PoE Gigabit Managed Switch

User Guide

Document version:V1.0

Contents

1 Product Overview

1.1 Product Introduction

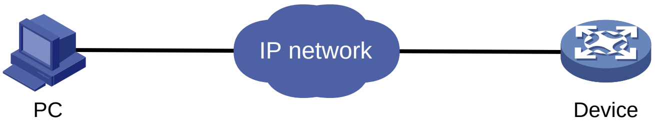
The PoE Gigabit Managed Switch can be configured through the command line interface (CLI), web interface, and SNMP/MIB. These configuration methods are suitable for different application scenarios.

- The web interface supports all PoE Gigabit Managed Switch configurations.
- The CLI provides some configuration commands to facilitate your operation. To perform other configurations not supported by the web interface, use the CLI.

1.1.1 Web-based network management operating environment

The PoE Gigabit Managed Switch provide web-based management function to facilitate the operations and maintenance on devices, through this function, the administrator can visually manage and maintain switch as below.

Figure 1.1-1 Web-based management operating environment



1.1.2 Login the web management interface

The device is provided with the default Web login information. You can use the default information to log in to the web interface.

Table 1.1-2 The default web login interface information.

Items	Default information
Username	admin
Password	admin
IP address of the device (VLAN-interface 1)	Default IP address :192.168.1.110

1.1.3 Logout the web management interface

Click “**Logout”** in the upper-right corner of the Web page to quit the web interface.

CAUTION:

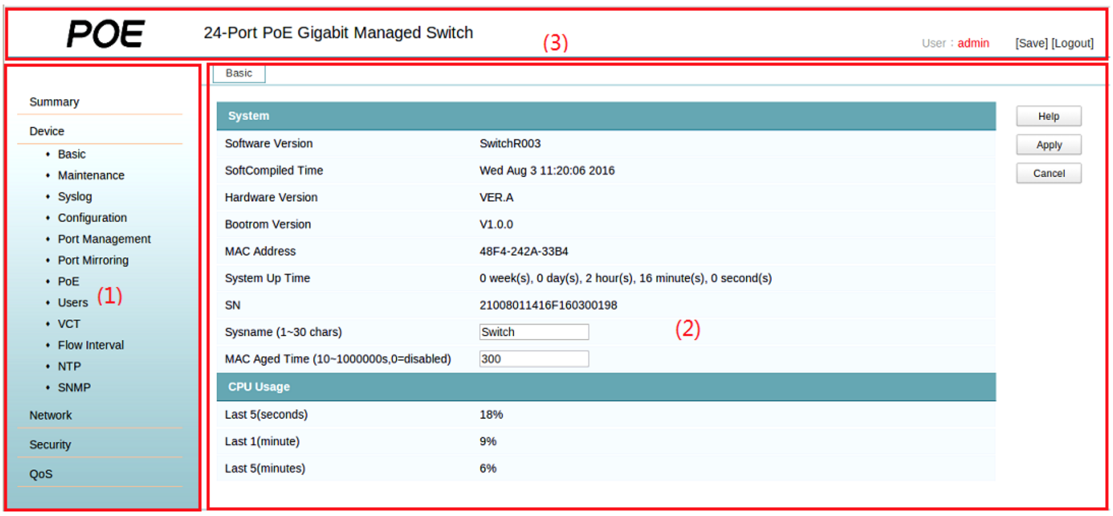
- It's not recommend to logout directly by closing the browser as the system won’t save automatically. It’s better to save the current configuration before logout.
- For security purposes, please log out of the Web interface after you finish your operations.

2 System overview

2.1 Introduction to the web interface

The Web interface is composed of three parts: navigation bar, title area, and body area, as shown in Figure 2.1-1.

Figure 2.1-1 Web-based configuration



System

Software Version	SwitchR003
SoftCompiled Time	Wed Aug 3 11:20:06 2016
Hardware Version	VER.A
Bootrom Version	V1.0.0
MAC Address	48F4-242A-33B4
System Up Time	0 week(s), 0 day(s), 2 hour(s), 16 minute(s), 0 second(s)
SN	21008011416F160300198
Sysname (1~30 chars)	Switch
MAC Aged Time (10~1000000s,0=disabled)	300

CPU Usage

Last 5(seconds)	18%
Last 1(minute)	9%
Last 5(minutes)	6%

(1) Navigation bar	(2)Body area	(3) Title area

- Navigation bar—organizes the web-based NM functions as a navigation tree, where you can select and configure functions as needed. The result is displayed in the body area.
- Body area— allows you to configure and display features.
- Title area— display basic system information, Logout /Save option etc.

2.2 Web-based NM functions

Web user levels, from low to high, are monitor and administrator. A user with a higher level has all the operating rights of a user with a lower level.

- Monitor—Users of this level can only access the device data but cannot configure the device.
- Administrator—Users of this level can perform any operations to the device.

Table 2.2-1 Description of Web-based NM functions

Function menu		Description	User level
Summary	System Information	Display the basic system information: system resource status, and operation logs.	Monitor

Function menu			Description	User level
Device	Basic	System Name	Display and allow you to configure the system name	Administrator
	Maintenance	Software Upgrade	Upgrade the system software.	Administrator
		Reboot	Reboot the switch.	Administrator
		Diagnostic Information	Generates diagnostic information file, and allows you to view or save the file to local host.	Administrator
	Syslog	Loglist	Display and refresh system logs.	Monitor
			Clear system logs.	Administrator
		Log host	Display and configure the log host.	Administrator
	Configuration	Backup	Download the configuration file from the device to host.	Administrator
		Restore	Upload the configuration to be used at the next startup from the device to the host of the current user.	Administrator
		Save	Save the current configuration to the configuration file to be used at the next startup.	Administrator
		Initialize	Restore the factory default settings.	Administrator
	Port Management	Summary	Display port information by features.	Monitor
		Detail	Display feature information by ports.	Monitor
		Setup	Create, modify, delete, and enable/disable a port, and clear port statistics.	Administrator
	Port Mirroring	Summary	Display the configuration information of a port mirroring group.	Monitor
		Create	Create a port mirroring group.	Administrator
		Remove	Remove a port mirroring group.	Administrator
		Modify Port	Configure ports for a mirroring group.	Administrator
	PoE	Summary	Display PSE information and PoE interface information.	Monitor
		Setup	Configure a PoE interface.	Administrator
	Users	Web Idle Timeout	Display and allows you to configure the idle timeout period for logged-in users.	Administrator

Function menu			Description	User level
		Summary	Display the brief information of FTP and Telnet users.	Monitor
		Super Password	Configure a password for a lower-level user to switch from current access level to the management level.	Administrator
		Create	Create an FTP or Telnet user.	Administrator
		Modify	Modify FTP or Telnet user information.	Administrator
		Remove	Remove an FTP or a Telnet user.	Administrator
	VCT	VCT	Check the status of the cables connected to Ethernet ports.	Administrator
	Flow Interval	Port Traffic Statistics	Display the average rate at which the interface receives and sends packets within a specified time interval.	Monitor
		Interval Configuration	Set an interval for collecting traffic statistics on interfaces.	Administrator
	NTP	System Time	Display and configure the system date and time.	Administrator
	SNMP	Setup	Display and refreshes SNMP configuration and statistics information.	Monitor
			Configure SNMP.	Administrator
		Community	Display SNMP community information.	Monitor
			Create, modify and delete an SNMP community.	Administrator
		Group	Display SNMP group information.	Monitor
			Create, modify and delete an SNMP group.	Administrator
		User	Display SNMP user information.	Monitor
			Create, modify and delete an SNMP user.	Administrator
		Trap	Display the status of the SNMP trap function and information about target hosts.	Monitor
			Enable or disable the SNMP trap function, or create, modify and delete a target host.	Administrator
		View	Display SNMP view information.	Monitor
			Create, modify and delete an SNMP view.	Administrator
Network	VLAN	Select VLAN	Select a VLAN range.	Monitor

Function menu			Description	User level
		Create	Create VLANs.	Administrator
		Port Detail	Display the VLAN-related details of a port.	Monitor
		Detail	Display the member port information of a VLAN.	Monitor
		Modify VLAN	Modify the description and member ports of a VLAN.	Administrator
		Modify Port	Change the VLAN to which a port belongs.	Administrator
		Remove	Remove VLANs.	Administrator
	VLAN Interface	Summary	Display information about VLAN interfaces by address type.	Monitor
		Create	Create VLAN interfaces and configure IP addresses for them.	Administrator
		Modify	Modify the IP addresses and status of VLAN interfaces.	Administrator
		Remove	Remove VLAN interfaces.	Administrator
	DHCP snooping	DHCP Snooping	Display the status, trusted and untrusted ports and DHCP client information of DHCP snooping.	Monitor
		DHCP Snooping Port	Enable/disable DHCP snooping, and configure DHCP snooping trusted and untrusted ports.	Administrator
	MAC Filter	MAC	Display MAC address information.	Monitor
			Create and remove MAC addresses.	Administrator
		Setup	Display and allows you to configure MAC address aging time.	Administrator
	Link Aggregation	Summary	Display information about link aggregation groups.	Monitor
		Create	Create link aggregation groups.	Administrator
		Modify	Modify link aggregation groups.	Administrator
		Remove	Remove link aggregation groups.	Administrator
	LLDP	Port Setup	Display the LLDP configuration information, local information, neighbor information, statistics information, and status information of a port.	Monitor
			Modify LLDP configuration on a port.	Administrator
		Global Setup	Display global LLDP configuration information.	Monitor

Function menu			Description	User level
			Configure global LLDP parameters.	Administrator
		Global Summary	Display global LLDP local information and statistics.	Monitor
		Neighbor Summary	Display global LLDP neighbor information.	Monitor
	IGMP Snooping	Basic	Display global IGMP snooping configuration information or the IGMP snooping configuration information in a VLAN, and allows you to view the IGMP snooping multicast entry information.	Monitor
			Configure IGMP snooping globally or in a VLAN.	Administrator
		Advanced	Display the IGMP snooping configuration information on a port.	Monitor
			Configure IGMP snooping on a port.	Administrator
	IPv4 Routing	Summary	Display the IPv4 active route table.	Monitor
		Create	Create an IPv4 static route.	Administrator
		Remove	Delete the selected IPv4 static routes.	Administrator
	Telnet	Service	Display the states of services: enabled or disabled.	Administrator
			Enable/disable services, and set related parameters.	Administrator
Security	IP Filter	White List	Configure authorized IP.	Monitor
		Port Filter	Display the configurations of authorized IP, the associated IPv4 ACL list	Administrator
	ARP Defense	Global Setup	Display ARP table information.	Monitor
		Port Setup	Display ARP table information.	Administrator
		User Rules	Add, modify, and remove ARP entries.	Administrator
	Loopback Detection	Loopback Detection	Display and configure system loopback detection parameters and port loopback detection parameters.	Administrator
QoS	Ports Rate Limit	Summary	Display time range configuration information.	Monitor
		Setup	Configure the line rate.	Administrator
	QoS	Priority Mapping	Display priority mapping table information.	Monitor
			Modify the priority mapping entries.	Administrator

2.3 Configuration guidelines

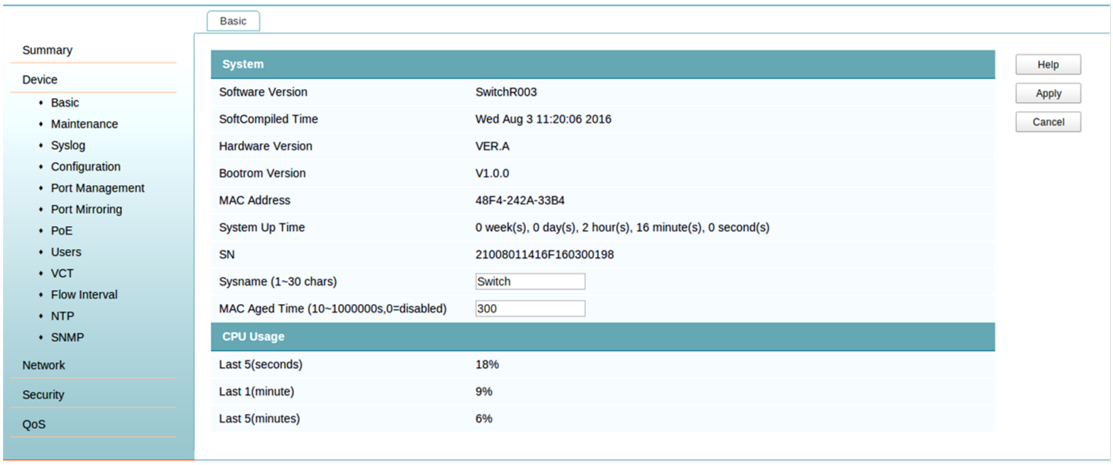
- The web console mainly supports Google Chrome and Mozilla Firefox Explorer.
- The web console does not support the Back, Next, Refresh buttons provided by the browser. Using these buttons may result in abnormal display of web pages.
- When the device is performing the spanning tree calculation, you cannot log in or operate the web interface.
- The Windows firewall limits the number of TCP connections, so when you use IE to log in to the web, maybe you can’t open the web. Turn off the Windows firewall before login to avoid this problem.
- If the software version of the device changes, please delete the temporary Internet files of IE when you log in through web interface, otherwise, the web page may not be displayed correctly.

3 Device management

3.1 Basic information

After you login the web, the following System Information would appear by default, as shown in Figure 3.1-1. It has 2 parts including “Basic system information” and “CPU Usage”.

Figure 3.1-1 System information



System

Software Version SwitchR003
SoftCompiled Time Wed Aug 3 11:20:06 2016
Hardware Version VER.A
Bootrom Version V1.0.0
MAC Address 48F4-242A-33B4
System Up Time 0 week(s), 0 day(s), 2 hour(s), 16 minute(s), 0 second(s)
SN 21008011416F160300198
Sysname (1~30 chars) Switch
MAC Aged Time (10~1000000s,0=disabled) 300

CPU Usage

Last 5(seconds) 18%
Last 1(minute) 9%
Last 5(minutes) 6%

Table 3.1-1 Display and configure partial system parameters

Item	Description
Software Version	Current version number
Soft Compiled time	The time when the switch system was compiled.
Hardware Version	Current version number
Boot Rom version	Current version number
MAC address	MAC address of the interface management.
System Up time	Running time from boot
SN	Serial number.
Sysname	System name of the switch.
MAC aged time	Dynamic MAC aged time.

3.2 Maintenance

3.2.1 Software upgrade

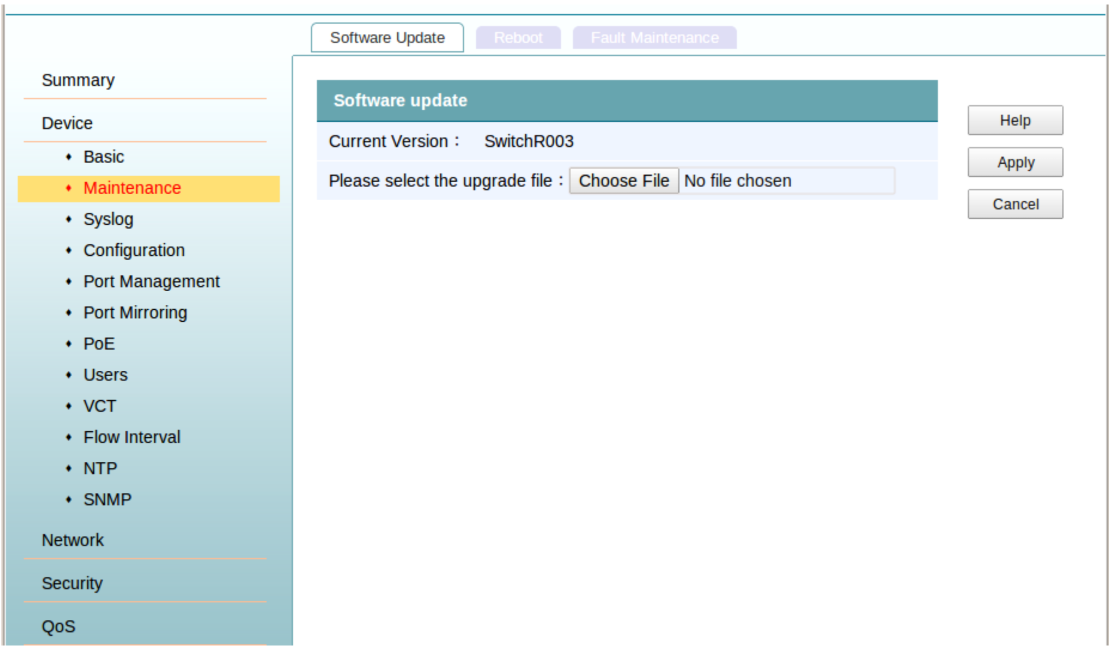
A system software image file is used to boot the device. Software upgrade allows you to obtain a target system software image file from the local host and set the file as the startup configuration file. In addition, user can upgrade system via WEB, and the system would reboot automatically after completing upgrading operation.

CAUTION:

Software upgrade takes some time. Avoid performing any operation on the web interface during the upgrading procedure. Otherwise, the upgrade operation may be interrupted.

Select Device-->Maintenance from the navigation tree to enter software upgrade configuration page, as shown in Figure 3.2-1.

Figure 3.2-1 Software upgrade



Current Version : SwitchR003

Please select the upgrade file : Choose File No file chosen

Table 3.2-1 Software upgrade configuration items

Item	Description
Choose File	Specifies the filename of the local system software image file, which must be with an extension .bin.

