Abort	Number of discarded frames which are delayed for sending for over 15 times due to collision detection in half duplex
Differred	Increasing by 1 when the packet fails to be sent once because the system has detected that the carrier is being declared in half duplex
LateCollisions	Packet failing to be sent due to detected collision when the first 64 bytes of the data part in an Ethernet frame enter the line in half duplex
NoCarrier	No carrier, for the serial WAN interface, increasing by 1 if the carrier does not appear when the system tries to send frames
LostCarrier	Lost carrier, for the serial WAN interface, increasing by 1 when a carrier is lost in sending
MacTransmitError	MAC transmission errored packets
Bit/Rate	Bit statistics
Ingress Bits	Number of bits of input information
Egress Bits	Number of bits of output information

2.3 Device Config

2.3.1 Config Maintain

Scenario

After configurations are complete, save them to the Gazelle S1000i-LI and new configurations will override original configurations. Otherwise, new configurations will lost upon next restart and original configurations will work.

When the Gazelle S1000i-LI fails, you can try to troubleshoot it by restarting it according to actual conditions.

On this interface, you can configure and manage the Gazelle S1000i-LI, including erasing configurations, saving configurations, and restarting the Gazelle S1000i-LI. You can also view and configure related startup items as required.

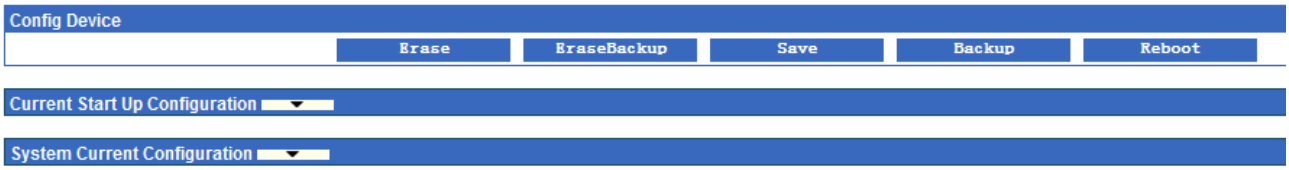
Configuration steps

Step 1 In the navigation bar, choose **Basic Config** > **Device Config** > **Config Maintain**. The Config Maintain page appears.

Step 2 You can do the following operations in the Config Device page.

- To erase current startup configurations, click **Erase**.
- To erase backup startup configurations, click **EraseBackup**.
- To back up current configurations, click **Backup**.
- To save running configurations to the startup configuration file, click **Save**.
- To restart the Gazelle S1000i-LI, click **Reboot**. The system will prompt whether to restart. Click **OK**.

Figure 2-6 Config Device page



Caution

- If some configurations are not saved before restart, they will be lost. Thus save configurations before restart.
- After the Gazelle S1000i-LI is restarted, you need to log in to the Web network management system again.

Step 3 In the Current Start Up Configuration area, you can view configurations for next startup in the Flash.

Step 4 In the System Current Configuration area, you can view current configurations in the Flash.

Step 5 After configurations are complete, click **Save** to save configurations.

Note

Click the button on the right part to collapse or expand details. The button will be ▲ for collapse or ▼ for expansion.

Configuration items

N/A

2.3.2 Import/Export

Scenario

You can import a configuration file from a server to restore the original configuration file or update the configuration file to the latest.

You can export a configuration file from the Gazelle S1000i-LI to the server for backup.

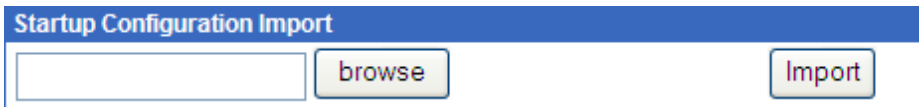
Configuration steps

Import a configuration file as below:

Step 1 In the navigation bar, choose **Basic Config** > **Device Config** > **Import/Export**. The Import/Export page appears.

Step 2 In the Startup Configuration Import area or Backup Configuration Import area, click **Browse** to choose a configuration file to be imported.

Figure 2-7 Startup Configuration Import page



Step 3 Click **Import**. The system prompts successful import.

Step 4 After configurations are complete, click **Save** to save configurations.

Note

After importing a configuration file, restart the Gazelle S1000i-LI to make the configuration file take effect.

Export a configuration file as below:

Step 1 In the navigation bar, choose **Basic Config** > **Device Config** > **Import/Export**. The **Import/Export** page appears.

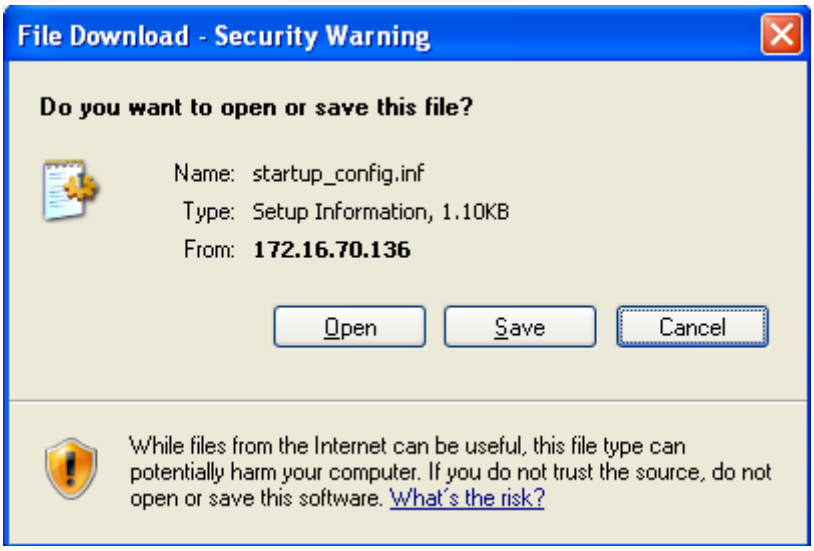
Figure 2-8 Startup Configuration Export page

Step 2 Click **Export**. A File Download dialog box appears.

- Click **Open** to view the configuration file.
- Click **Save**. A Save As dialog box appears. Choose a path to save the configuration file, and click **Save**.

Step 3 After configurations are complete, click **Save** to save configurations.

Figure 2-9 File Download page



Configuration items

N/A

2.3.3 System Upgrade

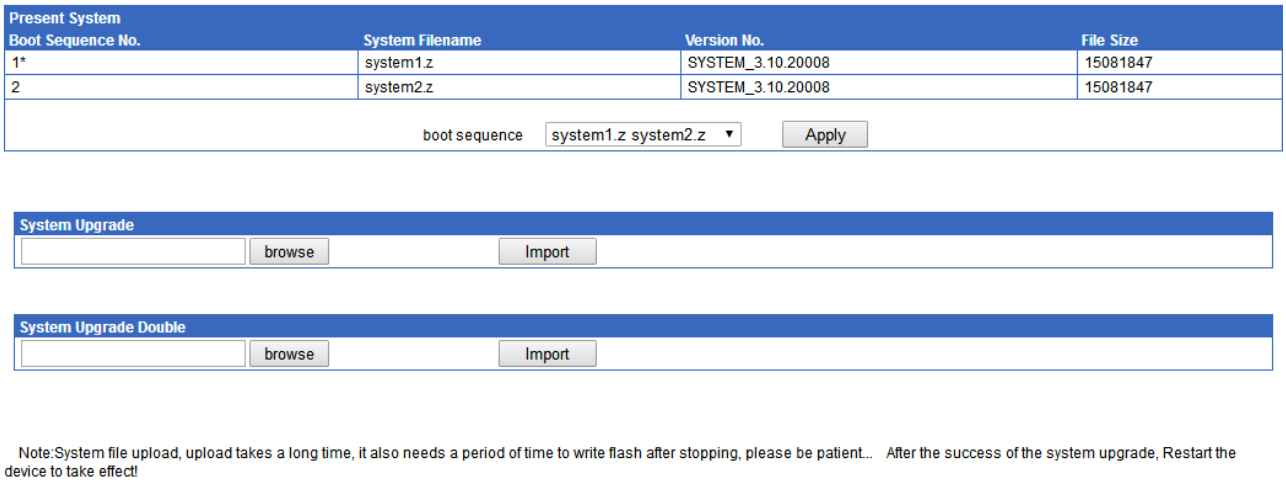
Scenario

To add features, optimize existing features, or fix existing bugs, you can upgrade the Gazelle S1000i-LI on this interface. You can upgrade system software on this interface.

Configuration steps

Step 1 In the navigation bar, choose **Base Config** > **Device Config** > **System Upgrade**. The System Upgrade page appears.

Figure 2-10 System Upgrade page



Step 2 Configure the boot sequence in the Present System area, and click **Apply**.

Note

If the boot sequence is system 2.z system 1.z, the system to be started is still the original system 2 instead of system 1, though system 1 is upgraded.

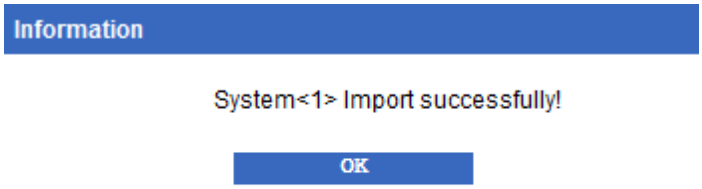
Step 3 Click **Browse** after system1.z system 2.z or system2.z system 1.z to choose the system software for upgrade.

Step 4 Click **Import**. An alert dialog box appears, prompting whether to upgrade. Click **OK**. The system upgrade process starts.

Figure 2-11 Alert dialog box for upgrading system software

Step 5 A dialog box appears, prompting successful import. Click **OK**.

Figure 2-12 Successful prompt for importing system software



Step 6 After configurations are complete, click **Save** to save configurations.

Note

Upgrading system software takes a long time. When saving system software to the Flash, ensure the Gazelle S1000i-LI is powered on stably and connected to the network properly.
To make the configuration file take effect, restart the Gazelle S1000i-LI by clicking **Reboot** from **Base Config** > **Device Config** > **Config Maintain**.

Configuration items

N/A

2.4 SNTP

2.4.1 Introduction

Simple Network Time Protocol (SNTP) is used to synchronize time of the Gazelle S1000i-LI with the SNTP server. The synchronization time through SNTP is the Greenwich Mean Time (GMT), which can be converted into the local time according to the time zone.

2.4.2 Global Config

Scenario

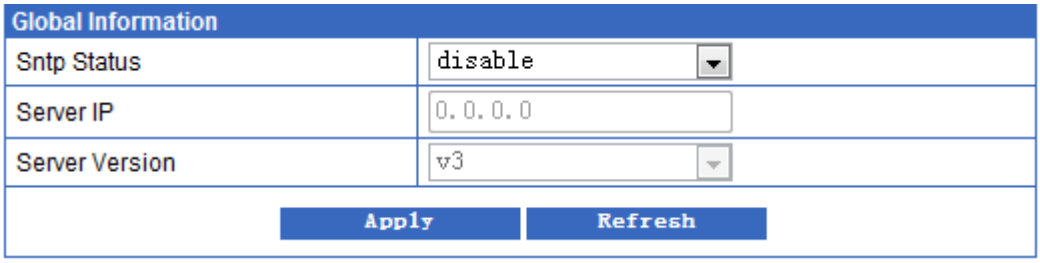
You can synchronize the Gazelle S1000i-LI with the SNTP server on this interface.

Configuration steps

Step 1 In the navigation bar, choose **Basic Config** > **SNTP** > **Global Config**. The Global Config page appears.

Step 2 Configure related items. Click **Apply**.

Figure 2-13 SNTP Global Information page



Note

After the IP address of the SNTP server is configured, the Gazelle S1000i-LI tries to obtain clock signals from the SNTP server every 10s. The maximum expiration time for obtaining clock signals from the SNTP server is 60s.

Step 3 Click **Refresh** to view current SNTP configurations.

Step 4 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 2-7 Configuration items on SNTP Global Information page

Configuration item	Description
Sntp Status	SNTP status • Enable • Disable By default, SNTP is disabled.
Server IP	IP address of the SNTP server
Server Version	Version of the SNTP server, including: • V1 • V2 • V3 • V4

2.5 Clock

2.5.1 Introduction

With development and extension of the Internet in all aspects, multiple applications involved in clock need accurate and reliable time, such as online real time transaction, distributed network calculation and processing, transport and flight management, and data management.

To ensure precision of the system time, the Gazelle S1000i-LI provides complete time management. You can configure system time and time zones, Daylight Saving Time (DST), and Simple Network Time Protocol (SNTP) for the Gazelle S1000i-LI.

Time and time zone

Generally, the system time is configured to the local real time. In other words, configure the time zone of countries by reference to Greenwich Mean Time (GMT) (Beijing of China is located in the eastern time zone by reference to GMT, so configure its time zone to +8:00).

The Gazelle S1000i-LI supports displaying the time and time zone offset in the format of "yyyy-mm-dd,hh:mm:ss". You can configure the time and time zone manually.

DST

DST is established locally to save energy. Generally, you can adjust the clock an hour faster, thus reducing lighting consumption but vary with countries and areas. Thus, you need to consider detailed DST rules locally before configuration.

2.5.2 Clock Config

Scenario

Configure the system time for the Gazelle S1000i-LI on this page to ensure the precision of system time. This configuration will not be lost even upon power failure, and the configured time takes effect immediately regardless of SNTP enabling status.

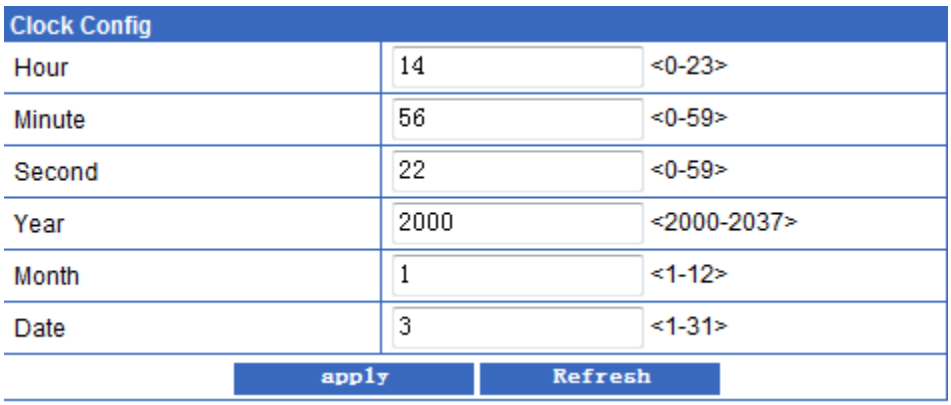
Configuration steps

Step 1 In the navigation bar, choose **Basic Config** > **Clock** > **Clock Config**, and the Clock Config page appears.

Step 2 Configure related items, and click **Apply**.

Step 3 After configurations are complete, click **Save** to save configurations.

Figure 2-14 Clock Config page



Clock Config		
Hour	14	<0-23>
Minute	56	<0-59>
Second	22	<0-59>
Year	2000	<2000-2037>
Month	1	<1-12>
Date	3	<1-31>
	apply	Refresh

Table 2-8 Configuration items on Clock Config page

Configuration item	Description
Hour	Hour, an integer, ranging from 0 to 23
Minute	Minute, an integer, ranging from 0 to 59
Second	Second, an integer, ranging from 0 to 59
Year	Year, an integer, ranging from 2000 to 2099
Month	Month, an integer, ranging from 1 to 12
Date	Date, an integer, ranging from 1 to 31

2.5.3 Clock Display

Scenario

The format for displaying time varies with configured modes of displaying time.

- When the mode of displaying time is configured to default, the format of displaying time is "yyyy-mm-dd,hh:mm:ss".
- When the mode of displaying time is configured to UTC, the format of displaying time is "dd.mm.yyyy-hh:mm:ss".

Configuration steps

Step 1 In the navigation bar, choose **System Management** > **Clock** > **Clock Display**, and the System time display page appears.

Step 2 Configure related items, and click **Apply.**

Step 3 After configurations are complete, click **Save** to save configurations.

Figure 2-15 System time display information page

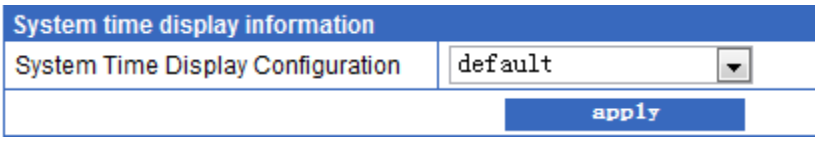


Table 2-9 Configuration items on System time display information page

Configuration item	Description
System Time Display Configuration	Modes of displaying system time, including: • default • UTC By default, the mode of displaying the system time is default.