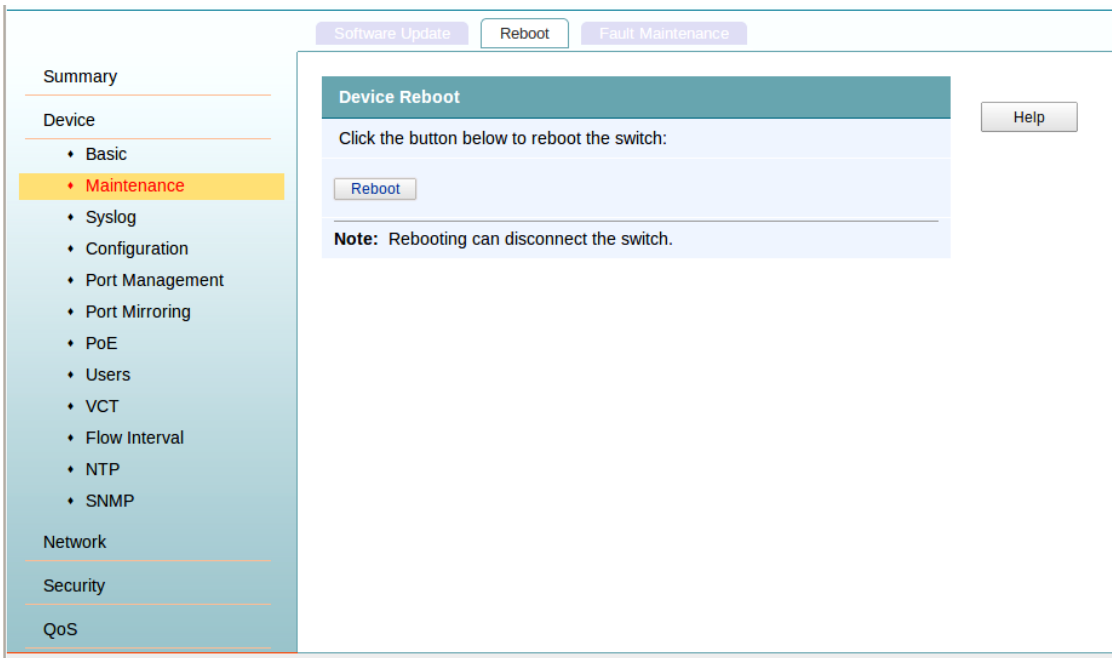
3.2.2 Device Reboot

CAUTION:

- Before rebooting the device, save the configuration; otherwise, all unsaved configuration will be lost after device reboot.
- When the device reboots, you need to re-log in to the web interface.

Select Device-->Maintenance, click "Reboot" to enter into corresponding page, as shown in Figure 3.2-2

Figure 3.2-2 Device reboot



Device Reboot

Click the button below to reboot the switch:

Note: Rebooting can disconnect the switch.

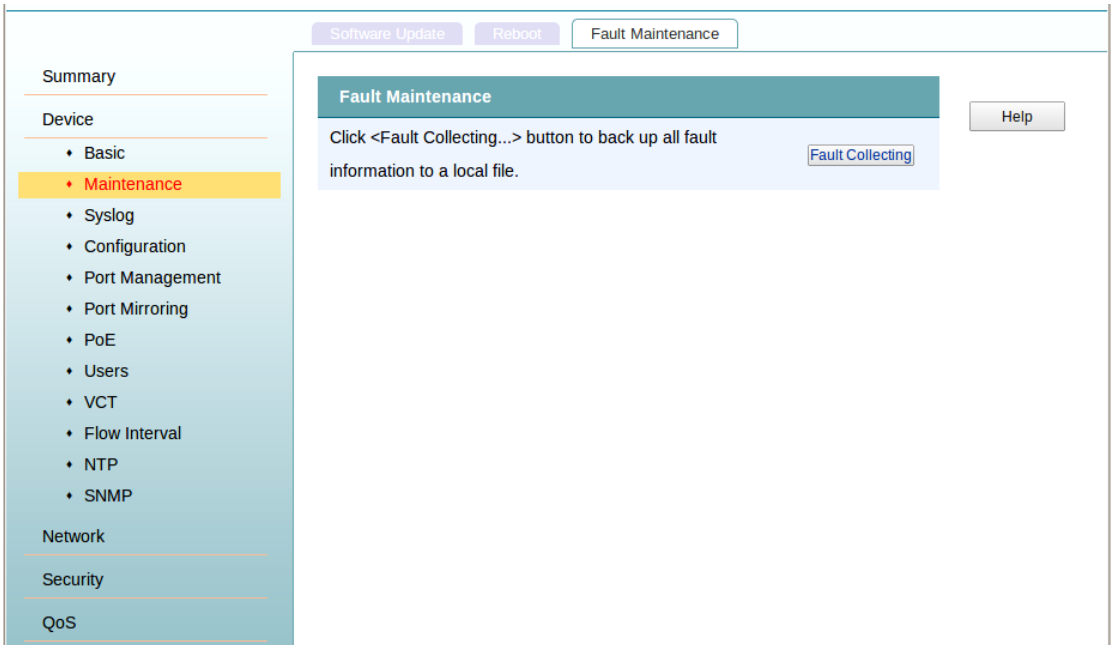
Click "Reboot" to reboot the device.

3.2.3 Fault Maintenance

Each functional module has its own running information, and generally, you view the output information for each module one by one. In order to get as much information as possible in one time during daily maintenance or when system failure occurs, the diagnostic information module allows to save the running statistics of multiple functional modules to a file named default.txt, and then user can locate problems faster by checking this file.

Select Device-->Fault Maintenance, and click "Fault Collecting" to enter the page as shown in Figure 3.2-3.

Figure 3.2-3 Falut Maintenance



Click <Fault Collecting...> button to back up all fault information to a local file.

When click “Fault Collecting”, the system begins to generate a diagnostic information file, and after the file is generated, the “File Download” dialog box appears. User can open or save this file.

NOTE:

The generation of the diagnostic file takes some time. During this process, do not perform any operation on the web page.

3.3 Syslog

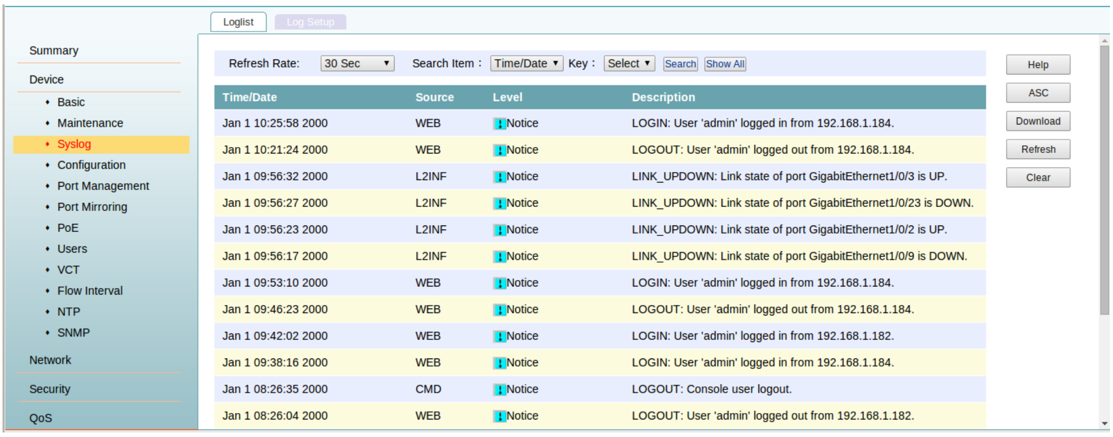
System logs contain a large amount of network and device information, including running status and configuration changes. System logs are very important for administrators to know network and device status. With system log information, administrators can take corresponding actions against network problems and security problems.

System logs can be stored in the log buffer, or sent to the log server.

3.3.1 Displaying Loglist

Select Device-->Syslog to enter into corresponding page shown in Figure 3.3-1.

Figure 3.3-1 Display syslog



Refresh Rate: 30 Sec ▾ Search Item : Time/Date ▾ Key : Select ▾

Time/Date	Source	Level	Description
Jan 1 10:25:58 2000	WEB	Notice	LOGIN: User 'admin' logged in from 192.168.1.184.
Jan 1 10:21:24 2000	WEB	Notice	LOGOUT: User 'admin' logged out from 192.168.1.184.
Jan 1 09:56:32 2000	L2INF	Notice	LINK_UPDOWN: Link state of port GigabitEthernet1/0/3 is UP.
Jan 1 09:56:27 2000	L2INF	Notice	LINK_UPDOWN: Link state of port GigabitEthernet1/0/23 is DOWN.
Jan 1 09:56:23 2000	L2INF	Notice	LINK_UPDOWN: Link state of port GigabitEthernet1/0/2 is UP.
Jan 1 09:56:17 2000	L2INF	Notice	LINK_UPDOWN: Link state of port GigabitEthernet1/0/9 is DOWN.
Jan 1 09:53:10 2000	WEB	Notice	LOGIN: User 'admin' logged in from 192.168.1.184.
Jan 1 09:46:23 2000	WEB	Notice	LOGOUT: User 'admin' logged out from 192.168.1.184.
Jan 1 09:42:02 2000	WEB	Notice	LOGIN: User 'admin' logged in from 192.168.1.182.
Jan 1 09:38:16 2000	WEB	Notice	LOGIN: User 'admin' logged in from 192.168.1.184.
Jan 1 08:26:35 2000	CMD	Notice	LOGOUT: Console user logout.
Jan 1 08:26:04 2000	WEB	Notice	LOGOUT: User 'admin' logged out from 192.168.1.182.

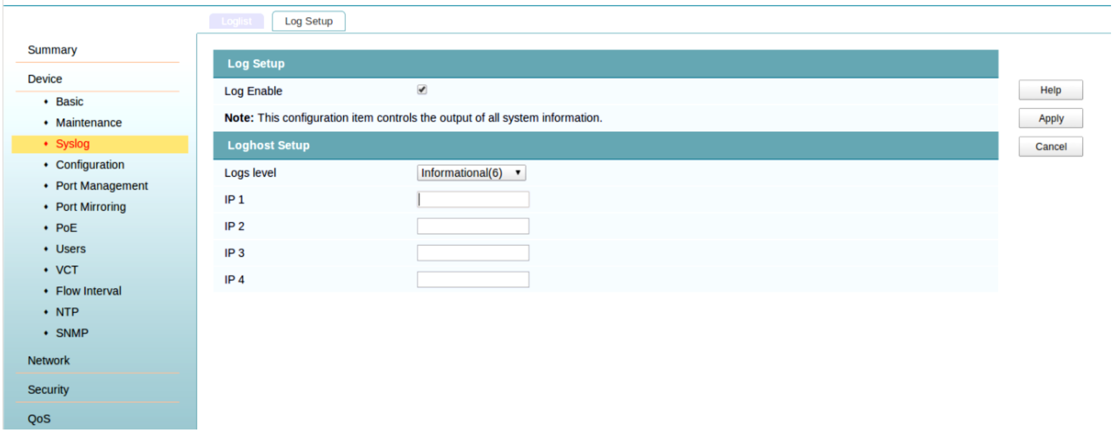
Table 3.3-1 Syslog display

Item	Description
Refresh Rate	Set refresh rate
Search Item	Select the needed query to check the log information
Key	Keywords query
Time/Date	Display the time/date when system logs are generated.
Source	Display the module that generates system logs.
Level	Display the severity level of system logs. For more information about severity levels, see Table 3.3-2.
Description	Display the contents of system logs.

3.3.2 Setting loghost

Select Device-->Syslog, and click “Log Setup” to enter corresponding page shown in Figure 3.3-2.

Figure 3.3-2 Loghost Setup



Log Setup

Log Enable ☑

Note: This configuration item controls the output of all system information.

Loghost Setup

Logs level Informational(6)

IP 1

IP 2

IP 3

IP 4

Table 3.3-2 Severity level

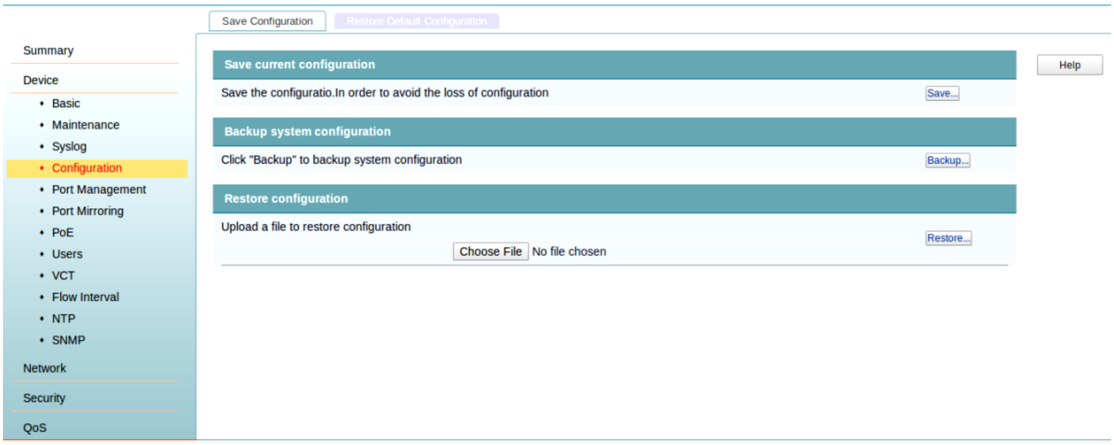
Severity level	Description	Value
Emergency	The system is unavailable.	0
Alert	Demands prompt reaction	1
Critical	Critical information	2
Error	Error information	3
Warning	Warnings	4
Notification	Normal information that needs to be noticed	5
Informational	Informational information to be recorded	6
Debugging	Information generated during debugging	7
Note: A smaller value represents a higher severity level.		

3.4 Configuration Management

3.4.1 Save configuration management

Select Device-->Configuration, as shown in Figure 3.4-1.

Figure 3.4-1 Save configuration



Save current configuration

Save the configuratio.In order to avoid the loss of configuration

Backup system configuration

Click "Backup" to backup system configuration

Restore configuration

Upload a file to restore configuration

No file chosen

Table 3.4-1 Configuration management

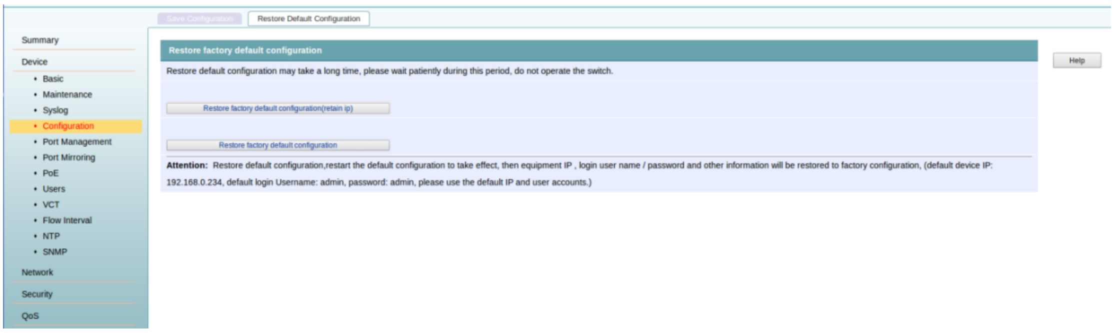
Item	Description
Save current configuration	Save the current configuration to .cfg file.
Backup system configuration	Back up the configuration file (.cfg file) Click “Backup”, a file download dialog box appears. Users can view the .cfg file or save the file locally.
Restore configuration	Upload the .cfg file. Click “Browse”, the file upload dialog box appears. Select the .cfg file to be uploaded, and then click “OK”.

3.4.2 Initialize

This operation resumes the system to factory defaults, deletes the current configuration file, and reboots the device.

Select Device-->Configuration, and then click “Restore factory configuration(retain ip)”to enter the initialize confirmation page or click “Restore factory default configuration” to restore the system to factory defaults as shown in Figure 3.4-2.

Figure 3.4-2 Initialize configuration



Restore factory default configuration

Restore default configuration may take a long time, please wait patiently during this period, do not operate the switch.

Attention: Restore default configuration,restart the default configuration to take effect, then equipment IP , login user name / password and other information will be restored to factory configuration, (default device IP: 192.168.0.234, default login Username: admin, password: admin, please use the default IP and user accounts.)

Table 3.4-2 Configuration management

Item	**Description**
Restore factory default configuration(retain IP)	Resume the default configuration, but retain the switch management IP address, and restart automatically to take effect. The password would be changed to default Settings, please use the default password when login.
Restore factory default configuration	Resume the default configuration and restart automatically to take effect. the password would be change to default Settings, please use the default password when login.

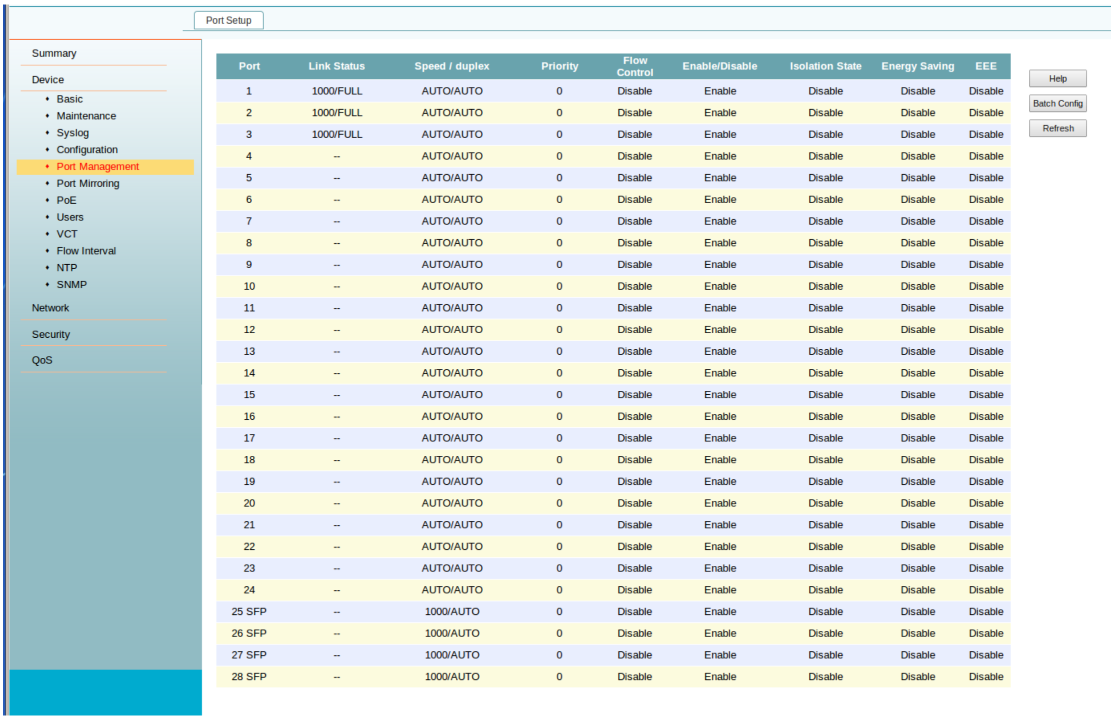
3.5 Port Management

You can use the port management feature to set and view the operation parameters of a Layer 2 Ethernet port, including but not limited to its state, speed, duplex mode, link status, port isolation state, port priority, flow control settings, energy setting, and EEE setting.

3.5.1 The summary

Select **Device** -->**Port Management** to enter the corresponding page by default as shown in Figure 3.5-1.

Figure 3.5-1 Port Management



Port	Link Status	Speed / duplex	Priority	Flow Control	Enable/Disable	Isolation State	Energy Saving	EEE
1	1000/FULL	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
2	1000/FULL	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
3	1000/FULL	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
4	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
5	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
6	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
7	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
8	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
9	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
10	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
11	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
12	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
13	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
14	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
15	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
16	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
17	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
18	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
19	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
20	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
21	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
22	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
23	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
24	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
25 SFP	--	1000/AUTO	0	Disable	Enable	Disable	Disable	Disable
26 SFP	--	1000/AUTO	0	Disable	Enable	Disable	Disable	Disable
27 SFP	--	1000/AUTO	0	Disable	Enable	Disable	Disable	Disable
28 SFP	--	1000/AUTO	0	Disable	Enable	Disable	Disable	Disable

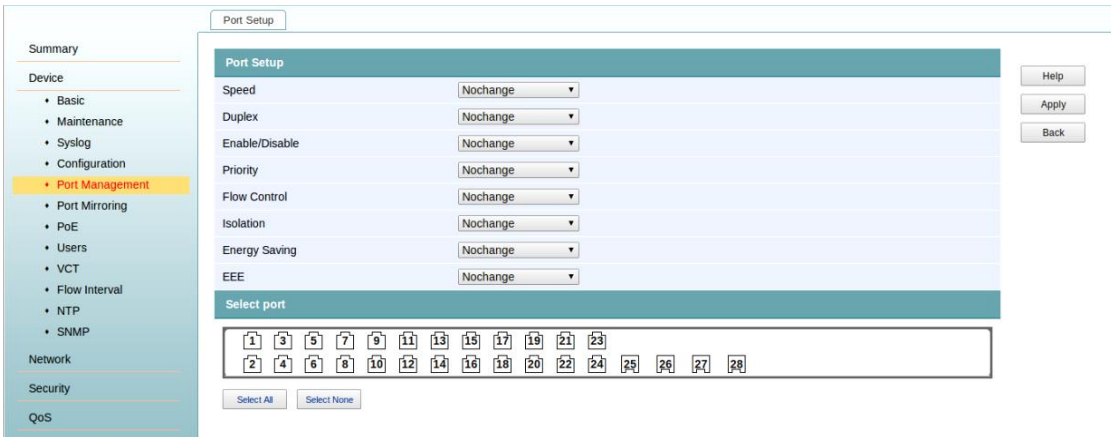
Table 3.5-1 Port state

Item	Description
Port	Corresponding to a port number.
Link Status	Show the port link speed and duplex mode
Speed/duplex	Show the port configuration of speed and duplex.
Priority	Port priority.
Flow control	Show the port flow control state: enable or disable
Enable/Disable	Enable or disable port forwarding.
Isolation State	Port Isolation is enabled or disabled. When enabled, the ports in the same isolation group can't forward packets.
Energy Saving	Port energy saving is enabled or disabled.
EEE	The function of EEE the port has been opened. Port can make EEE energy-saving function, if after a period of time (determined by the chip specifications) within the interface state is always up, and does not receive and send any message, interface automatically into energy saving mode; When the interface need receive or send article, interface automatic recovery mode to work, so as to achieve energy saving effect.

3.5.2 Configuring a port

Select Device -->Port Management, and then enter the corresponding page as shown in Figure 3.5-2, then select the needed port. It supports batch configuration to select the needed ports at the same time.

Figure 3.5-2 Configure operation parameters for a port



Port Setup

Speed: Nochange

Duplex: Nochange

Enable/Disable: Nochange

Priority: Nochange

Flow Control: Nochange

Isolation: Nochange

Energy Saving: Nochange

EEE: Nochange

Table 3.5-2 Port configuration items

Item	Description
Speed	Set the transmission rate of the port. Available options include: 10: 10 Mbps 100: 100 Mbps 1000: 1000 Mbps Auto: auto-negotiation Auto 10: auto-negotiated to 10 Mbps Auto 100: auto-negotiated to 100 Mbps Auto 1000: auto-negotiated to 1000 Mbps Auto 10 100: auto-negotiated to 10 or 100 Mbps Auto 10 1000: auto-negotiated to 10 or 1000 Mbps Auto 100 1000: auto-negotiated to 100 or 1000 Mbps Auto 10 100 1000: auto-negotiated to 10, 100, or 1000 Mbps ⓘIMPORTANT: SFP optical ports do not support the 10 or 100 option.

Item	Description
Duplex	Set the duplex mode of the port. Auto: auto-negotiation Full: full duplex Half: half duplex ⓘIMPORTANT: Ethernet electrical ports whose transmission rate is configured as 1000 Mbps and SFP optical ports do not support the half option.
Enable/Disable	Enable or disable the port. Sometimes, after you modify the operation parameters of a port, you need to disable and then enable the port to make the modifications take effect.
Priority	Priority of the port. 0 for the lowest, 7 for the highest
Flow Control	Enable or disable flow control on the port. With flow control enabled at both sides, when traffic congestion occurs on the ingress port, the ingress port will send a Pause frame notifying the egress port to temporarily suspend the sending of packets. The egress port is expected to stop sending any new packet when it receives the Pause frame. In this way, flow control helps to avoid dropping of packets. ⓘIMPORTANT: Flow control works only after it is enabled on both the ingress and egress ports.
Isolation	To implement Layer 2 isolation, you can add different ports to different VLANs. However, this will waste the limited VLAN resource. With port isolation, the ports can be isolated within the same VLAN. Thus, you need only to add the ports to the isolation group to implement Layer 2 isolation. This provides you with more secure and flexible networking schemes.
Energy Saving	Enable or disable auto power down on the port. With auto power down enabled, when an Ethernet port does not receive any packet for a certain period of time, it automatically enters the power save mode and resumes its normal state upon the arrival of a packet. By default, auto power down is disabled.
EEE	Enable or disable Energy Efficient Ethernet (EEE) on a link-up port. With EEE enabled, when a link-up Ethernet port does not receive any packet for a certain period, it automatically enters low power mode. When a packet arrives later, the device restores power supply to the port and the port resumes its normal state.

3.6 Port Mirroring

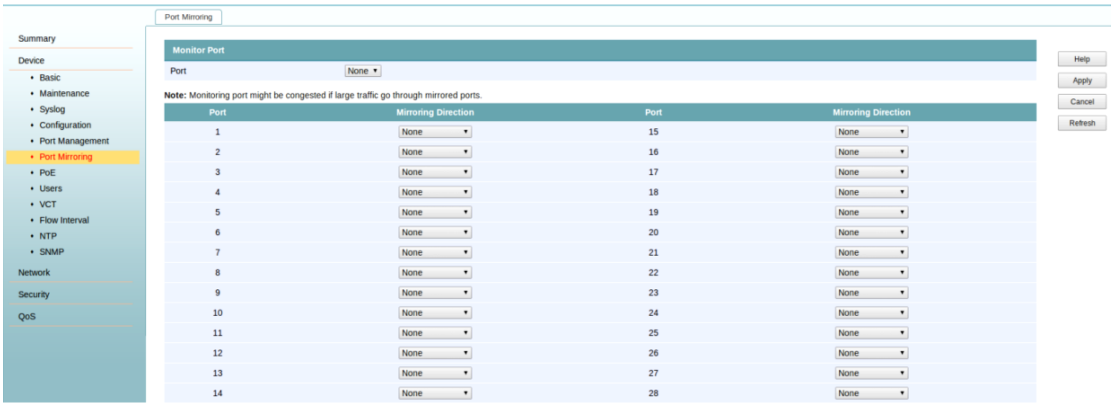
Port mirroring is the process of copying the packets passing through a port (called a mirroring port) to another port (called the monitor port) connected with a monitoring device for packet analysis.

You can mirror inbound, outbound, or bidirectional traffic on a port as needed.

3.6.1 Configuring ports for a mirroring group

Select Device-->Port Mirroring to enter the page as shown in Figure 3.6-1. To configure local port mirroring, you must specify the mirroring ports and monitor port.

Figure 3.6-1 Port Mirroring



Monitor Port

Port: None

Note: Monitoring port might be congested if large traffic go through mirrored ports.

Port	Mirroring Direction	Port	Mirroring Direction
1	None	15	None
2	None	16	None
3	None	17	None
4	None	18	None
5	None	19	None
6	None	20	None
7	None	21	None
8	None	22	None
9	None	23	None
10	None	24	None
11	None	25	None
12	None	26	None
13	None	27	None
14	None	28	None

Table 3.6-1 Configuration items of a mirroring group

Item	Description
Monitor port	• Select port mirroring monitor port. • None: do not use the port mirror function.
Port	Corresponding to a port number
Mirroring Direction	• Both: Mirrors both received and sent packets on mirroring ports. • Inbound: Mirrors only packets received by mirroring ports. • Outbound: Mirrors only packets sent by mirroring ports.

3.6.2 Configuration guidelines

Pay attention to the following points during local port mirroring configuration:

- Do not enable STP, MSTP, or RSTP on the monitor port.
- Can configure multiple mirroring ports but only one monitor port for a local mirroring group.

3.7 POE

Power over Ethernet (PoE) means that power sourcing equipment (PSE) supplies power to powered devices (PDs) through twisted pair cables and Ethernet interface.

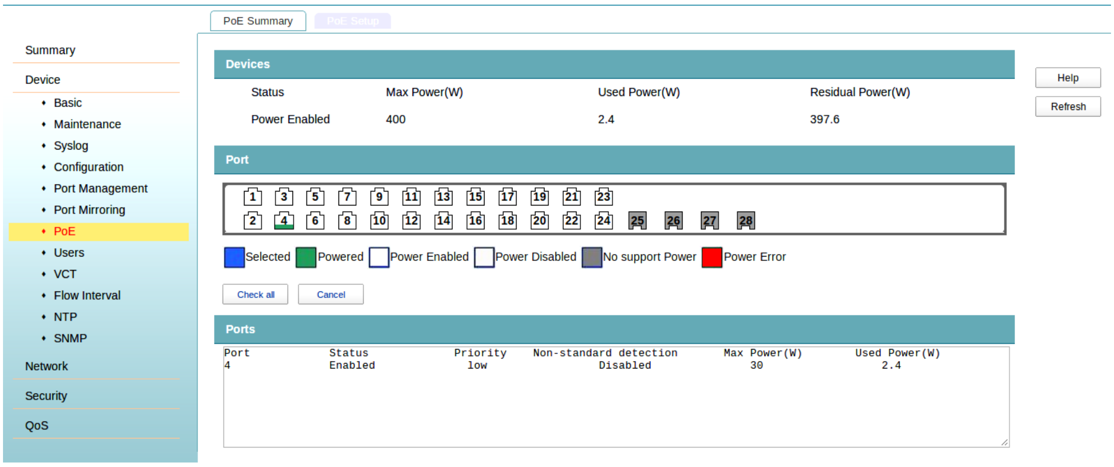
Advantages:

- Reliable—Power is supplied in a centralized way so that it is very convenient to provide a backup power supply.
- Easy to connect—A network terminal requires no external power supply but only an Ethernet cable.
- Standard—In compliance with IEEE 802.3af&IEEE 802.3at, and a globally uniform power interface is adopted.
- Promising—It can be applied to IP telephones, wireless LAN access points (APs), portable chargers, card readers, web cameras, and data collectors.

3.7.1 Configuring PoE

Select PoE-->PoE **Summary** to enter the page of the Summary as shown in Figure 3.7-1.

Figure 3.7-1 PoE Summary



Status	Max Power(W)	Used Power(W)	Residual Power(W)
Power Enabled	400	2.4	397.6

```
Port          Status          Priority   Non-standard detection      Max Power(W)       Used Power(W)
4             Enabled          low                 Disabled              30                 2.4
```

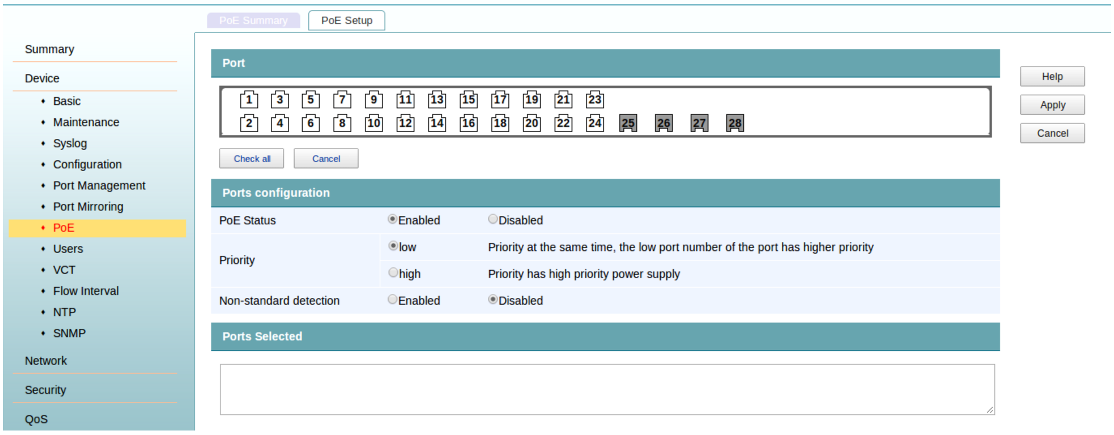
Table 3.7-1 PoE port configuration & display

Item		Description
Devices	Status	Default is enabled.
	Max power	Maximum allowable external power supply.
	Used Power	The used PoE power value.
	Residual Power	The rest of the PoE power.
port	Select a port	Select a certain port specified in the list of ports to check the selected PoE work status and configuration information.
ports	Port display	Display the selected port working state and configuration information.

3.7.2 Configuring PoE ports

Click “Port Setup” menu to set configuration for ports and click “Apply” after complete setting. As shown in Figure 3.7-2.

Figure 3.7-2 PoE Setup



PoE Status	● Enabled	○ Disabled
Priority	● low	Priority at the same time, the low port number of the port has higher priority
	○ high	Priority has high priority power supply
Non-standard detection	○ Enabled	● Disabled

Table 3.7-2 PoE port setting

Item	Description
Select a Port	Select a port to be configured and it will be displayed in the Selected Ports list box.
Power Status	Enable or disable PoE on the selected ports. By default, PoE is enabled on a PoE port. ❗IMPORTANT: PSE power overload—When the sum of the power consumption of all ports exceeds the maximum power of PSE, it means the PSE is overloaded.
Power Level	Set the power supply priority for a PoE port. The priority levels of a PoE port include low, high, and critical in ascending order. When the PoE power is insufficient, power is first supplied to PoE ports with a higher priority level. When the PSE power is overloaded, the PoE port with a lower priority is first disconnected to ensure the power supply to the PD with a higher priority. By default, the power priority of a PoE port is low.
Non-standard detection	Enable or disable non-standard PD detection
The selected port	According to the selected port.