3 Ethernet Config

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

- MAC
- VLAN Config
- LBD
- Port Mirror

3.1 MAC

3.1.1 Introduction

Forwarding modes for MAC addresses

When forwarding packets, based on the information about MAC addresses, the Gazelle S1000i-LI adopts 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 Gazelle S1000i-LI 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 Gazelle S1000i-LI broadcasts the packet.
- Multicast: with multicast enabled, when the Gazelle S1000i-LI receives a packet of which the destination MAC address is a multicast address, it sends the packet from the egress interface contained in the MAC address entry if this entry is listed in the MAC address table, or it discards the packet if this entry is not listed. With multicast disabled, it broadcasts the packet.
- Broadcast: when the Gazelle S1000i-LI receives an all-F packet, or this MAC address is not listed in the MAC address table, the Gazelle S1000i-LI forwards the packet to all interfaces except the receiving interface.

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 restarted.
- Dynamic MAC address entry: the Gazelle S1000i-LI 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 restarted.

3.1.2 Static MAC Config

Scenario

The static MAC address can be configured for a fixed server, special persons (manager, financial staff, and so on), fixed and important hosts to ensure that all data flow forwarded to these MAC addresses are forwarded from static MAC address related interface in priority.

You can disable MAC address learning on the interface with a fixed static MAC address.

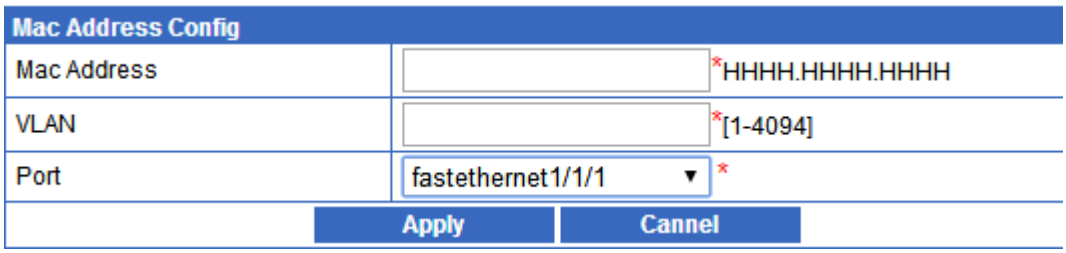
Configuration steps

Step 1 In the navigation bar, choose **Ethernet Config** > **MAC** > **MAC Config** > **Static MAC Config**. The Static MAC Config page appears.

Step 2 You can view configured static MAC addresses.

- To modify a configured item, click **Modify** to enter the modification page. Configure related items, and click **Apply**.
- To add an item, click **Add** to enter the adding page. Configure related items, and click **Apply**.
- To delete an item, click **Delete** in the corresponding row.

Figure 3-1 MAC Address Config page



Step 3 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 3-1 Configuration items on MAC Address Config page

Configuration item	Description
MAC Address	Static MAC address, in dotted hexadecimal notation

Configuration item	Description
VLAN	VLAN ID associated with the MAC address, an integer, ranging from 1 to 4094
Port	Interface ID associated with the MAC address

3.1.3 MAC Global Config

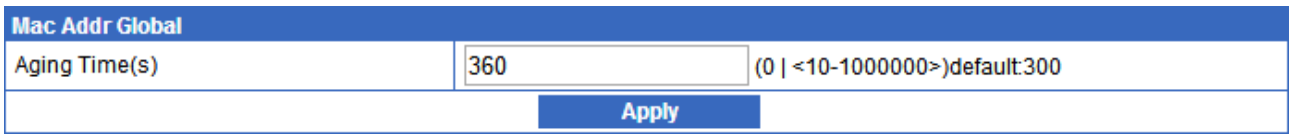
Scenario

To prevent the MAC address table from saving excessive MAC address entries to exhaust MAC address resources, configure the aging time of the MAC address table to age dynamic MAC addresses.

Configuration steps

Step 1 In the navigation bar, choose **Ethernet Config** > **MAC** > **MAC Config** > **MAC Global Config**. The MAC Global Config page appears.

Figure 3-2 MAC Global Config page



Step 2 Configure related items, and click **Apply**.

Step 3 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 3-2 Configuration items on MAC Global Config page

Configuration item	Description
Aging Time(s)	Aging time of dynamic MAC addresses, an integer, ranging from 10 to 1 000 000 or being 0, in units of second, value 0 indicating no aging, being 300 by default

3.1.4 MAC Learn

Scenario

You can configure interface MAC address learning on this page:

- After this function is disabled, the interface cannot dynamically learn MAC addresses.

- After this function is enabled, the interface will learn the source MAC address of a packet sent from the interface. After receiving the packet, the Gazelle S1000i-LI searches for the MAC address entry corresponding to the destination MAC address of the packet. If the entry exists, the Gazelle S1000i-LI forwards the packets from the corresponding interface in the MAC address table.

Configuration steps

Step 1 In the navigation bar, choose **Ethernet Config** > **MAC** > **MAC Config** > **MAC Learn**. The MAC Learn page appears.

Figure 3-3 MAC Learn page

Port Mac Learning State		
Port	Learning State	Switch
fastethernet1/1/1	enable	Change
fastethernet1/1/2	enable	Change
fastethernet1/1/3	enable	Change
fastethernet1/1/4	enable	Change

Step 2 Click **Change** to change MAC address learning status.

Step 3 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 3-3 Configuration items on MAC Learn page

Configuration item	Description
Port	Interface ID
Learning State	Current MAC address learning status on the specified interface: • Enable: learning MAC addresses • Disable: not learning MAC addresses By default, the interface learns MAC addresses.
Switch	Switch MAC address learning status. By default, MAC address learning is enabled.

3.1.5 MAC Threshold Config

Scenario

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

The MAC address limit improves the speed of forwarding packets.

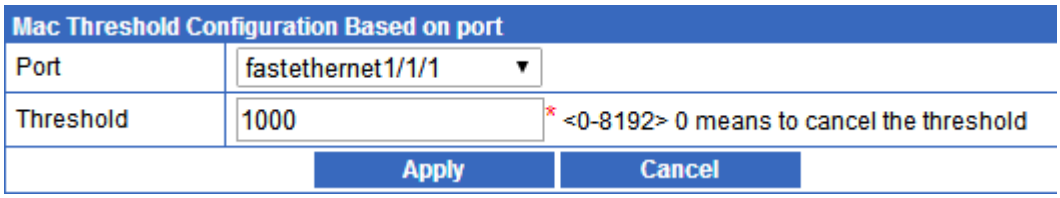
Configuration steps

Step 1 In the navigation bar, choose **Ethernet Config** > **MAC** > **MAC Config** > **MAC Threshold Config** > **Port Threshold Config**. The Port Threshold Config page appears.

Step 2 You can view MAC threshold of each interface based on interface.

To modify a configured item, click **Modify** to enter the modification interface. Configure related items, and click **Apply**.

Figure 3-4 Mac Threshold Configuration Based on port page



Step 3 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 3-4 Configuration items on Mac Threshold Configuration Based on port+vlan page

Configuration item	Description
Port	Interface ID
Threshold	MAC address limit, an integer, ranging from 0 to 16383, being 0 by default (no limit)

3.1.6 MAC Address Information

Scenario

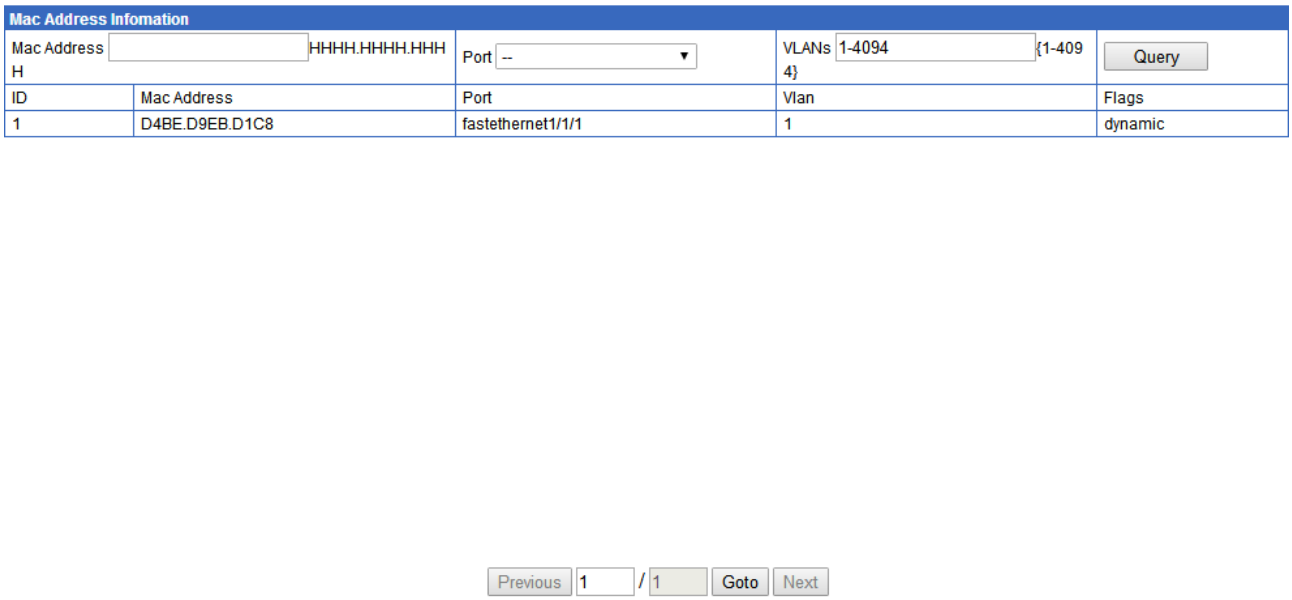
You can view information about MAC addresses on the specified interface or in the specified VLAN on this page.

Configuration steps

Step 1 In the navigation bar, choose **Ethernet Config** > **MAC** > **MAC Config** > **MAC Address Information**. The MAC Address Information page appears.

Step 2 You can view MAC threshold of each interface.

Figure 3-5 MAC Address Information page



Step 3 Configure related items, and click **Query**. Information about specified MAC addresses will be displayed below.

Configuration items

Table 3-5 Configuration items on MAC Address Information page

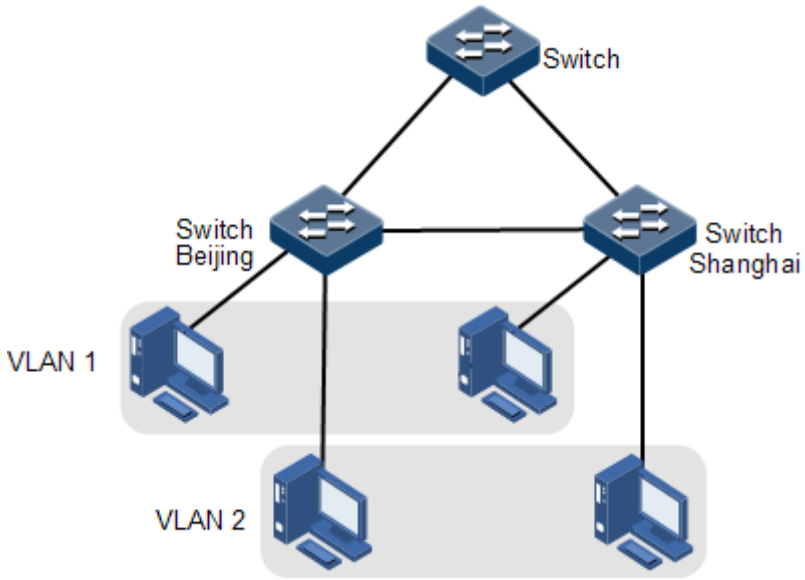
Configuration item	Description
Mac Address	Show information about the specified MAC address.
Port	Show information about the MAC address of the specified interface.
Vlan	Show information about the MAC address in the specified VLAN.

3.2 VLAN Config

3.2.1 Introduction

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, as shown in Figure 3-6.

Figure 3-6 VLAN partitions



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

3.2.2 Base Config

Scenario

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

- In a small LAN, several VLANs are created on a device, and 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.
- In a 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 enterprises that have many employees and need a large number of hosts, or in the department that have different divisions in different locations. The hosts in one department can access one another, so users have to partition VLANs on multiple devices. Layer 3 devices like router are required if users want to communicate among different VLAN. The cascade interfaces among devices are configured in Trunk mode.

By partitioning VLANs, the network isolates hosts without interconnection requirements, thus enhancing network security, reducing broadcast traffic and storms.

You can view or modify VLAN information, or create VLANs on this interface.

Configuration steps

Step 1 In the navigation bar, choose **Ethernet Config** > **VLAN Config** > **Base VLAN**. The Base VLAN page appears.

Step 2 You can view configurations of each VLAN.

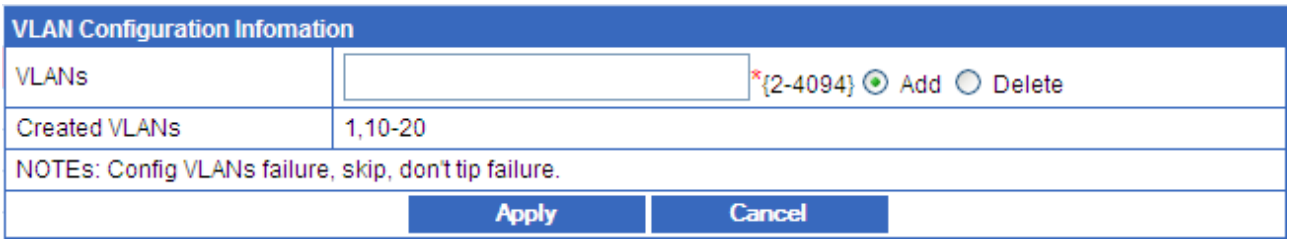
- To search for a VLAN ID, choose its range from the drop-down list, input it in the text box, and click **Search**.
- To modify a static VLAN, click **Modify** to enter the modification page. Configure related items, and click **Apply**.
- To delete configurations of a static VLAN, search for it first, and then click **Delete**.

Note

- VLAN 1 is system VLAN, so you do not need to create them nor cannot delete them.
- Enter a VLAN ID in the text box, such as 11, the row including this VLAN ID becomes Red, and port/VLAN membership information changes accordingly.
- If you choose a row, the information in the text box for search will become the VLAN ID in the selected row.
- If the entered VLAN does not exist, a dialog box will appear.

Step 3 To configure VLAN information, click **Configure** to enter the configuration interface. Configure related items, choose VLAN processing action, and click **Apply**.

Figure 3-7 VLAN Configuration Information page



Step 4 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 3-6 Configuration items on Base Config page for VLAN Config

Configuration item	Description
Search	Search for a VLAN ID. • Enter a VLAN ID in the text box, such as 11, the row including this VLAN ID becomes Red, and port/VLAN membership information changes accordingly. • If the entered VLAN does not exist, a dialog box will appear. • If you choose a row, the information in the text box for search will become the VLAN ID in the selected row.

Configuration item	Description
Port/VLAN membership	Membership between an interface and a VLAN, including interface name, and membership with the VLAN: • -: None, unrelated interface • M: Member, member interface • U: Untagged, untagged interface • F: Fobidden, forbidden interface **Note** When you choose a row, it becomes red, and the port/VLAN membership changes accordingly.
VLANs	VLAN list, an integer, ranging from 1 to 4094
Name	VLAN name
VLANs	VLAN list • Static: static VLAN • Dynamic: dynamic VLAN

3.2.3 VLAN Port Config

Scenario

There are two interface modes: Access mode and Trunk mode, as listed in Figure 3-6.

Table 3-7 Interface mode and packet processing

Interface type	Processing ingress packets		Processing egress packets
	Untagged packets	Tagged packets	
Access	Add the Access VLAN Tag to the packet.	• If the VLAN ID of the packet is equal to the Access VLAN ID, the interface will receive the packet. • If the VLAN ID of the packet is not equal to the Access VLAN ID, the interface will discard the packet.	• If the VLAN ID of the packet is equal to the Access VLAN ID, the interface will remove the Tag and send the packet. • If the VLAN ID of the packet is excluded from the list of VLANs of which packets are allowed to pass by the interface, the interface will discard the packet.

Interface type	Processing ingress packets		Processing egress packets
	Untagged packets	Tagged packets	
Trunk	Add the Native VLAN Tag to the packet.	• If the VLAN ID of the packet is included in the list of VLANs of which packets are allowed to pass by the interface, the interface will receive the packet. • If the VLAN ID of the packet is excluded from the list of VLANs of which packets are allowed to pass by the interface, the interface will discard the packet.	• If the VLAN ID of the packet of the packet is equal to the Native VLAN ID, the interface will remove the Tag and send the packet. • If the VLAN ID of the packet is not equal to the Native VLAN ID and the interface allows packets of the VLAN to pass, the interface will keep the original Tag and send the packet.

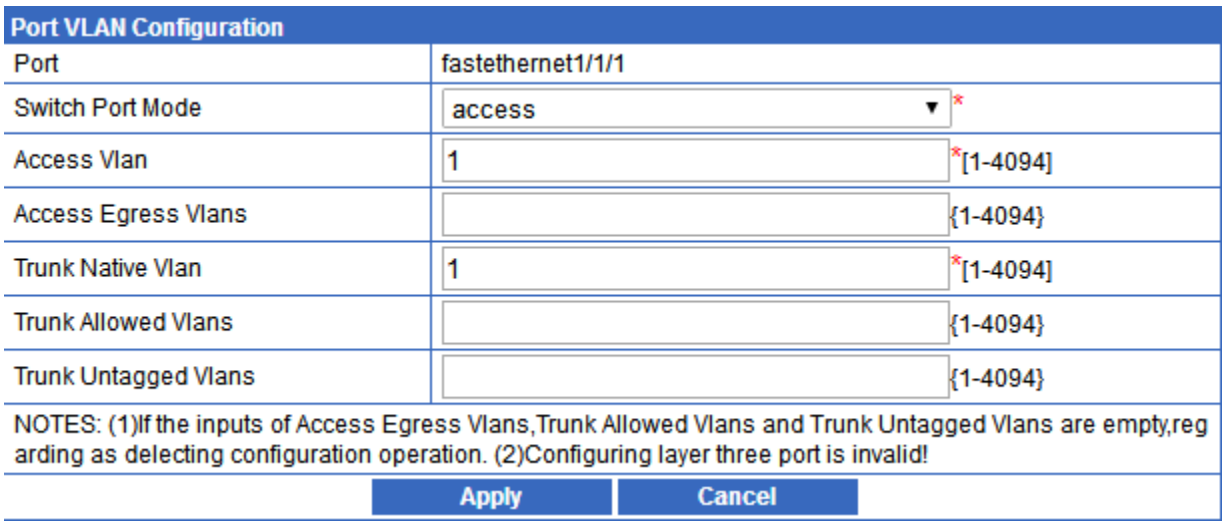
You can view or modify VLAN configurations on the current page on the Web interface.

Configuration steps

Step 1 In the navigation bar, choose **Ethernet Config** > **VLAN Config** > **VLAN Port Config**. The VLAN Port Config page appears.

Step 2 You can view VLAN configurations on the current interface. To modify VLAN configurations on an interface, click **Modify** in the corresponding row to enter the modification page.

Figure 3-8 Port VLAN Configuration page



Step 3 Configure related items, and click **Apply**. A confirmation dialog box appears. Click **OK**.

Step 4 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 3-8 Configuration items on Port VLAN Configuration page

Configuration item	Description
Port	Interface name, read only
Switch Port Mode	Interface switching mode, including: • access • trunk By default, all physical layer interfaces are in Access mode.
Access VLAN	VLAN for the Access interface This is required when Switch Port Mode is configured to access.
Access Egress Vlans	VLANs allowed to pass by the Access interface, in the following forms: • x-y: a VLAN range • x,y: multiple VLANs This is optional when Switch Port Mode is configured to access.
Trunk Native Vlan	VLAN for the Trunk interface This is required when Switch Port Mode is configured to trunk.
Trunk Allowed Vlans	VLANs allowed to pass by the Trunk interface, in the following forms: • x-y: a VLAN range • x,y: multiple VLANs This is optional when Switch Port Mode is configured to trunk.
Trunk Untagged Vlans	Untagged VLANs for the Trunk interface, in the following forms: • x-y: a VLAN range • x,y: multiple VLANs This is optional when Switch Port Mode is configured to trunk.

3.3 LBD

3.3.1 Introduction

Loop detection can eliminate the influence on network caused by a loop, thus providing 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.

Principle for processing loops

The Gazelle S1000i-LI processes loops as below:

- 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 smaller 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).

Action for processing loops

The action for processing loops is the method for the Gazelle S1000i-LI to use upon loop detection. You can define different actions on the specified interface according to actual situations, including:

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

3.3.2 LBD config

Scenario

You can configure global configurations of loop detection on this page, such as the loop detection mode, loop detection period, and automatic recovery time.

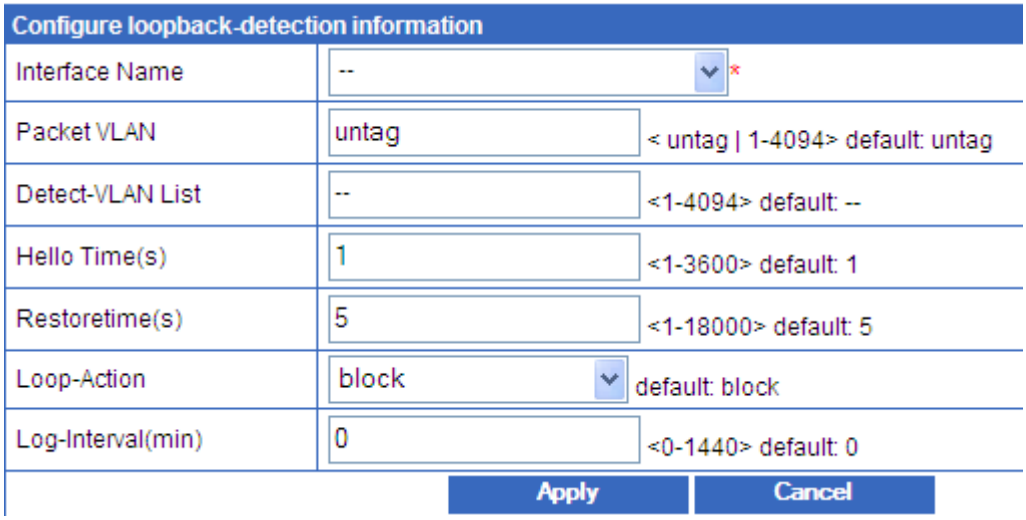
Configuration steps

Step 1 In the navigation bar, choose **Ethernet Config** > **LBD** > **LBD Config**. The Port Loopback Detection page appears.

Step 2 You can view configured static ARP entries.

- To add an item, click **Add** to enter the adding page. Configure related items, and click **Apply**.
- To modify a configured item, click **Modify** to enter the modification page. Configure related items, and click **Apply**.
- To delete an item, click **Delete** in the corresponding row.

Figure 3-9 Configure loopback-detection information page



Step 3 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 3-9 Configuration items on Configure loopback-detection information page

Configuration item	Description
Interface Name	Interface to be enabled with loop detection
Packet VLAN	ID of the VLAN for sending loop detection packets, an integer, ranging from 1 to 4094, specifying packets not to carry Tag
Detect VLAN List	List of loop detection VLAN, an integer, ranging from 2 to 4094 It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".
HelloTime(s)	Loop detection period, an integer, ranging from 1 to 3600, in units of second, being 1s by default
Restore Time(s)	Loop restoration period, an integer, ranging from 1 to 18000, in units of second, being 5s by default
Loop-Action	Action taken upon detection of a loop, being block by default: • Block: send Trap, and block the interface. • Trap-only: send Trap only. • Shutdown: send Trap, and shut down the interface.
Log Interval(min)	Logging interval, an integer, ranging from 0 to 1440, in units of minute, being 0 by default. The value 0 indicates no periodic reporting.

3.3.3 Port Statistics Information

Scenario

You can view statistics on loop detection, and restart the interface that is shut down due to a detected loop.

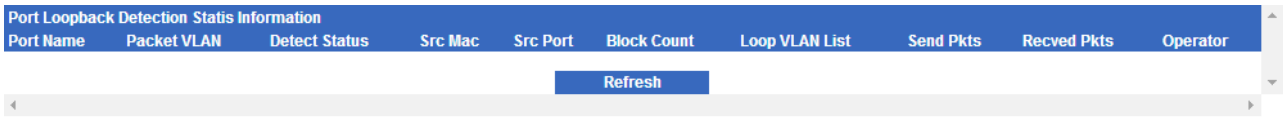
Configuration steps

Step 1 In the navigation bar, choose **Ethernet Config** > **LBD** > **Port Statistics Information**. The Port Loopback Detection Statis Information page appears.

Step 2 You can view statistics on loop detection.

- To restart an interface that is shut down due to a detected loop, click **Restore**.
- To clear statistics, click **Clear**.

Figure 3-10 Port Loopback Detection Statis Information page



Step 3 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 3-10 Configuration items on Configure loopback-detection information page

Configuration item	Description
Port Name	Interface ID
Packet VLAN	ID of the VLAN of which loop detection packets are sent, an integer, ranging from 1 to 4094, used to enable packets not to carry Tag
Detect Status	Loop detection status
Src Mac	Source MAC address of received loop detection packets from another device
Src Port	Source interface ID of received loop detection packets from another device
Block Count	Number of times for blocking the interface due to detected loop
Loop VLAN list	List of VLANs where the loop is generated
Send Pkts	Number of times for sending loop detection packets to the same source MAC address and source interface
Recved Pkts	Number of times for receiving loop detection packets from the same source MAC address and source interface

Configuration item	Description
Operator	Clear statistics or resume statistics.

3.3.4 Port Vlan Statistics Information

Scenario

You can view statistics on VLAN loop detection.

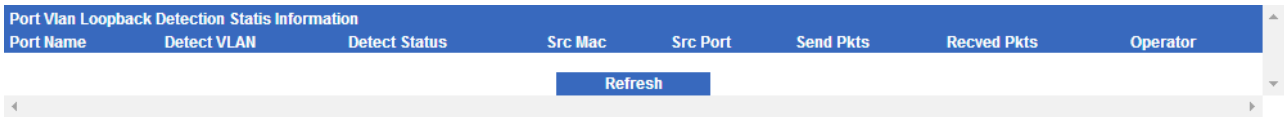
Configuration steps

Step 1 In the navigation bar, choose **Ethernet Config** > **LBD** > **Port Vlan Statistics Information**. The Port Vlan Loopback Detection Statis Information page appears.

Step 2 You can view statistics on VLAN loop detection.

- To restart an interface that is shut down due to a detected loop, click **Restore**.
- To clear statistics, click **Clear**.

Figure 3-11 Port Loopback Detection Statis Information page



Step 3 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 3-11 Configuration items on POE Config page

Configuration item	Description
Port Name	Interface ID
Detect VLAN	ID of the VLAN in which loop detection is enabled, an integer, ranging from 1 to 4094
Detect Status	Whether a loop is detected
Src Mac	Source MAC address of the received loop detection packet from other devices
Src Port	Interface ID of the received loop detection packet from other devices
Send Pkts	Number of times for sending loop detection packets to the same source MAC address and source interface
Recved Pkts	Number of times for receiving loop detection packets to the same source MAC address and source interface

Configuration item	Description
Operator	Clear or restore statistics.

3.4 Port Mirror

3.4.1 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 relevant network conditions.

The Gazelle S1000i-LI supports data stream mirroring on the ingress port and egress port. The packets on 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.

3.4.2 Group Mirror Config

Scenario

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

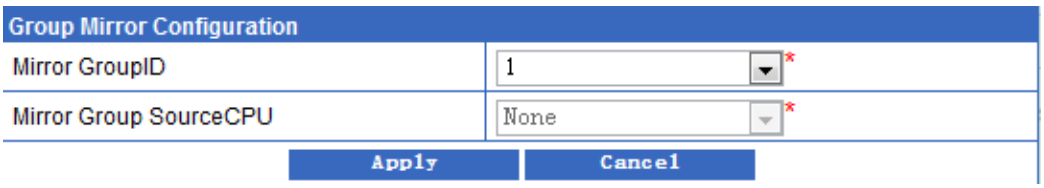
Port mirroring copies the port traffic monitored to a monitor port or CPU to obtain the flow upon failure or abnormality of an ingress/egress port for analysis, and helps discover the root cause and solve them timely.

Configuration steps

Step 1 In the navigation bar, choose **Ethernet Config** > **Port Mirror** > **Group Mirror Config**. The Group Mirror Config page appears.

Step 2 Click **Add**. On the Group Mirror Config page, configure related items, and click **Apply**.

Figure 3-12 Group Mirror Config page



Step 3 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 3-12 Configuration items on Group Mirror Config page

Configuration item	Description
Mirror Group ID	ID of the mirroring group, ranging from 1 to 4
Mirror Group Source CPU	Type of the traffic of which the mirroring group CPU needs to be configured: • None: port mirroring is enabled while source CPU mirroring is disabled.

3.4.3 Port Mirror Config

Scenario

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

Port mirroring copies the port flow monitored to a monitor port or CPU to obtain the flow upon failure or abnormality of an ingress/egress port for analysis, and helps discover the root cause and solve them timely.

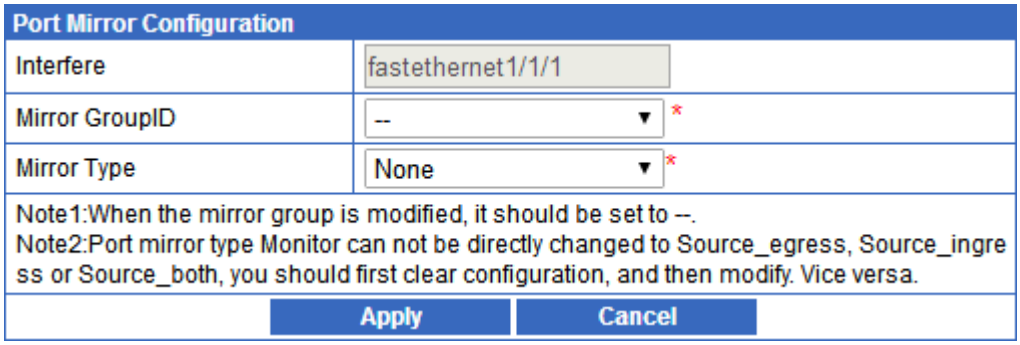
Configuration steps

Step 1 In the navigation bar, choose **Ethernet Config** > **Port Mirror** > **Port Mirror Config**. The Port Mirror Config page appears.

Step 2 Choose an item. Click **Modify**.

Step 3 On the Port Mirror Configuration page, configure related items, and click **Apply**.

Figure 3-13 Port Mirror Configuration page



Step 4 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 3-13 Configuration items on Mirror Port Config page

Configuration item	Description
Interface	Interface ID
Mirror Group ID	ID of the mirroring group to which the interface belongs
Mirror Type	Type of the mirroring port: None: port mirroring is disabled.

Caution

- To modify the Mirror Group ID, modify it to "–" first.
- To modify the Mirror Type, clear configurations first. For example, if it is Monitor, you cannot directly modify it to Source_egress, Source_ingress, or Source_both, but clear configurations and modify it to other types.

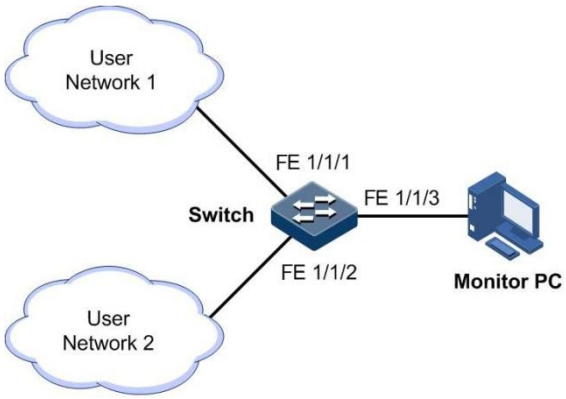
3.4.4 Example for configuring port mirroring

Networking requirements

As shown in Figure 3-14, the network administrator wants to monitor packets received by and sent from user network 1 and user network 2 through the monitor PC, thus able to capture traffic upon fault or abnormality, and analyze and discover the root cause, and solve them timely. Detailed requirements are as below:

- Monitor port: FE 1/1/3
- Source mirroring port list: FE 1/1/1 and FE 1/1/2
- Mirrored packets: packets in both the ingress and egress directions of the interface

Figure 3-14 Port mirroring networking



Configuration principles

Configuration principles of port mirroring are as below:

- Create a mirroring group.
- Configure the monitor port.
- Configure the source mirroring port list.