3.8 Users management

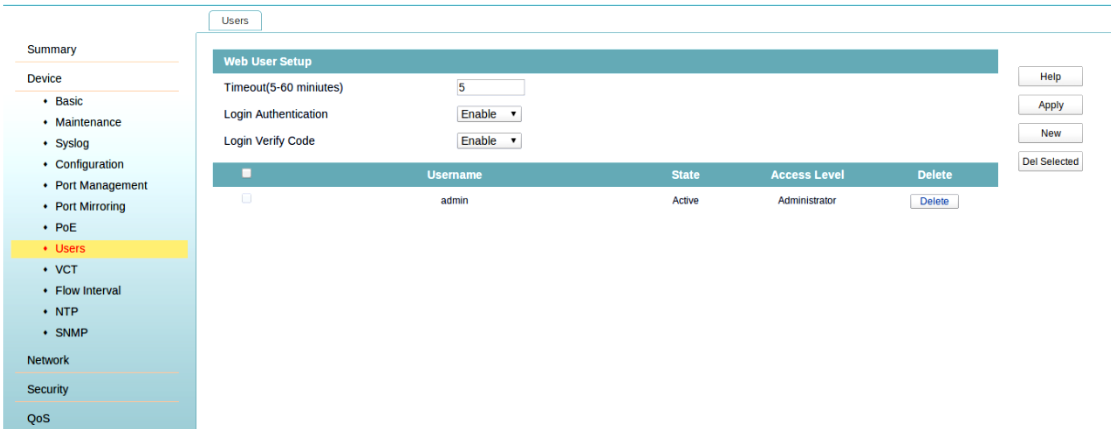
The switch provides the following user management functions:

- Add local user accounts for Telnet users, and specify the password, access level, and service types for each user.
- Set the super password for non-management level users to switch to the management level.
- Switch to the management level from a lower level.

3.8.1 Configuring user information

Select Device →Users from the navigation tree, and then click "Timeout" to enter the page for configuring idle timeout period, as shown in Figure 3.8-1.

Figure 3.8-1 Configure idle timeout period



Web User Setup

Timeout(5-60 miniutes) 5

Login Authentication Enable

Login Verify Code Enable

□	Username	State	Access Level	Delete
□	admin	Active	Administrator	Delete

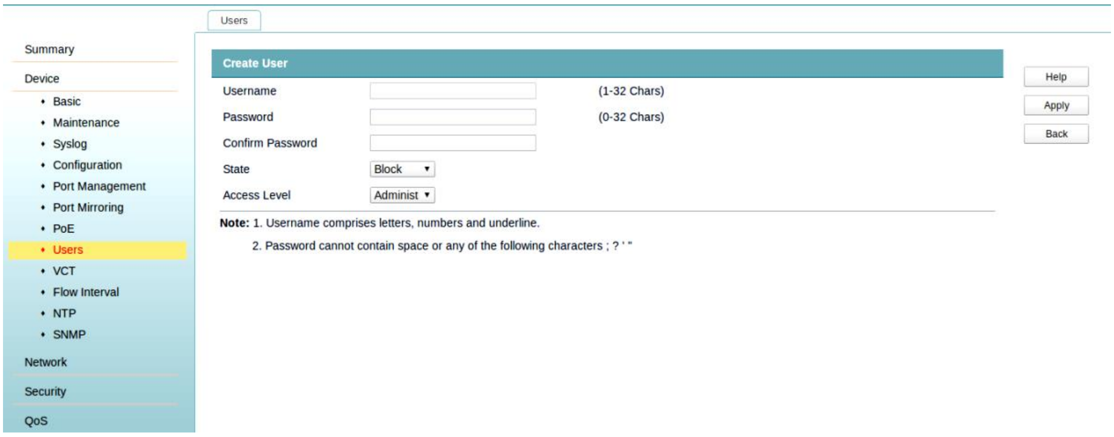
Table 3.8-1 Idle timeout period configuration item

Item	Description
Timeout	Configuring web user timeout.
Login authentication	Enable or disable login authentication.
Login Verify Code	Enable or disable login verify code.
New	Create a new local user.
Del Selected	Delete the selected local users.

3.8.2 Adding a local user

Select Device→Users from the navigation tree, and click "New" to add a local user, as shown in Figure 3.8-2.

Figure 3.8-2 Add a user



Username (1-32 Chars)

Password (0-32 Chars)

Confirm Password

State Block

Access Level Administ

Note: 1. Username comprises letters, numbers and underline.

2. Password cannot contain space or any of the following characters ; ? ' "

Table 3.8-2 Local user configuration items

Item	Description
Username	Set a username
Password	Set password
Confirm Password	Enter the same password again. Otherwise, the system will prompt that the two passwords are not consistent when you apply the configuration.
State	Active: Allow to login. Block: Ban to login.
Access Level	Select an access level. Monitor: Users of this level can view information Administrator: Users of this level can perform any operations on the switch.

3.9 VCT

NOTE:

The fiber interface of a SFP port does not support this feature.

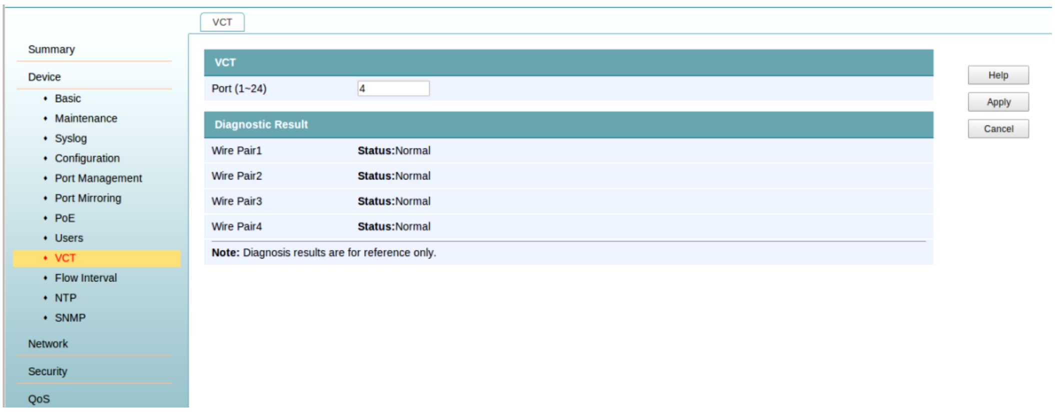
A link in the up state goes down and then up automatically if you perform this operation on one of the Ethernet interfaces forming the link.

You can use the Virtual Cable Test (VCT) function to check the status of the cable connected to an Ethernet port. The result would be returned within 5 seconds, which covers short circuit or open circuit occurring on the cable and where the malfunction is.

3.9.1 Testing cable status

Select Device-->VCT to enter the page of testing cable status. Select the port you want to test and then click Apply. The test result would be returned within 5 seconds and displayed in the **Diagnostic** Result text box, as shown in Figure 3.9-1.

Figure 3.9-1 Cable status



VCT

Port (1~24) 4

Diagnostic Result

Wire Pair1	**Status:**Normal
Wire Pair2	**Status:**Normal
Wire Pair3	**Status:**Normal
Wire Pair4	**Status:**Normal

Note: Diagnosis results are for reference only.

Table 3.9-1 Description of the test result

Item	**Description**
Cable status	Status and length of the cable. The cable status may be normal, abnormal, abnormal(open).

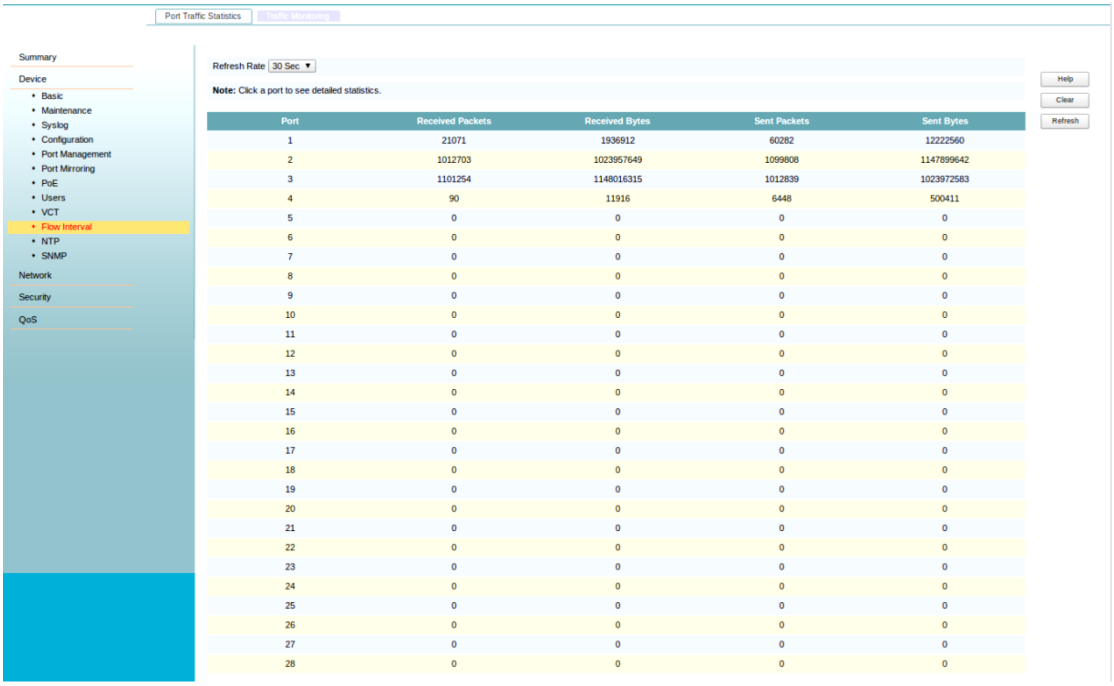
3.10 Flow interval

With the flow interval module, you can view the number of packets and bytes sent/received by a port over the specified interval.

3.10.1 Viewing port traffic statistics

Select Device-->Flow interval to enter Port Traffic Statistics as shown in Figure 3.10-1. That user can view the number of packets and bytes sent/received by each port over the last interval.

Figure 3.10-1 Ports traffic statistics



Refresh Rate 30 Sec

Note: Click a port to see detailed statistics.

Port	Received Packets	Received Bytes	Sent Packets	Sent Bytes
1	21071	1936912	60282	12222560
2	1012703	1023957649	1099808	1147899642
3	1101254	1148016315	1012839	1023972583
4	90	11916	6448	500411
5	0	0	0	0
6	0	0	0	0
7	0	0	0	0
8	0	0	0	0
9	0	0	0	0
10	0	0	0	0
11	0	0	0	0
12	0	0	0	0
13	0	0	0	0
14	0	0	0	0
15	0	0	0	0
16	0	0	0	0
17	0	0	0	0
18	0	0	0	0
19	0	0	0	0
20	0	0	0	0
21	0	0	0	0
22	0	0	0	0
23	0	0	0	0
24	0	0	0	0
25	0	0	0	0
26	0	0	0	0
27	0	0	0	0
28	0	0	0	0

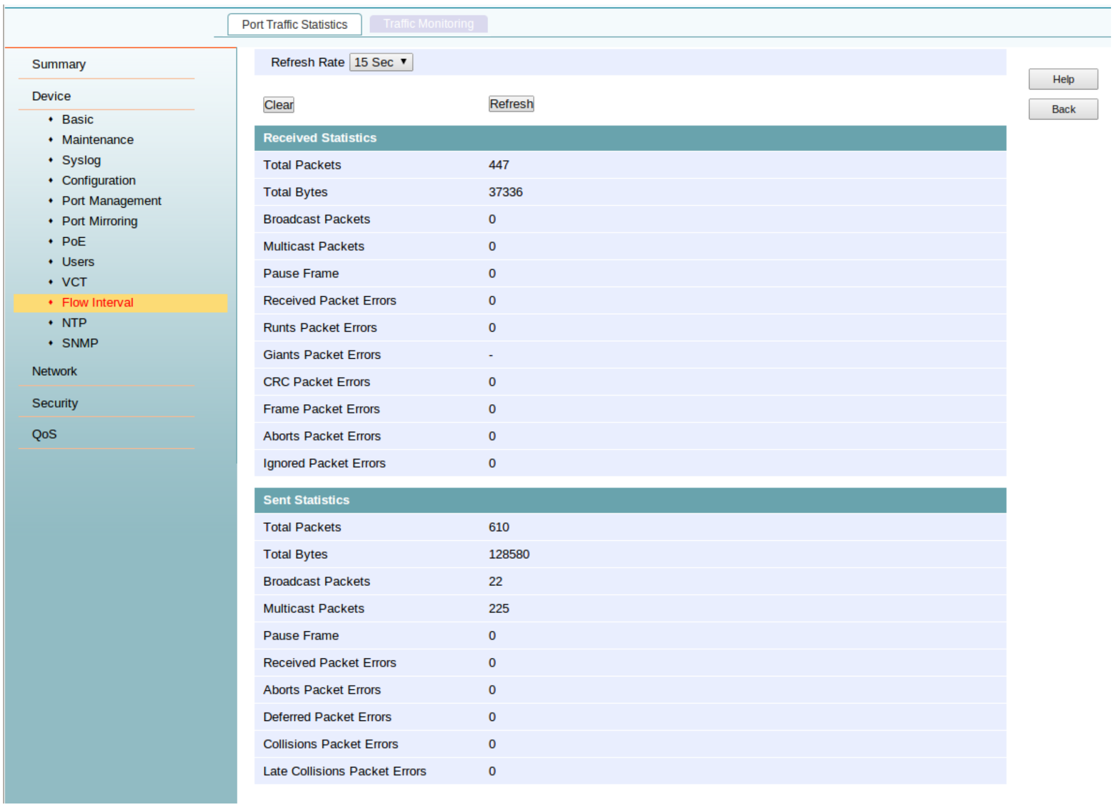
Table 3.10-1 Ports traffic statistics

Item	Remarks
Refresh Rate	Set the interval for generating port traffic statistics.
Port	Corresponding to port number, click to inquire the port statistical information in detail.
Received Packets	Statistics the total receiving number of packets.
Received Bytes	Statistics the total receiving number of bytes.
Sent Packets	Statistics the total sending number of packets.
Sent Bytes	Statistics the total sending number of bytes.
Clear	Empty all statistics.
Refresh	Refresh the statistical information of all ports.

3.10.2 Viewing the specified port traffic statistics

Click a port to see detailed statistics, as shown in Figure 3.10-2.

Figure 3.10-2 Port traffic statistics



Refresh Rate 15 Sec

Received Statistics	
Total Packets	447
Total Bytes	37336
Broadcast Packets	0
Multicast Packets	0
Pause Frame	0
Received Packet Errors	0
Runts Packet Errors	0
Giants Packet Errors	-
CRC Packet Errors	0
Frame Packet Errors	0
Aborts Packet Errors	0
Ignored Packet Errors	0

Sent Statistics	
Total Packets	610
Total Bytes	128580
Broadcast Packets	22
Multicast Packets	225
Pause Frame	0
Received Packet Errors	0
Aborts Packet Errors	0
Deferred Packet Errors	0
Collisions Packet Errors	0
Late Collisions Packet Errors	0

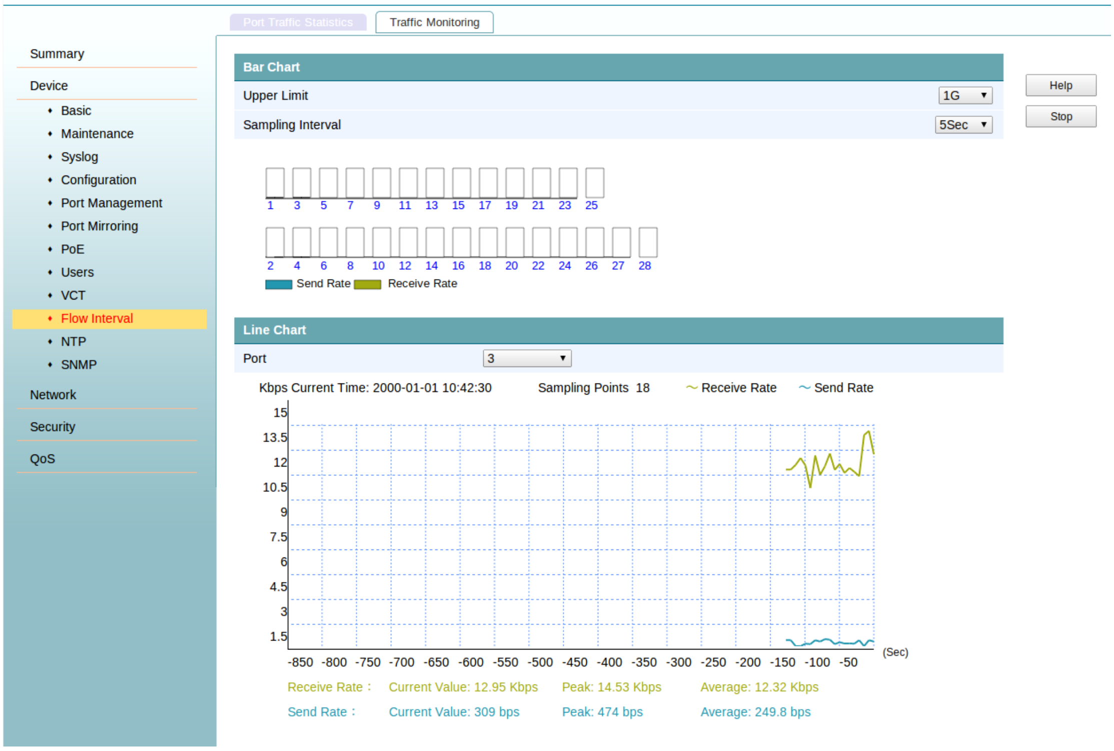
Table 3.10-2 Detailed statistics

Item	Remarks
Refresh Rate	Set the interval for generating port traffic statistics.
Clear	clear up the statistical information
Refresh	Refresh the port statistical information.
Receive statistics	Receive the detailed statistics information.
Send statistical	Send the detailed statistics information.

3.10.3 Port traffic monitoring

Select Device-->Flow interval, and click Traffic Monitoring tab to enter the page shown in Figure 3.10-3.