Configuration steps

Step 1 Create a mirroring group.

1. In the navigation bar, choose **Ethernet Config** > **Port Mirror** > **Group Mirror Config**. The Group Mirror Config page appears.
2. Click **Modify**. On the Group Mirror Config page, configure related items, and click **Apply**.

Figure 3-15 Configuring port mirroring

Mirror GroupID	MirrorGroupSourceCPU	
3	None	Modify Delete
4	None	Modify Delete

Step 2 Configure the monitor port.

1. In the navigation bar, choose **Ethernet Config** > **Port Mirror** > **Port Mirror Config**. The Port Mirror Config page appears.
2. Choose FE 1/1/3. Click **Modify**. Configure the Mirror Type to Monitor. Click **Apply**.

Step 3 Configure the source mirroring port list.

1. In the navigation bar, choose **Ethernet Config** > **Port Mirror** > **Port Mirror Config**. The Port Mirror Config page appears.
2. Choose FE 1/1/1 and FE 1/1/2 respectively. Click **Modify**. Configure the Mirror Type to Both. Click **Apply**.

Figure 3-16 Configuring port mirroring rules

Interface	MirrorPortInGroup	MirrorPortType	
fastethernet1/1/1	--	None	Modify Clear
fastethernet1/1/2	--	None	Modify Clear
fastethernet1/1/3	--	None	Modify Clear
fastethernet1/1/4	--	None	Modify Clear

Step 4 After configurations are complete, click **Save**.

Checking results

Packets coming from and going to FE 1/1/1 and FE 1/1/2 are mirrored to monitoring port FE 1/1/3.

You can monitor the receiving and sending of these packets through the monitor PC, capture traffic upon fault or abnormality, analyze and discover the root cause, and solve them timely.

4 Route Config

This chapter describes basic principles and configuration procedures of route configurations, including the following section:

- IP Config

4.1 IP Config

4.1.1 Introduction

The Gazelle S1000i-LI supports being configured with an IP address for its VLAN interface.

IP interface

The Layer 3 interface, namely, 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. Each Layer 3 interface will correspond to an IP address and associate with at least one VLAN.

If only one IP address is configured on the Layer 3 interface on the Gazelle S1000i-LI, only some hosts can communicate with external networks through the Gazelle S1000i-LI. To enable all hosts to communicate with external networks, configure the secondary IP address of the interface. To enable hosts in two network segments to interconnect with each other, configure the switch as the gateway for all hosts.

SNMP interface

To connect to the NMS through the SNMP interface or Telnet the device through the SNMP interface, configure the IP address of the SNMP interface so that the device can be connected to the NMS and PC.

Loopback interface

Use the IP address of the loopback interface to log in through Telnet so that the Telnet session will not become Down due to the change of the physical interface status. The ID of the loopback interface is used as the unique identity of the device for dynamic routing protocols, such as the Router ID for OSPF.

4.1.2 IP Config

Scenario

You can configure an IP interface for the SNMP interface, IP interface, or loopback interface.

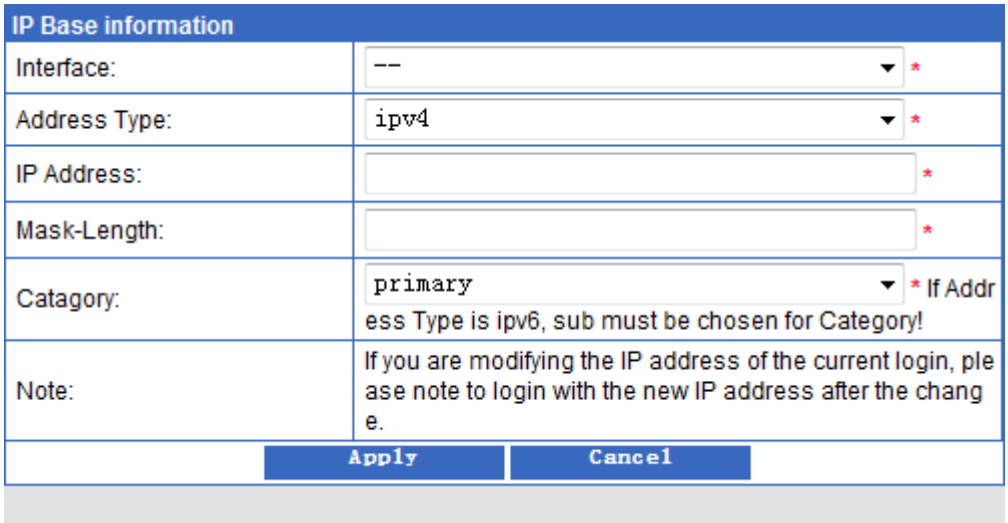
Configuration steps

Step 1 In the navigation bar, choose **Route Config** > **IP Config** > **IP Config**. The IP Config page appears.

Step 2 You can view configurations of the IPv4 address of the Layer 3 interface.

- To add an item, click **Add** to enter the adding page. Configure related items, and click **Apply**.
- To modify a configured item, click **Modify** to enter the modification page. Configure related items, and click **Apply**.
- To delete an item, click **Delete** in the corresponding row.

Figure 4-1 IP Base information page



Step 3 In Vlan Interface Information area, you can view the list of VLAN interfaces.

- To add an item, click **Add** to enter the adding page. Configure related items, and click **Apply**.
- To delete an item, click **Delete** in the corresponding row.

Figure 4-2 IP Vlan Information page

Step 4 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 4-1 Configuration items on IP Config page

Configuration item	Description
Interface	VLAN interface ID
Address Type	Type of the IP address of the interface, including: • ipv4: IPv4 address • ipv6: IPv6 address
Ip Address	IP address of the interface • When the Address Type is ipv4, the IP address is in dotted decimal notation. • When the Address Type is ipv4, the IP address is in colon hexadecimal notation.
Mask-Length	Length of the network mask, an integer
Category	Primary/Subsidiary IP address, including: • primary: primary IP address • sub: subsidiary IP address, chosen mandatorily for the IPv6 address
VLAN List	List of VLANs mapped by Layer 3 interfaces The number of configured VLANs associated with each Layer 3 interface cannot exceed 24. The associated VLAN to be configured must differ from the VLAN associated with other Layer 3 interfaces.

4.1.3 Static Route Config

Scenario

For a network with simple topology, you can configure a static route. The static route needs to be configured manually. You can create an intercommunication network by configuring the static route.

Configuration steps

Step 1 In the navigation bar, choose **Route Config** > **Static Route** > **Static Route Config**. The Static Route Config page appears.

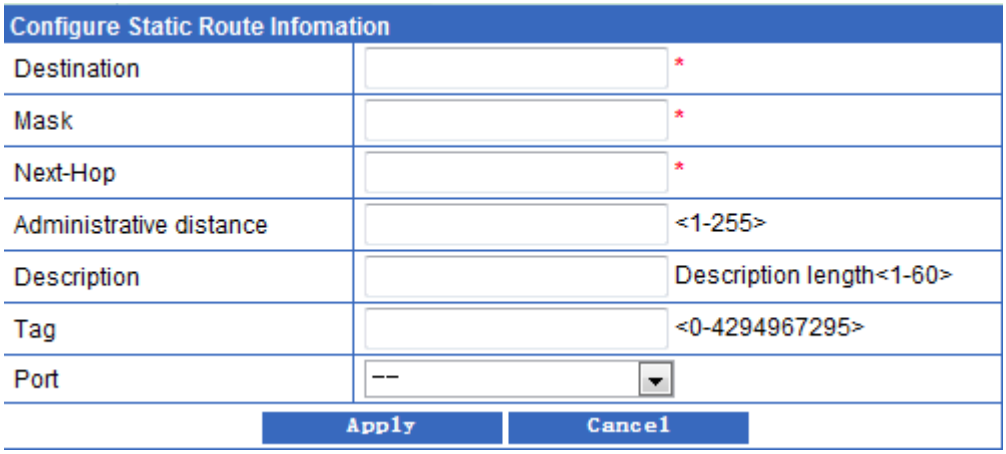
Step 2 In Static Global Information area, you can view the number of static routes. Configure related items, and click **Apply**.

Step 3 In the lower area, you can view configured static route information.

- To modify a configured item, click **Modify** to enter the modification page. Configure related items, and click **Apply**.
- To add an item, click **Add** to enter the adding page. Configure related items, and click **Apply**.

- To delete an item, click **Delete** in the corresponding row.

Figure 4-3 Configure Static Route Information page



Step 4 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 4-2 Configuration items on Static Route Config page

Configuration item	Description
Destination	Destination IP address
Mask	Subnet mask of the destination network, in dotted decimal notation
Next-Hop	IP address of the next hop address for the destination network, in dotted decimal notation The next hop device must be directly connected to the Gazelle S1000i-LI, otherwise this configuration is invalid.
Administrative distance	Administrative distance of the static routing protocol, an integer, ranging from 1 to 255
Description	Description of the static route, a string of 1 to 60 characters
Tag	Tag value, identifying attributes of a static route, classifying static routes to implement different route management policies
Port	Interface ID

5 Multicast Config

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

- Snooping
- MLD

5.1 Snooping

5.1.1 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 Gazelle S1000i-LI to monitor IGMP sessions between the host and multicast router. When monitoring a group of IGMP Report from host, the Gazelle S1000i-LI will add host-related interface to the forwarding entry of this group. Similarly, when a forwarding entry reaches the aging time, the Gazelle S1000i-LI will delete host-related interface from forwarding entry.

IGMP Snooping forwards multicast data through Layer 2 multicast forwarding entry. When receiving multicast data, the Gazelle S1000i-LI 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 Gazelle S1000i-LI effectively.

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

5.1.2 Snooping Config

Scenario

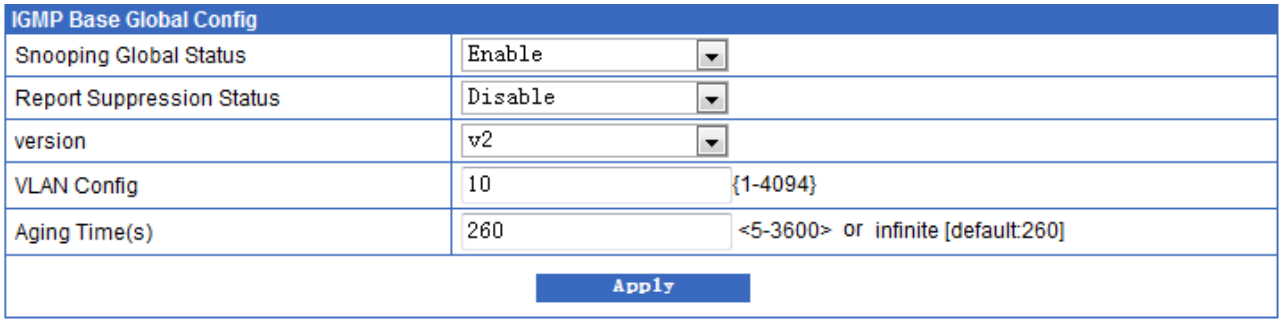
Multiple hosts belonging to a VLAN receive data from the multicast source. Enable IGMP Snooping on the Switch that connects the multicast router and hosts. By listening IGMP packets transmitted between the multicast router and hosts, creating and maintaining the multicast forwarding table, you can implement Layer 2 multicast.

Configuration steps

Step 1 In the navigation bar, choose **Multicast Config** > **Snooping Base** > **Snooping Base Config**. The Snooping Base Config page appears.

Step 2 Configure related items, and click **Apply**.

Figure 5-1 IGMP Base Global Config page



Step 3 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 5-1 Configuration items on Configuration page for IGMP Snooping

Configuration item	Description
Snooping Global Status	Global IGMP Snooping status, including: • Enable • Disable By default, global IGMP Snooping is disabled.
Report Suppression Status	Report suppression status, including: • Enable: enabled • Disable: disabled By default, report suppression is disabled.
Version	IGMP version, including: • V2 • V3
VLAN Config	VLAN to be configured with IGMP Snooping, an integer, ranging from 1 to 4094 It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".
Aging Time (s)	Aging time of IGMP members, an integer, ranging from 5 to 3600 or being infinite, in units of second, being 260s by default

5.2 MLD

5.2.1 Introduction

Multicast Listener Discover (MLD) is a network protocol used in multicast technologies. The IPv6 router can discover multicast snoopers in the directly connected network segment.

Through MLD, a router can snoop whether there is a snooper of the IPv6 multicast group in the connected network segment, and then record the result in the database. The router also maintains timer information about these IPv6 multicast addresses.

The MLD router uses the local address of IPv6 unicast link as the source address to send MLD packets, and uses ICMPv6 packets. All MLD packets are limited to local links, with hops of 1.

5.2.2 GMRP Config

Scenario

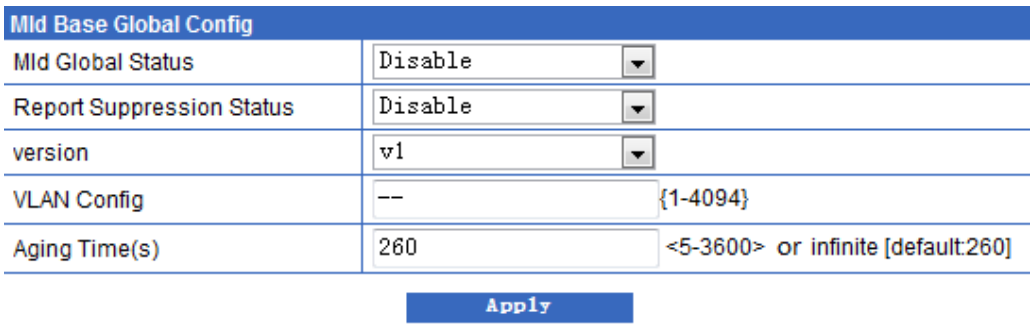
Multicast arising in the IPv4 era implements single-point sending and multi-point receiving, and transmits data efficiently point to multiple points on the network, thus saving network bandwidth and lowering network load. It is enhanced on the IPv6 network. By listening MLD messages and thus creating a forwarding table for multicast packets, the Gazelle S1000i-LI can manage and control the forwarding of multicast packets, and forward multicast packets to the target host.

Configuration steps

Step 1 In the navigation bar, choose **Multicast Config** > **Mld Base** > **Mld Base Config**. The Mld Base Config page appears.

Step 2 Configure related items, and click **Apply**.

Figure 5-2 Gmrp Port Configuration Modify page



Step 3 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 5-2 Configuration items on GMRP Config page

Configuration item	Description
Mld Global Status	Global MLD Snooping status, including: • Enable • Disable By default, global MLD Snooping is disabled.
Report Suppression Status	Report suppression status, including: • Enable: enabled • Disable: disabled By default, report suppression is disabled.
Version	MLD version, including: • V1 • V2
VLAN Config	VLAN to be configured with MLD Snooping, an integer, ranging from 1 to 4094 It supports specific values, such as "1,2,3"; it also supports a range, such as "1-3".
Aging Time (s)	Aging time of MLD members, an integer, ranging from 5 to 3600 or being infinite, in units of second, being 260s by default

6 Security Config

This chapter describes basic principles and configuration procedures of security configurations, including the following sections:

- Storm Control
- MAC Security

6.1 Storm Control

6.1.1 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.

Storm control can filter broadcast packets and unknown unicast or multicast packets that may lead to broadcast storm. 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.

6.1.2 Port Threshold Config

Scenario

You can configure thresholds of storm control on this page. When the interface rate exceeds the configured threshold, the Gazelle S1000i-LI identifies storm occurrence. Thus you must configure thresholds of storm control.

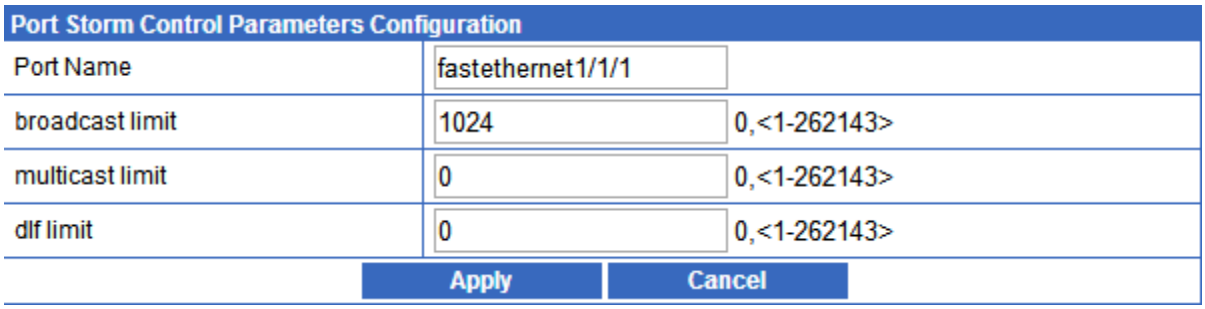
Configuration steps

Step 1 In the navigation bar, choose **Security Config** > **Storm Control** > **Port Threshold Config**. The Port Threshold Config page appears.

Step 2 You can view storm control thresholds on each interface.

To modify a configured item, click **Modify** to enter the modification page. Configure related items, and click **Apply**.

Figure 6-1 Port Storm Control Parameters Configuration page



Step 3 Configure related items, and click **Apply**.

Step 4 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 6-1 Configuration items on Port Storm Control Threshold Configuration page

Configuration item	Description
Port name	Interface ID
Broadcast limit	Broadcast storm control rate threshold, an integer When the Ctrl Type is pps, it is 0 or ranges from 1 to 262143, in units of ps, being 1024 pps by default.
Multicast limit	Multicast storm control rate threshold, an integer When the Ctrl Type is pps, it is 0 or ranges from 1 to 262143, in units of ps, being 0 pps by default which indicates no rate limiting.
DLF limit	Unknown unicast storm control rate threshold, an integer When the Ctrl Type is pps, it is 0 or ranges from 1 to 262143, in units of ps, being 0 pps by default which indicates no rate limiting.

6.2 MAC Security

6.2.1 Introduction

Port security MAC is used for the switching device on the edge of the network user side, which can ensure the security of access data in some interface, control the incoming packets according to 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.

Classification of secure MAC addresses

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 set the learnt MAC address to secure MAC address in the range of the maximum number of learnt MAC address. The dynamic secure MAC addresses ages and does not support configuration load.

Dynamic secure MAC address can be converted to sticky secure MAC address if necessary, so as not to be aged and support configuration auto-loading.

- Sticky secure MAC address

The 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. The system supports loading configurations.
- When sticky learning is disabled, sticky secure MAC address will lose effectiveness and be saved only in the system.

Note

- When sticky learning is enabled, all dynamic secure MAC addresses learnt from an interface will be converted to sticky secure MAC addresses.
- When sticky learning is disabled, all sticky secure MAC addresses (including dynamic secure MAC addresses and manually configured sticky secure MAC addresses) on an interface will be converted to dynamic secure MAC addresses.

Processing mode for violating secure MAC address

When the number of secure MAC addresses has already reached the maximum number, the entering of packets from a strange source MAC address will be regarded as violation

operation. For the illegal user access, there are different processing modes to configure the switch according to secure MAC violation policy:

- Protect mode: for illegal access users, secure interface will discard the user's packets directly.
- Restrict mode: for illegal access users, secure interface will discard the user's packets, and the console will print Syslog information and send alarm to the network management system.
- Shutdown mode: for illegal access users, secure interface will discard the user's packets, and the console will print Syslog information, send alarm to the network management system, and then shut down the secure interface.

Caution

When the MAC address is in drift, that is, the secure interface A receives one user access corresponding a secure MAC address on secure interface B, secure interface A will take it as violation processing.

6.2.2 MAC Security Config

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.

Configure the MAC address as dynamic secure MAC address and sticky secure MAC address according to actual conditions as required. The MAC address will be aged and its aging time can be manually configured.

Caution

- 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 address limit are mutually exclusive, which cannot be configured concurrently.

Configuration steps

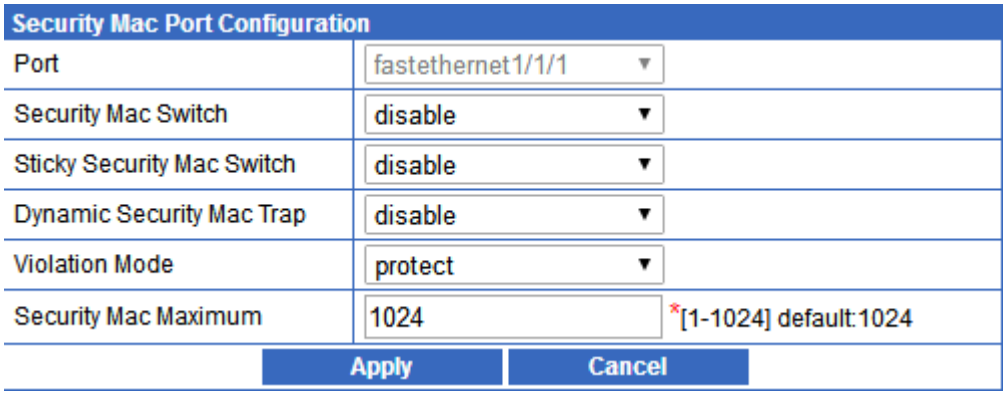
Step 1 In the navigation bar, choose **Security Config** > **MAC Security** > **MAC Security Config**. The MAC Security Config page appears.

Step 2 In the Global Information area, configure aging time and recovery time in the Security Mac Aging Time and Recovery Time text boxes respectively, and click **Apply**.

Step 3 In the Security Mac Port Configuration area, you can view configurations of port security MAC.

To modify a configured item, click **Modify** to enter the modification page. Configure related items, and click **Apply**.

Figure 6-2 Security Mac Port Configuration page



Step 4 After configurations are complete, click **Save**.

Configuration items

Table 6-2 Configuration items on Security Mac Port Configuration page

Configuration item	Description
Port	Interface ID
Security MAC Switch	Port security MAC status, including: • enable: enabled • disable: disabled By default, port security MAC is disabled.
Sticky Security MAC Switch	Port sticky security MAC status, including: • enable: enabled • disable: disabled By default, port sticky security MAC learning is disabled.
Dynamic Security Mac Trap	Port security MAC learning Trap status, including: • enable: enabled • disable: disabled By default, port security MAC learning Trap is disabled.
Violation Mode	Processing mode for port violation, including: • Protect: protection mode • Restrict: restriction mode • Shutdown: shutdown mode By default, processing mode for port violation is Protect.
Security Mac Maximum	Maximum number of secure MAC addresses on the interface, ranging from 1 to 100, being 1 by default

6.2.3 Security Mac Config

Scenario

To ensure security of data incoming from a switch interface, control ingress packets by source MAC address. Static secure MAC address is configured by user on secure interface manually; this MAC address will take effect when port security MAC is enabled. Static secure MAC address is not aged and supports loading configuration.

Caution

We do not recommend enabling port security MAC while configuring static MAC address through MAC address management. Otherwise, security MAC will be invalid.

Configuration steps

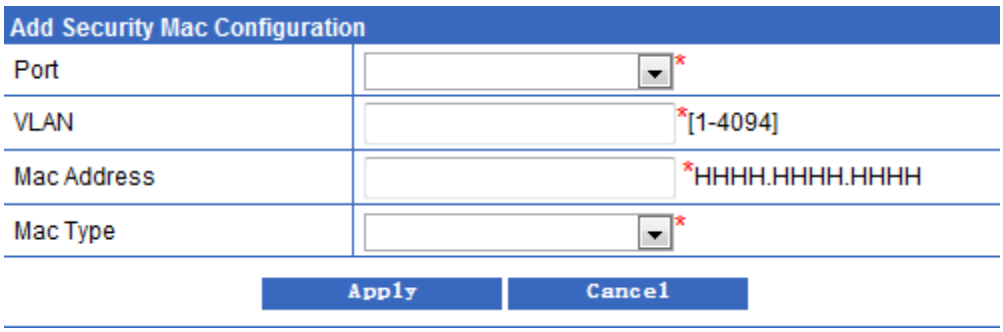
Step 1 In the navigation bar, choose **Security Config** > **MAC Security** > **Security Mac Config**. The Security Mac Config page appears.

Step 2 In the Clear Security Mac Configuration area, configure related items, and click **Clear**. A confirmation dialog box appears. Click **OK**.

Step 3 In the Security Mac Configuration And Management area, you can view configurations of security MAC.

- To modify a configured item, click **Modify** to enter the modification page. Configure related items, and click **Apply**.
- To add an item, click **Add** to enter the adding page. Configure related items, and click **Apply**.
- To delete an item, click **Delete** in the corresponding row.

Figure 6-3 Add Security Mac Configuration page



Step 4 Click **Refresh** to view current configurations of security MAC.

Step 5 After configurations are complete, click **Save**.

Configuration items

Table 6-3 Configuration items on Add Security Mac Configuration page

Configuration item	Description
Port	Interface ID
VLAN	VLAN ID, ranging from 1 to 4094
Mac Address	Type of secure MAC addresses, including: • configured: static secure MAC address • sticky: sticky secure MAC address
Mac Type	Secure MAC address, in dotted hexadecimal notation

6.2.4 MAC Security Information

Scenario

You can view port security MAC configurations and learning information, including:

- Port ID
- Port security MAC status
- Maximum number of secure MAC addresses allowed to access
- Current number of secure MAC addresses
- Maximum number of historical secure MAC addresses
- Number of violating secure MAC addresses
- Processing mode for violation

Configuration steps

Step 1 In the navigation bar, choose **Security Config** > **MAC Security** > **Security MAC Information**. The Security MAC Information page appears.

Step 2 You can view configurations of port security MAC.

Figure 6-4 Mac Security State Information page

Mac Security State Information

Port	Security Mac Switch	Allowed Max Number	Current Number	History Max Number	Violation Mode	Violation Count
fastethernet1/1/1	disable	1024	0	0	protect	0
fastethernet1/1/2	disable	1024	0	0	protect	0
fastethernet1/1/3	disable	1024	0	0	protect	0
fastethernet1/1/4	disable	1024	0	0	protect	0

Step 3 Click **Refresh** to view current configurations of port security MAC.

Step 4 After configurations are complete, click **Save**.

Configuration items

Table 6-4 Configuration items on Mac Security State Information page

Configuration item	Description
Port	Port ID
Security Mac Switch	Port security MAC status • enable • disable By default, port security MAC is disabled.
Allowed Max Number	Maximum number of secure MAC addresses allowed to access by the port, ranging from 1 to 100
Current Number	Current number of secure MAC addresses on the port, ranging from 1 to 100
History Max Number	Maximum number of historical secure MAC addresses, ranging from 0 to 65535
Violation Mode	Processing mode for port violation, including: • Protect: protection mode • Restrict: restriction mode • Shutdown: shutdown mode.
Violation Count	Number of interface violations, ranging from 0 to 65535

7 Reliability Config

This chapter describes basic principles and configuration procedures of reliability configurations, including the following section:

- Link Aggregate

7.1 Link Aggregate

7.1.1 Introduction

With link aggregation, multiple physical Ethernet interfaces are combined to form a Logical Aggregation Group (LAG). Multiple physical links in one LAG are regarded as a logical link. The link aggregation helps share traffics among members in an LAG. Link aggregation not only effectively improves reliability of links between devices, but also helps gain higher bandwidth without upgrading hardware.

There are several methods of link aggregation:

- Manual aggregation mode

This mode is to add several physical interfaces into a LAG; all the Up interfaces make up a logical interface. The link under one logical link can realize load sharing. This mode does not need LACP packet interaction.

- Static LACP aggregation mode

Link Aggregation Control Protocol (LACP) is based on IEEE802.3ad recommendation. LACP exchanges information with peer through Link Aggregation Control Protocol Data Unit (LACPDU). After enabling LACP of an interface, it notifies the peer of its own LACP priority, system MAC, interface LACP priority, interface ID and operation Key by sending LACPDU.

The peer receives LACPDU, compares information with that received by other interfaces, and chooses the interface in active status. The interfaces at both ends become consistent in active status.

Every member interface in a LAG has an operation key which indicates the aggregation ability of this interface. The operation key is created according to the interface configurations (LAG number, speed, and duplex mode). Any change of the configurations will lead to

recount of the operation Key. In a LAG, all the active interfaces must have the same operation key.

Among Ethernet reliability technologies, link aggregation is the most widely used and most simple.

7.1.2 Link Aggregate Group Config

Scenario

To provide higher bandwidth and reliability for a link between two devices, configure link aggregation.

With link aggregation, multiple physical Ethernet interfaces are added to a LAG and are aggregated to a logical link. Link aggregation helps share uplink and downlink traffic among members in one LAG. Therefore, the link aggregation helps obtain higher bandwidth and helps members in one LAG back up data for each other, which improves reliability of Ethernet connection.

Configuration steps

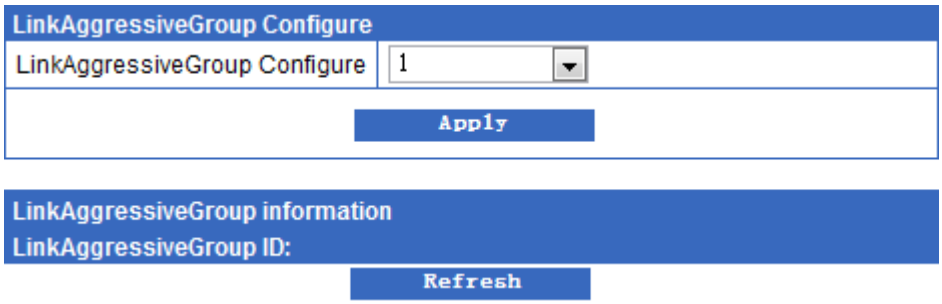
Step 1 In the navigation bar, choose **Reliability Config** > **Link Aggregate** > **Link Aggregate Group Config**. The Link Aggregate Group Config page appears.

Step 2 In the LinkAggressiveGroup Configure area, configure related items, and click **Apply**.

Step 3 In the LinkAggressiveGroup information area, you can view created LAGs.

- To delete an item, click **Delete** in the corresponding row.
- To modify a configured item, click **Modify** to enter the modification page. Configure related items, and click **Apply**.

Figure 7-1 Link Aggregate Group Config page



Step 4 Click **Refresh** to view current configurations of LAGs.

Step 5 After configurations are complete, click **Save**.

Configuration items

Table 7-1 Configuration items on Link Aggregate Group Config page

Configuration item	Description
LinkAggressiveGroup Configure	ID of the LAG interface, an integer, ranging from 1 to 8

7.1.3 Link Aggregate Config

Scenario

In static LACP link aggregation mode, active interfaces selected by devices at both ends must be consistent, otherwise the LAG will fail to be established.

After the active interface at the active end is determined, the passive end must select the active interface according to the selected active interface at the active end. To keep active interfaces at both ends consistent, determine the active end and passive end first.

To distinguish priorities of devices at both ends, configure the local system priority of the device. The device with the higher priority is the active end.

Configuration steps

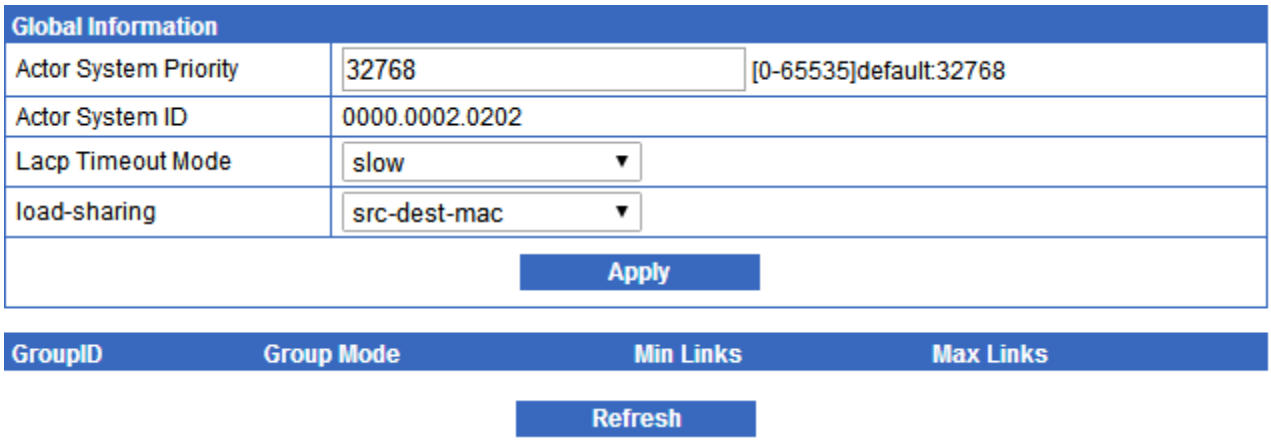
Step 1 In the navigation bar, choose **Reliability Config** > **Link Aggregate** > **Link Aggregate Config**. The Link Aggregate Config page appears.