Figure 3.10-3 Traffic monitoring



Bar Chart

Upper Limit 1G

Sampling Interval 5Sec

▬ Send Rate ▬ Receive Rate

Line Chart

Port 3

Kbps Current Time: 2000-01-01 10:42:30 Sampling Points 18 ~ Receive Rate ~ Send Rate

Receive Rate : Current Value: 12.95 Kbps Peak: 14.53 Kbps Average: 12.32 Kbps

Send Rate : Current Value: 309 bps Peak: 474 bps Average: 249.8 bps

Table 3.10-3 Port traffic monitoring

Item	Remarks
Bar Chart	Show the port flow conditions.
Line Chart	Show the selected port flow conditions.
Upper Limit	Show the ratio of current flow and flow limit, can choose 1M to 10M, 100M or 1G.
Sampling Interval	Refresh the page according to sampling interval.
Port	Port and column subscript is one-to-one correspondence in the port
Sampling Points	Show all the number of sampling points.
Current Value	Show the current value of traffic.
Peak	Show the peak value of traffic
Average	Show the average value of traffic

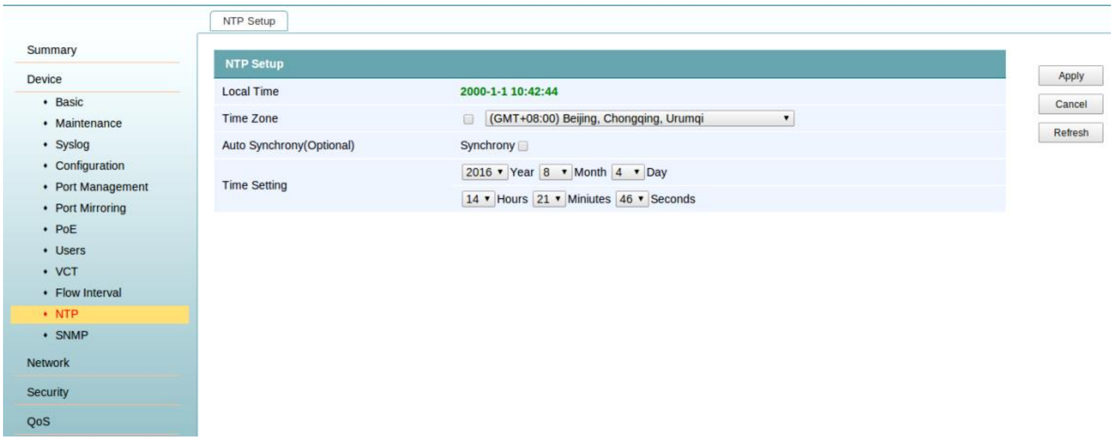
3.11 NTP

Network Time Protocol(NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

3.11.1 Configuring system time

Click “**Device**” menu and then select “**NTP**” option. The system time configuration page would be shown by default, as shown in Figure 3.111-1. The current system time and clock status are displayed.

Figure 3.111-1 NTP setup



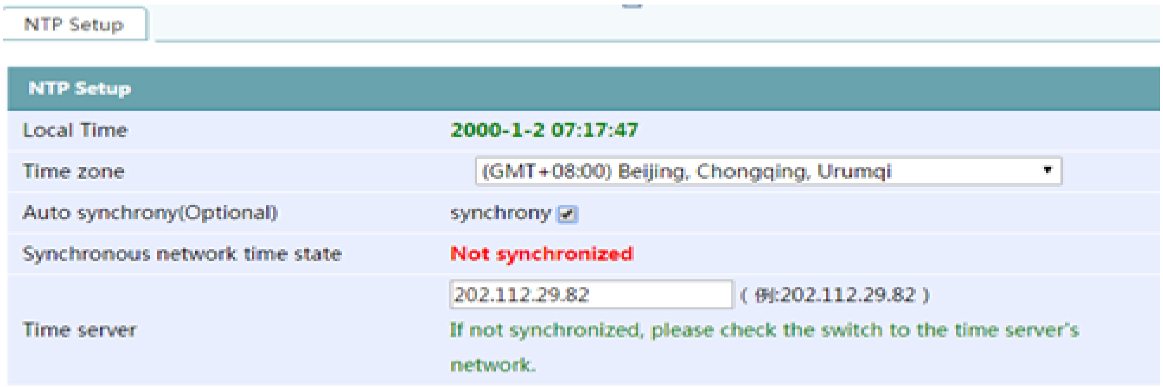
NTP Setup

Local Time	2000-1-1 10:42:44
Time Zone	□ (GMT+08:00) Beijing, Chongqing, Urumqi ▾
Auto Synchrony(Optional)	Synchrony □
Time Setting	2016 ▾ Year 8 ▾ Month 4 ▾ Day 14 ▾ Hours 21 ▾ Miniutes 46 ▾ Seconds

Table 3.11-1 NTP setup interface

Item	Remarks
Local Time	Show the system date and time.
Time Zone	Set the time zone for the system.
Auto Synchrony(Optical)	Click to enable time synchronized.
Time setting	Set the system date and time.

Figure 3.11-2 Auto synchrony setup



NTP Setup

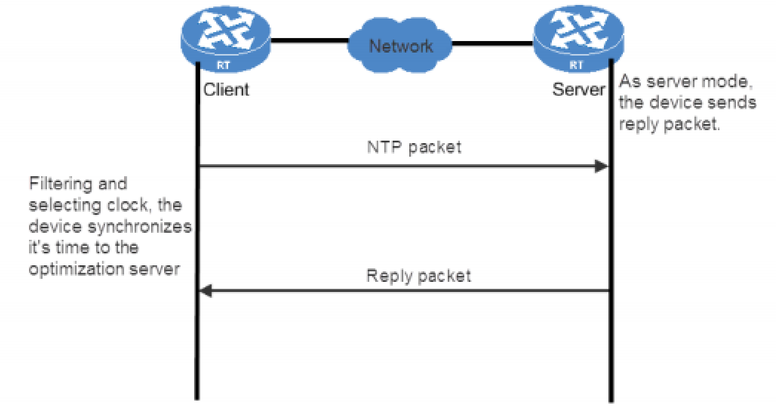
Local Time	2000-1-2 07:17:47
Time zone	(GMT+08:00) Beijing, Chongqing, Urumqi ▾
Auto synchrony(Optional)	synchrony ☑
Synchronous network time state	Not synchronized
Time server	202.112.29.82 (例:202.112.29.82) If not synchronized, please check the switch to the time server's network.

Table 3.11-2 Auto synchrony setup

Item	Remarks
Synchronous network time state	Display the synchronization status of the system clock.
Time server	Configures NTP server IP address.

The following is the network diagram for the NTP client and server mode as shown in Figure 3.111-3.

Figure 3.111-3 Network for NTP


RT
Client
Network
RT
Server
As server mode, the device sends reply packet.
NTP packet
Filtering and selecting clock, the device synchronizes it's time to the optimization server
Reply packet

3.11.2 Configuration guidelines

The clock status may be unsynchronized after your configuration because the process would take some time. You can refresh the page to view the clock status and system time later.

3.12 SNMP Configuration

Simple Network Management Protocol (SNMP) as standard internet protocol has been widely used as a management station to access and operate the devices on network, regardless of their vendors, physical characteristics and interconnect technologies.

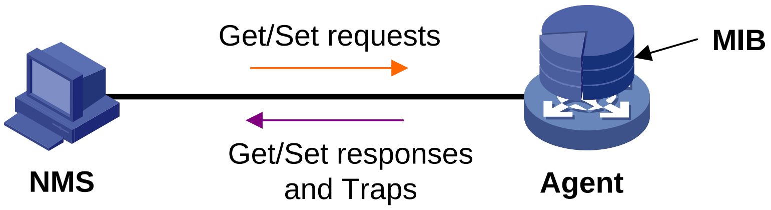
SNMP enables network administrators to read and set variables on managed devices to monitor their operating and health state, diagnose network problems, and collect statistics for management purposes.

3.12.1 SNMP mechanism

SNMP framework comprises the following items:

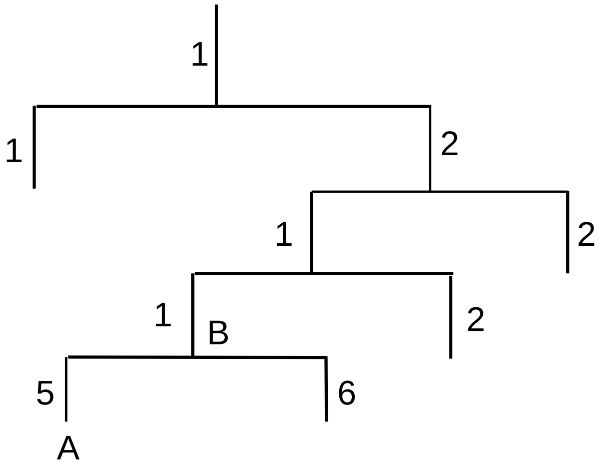
- SNMP manager—works on a network management workstation (NMS) to monitor and manage the SNMP-capable devices as shown in Figure 3.12-1.
- SNMP agent—works on managed device to receive and handle requests from NMS, and send traps to NMS when some events, such as interface state change, occur.
- Management Information Base (MIB)—Specifies the variables (such as interface status and CPU usage) maintained by the SNMP agent for the SNMP manager to read and set.

Figure 3.12-1 Relationship between NMS, agent and MIB



A MIB stores variables called "nodes" or "objects" in a tree hierarchy and identifies each node with a unique OID. An OID is a string of numbers that describes the path from the root node to a leaf node. For example, the object B in Figure 3.122-2 is uniquely identified by the OID {1.2.1.1}.

Figure 3.122-2 MIB tree



SNMP provides the following four basic operations:

- Get—NMS retrieves SNMP object nodes in an agent MIB.
- Set—NMS modifies the value of an object node in the agent MIB.
- Trap—SNMP agent sends traps to report events to the NMS.
- Inform—NMS sends alarms to other NMSs.

3.12.1.1 SNMP protocol version

SNMP agents support three SNMP protocol versions: SNMPv1, SNMPv2c, and SNMPv3.

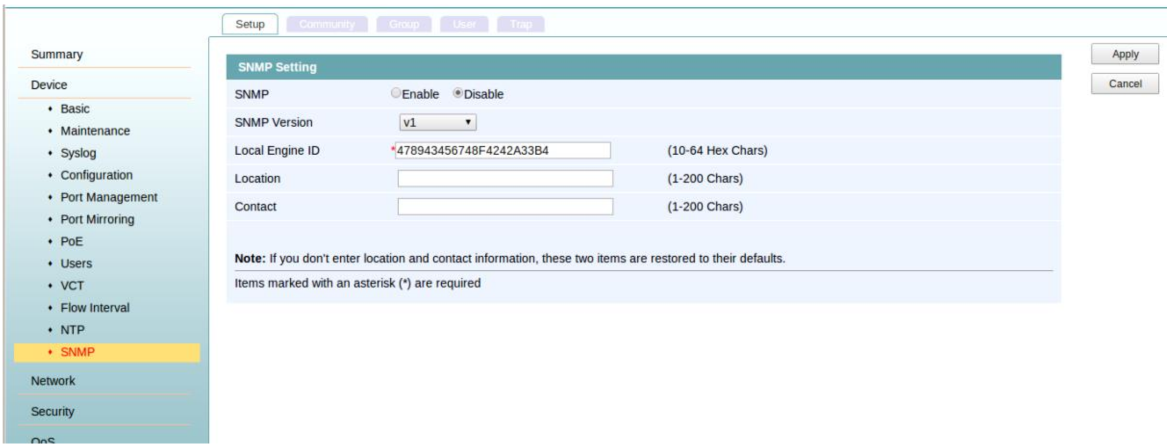
- SNMPv1 uses community names for authentication. A community name performs a similar role as a password to regulate access from NMS to agent. If the community name provided by NMS is different from the community name set on the agent, the SNMP connection cannot be established and the NMS fails to access to agent.
- SNMPv2c uses community names for authentication. SNMPv2c is compatible with SNMPv1, but it provides more operation modes, supports more data types, and provides various error codes for troubleshooting.
- SNMPv3 offers authentication based on the User-based Security Model (USM), which allows network administrators to set authentication and privacy functions. The authentication function is used to authenticate the validity of the sending end of the authentication packets, preventing access of unauthorized users. The privacy function is used to encrypt packets between the NMS and agents, preventing the packets from being intercepted. USM ensures more secure communication between NMSs and agents by providing authentication and privacy functions.

Successful interaction between an NMS and the agents requires consistency of SNMP versions configured on them.

3.12.2 SNMP Setup

Select Device-->SNMP to enter the SNMP configuration page, as shown in Figure 3.12-3. Select enable or disable SNMP and configure parameters such as SNMP version; Also can view SNMP statistics, which helps us understand the running status of SNMP after configuration.

Figure 3.122-3 SNMP Setup



SNMP Setting

SNMP	○Enable ●Disable	
SNMP Version	v1	
Local Engine ID	*478943456748F4242A33B4	(10-64 Hex Chars)
Location		(1-200 Chars)
Contact		(1-200 Chars)

Note: If you don't enter location and contact information, these two items are restored to their defaults.

Items marked with an asterisk (*) are required

Table 3.12-1 Configuration items

Item	Description
SNMP	Specify to enable or disable SNMP
SNMP Version	Set SNMP version

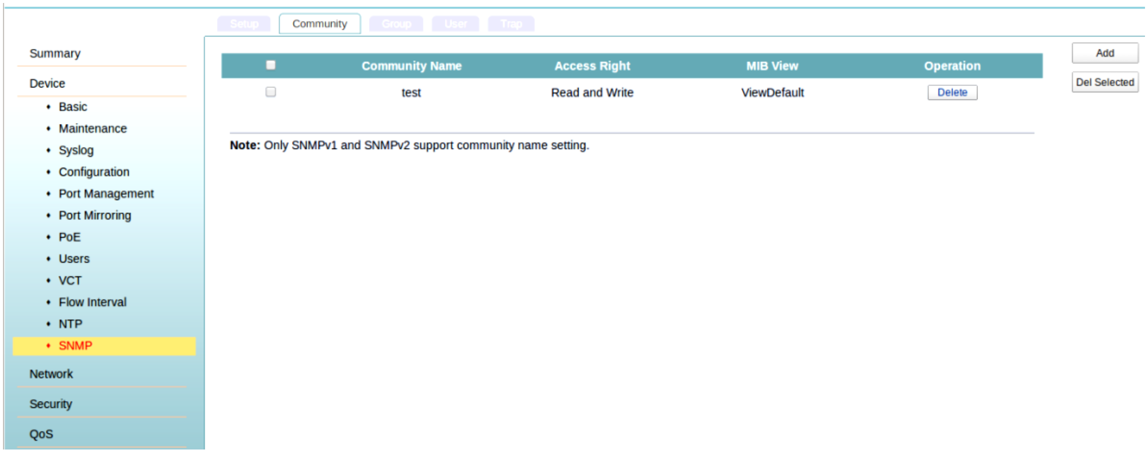
Item	Description
Local Engine ID	Configure the local engine ID. The validity of a user after it is created depends on the engine ID of the SNMP agent. If the engine ID is not identical to the current engine ID, the user is invalid.
Location	Describe the physical location of the device.
Contact	Describe the contact information.

3.12.3 Configuring an SNMP community

1. Select **Device-->SNMP**.
2. Click **Community** to enter the page as shown in Figure 3.122-4.
3. Click **Add** to enter the page as shown in Figure 3.12-5.

If need to modify "SNMP Community", click the related option as shown in Figure 3.12-6, if need to delete it, click "Delete".

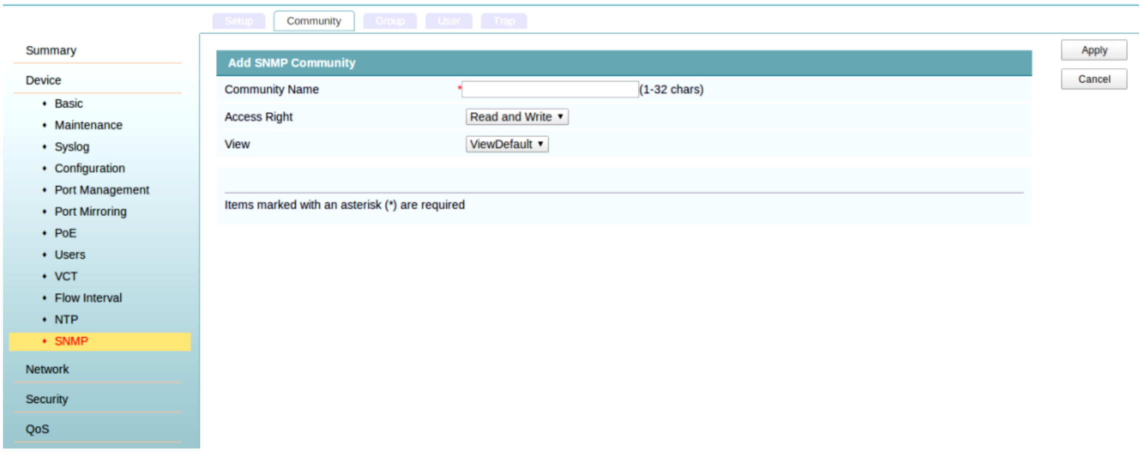
Figure 3.12-4 Configure an SNMP community



□	Community Name	Access Right	MIB View	Operation
□	test	Read and Write	ViewDefault	Delete

Note: Only SNMPv1 and SNMPv2 support community name setting.

Figure 3.12-5 Create an SNMP Community



Add SNMP Community

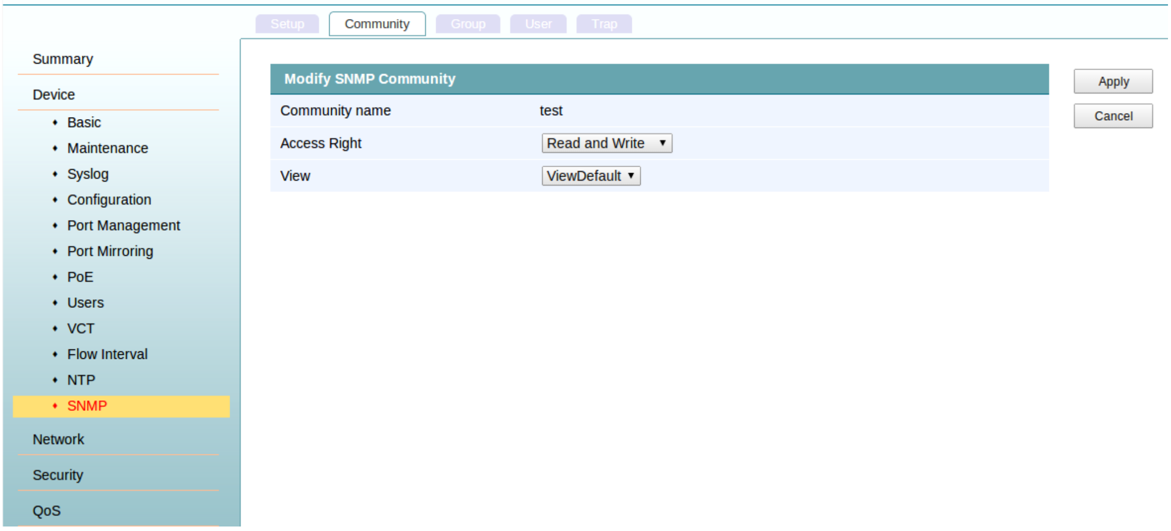
Community Name * (1-32 chars)

Access Right: Read and Write ▾

View: ViewDefault ▾

Items marked with an asterisk (*) are required

Figure 3.122-6 Modify an SNMP Community



Modify SNMP Community

Community name test

Access Right Read and Write

View ViewDefault

Table 3.12-2 Configuration items for configuring an SNMP community

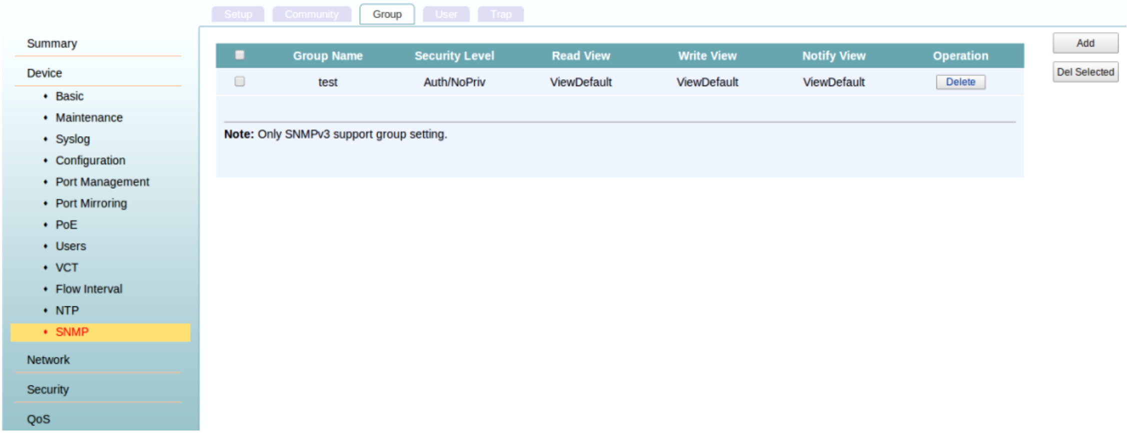
Item	Description
Community Name	Set SNMP community name.
Access Right	Configure SNMP NMS access right Read only—NMS can only perform read operation to MIB objects Read and write—NMS can perform both read and write operations to the MIB objects
View	Specify the view associated with the community to limit the MIB objects that can be accessed by NMS.

3.12.4 Configuring an SNMP group

1. Select **Device**-->**SNMP**;
2. Click **Group** to enter the page as shown in Figure 3.12-7.
3. Click **Add** to enter the page as shown in Figure 3.122-8.

If need to modify “SNMP Group”, click the related group as shown in Figure 3.12-9, if need to delete it, click “Delete”.

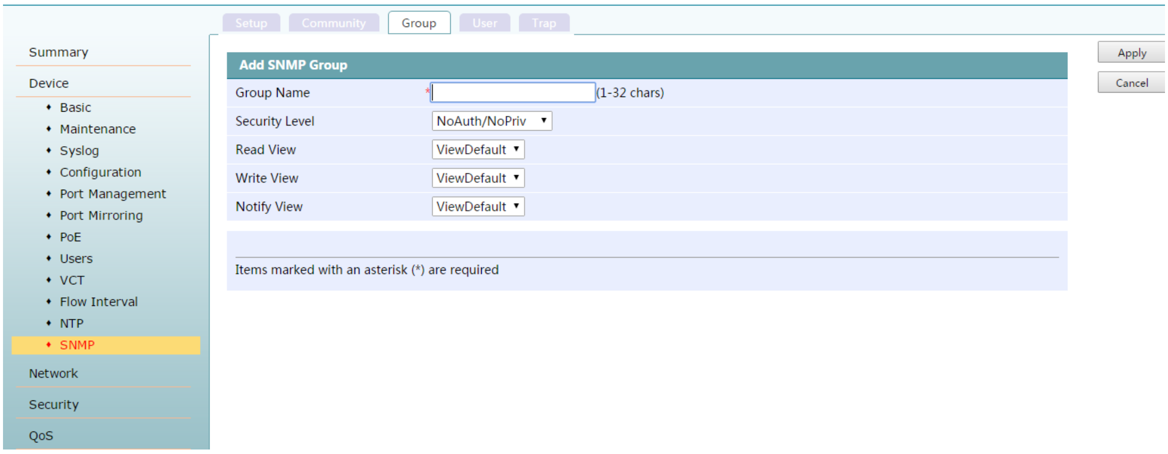
Figure 3.122-7 SNMP group



□	Group Name	Security Level	Read View	Write View	Notify View	Operation
□	test	Auth/NoPriv	ViewDefault	ViewDefault	ViewDefault	Delete

Note: Only SNMPv3 support group setting.

Figure 3.122-8 Create an SNMP group

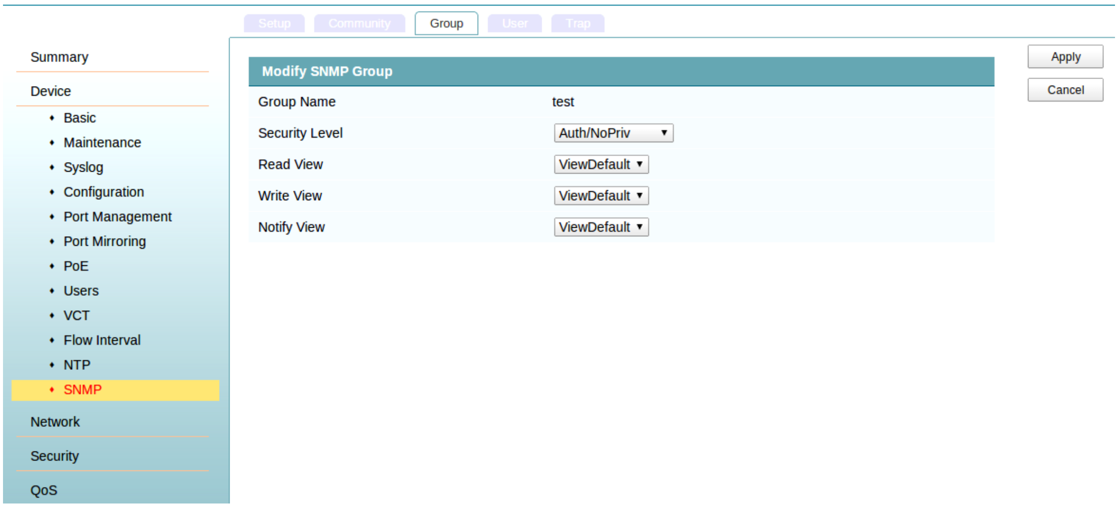


Add SNMP Group

Group Name	* (1-32 chars)
Security Level	NoAuth/NoPriv ▾
Read View	ViewDefault ▾
Write View	ViewDefault ▾
Notify View	ViewDefault ▾

Items marked with an asterisk (*) are required

Figure 3.122-9 Modify an SNMP group



Modify SNMP Group

Group Name	test
Security Level	Auth/NoPriv ▾
Read View	ViewDefault ▾
Write View	ViewDefault ▾
Notify View	ViewDefault ▾

Table 3.12-3 Configuration items for creating an SNMP group

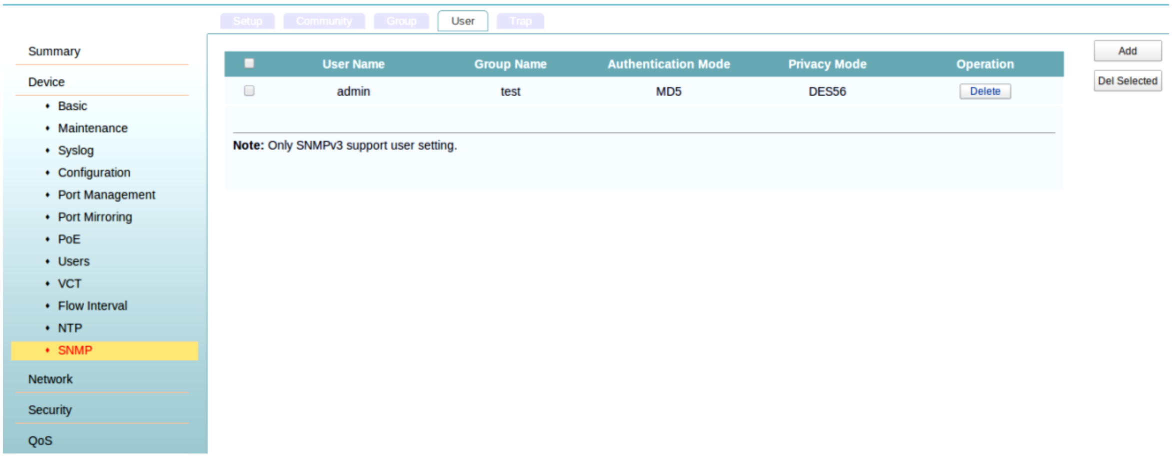
Item	Description
Group Name	Set SNMP group name.
Security Level	Select security level for SNMP group. The available security levels are: NoAuth/NoPriv—No authentication no privacy. Auth/NoPriv—Authentication without privacy. Auth/Priv—Authentication and privacy. IMPORTANT: For an existing SNMP group, its security level cannot be modified.
Read View	Select Read view.
Write View	Select write view. If no write view is configured, NMS cannot perform write operations to all MIB objects.
Notify View	Select notify view. If no notify view is configured, the agent can’t send traps to NMS.

3.12.5 Configuring an SNMP user

1. Select **Device**--> **SNMP**.
2. Click **User** to enter the page as shown in Figure 3.12-10.
3. Click **Add** to enter the Add SNMP User page, as shown in Figure 3.12-11.

If need to modify “SNMP User”, click related name as shown in Figure 3.122-12, if need to delete it, click “Delete”.

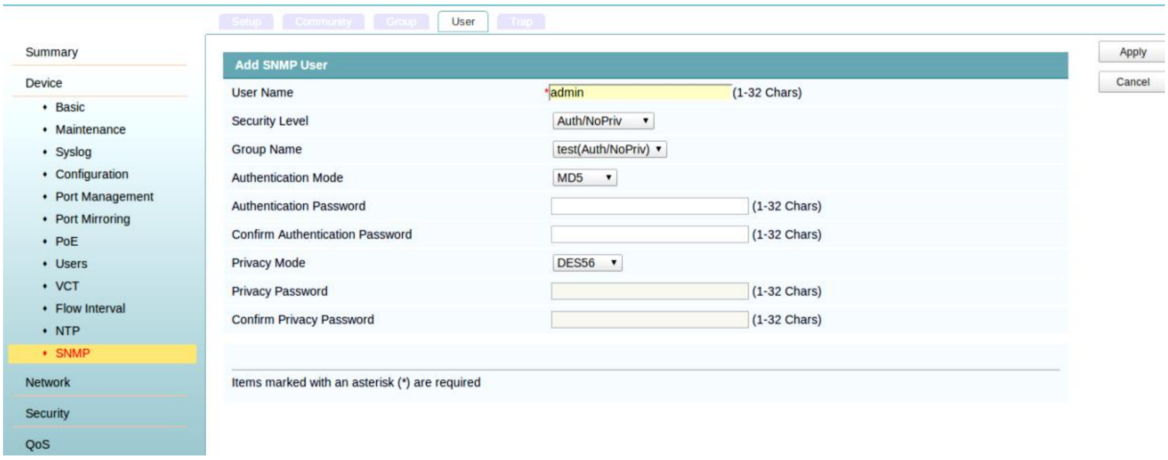
Figure 3.12-10 SNMP user



□	User Name	Group Name	Authentication Mode	Privacy Mode	Operation
□	admin	test	MD5	DES56	Delete

Note: Only SNMPv3 support user setting.

Figure 3.122-11 Create an SNMP user

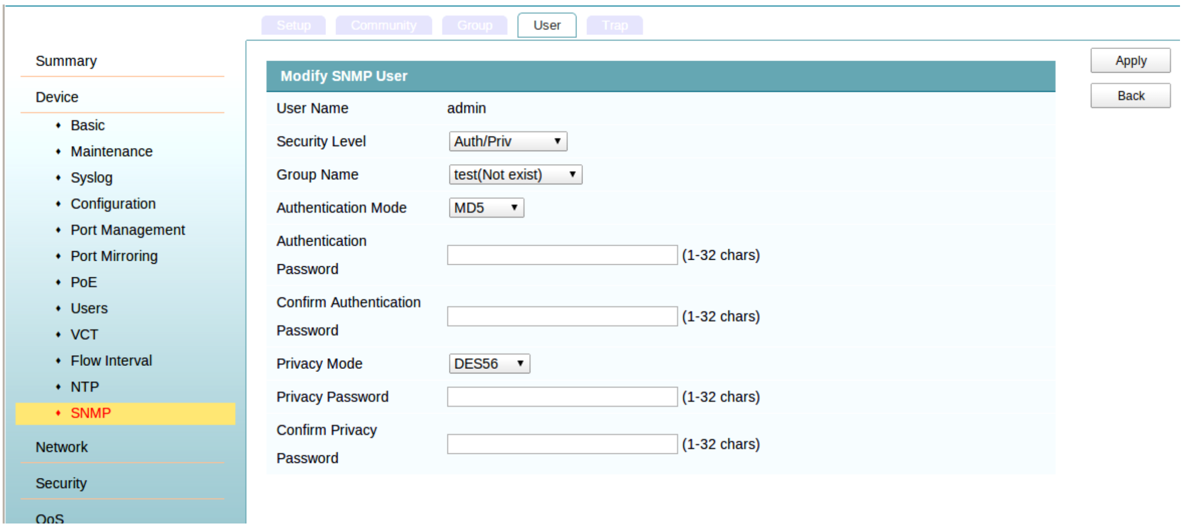


Add SNMP User

User Name	*admin	(1-32 Chars)
Security Level	Auth/NoPriv	
Group Name	test(Auth/NoPriv)	
Authentication Mode	MD5	
Authentication Password		(1-32 Chars)
Confirm Authentication Password		(1-32 Chars)
Privacy Mode	DES56	
Privacy Password		(1-32 Chars)
Confirm Privacy Password		(1-32 Chars)

Items marked with an asterisk (*) are required

Figure 3.12-12 Modify an SNMP user



Modify SNMP User

User Name	admin	
Security Level	Auth/Priv	
Group Name	test(Not exist)	
Authentication Mode	MD5	
Authentication Password		(1-32 chars)
Confirm Authentication Password		(1-32 chars)
Privacy Mode	DES56	
Privacy Password		(1-32 chars)
Confirm Privacy Password		(1-32 chars)

Table 3.12-4 Configuration items for creating an SNMP user

Item	Description
User Name	Set SNMP user name.
Security Level	Select security level for the SNMP group. The following is the available Security levels: NoAuth/NoPriv—No authentication no privacy. Auth/NoPriv—Authentication without privacy. Auth/Priv—Authentication and privacy.