Step 2 In the Global Information area, configure related items, and click **Apply**.

Step 3 In the lower area, you can view configurations of LAGs.

- To refresh current configurations of LAGs, click **Refresh**.
- To modify a configured item, click **Modify** to enter the modification page. Configure related items, and click **Apply**.

Figure 7-2 Modify page for link aggregation



Step 4 After configurations are complete, click **Save**.

Configuration items

Table 7-2 Configuration items on Link Aggregate Config page (1)

Configuration item	Description
Actor System Priority	System LACP priority, an interger, ranging from 0 to 65535 By default, it is 32768.
Actor System ID	Local system MAC address
Lacp Timeout Mode	LACP timeout mode, including: • fast: the period for the peer end to send LACP packets is 1s. • slow: the period for the peer end to send LACP packets is 30s. By default, it is slow.
Load-sharing	Load balancing mode, including: • src-mac • dest-mac • src-dest-mac • src-ip • dest-ip • src-dest-ip

Table 7-3 Configuration items on Link Aggregate Config page (2)

Configuration item	Description
Group ID	LAG ID, an integer, ranging from 1 to 32
Group Mode	LAG mode, including: • manual: manual link aggregation • lacp-static: static LACP link aggregation By default, it is lacp-static.
Min Links	Minimum number of active interfaces in the LAG, an integer, ranging from 1 to 8
Max Links	Maximum number of active interfaces in the LAG, an integer, ranging from 1 to 8 **Note** The maximum number of active interfaces in the LAG must be greater than or equal to the minimum number, otherwise the system will prompt that the entered maximum number of links is invalid.

Figure 7-3 Modify page for link aggregation

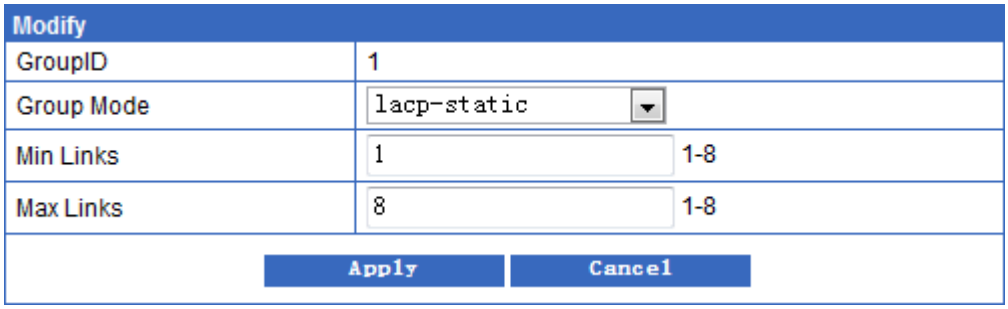


Table 7-4 Configuration items on modify page for link aggregation

Configuration item	Description
Group ID	LAG ID, an integer, ranging from 1 to 8
Group Mode	LAG mode, including: • manual: manual link aggregation • lacp-static: static LACP link aggregation By default, it is lacp-static.
Min Links	Minimum number of active interfaces in the LAG, an integer, ranging from 1 to 8
Max Links	Maximum number of active interfaces in the LAG, an integer, ranging from 1 to 8 **Note** The maximum number of active interfaces in the LAG must be greater than or equal to the minimum number, otherwise the system will prompt that the entered maximum number of links is invalid.

7.1.4 Link Aggregate Port Config

Scenario

In a static LACP LAG, the interface is in active or standby status. The active or standby interface can receive and send LACP packets, but the standby interface cannot forward user packets.

The system chooses the 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.

You can modify the interface priority and mode for sending LACP packets on this page.

Configuration steps

Step 1 In the navigation bar, choose **Reliability Config** > **Link Aggregate** > **Link Aggregate Port Config**. The Link Aggregate Port Config page appears.

Step 2 You can view configurations of link aggregation on interfaces.

Figure 7-4 Port Configuration page for link aggregation

Port Configuration port	Port-channel ID	Actor Port-Prio	Lacp Port Mode	Efficient Port	
fastethernet1/1/1	0	32768	active	invalid	Modify
fastethernet1/1/2	0	32768	active	invalid	Modify
fastethernet1/1/3	0	32768	active	invalid	Modify
fastethernet1/1/4	0	32768	active	invalid	Modify

To modify a configured item, click **Modify** to enter the modification page. Configure related items, and click **Apply**.

Step 3 Click **Refresh** to view current configurations of link aggregation on interfaces.

Step 4 After configurations are complete, click **Save**.

Figure 7-5 Modify port configuration page for link aggregation

modify port configuration	
Port	fastethernet1/1/1
Port-channel ID	0 [0-0] 0:removing port After a number: the number of configura ble aggregation group ID. Note:When ID is modified, the ID of the group is first remo ved, that is, the ID is set to 0.
Actor Port-Prio	32768 [0-65535]default:32768
Lacp Port Mode	active
NOTES : Don't allow to disable Lacp if the port is member of static group .	
Apply	Cancel

Note

The Port-channel ID in the figure above show the number of configured LAGs.

Configuration items

Table 7-5 Configuration items on modify port configuration page

Configuration item	Description
Port	Interface ID An interface can be added to only one LAG.

Configuration item	Description
Port-channel ID	LAG ID, an integer, ranging from 0 to 8, with the value 0 indicating that the system deletes the current interface
Actor System Priority	LACP priority, an integer, ranging from 0 to 65535, being 32768 by default The smaller the value is, the higher the priority is and the more possible the Gazelle S1000i-LI becomes the active end.
Lacp Port Mode	Interface LACP mode, including: • active: the interface actively sends LACP packets to the peer periodically for negotiation. • passive: the interface passively receives LACP packets from the peer, and then responds, but never actively sends LACP packets. By default, interface LACP mode is active.

7.1.5 Link Aggregate Information

Scenario

You can view LAG information about a specified interface on this page.

Configuration steps

Step 1 In the navigation bar, choose **Reliability Config** > **Link Aggregate** > **Link Aggregate Information**. The Link Aggregate Information page appears.

Step 2 You can view LAG information about a specified interface.

Figure 7-6 Link Aggregate Information page

Port: fastethernet1/1/1			
lacp internal information:			
Port-State	0x00	PortPriority	32768
AdminKey	0	OperateKey	0
TimeOut Mode	--	Port Active Mode	--
Aggregation	--	Synchronize	--
Collect	--	Distribut	--
Defaulted	--	Expired	--
lacp neighbor operating information:			
OperateState	0x00	OperatePortPriority	0
OperateSysID	0	OperateKey	0
TimeOut Mode	--	Port Active Mode	--
Aggregation	--	Synchronize	--
Collect	--	Distribut	--
Defaulted	--	Expired	--
Partner Operate Port	0		

Step 3 Click **Refresh** to view current LAG information about a specified interface.

Configuration items

N/A

7.1.6 Link Aggregate Packet Information

Scenario

You can view statistics of received and sent LACP packets on a specified interface on this page.

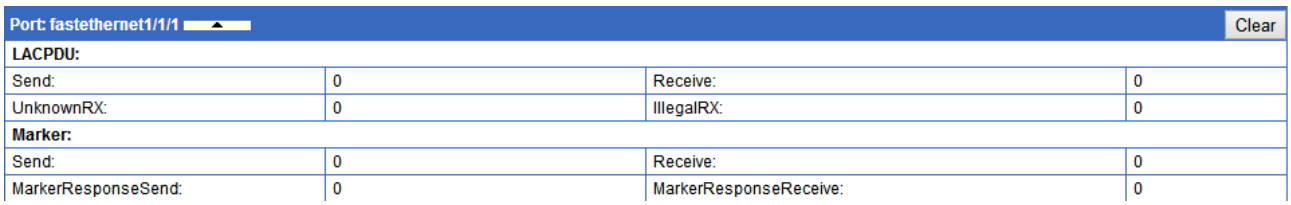
Configuration steps

Step 1 In the navigation bar, choose **Reliability Config** > **Link Aggregate** > **Link Aggregate Packet Information**. The Link Aggregate Packet Information page appears.

Step 2 You can view statistics of received and send LACP packets on each interface.

To clear statistics on an interface, click **Clear** in the corresponding row.

Figure 7-7 Link Aggregate Packet Information page



Port: fastethernet1/1/1			Clear
LACPDU:			
Send:	0	Receive:	0
UnknownRX:	0	IllegalRX:	0
Marker:			
Send:	0	Receive:	0
MarkerResponseSend:	0	MarkerResponseReceive:	0

Step 3 Click **Refresh** to view current statistics of received and send LACP packets on each interface.

Configuration items

Table 7-6 Configuration items on Link Aggregate Packet Information page

Configuration item	Description
LACPDU	LACP packets
Send	Number of sent LACPDU packets
Receive	Number of received LACPDU packets
UnknownRX	Number of received unknown LACPDU packets
IllegalRX	Number of received invalid LACPDU packets
Marker	Marker packets
Send	Number of sent marker packets
Receive	Number of received marker packets
MarkerResponsedSend	Number of sent marker response packets
MarkerResponseReceive	Number of received marker response packets

7.1.7 Example for configuring static LACP link aggregation

Networking requirements

As shown in Figure 7-8, to enhance reliability of links between Switch A and Switch B, configure static LACP between them. Add FE 1/1/1 and FE 1/1/2 on Switch A and Switch B to LAG 1. Configure FE 1/1/1 as the active interface and FE 1/1/2 as the standby linterface.

Figure 7-8 Static LACP link aggregation networking

Configuration principles

Configuration principles of static LACP link aggregation are as below:

- Configure global information about link aggregation.
- Create a LAG.
- Add interfaces to the LAG.

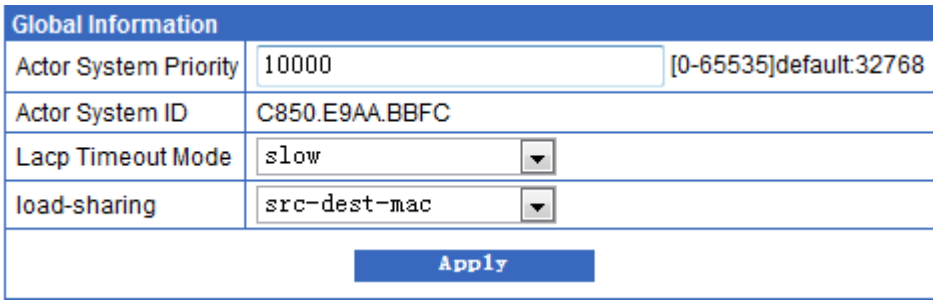
Configuration steps

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

Step 1 Configure global information about link aggregation.

1. In the navigation bar, choose **Reliability Config** > **Link Aggregate** > **Link Aggregate Config**. The Link Aggregate Config page appears.
2. In the LinkAggressiveGroup Configure area, configure the Actor System Priority to 1000.

Figure 7-9 Global Information page for link aggergation

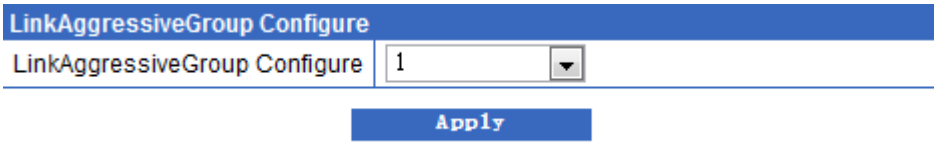


3. Click **Apply**.

Step 2 Create a LAG.

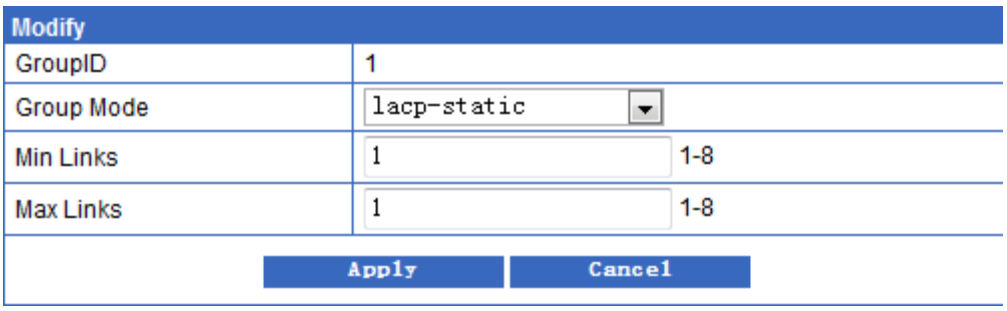
1. In the navigation bar, choose **Reliability Config** > **Link Aggregate** > **Link Aggregate Group Config**. The Link Aggregate Group Config page appears.

Figure 7-10 LinkAggressiveGroup Configure page



2. In the navigation bar, choose **Reliability Config** > **Link Aggregate** > **Link Aggregate Config**. The Link Aggregate Config page appears.
3. Click **Modify** according to LAG 1. On the Modify page, configure the Min Links and Max Links to 1 so that only one link in LAG 1 is the active link.

Figure 7-11 Modify page for link aggregation links

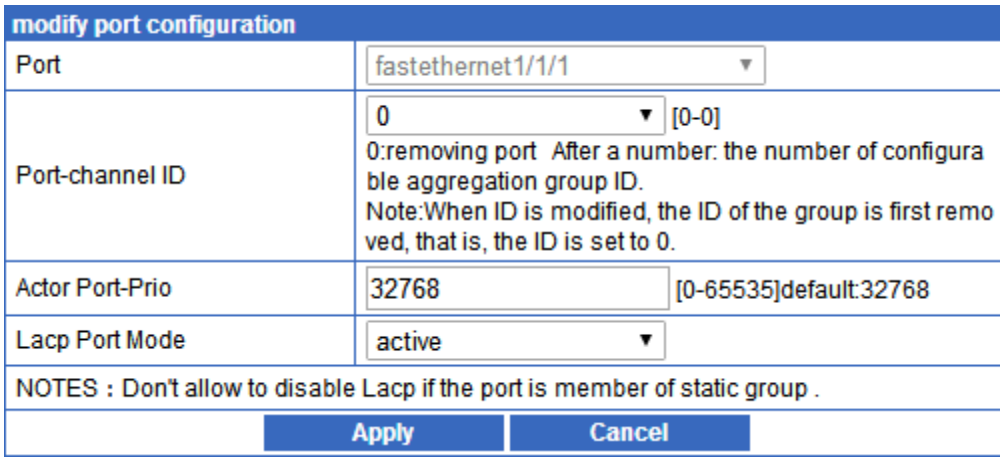


4. Click **Apply**.

Step 3 Add interfaces the LAG.

1. In the navigation bar, choose **Reliability Config** > **Link Aggregate** > **Link Aggregate Port Config**. The Link Aggregate Port Config page appears.
2. Click **Modify** corresponding to FE 1/1/1. On the Modify page, configure related items.

Figure 7-12 Modify port configuration page for FE 1/1/1



3. Click **Modify** corresponding to FE 1/1/2. On the Modify page, configure related items.

Figure 7-13 Modify port configuration page for FE 1/1/2

modify port configuration	
Port	fastethernet1/1/2
Port-channel ID	0 [0-0] 0:removing port After a number: the number of configura ble aggregation group ID. Note:When ID is modified, the ID of the group is first remo ved, that is, the ID is set to 0.
Actor Port-Prio	32768 [0-65535]default:32768
Lacp Port Mode	active
NOTES : Don't allow to disable Lacp if the port is member of static group .	
Apply Cancel	

4. Click **Apply**.

Step 4 In the navigation bar, choose **Base Config** > **Device Config** > **Config Maintain**. Click **Save**.

Checking results

Manuall disconnect the link between FE 1/1/1 on Switch A and FE 1/1/1 on Switch B to emulate a fault. View information about link aggregation on Switch A or Switch B. The link with the FE 1/1/2 becomes active, so link aggregation is enhanced.

8 System Management

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

- Log
- SNMP

8.1 Log

8.1.1 Introduction

The system log refers that the Gazelle S1000i-LI records the system information and debugging information in a log and sends the log to the specified destination. When the Gazelle S1000i-LI 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 into Trap, and output Trap to the SNMP server.

According to the severity level, logs are identified by 8 severity levels, as listed in Table 8-1.

Table 8-1 Log levels

Severity	Level	Description
Emergency	0	The system cannot be used.
Alert	1	Need to deal immediately.
Critical	2	Serious status

Severity	Level	Description
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; in other words, the severity ranges from emergencies to errors, can be sent.

8.1.2 Operation Log

Scenario

You can configure operation logs on this page. Logs record users' operations and device abnormalities, thus providing important evidence for maintaining and diagnosing the system.

Configuration steps

Step 1 In the navigation bar, choose **System Management** > **Log** > **Config** > **Operation Log**. The Operation Log page appears.

Step 2 Configure related items, and click **Apply**.

Figure 8-1 Operation Log page

Step 3 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 8-2 Configuration items on Operation Log page

Configuration item	Description
Operation Log Status	Operation log status, including: • Enable • Disable By default, operation log is disabled.

8.1.3 System Log

Scenario

The Gazelle S1000i-LI 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.

Logs record important status and operations during system operation, and are divided into Console, Host, Monitor, File, Buffer, and SNMP server.

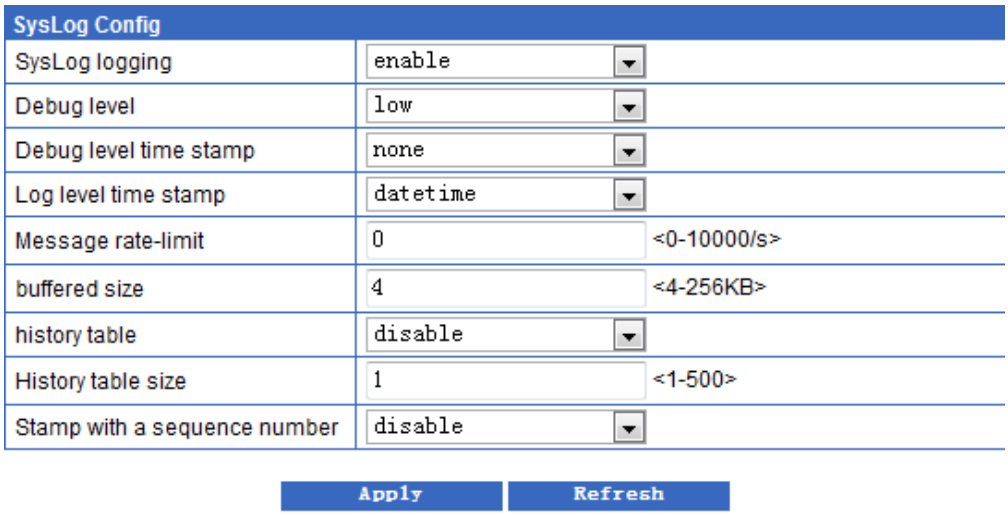
You can configure the Gazelle S1000i-LI to output logs of the specified level or lower levels to the log server on this page.

Configuration steps

Step 1 In the navigation bar, choose **System Management** > **Log** > **Config** > **System Log** > **Base Config**. The Base Config page appears.

Step 2 In the SysLog Config area, you can view configurations of system logs. Configure related items, and click **Apply**.

Figure 8-2 SysLog Config page



Step 3 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 8-3 Configuration items on SysLog Host Config page

Configuration item	Description
SysLog logging	System log status, including: • Enable • Disable By default, system log is disabled.
Debug level	Sending Debug (level 7) logs, including: • None: do not send debug information. • High: send high-level debug information. • Normal: send normal- and high-level debug information. • Low: send debug information in all levels. By default, the Debug level is Low.
Debug level time stamp	Debug (level 7) system log timestamp, including: • None: no timestamp • Datetime: the absolute time, a point, system time • Uptime: the relative time, a period, duration after system startup
Log level time stamp	System log timestamp for logs between emergencies level to informational level (levels 0–6), including: • None: no timestamp • Datetime: the absolute time, a point, system time • Uptime: the relative time, a period, duration after system startup
Message rate-limit	Rate for processing logs, number of logs processed per second, an integer, ranging from 1 to 10000, being 0 by default (no limit on processing rate)
Buffered size	Size of the log buffer, an integer, ranging from 4 to 256, in units of Kbyte, being 4 by default
History table	Status of outputting logs to the log historical table, including: • Enable • Disable By default, outputting logs to the log historical table is disabled.
History table size	Size of the log historical table, an integer, ranging from 1 to 500

Configuration item	Description
Stamp with a sequence number	Status of marking system logs with a sequence number, including: • Enable • Disable The sequence number is valid to outputting logs to the console, monitor, log files, and log buffer, and invalid to the log host and log historical table. By default, marking system logs with a sequence number is disabled.

8.1.4 Log Information

Scenario

You can view information about system logs on this page.

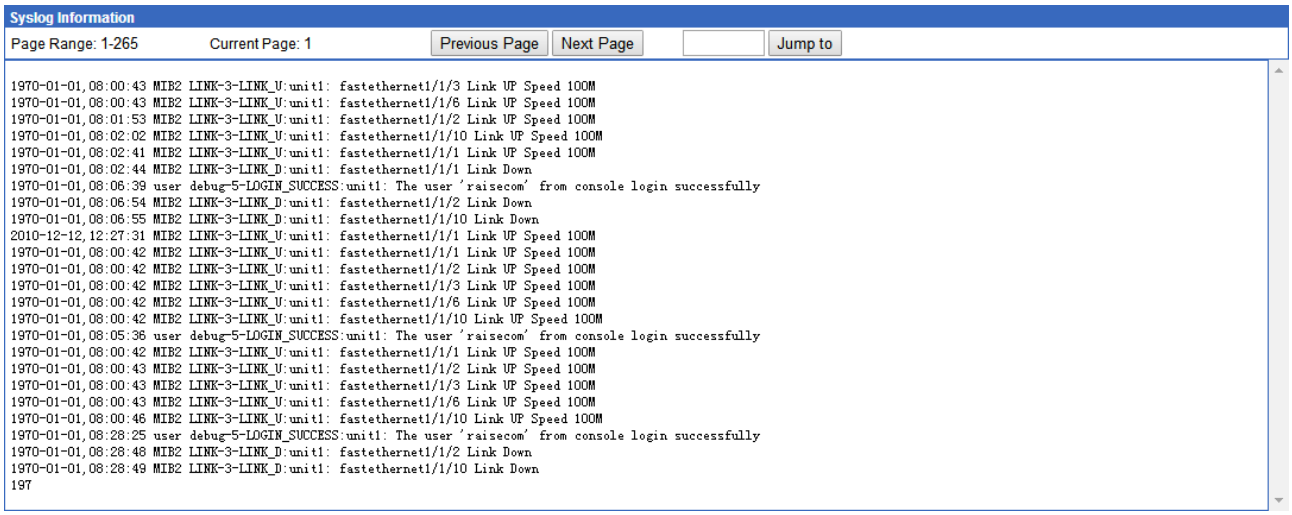
Configuration steps

View information about system logs as below:

Step 1 In the navigation bar, choose **System Management** > **Log** > **Config** > **Syslog View**. The Syslog Information page appears.

Step 2 You can view information about system logs.

Figure 8-3 SysLog Information page



Step 3 After configurations are complete, click **Save** to save configurations.

8.1.5 Syslog Export

Scenario

You can export system logs and operation logs on this page.

Configuration steps

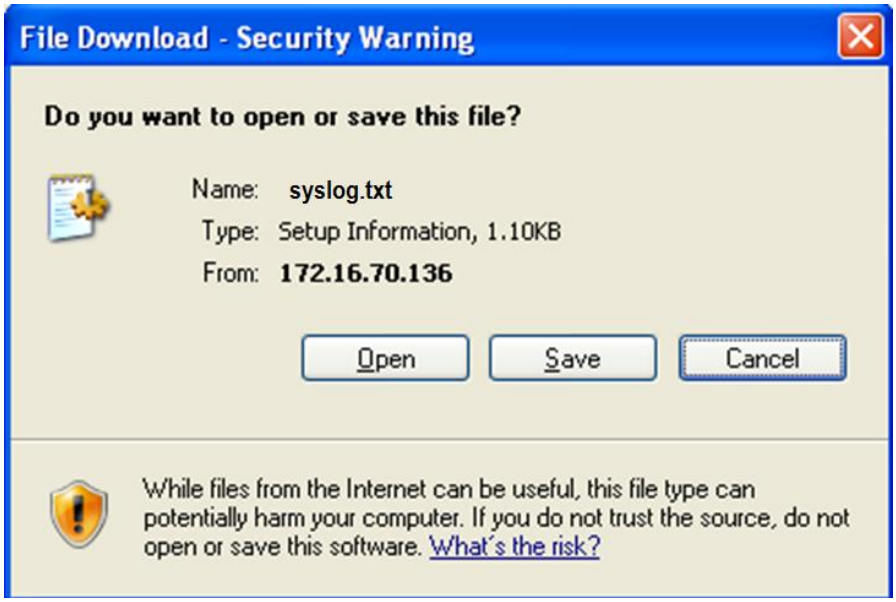
Step 1 In the navigation bar, choose **System Management** > **Log** > **Syslog Export**. The Syslog Export page appears.

Figure 8-4 Syslog Export page

Step 2 In the Startup Syslog Export area, click **Export** to export system logs. A File Download dialog box appears.

1. Click **Open** to view the syslog.
2. Click **Save**. A Save As dialog box appears. Choose a path to save the syslog, and click **Save**.

Figure 8-5 File Download page for syslog



Configuration items

N/A

8.2 SNMP

8.2.1 Introduction

Simple Network Management Protocol (SNMP) is designed by the Internet Engineering Task Force (IETF) to resolve problems in managing network devices connected to the Internet. Through SNMP, a network management system can manage all network devices that support SNMP, including monitoring network status, modifying configurations of a network device, and receiving network alarms. SNMP is the most widely used network management protocol in TCP/IP networks.

Principles of SNMP

SNMP is separated into two parts: Agent and NMS. The Agent and NMS communicate by SNMP packets being sent through UDP.

The Raisecom NView NNM system can provide friendly Human Machine Interface (HMI) to facilitate network management. The following functions can be realized through it:

- Send request packets to the managed device.
- Receive reply packets and Trap packets from the managed device, and show result.

The Agent is a program installed in the managed device, realizing the following functions:

- Receive/reply request packets from the NView NNM system
- Read/write packets and generate response 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 device when conditions are satisfied; reply module sends Trap packets to the NView NNM system through agent to report current status of device.

Note

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

Protocol versions

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

- SNMPv1 uses community name authentication mechanism. The community name, a string defined by an agent, acts like a secret. The network management system can visit the agent only by specifying its community name correctly. If the community name carried in a SNMP packet is not accepted by the Gazelle S1000i-LI, the packet will be dropped.
- Compatible with SNMPv1, SNMPv2c also uses community name authentication mechanism. SNMP V2c supports more operation types, data types, and errored codes, and thus better identifying errors.
- SNMPv3 uses User-based Security Model (USM) and View-based Access Control Model (VACM) security models. 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 Gazelle S1000i-LI supports v1, v2c, and v3 of SNMP.

MIB

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

- Name
- Access right
- Data type

The device-related statistic contents can be reached by accessing data items. Each proxy has its own MIB. MIB can be taken as a databasebetween the NMS and Agent, through which the NMS can read/write every managed object in the Agent to manage and monitor the Gazelle S1000i-LI.

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 Gazelle S1000i-LI supports standard MIB and Raisecom-customized MIB.

8.2.2 Snmp Config

Scenario

To log in to the Gazelle S1000i-LI through the NMS, configure basic functions of SNMP on the Gazelle S1000i-LI.

Complete the following tasks in advance:

- Configure the IP address of the interface.
- Configure the routing protocol to the route between the Gazelle S1000i-LI and NMS reachable.

Configuration steps

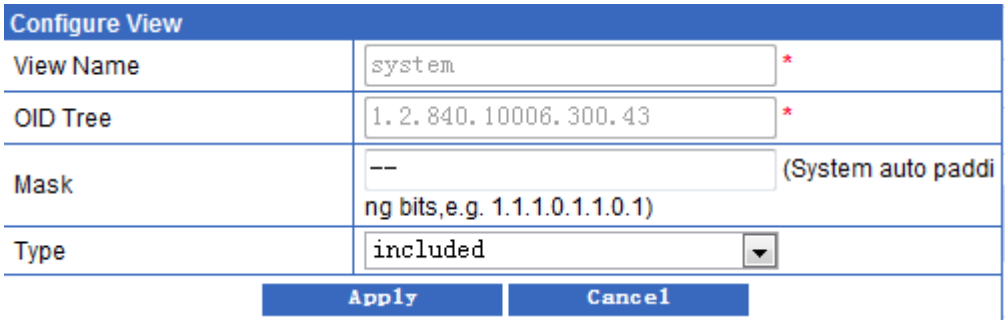
Step 1 In the navigation bar, choose **System Management** > **SNMP** > **Snmp Config**. The Snmp Config page appears.

Step 2 In the Basic Config area, configure related items, and click **Apply**.

Step 3 In the View Information area, you can view configured view information.

- To modify a configured item, click **Modify** to enter the modification page. Configure related items, and click **Apply**.
- To add an item, click **Add** to enter the adding page. Configure related items, and click **Apply**.
- To delete an item, click **Delete** in the corresponding row.

Figure 8-6 View Information page



Step 4 After configurations are complete, click **Save** to save configurations.

Configuration items

Table 8-4 Configuration items on Snmp Config page

Configuration item	Description
Device Location	Physical location of the device, being World China Raisecom by default You can modify the device location in the upper part in the Web configuration interface.
Network manager information	Network administrator ID and contact being support@Raisecom.com by default
Trap enable	Status for sending Trap to the NMS, including: • enable • disable By default, SNMP Trap is enabled.
View Name	View name, a string of 1 to 32 characters
OID Tree	OID of the MIB tree corresponding to the view
Mask	Mask of the sub-tree OID, supporting up to a length of 16, namely, supporting a sub-tree with depth up to 128, such as 1.1.1.1.0.1.1.1, with mask bits as 0 or 1 • If a bit is 0, it indicates that the corresponding bit in the MIB variable in the view is not necessarily identical to the bit of the sub-tree OID. • If a bit is 0, it indicates that the corresponding bit in the MIB variable in the view must be identical to the bit of the sub-tree OID.
Type	View type, including: • included: the MIB variable of the view is included in the sub-tree. • excluded: the MIB variable of the view is excluded from the sub-tree. By default, the view type is included.

8.2.3 Server authentication

Scenario

You can configure the authentication IP address of the SNMP server on this page.

Configuration steps

Step 1 In the navigation bar, choose **System Management** > **SNMP** > **server authentication**. The server authentication page appears.

Step 2 In the Base Config area, configure related items, and click **Apply**.

Step 3 In the SNMP Server IP Information area, you can view IP addresses of configured SNMP servers.

- To add an item, click **Add** to enter the adding page. Configure related items, and click **Apply**.
- To delete an item, click **Delete** in the corresponding row.

Figure 8-7 Add IP Address page

Step 4 After configurations are complete, click **Save**.

Configuration items

Table 8-5 Configuration items on server authentication page

Configuration item	Description
SNMP Server IP authentication	SNMP server authentication status, including: • enable • disable
Index	Index of the SNMP authentication server
IP Address	IP address of the SNMP, in dotted decimal notation

8.2.4 V1/V2

Scenario

To protect itself and prevent its MIB from unauthorized access, SNMP Agent proposes the concept of community. The management station in the same community must use the community name in all Agent operations. Otherwise, their requests will not be accepted.

The community name uses different SNMP string to identify different groups. Different communities can have read-only or read-write access authority. Groups with read-only authority can only query the device information, while groups with read-write authority can configure the device and query the device information.

SNMPv1/v2c uses the community name authentication scheme, and the SNMP packets which are inconsistent to the community name will be discarded.

Configuration steps

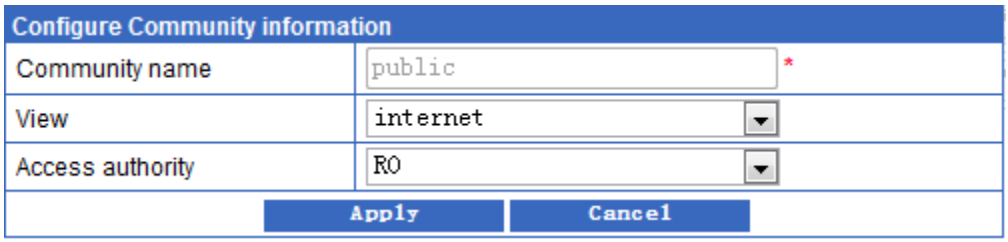
Configure the community as below:

Step 1 In the navigation bar, choose **System Management** > **SNMP** > **V1/V2** > **community config**. The community config page appears.