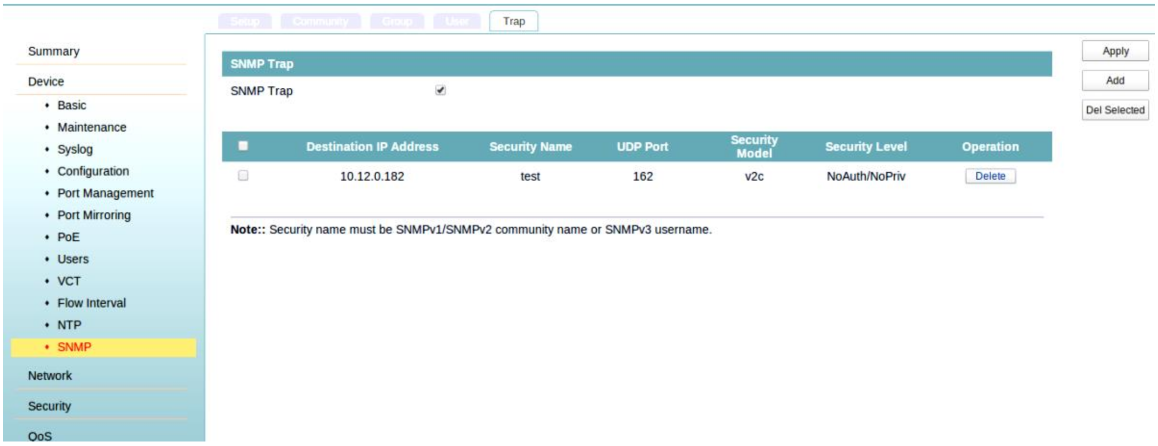
Item	Description
Group Name	Select an SNMP group to which the user belongs. When the security level is NoAuth/NoPriv, you can select an SNMP group without authentication & privacy. When the security level is Auth/NoPriv, you can select an SNMP group with no authentication no privacy or authentication without privacy. When the security level is Auth/Priv, you can select an SNMP group of any security level.
Authentication Mode	Select an authentication mode (including MD5 and SHA) when the security level is Auth/NoPriv or Auth/Priv.
Authentication Password	Set authentication password when the security level is Auth/NoPriv or Auth/Priv. The confirm authentication password must be the same with the authentication password.
Confirm Authentication Password	
Privacy Mode	Select a privacy mode (including DES56, AES128, and 3DES) when the security level is Auth/Priv.
Privacy Password	Set the privacy password when the security level is Auth/Priv. The confirm privacy password must be the same with the privacy password.

3.12.6 Configuring SNMP trap function

1. Select **Device**-->**SNMP;**
2. Click **Trap** to enter the page as shown in Figure 3.12-13.
3. Select to enable the **SNMP trap function** in the upper part of page and configure target hosts of the SNMP traps in the down part of page.
4. Click **Add** to enter the "**Add Trap Target Host**" page, as shown in Figure 3.12-24.

If need to modify "SNMP Trap Target Host", click related IP address as shown in Figure 3.122-35, if need to delete it, click "Delete".

Figure 3.122-43 Traps configuration



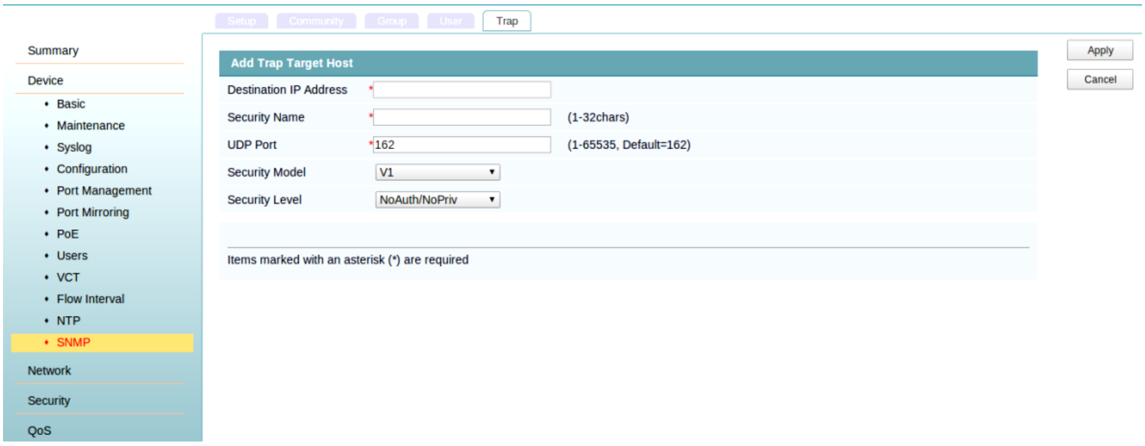
SNMP Trap

SNMP Trap ☑

■	Destination IP Address	Security Name	UDP Port	Security Model	Security Level	Operation
□	10.12.0.182	test	162	v2c	NoAuth/NoPriv	Delete

Note:: Security name must be SNMPv1/SNMPv2 community name or SNMPv3 username.

Figure 3.12-5 Add Trap Target Host

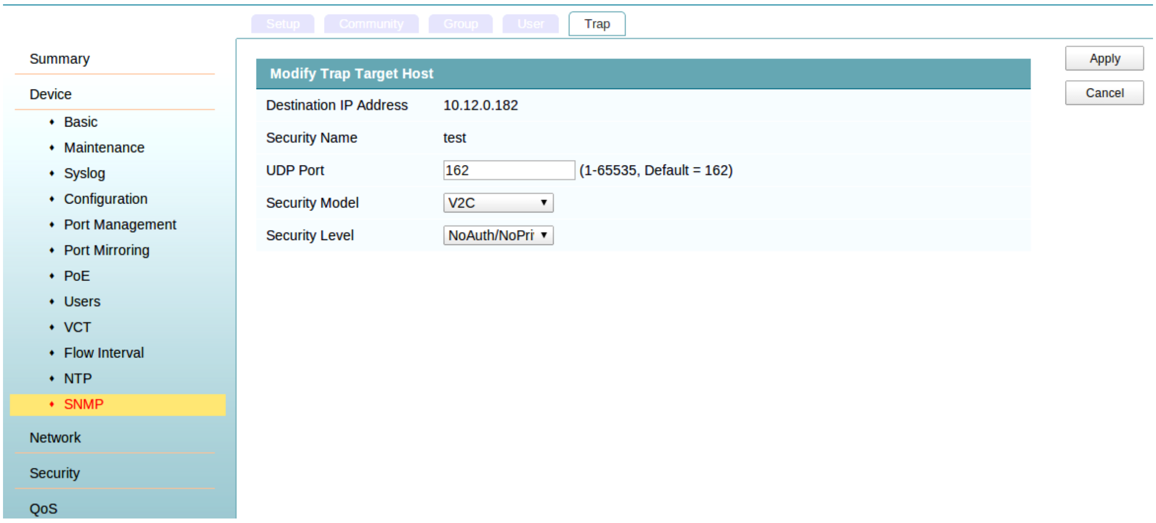


Add Trap Target Host

Destination IP Address	*	
Security Name	*	(1-32chars)
UDP Port	*162	(1-65535, Default=162)
Security Model	V1 ▾	
Security Level	NoAuth/NoPriv ▾	

Items marked with an asterisk (*) are required

Figure 3.12-6 Modify Trap Target Host



Modify Trap Target Host

Destination IP Address	10.12.0.182	
Security Name	test	
UDP Port	162	(1-65535, Default = 162)
Security Model	V2C ▾	
Security Level	NoAuth/NoPri ▾	

Table 3.12-5 Configuration items

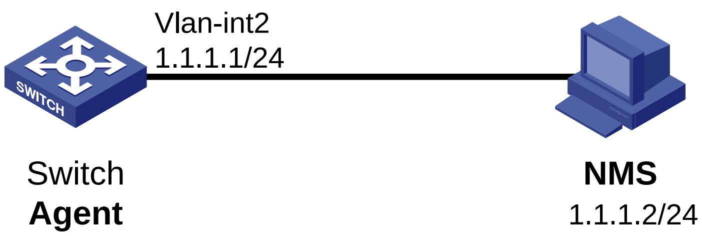
Item	Description
Destination IP Address	Set destination IP address: enter corresponding IP address according to the IP address type (IPv4).
Security Name	Set security name, which can be an SNMPv1 community name, an SNMPv2c community name, or an SNMPv3 user name.
UDP Port	Set UDP port number. ⓘIMPORTANT: The default port number is 162, which is the SNMP-specified port used for receiving traps on NMS. Generally (such as using iMC or MIB Browser as NMS), you can use the default port number. If need to change this number, please make sure the configuration is the same with that on NMS.
Security Model	Security model is SNMP version. Ensure the SNMP version is the same with that on NMS; otherwise, the NMS cannot receive any trap.
Security Level	Set the authentication and privacy mode for SNMP traps when the security model is selected as v3. The available security levels are: no authentication no privacy, authentication but no privacy, and authentication & privacy. When the security model is selected as v1 or v2c, the security level is no authentication no privacy, and cannot be modified.

3.12.7 SNMP configuration example

3.12.7.1 Network requirements

- As shown in Figure 3.12-176, NMS connects to the agent/Switch through an Ethernet.
- The IP address of NMS is 1.1.1.2/24.
- The IP address of the VLAN interface on Switch is 1.1.1.1/24.
- The NMS monitors the agent using SNMPv3. The agent reports errors or faults to the NMS.

Figure 3.12-16 Network diagram for SNMP configuration



3.12.7.2 Configuration procedure

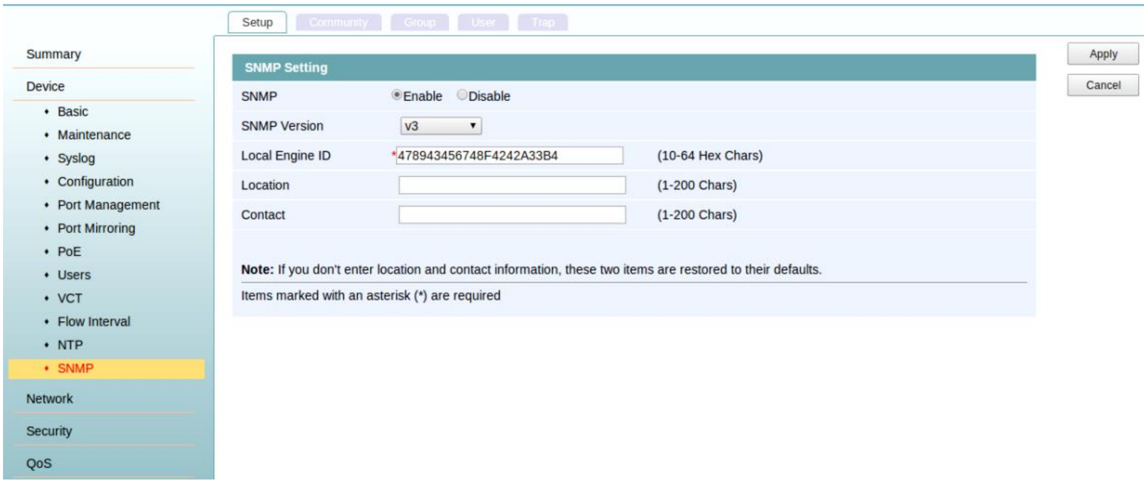
Table 1 Configure Agent

# Configuration IP addresses for the interfaces. (Procedure omitted)

# Enable SNMP.

1. Select Device-->SNMP to enter Setup page as shown in Figure 3.12-17.

Figure 3.12-17 SNMP setting configuration



SNMP Setting

SNMP	● Enable ○ Disable	
SNMP Version	v3	
Local Engine ID	*478943456748F4242A33B4	(10-64 Hex Chars)
Location		(1-200 Chars)
Contact		(1-200 Chars)

Note: If you don't enter location and contact information, these two items are restored to their defaults.

Items marked with an asterisk (*) are required

2. Select Enable.

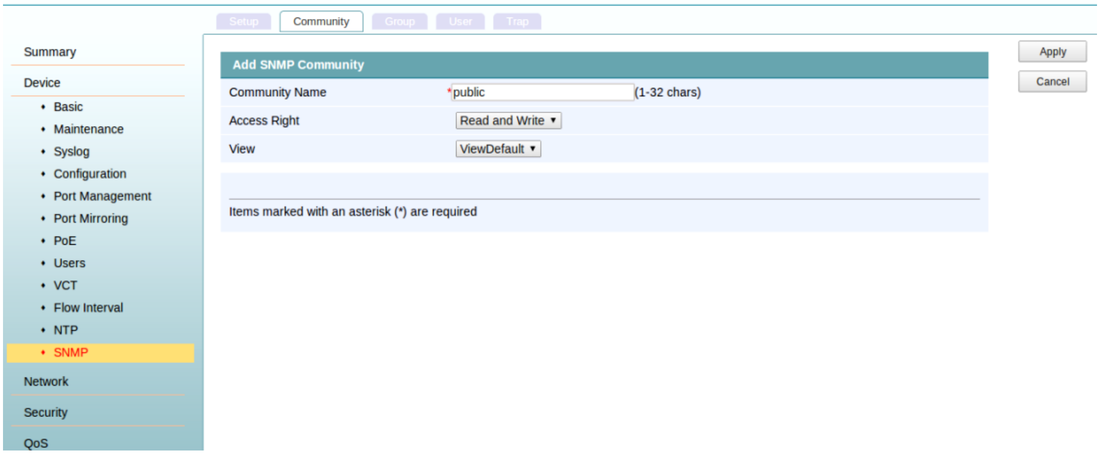
3. Select v3

4. Click Apply.

# Configure an SNMP Community .

1. Click Group and then click Add to enter the page as shown in Figure 3.12-18.

Figure 3.12-18 SNMP community configuration



Add SNMP Community

Community Name	*public (1-32 chars)
Access Right	Read and Write ▾
View	ViewDefault ▾

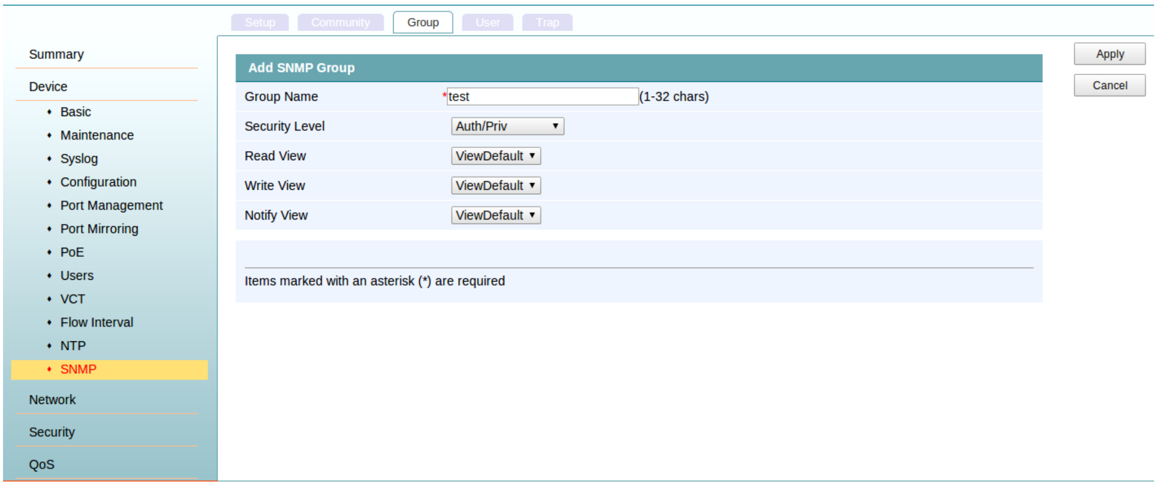
Items marked with an asterisk (*) are required

2. Fill in a name in column of “Community Name”.
3. Choose “**Read and Write**” in column of “Access Right”
4. Click Apply.

# Configure an SNMP group.

1. Click Group and then click Add to enter the page as shown in Figure 3.12-19.

Figure 3.12-19 SNMP Group configuration



Add SNMP Group

Group Name	*test (1-32 chars)
Security Level	Auth/Priv ▾
Read View	ViewDefault ▾
Write View	ViewDefault ▾
Notify View	ViewDefault ▾

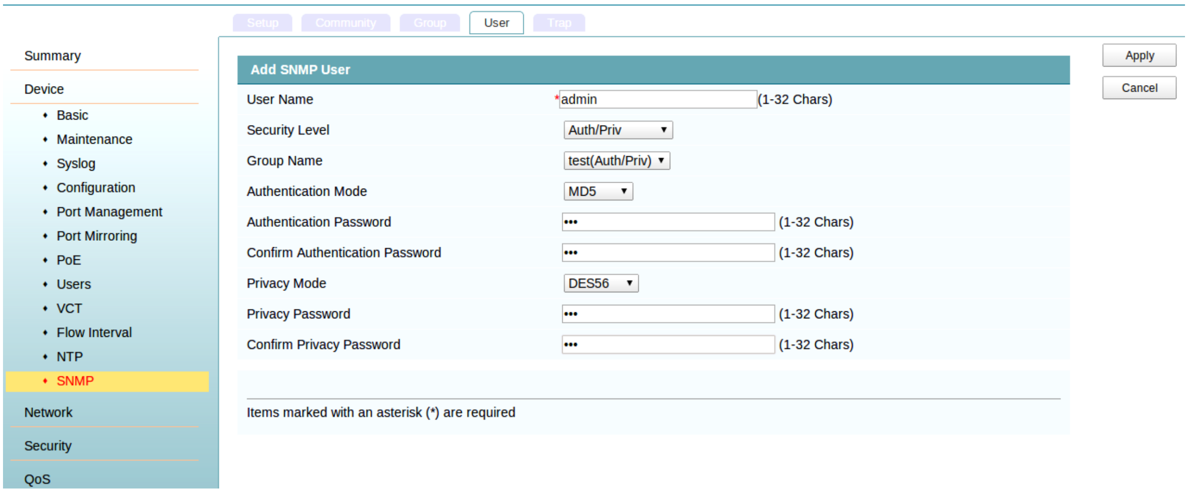
Items marked with an asterisk (*) are required

2. Enter group1 in column of Group Name.
3. Choose “Auth/Priv” in column of “Security Level”
4. Click Apply.

# Configure an SNMP user

1. Click User and then click Add to enter the page as shown in Figure 3.12-20.

Figure 3.12-20 SNMP user configuration



Add SNMP User

User Name	*admin	(1-32 Chars)
Security Level	Auth/Priv	
Group Name	test(Auth/Priv)	
Authentication Mode	MD5	
Authentication Password	•••	(1-32 Chars)
Confirm Authentication Password	•••	(1-32 Chars)
Privacy Mode	DES56	
Privacy Password	•••	(1-32 Chars)
Confirm Privacy Password	•••	(1-32 Chars)