Step 2 You can view configurations of created communities.

- To modify a configured item, click **Modify** to enter the modification page. Configure related items, and click **Apply**.
- To add an item, click **Add** to enter the adding page. Configure related items, and click **Apply**.
- To delete an item, click **Delete** in the corresponding row.

Figure 8-8 Community information page



Step 3 After configurations are complete, click **Save**.

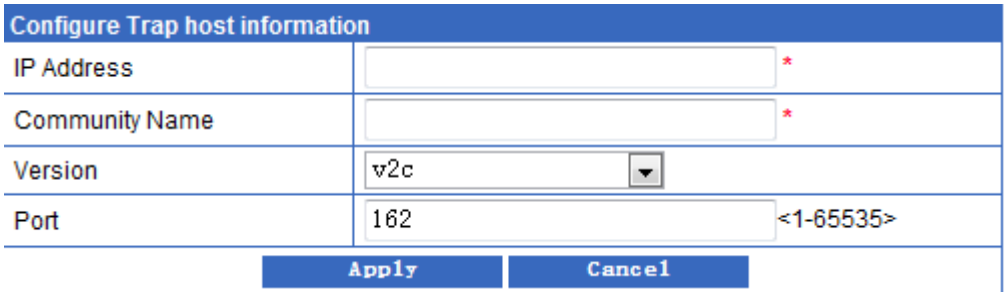
Configure the host as below:

Step 4 In the navigation bar, choose **System Management** > **SNMP** > **V1/V2** > **host config**. The host config page appears.

Step 5 You can view configurations of created hosts.

- To add an item, click **Add** to enter the adding page. Configure related items, and click **Apply**.
- To delete an item, click **Delete** in the corresponding row.

Figure 8-9 Trap host information page



Step 6 After configurations are complete, click **Save**.

Configuration items

Table 8-6 Configuration items on community config page

Configuration item	Description
Name	Community name, a string of 1 to 20 characters
View	View name
Access authority	Access authority of the community, including: • ro: the community has the read-only authority, and thus can only read Agent data. • rw: the community has the read-write authority, and thus can read Agent data and write data into the Agent.

Table 8-7 Configuration items on host config page for v1/v2

Configuration item	Description
IP Address	IP address of the target host, in dotted decimal notation
Port	Number of the UDP port on the target host to receive Trap, an integer, ranging from 1 to 65535 If this parameter is not configured, it is 162 by default.
Community Name	Community name
Version	SNMP version • v1: SNMPv1 • v2c: SNMPv2c

8.2.5 V3

Scenario

A SNMP view, a set of MIB variables, defines accessible MIB variables.

SNMPv3 uses USM mechanism. USM comes up with the concept of access group. One or more users correspond to one access group. Each access group sets the related read, write, and notification views. Users in an access group have access authorities of this view. The access group of users, who send Get and Set requests, must have authorities corresponding to the requests. Otherwise, the requests will not be accepted.

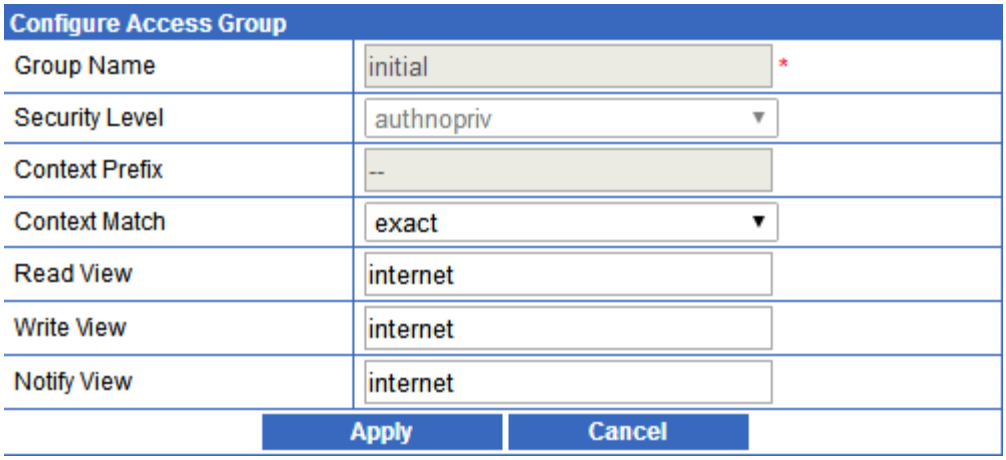
Configuration steps

Configure the access group as below:

Step 1 In the navigation bar, choose **System Management** > **SNMP** > **V3** > **group config**. The group config page appears.

Step 2 You can view information about configured access groups.

Figure 8-10 Configure Access Group page



- To modify a configured item, click **Modify** to enter the modification page. Configure related items, and click **Apply**.
- To add an item, click **Add** to enter the adding page. Configure related items, and click **Apply**.
- To delete an item, click **Delete** in the corresponding row.

Step 3 After configurations are complete, click **Save**.

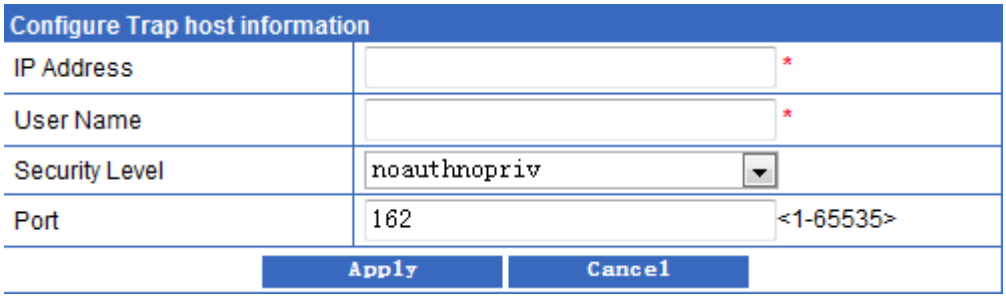
Configure the host as below:

Step 1 In the navigation bar, choose **System Management** > **SNMP** > **V1/V2** > **host config**. The host config page appears.

Step 2 You can view configurations of created hosts.

- To add an item, click **Add** to enter the adding page. Configure related items, and click **Apply**.
- To delete an item, click **Delete** in the corresponding row.

Figure 8-11 Trap host information page



Step 3 After configurations are complete, click **Save**.

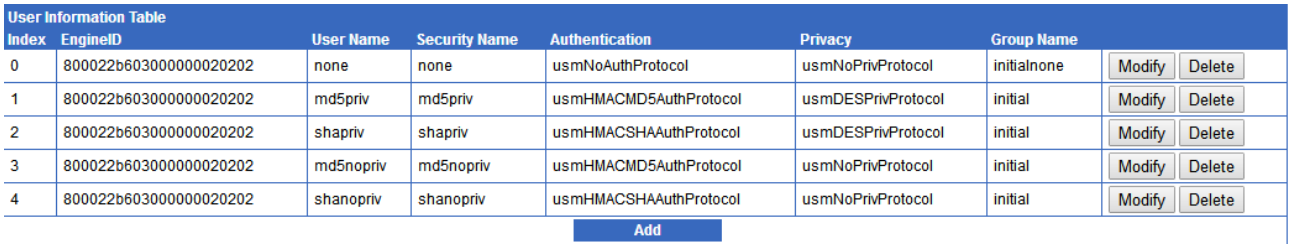
Configure the access group as below:

Step 1 In the navigation bar, choose **System Management** > **SNMP** > **V3** > **user config**. The user config page appears.

Step 2 You can view information about configured users.

- To modify a configured item, click **Modify** to enter the modification page. Configure related items, and click **Apply**.
- To add an item, click **Add** to enter the adding page. Configure related items, and click **Apply**.
- To delete an item, click **Delete** in the corresponding row.

Figure 8-12 User Information Table page



Step 3 After configurations are complete, click **Save**.

Configuration items

Table 8-8 Configuration items on group config page

Configuration item	Description
Group Name	Name of the SNMP group, a string of 1 to 30 characters
Context Prefix	Context name or prefix, a string of 1 to 30 characters
Security Model	SNMP security model, including: • v1sm: use SNMPv1 security model • v2sm: use SNMPv2c security model • usm: use the SNMPv3 security model, with authentication and encryption functions.

Configuration item	Description
Security Level	SNMP security level, including: • noauthnopriv: neither authenticate nor encrypt SNMP packets. • authnopriv: authenticate but encrypt SNMP packets. • authpriv: both authenticate and encrypt SNMP packets.
Context Prefix	Context name or prefix, a string of 1 to 30 characters
Context Match	Context matching type, including: • exact: exact matching • prefix: prefix matching
Read View	Readable view
Write View	Writable view
Notify View	View with notification function

Table 8-9 Configuration items on host config page for V3

Configuration item	Description
IP Address	IP address of the target host, in dotted decimal notation When configuring the IP address of a target host, you should make it different from the IP address of any existing target host.
Port	Number of the UDP port on the target host to receive Trap, an integer, ranging from 1 to 65535 If this parameter is not configured, it is 162 by default.
Community Name	User name in the SNMP group SNMPv3 uses the user name for authentication. If the user name in the NMS is different from the one configured on the Agent, Trap cannot be received.
Security Level	SNMP security level, including: • noauthnopriv: neither authenticate nor encrypt SNMP packets. • authnopriv: authenticate but encrypt SNMP packets. • authpriv: both authenticate and encrypt SNMP packets.

Table 8-10 Configuration items on user config page

Configuration item	Description
EngineID	ID of the remote SNMP engine, SNMP engine ID associated with the user name, necessarily named in a length of even Bytes

Configuration item	Description
User Name	User name in the SNMP group, a string of characters1 to 30
Security Name	SNMP security name
Authprotocol	Type of the authentication protocol, including: • usmNoAuthProtocol: does not authenticate SNMP packets. • usmHMACMD5AuthProtocol: authenticate SNMP packets through the MD5 Hash function. • usmHMACSHAAuthProtocol: authenticate SNMP packets through the SHA-1 Hash function.
Authentication password	Authentication key, generated through combination with the Hash function, used to authenticate users
Privacy	Type of the authentication protocol, including: • usmNoPrivProtocol: no authentication is used. • usmDESPrivProtocol: use the DESP algorithm for authentication.
Group Name	SNMP group name, a string of 1 to 32 characters

9 Appendix

This chapter describes terms and abbreviations involved in this document, including the following sections:

- Terms
- Acronyms and abbreviations

9.1 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 decides to receive or refuse the packets based on these rules.
Automatic Laser Shutdown (ALS)	The technology that is used for automatically shutting down the laser to avoid the maintenance and operation risks when the fiber is pulled out or the output power is over great.
Auto-negotiation	The interface automatically chooses the rate and duplex mode according to the result of negotiation. The auto-negotiation process is: the interface adapts its rate and duplex mode to the highest performance according to the peer interface; in other words, 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.

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 of 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

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.

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 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.

M

Multi-Mode Fiber (MMF)	In this fiber, multi-mode optical signals are transmitted.

N

Network Time Protocol (NTP)	A time synchronization protocol defined by RFC1305. It is used to synchronize time between distributed time server and clients. NTP is used to perform clock synchronization on all devices that have clocks in the network. Therefore, the devices can provide different applications based on a unified time. In addition, NTP can ensure a very high accuracy with an error of 10ms or so.

O

Open Shortest Path First (OSPF)	An internal gateway dynamic routing protocol, which is used to decide the route in an Autonomous System (AS)
Optical Distribution Frame (ODF)	A distribution connection device between the fiber and a communication device. It is an important part of the optical transmission system. It is mainly used for fiber splicing, optical connector installation, fiber adjustment, additional pigtail storage, and fiber protection.

P

Password Authentication Protocol (PAP)	PAP is an authentication protocol that uses a password in Point-to-Point Protocol (PPP). It is a twice handshake protocol and transmits unencrypted user names and passwords over the network. Therefore, it is considered unsecure.
Point-to-point Protocol over Ethernet (PPPoE)	PPPoE is a network protocol for encapsulating PPP frames in Ethernet frames. With PPPoE, the remote access device can control and account each access user.
Private VLAN (PVLAN)	PVLAN adopts Layer 2 isolation technology. Only the upper VLAN is visible globally. The lower VLANs are isolated from each other. If you partition each interface of the switch or IP DSLAM device into a lower VLAN, all interfaces are isolated from each other.

Q

QinQ	802.1Q in 802.1Q (QinQ), also called Stacked VLAN or Double VLAN, is extended from 802.1Q and defined by IEEE 802.1ad recommendation. This VLAN feature allows the equipment to add a VLAN tag to a tagged packet. The implementation of QinQ is to add a public VLAN tag to a packet with a private VLAN tag, making the packet encapsulated with two layers of VLAN tags. The packet is forwarded over the ISP's backbone network based on the public VLAN tag and the private VLAN tag is transmitted as the data part of the packet. In this way, the QinQ feature enables the transmission of the private VLANs to the peer end transparently. There are two QinQ types: basic QinQ and selective QinQ.

Quality of Service (QoS)	A network security mechanism, used to solve problems of network delay and congestion. When the network is overloaded or congested, QoS can ensure that packets of important services are not delayed or discarded and the network runs high efficiently. Depending on the specific system and service, it may relate to jitter, delay, packet loss ratio, bit error ratio, and signal-to-noise ratio.

R

Rapid Spanning Tree Protocol (RSTP)	Evolution of the Spanning Tree Protocol (STP), which provides improvements in the speed of convergence for bridged networks
Remote Authentication Dial In User Service (RADIUS)	RADIUS refers to a protocol used to authenticate and account users in the network. RADIUS works in client/server mode. The RADIUS server is responsible for receiving users' connection requests, authenticating users, and replying configurations required by all clients to provide services for users.

S

Simple Network Management Protocol (SNMP)	A network management protocol defined by Internet Engineering Task Force (IETF) used to manage devices in the Internet. SNMP can make the network management system to remotely manage all network devices that support SNMP, including monitoring network status, modifying network device configurations, and receiving network event alarms. At present, SNMP is the most widely-used network management protocol in the TCP/IP network.
Simple Network Time Protocol (SNTP)	SNTP is mainly used for synchronizing time of devices in the network.
Single-Mode Fiber (SMF)	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.

9.2 Acronyms and abbreviations

A

AAA	Authentication, Authorization, and Accounting
ABR	Area Border Router
ACL	Access Control List
ANSI	American National Standards Institute
APS	Automatic Protection Switching
ARP	Address Resolution Protocol
AS	Autonomous System
ASE	Autonomous System External
AWG	American Wire Gauge

B

BC	Boundary Clock
BDR	Backup Designated Router
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
DHCP	Dynamic Host Configuration Protocol
DiffServ	Differentiated Service
DNS	Domain Name System
DRR	Deficit Round Robin
DoS	Deny of Service
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

F

FCS	Frame Check Sequence
FIFO	First Input First Output

G

GARP	Generic Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
GVRP	Generic VLAN Registration Protocol

H

HDLC	High-level Data Link Control

I

IS-IS	Intermediate System to Intermediate System Routing Protocol
ISP	Internet Service Provider

L

LACP	Link Aggregation Control Protocol
LACPDU	Link Aggregation Control Protocol Data Unit
LCAS	Link Capacity Adjustment Scheme
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit

M

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
MTTR	Mean Time to Repair
MTU	Maximum Transmission Unit
MVR	Multicast VLAN Registration

N

NBMA	Non-Broadcast Multi-Access
NMS	Network Management System
NNM	Network Node Management
NTP	Network Time Protocol

O

OAMPDU	OAM Protocol Data Units
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
PoE	Power over Ethernet
PPPoE	PPP over Ethernet
PTP	Precision Time Protocol

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
SFTP	Secure File Transfer Protocol
SLA	Service Level Agreement
SNTP	Simple Network Time Protocol
SP	Strict-Priority
SPF	Shortest Path First
SSH	Secure Shell
STP	Spanning Tree Protocol

T

TACACS+	Terminal Access Controller Access Control System
TC	Transparent Clock
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
USM	User-Based Security Model

V

VRRP	Virtual Router Redundancy Protocol

W

WRED	Weighted Random Early Detection
WRR	Weight Round Robin

瑞斯康达科技发展股份有限公司
RAISECOM TECHNOLOGY CO.,LTD.

Address: Raisecom Building, No. 11, East Area, No. 10 Block, East Xibeiwang Road, Haidian District, Beijing, P.R.China Postal code: 100094 Tel: +86-10-82883305
Fax: 8610-82883056 http://www.raisecom.com Email: export@raisecom.com