Items marked with an asterisk (*) are required

2. Enter a name in column of User Name.

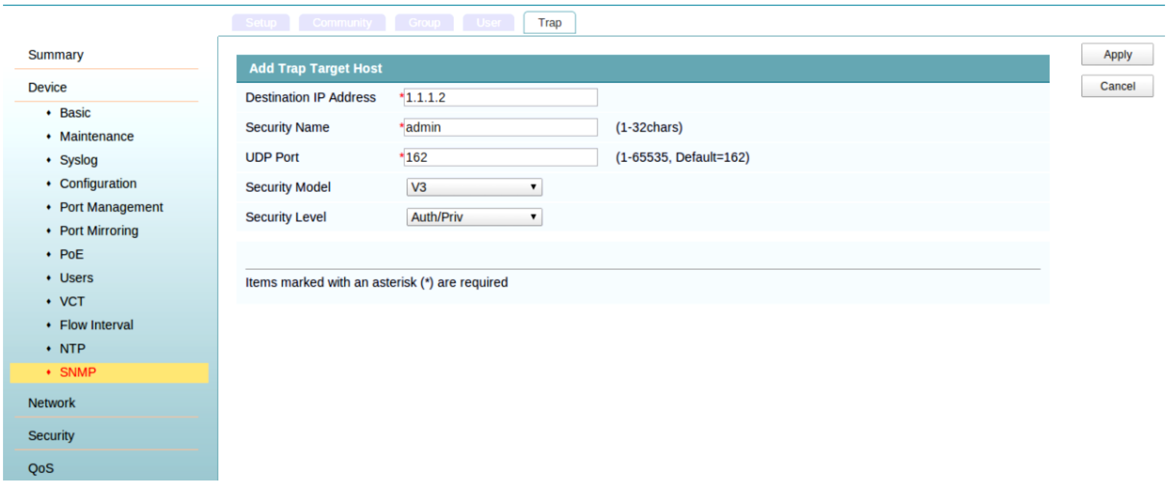
3. Choose “Auth/Priv” in the column of “Security level”
4. Select group name in the column of “Group Name”
5. Choose Authentication Mode
6. Enter Authentication Password
7. Re-enter Authentication Password to confirm
8. Choose privacy mode
9. Enter privacy password
10. Re-enter privacy Password to confirm

11. Click Apply.

# Enable the agent to send SNMP traps.

1. Click “Trap” menu and then click “add”, the following interface would be shown as Figure 3.12-21.

Figure 3.12-21 SNMP trap configuration



Add Trap Target Host

Destination IP Address	*1.1.1.2	
Security Name	*admin	(1-32chars)
UDP Port	*162	(1-65535, Default=162)
Security Model	V3	
Security Level	Auth/Priv	

Items marked with an asterisk (*) are required

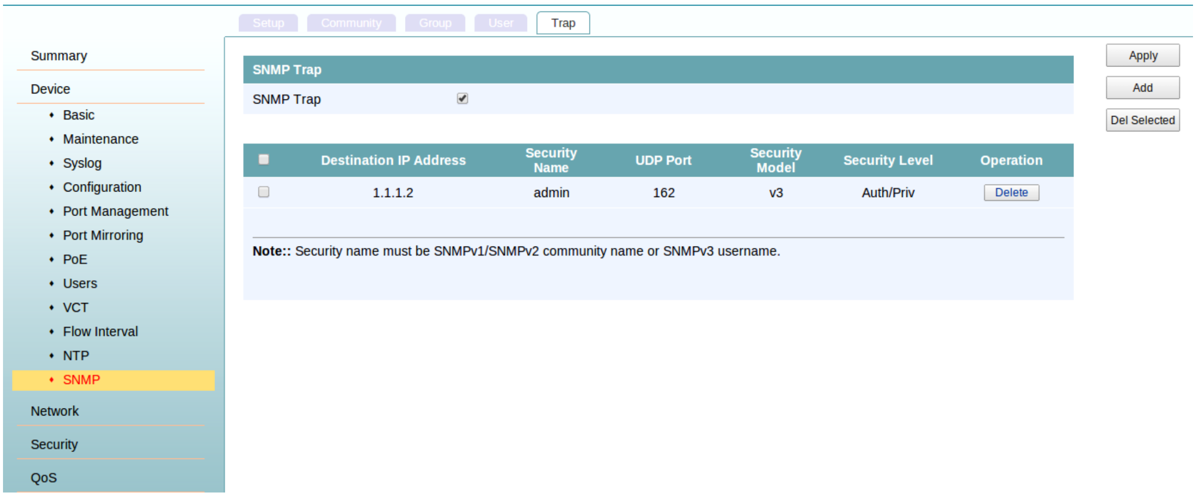
2. Type the destination address 1.1.1.2.

3. Type the Security name “admin”.

4. Select v3 from the column of Security Model.

5. Click Apply.

Figure 3.12-22 SNMP trap configuration



SNMP Trap

SNMP Trap ☑

□	Destination IP Address	Security Name	UDP Port	Security Model	Security Level	Operation
□	1.1.1.2	admin	162	v3	Auth/Priv	Delete

Note:: Security name must be SNMPv1/SNMPv2 community name or SNMPv3 username.

6. Select SNMP Trap

7. Click Apply.

Table 2 Configure NMS.

CAUTION:

The configuration on NMS must be consistent with that on the agent. Otherwise, you cannot perform corresponding operations.

SNMPv3 adopts a security mechanism of authentication and privacy. You must configure username and security level. According to the configured security level, you must configure the related authentication mode, authentication password, privacy mode, privacy password, and so on.

You must also configure the aging time and retry times. After these configurations, you can configure the device as needed through NMS. For more information about NMS configuration, see the NMS manual.

3.12.7.3 Configuration verification

- After above configuration, NMS can establish an SNMP connection with agent to query and reconfigure values of objects in the agent MIB.
- If an idle interface on the agent is shut down or brought up, the NMS can receive atrap information from agent.

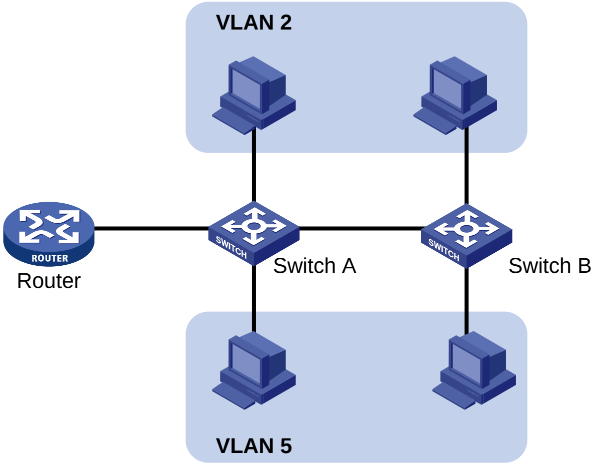
4 Network management

4.1 VLAN Configuration

4.1.1 Introduction to VLAN

Ethernet is a network technology based on the Carrier Sense Multiple Access/Collision Detect (CSMA/CD) mechanism. As the medium is shared, collisions and excessive broadcasts are common on Ethernet networks. To address the issue, virtual LAN (VLAN) was introduced to break a LAN down into separate VLANs. VLANs are isolated from each other at Layer 2. A VLAN is a bridging domain, and all broadcast traffic is contained within it, as shown in Figure 4.1-1.

Figure 4.1-1 A VLAN diagram



A VLAN is logically divided on an organizational basis rather than on a physical basis. For example, all workstations and servers used by a particular workgroup can be connected to the same LAN, regardless of their physical locations.

VLAN technology delivers the following benefits:

- Confining broadcast traffic within individual VLANs. This reduces bandwidth waste and improves network performance.
- Improving LAN security. By assigning user groups to different VLANs, you can isolate them at Layer 2 routers or Layer 3 switches are required to enable communication between VLANs.
- Flexible virtual workgroup creation. As users from the same workgroup can be assigned to the same VLAN regardless of their physical location and, network construction so that the maintenance is much easier and more flexible.

The following table shows how ports of different link types handle frames:

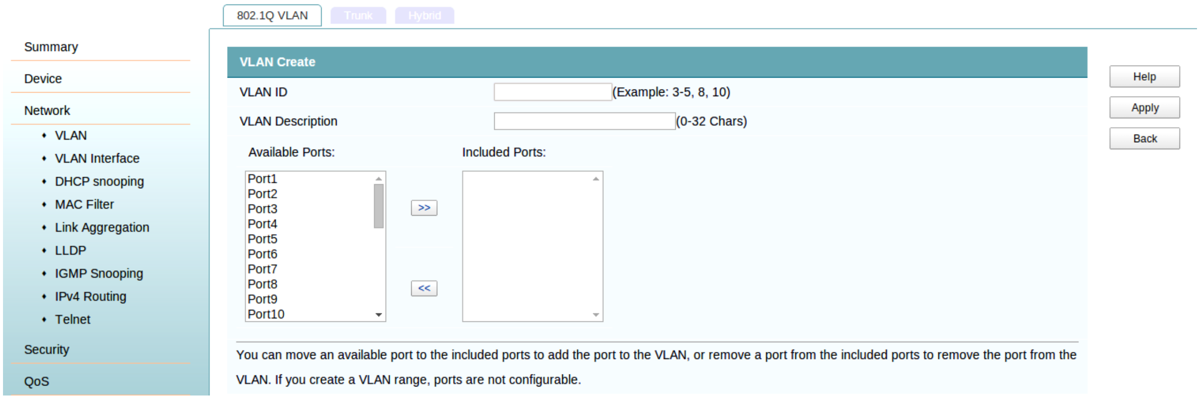
Table 4.1-1 Port type

Port type	Actions (in the inbound direction)		Actions (in the outbound direction)
	Untagged frame	Tagged frame	
Access	Tags the frame with PVID tag.	Receives the frame if its VLAN ID is the same with PVID. Drops the frame if its VLAN ID is different from PVID.	Removes the VLAN tag and sends the frame.
Trunk	Checks whether the PVID is carried on the port: If yes, tags the frame with PVID tag. If not, drops the frame.	Receives frame if its VLAN is carried on the port. Drops frame if its VLAN is not carried on the port.	Removes the tag and sends the frame if the frame carries the PVID tag and the port belongs to the PVID. Sends the frame without removing the tag if its VLAN is carried on the port but is different from the PVID.
Hybrid			Sends the frame if its VLAN is carried on the port. The frame is sent with the VLAN tag removed or intact depending on your configuration.

4.1.2 Add/Modify VLAN

Select Network-->VLAN-->**802.1.Q VLAN** to enter the page as shown in Figure 4.1-2.

Figure 4.1-2 Create VLAN



VLAN Create

VLAN ID (Example: 3-5, 8, 10)

VLAN Description (0-32 Chars)

Available Ports: Port1, Port2, Port3, Port4, Port5, Port6, Port7, Port8, Port9, Port10

Included Ports:

You can move an available port to the included ports to add the port to the VLAN, or remove a port from the included ports to remove the port from the VLAN. If you create a VLAN range, ports are not configurable.

Table 4.1-2 Configuration items

Item	Description
VLAN ID	VLAN ID number.
VLAN Description	Description of VLAN information. If this is null, set the VLAN described as default configuration information.

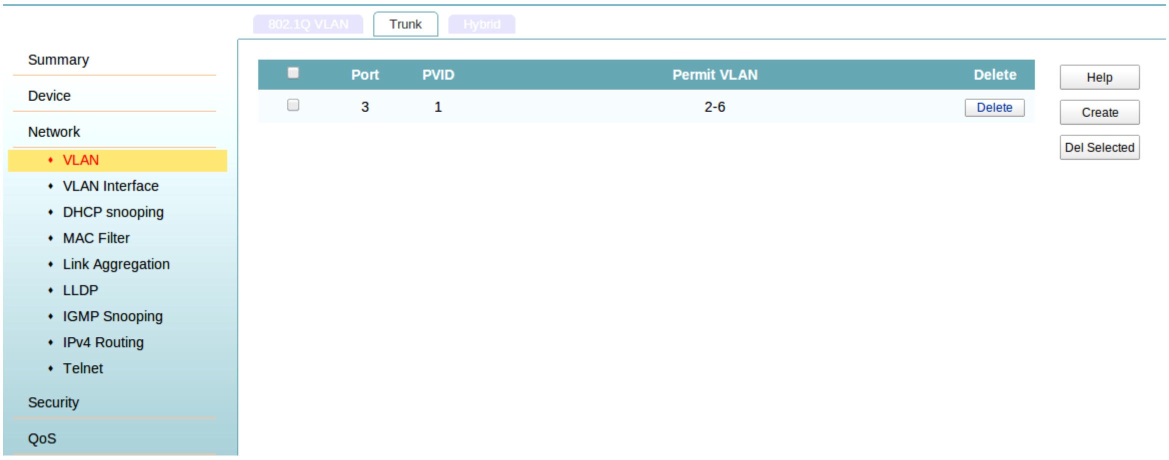
Item	Description
Available Ports	Display the list of available port.
Included Ports	Show the current port.

4.1.3 Trunk port display

A trunk port can carry multiple VLANs to receive and send traffic for them. Except traffic from the port VLAN ID (PVID), traffic sent through a trunk port will be VLAN tagged. Usually, ports connecting network devices are configured as trunk ports.

Select Network-->VLAN. Click Trunk and select VLANs as shown in Figure 4.1-3.

Figure 4.1-3 Select VLAN



□	Port	PVID	Permit VLAN	Delete
□	3	1	2-6	Delete

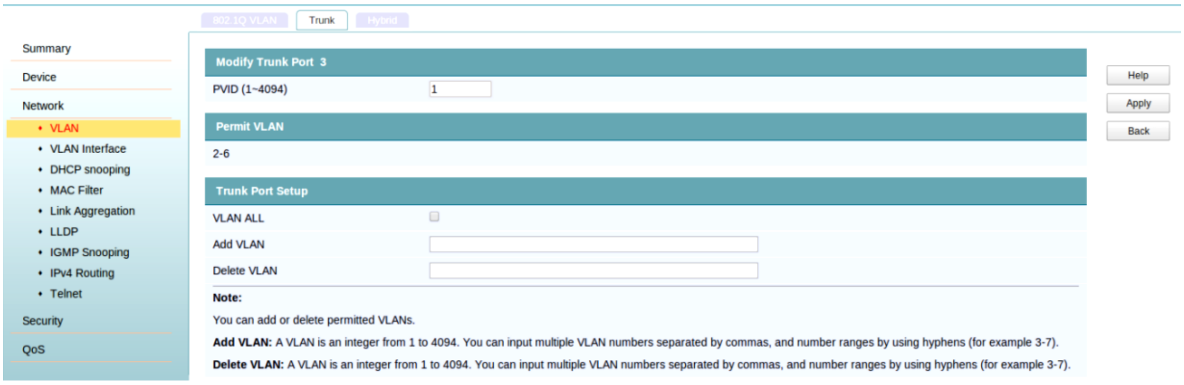
Table 4.1-3 Configuration items of selecting VLANs

Item	Description
Port	Trunk port, click to modify the Trunk port configuration
PVID	Default VLAN Trunk port ID
Permit VLAN	Allow able VLAN
Delete	Delete Trunk port

4.1.4 Create Trunk port

Click **Create**, then user can create a trunk port as shown in Figure 4.1-4.

Figure 4.1-4 Create a trunk port



Modify Trunk Port 3

PVID (1~4094) 1

Permit VLAN

2-6

Trunk Port Setup

VLAN ALL □

Add VLAN

Delete VLAN

Note:

You can add or delete permitted VLANs.

Add VLAN: A VLAN is an integer from 1 to 4094. You can input multiple VLAN numbers separated by commas, and number ranges by using hyphens (for example 3-7).

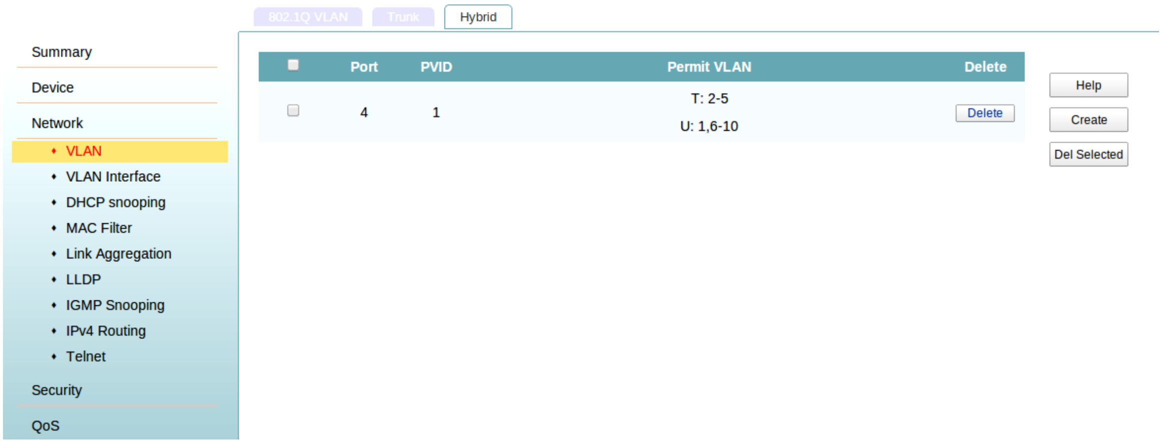
Delete VLAN: A VLAN is an integer from 1 to 4094. You can input multiple VLAN numbers separated by commas, and number ranges by using hyphens (for example 3-7).

4.1.5 Hybrid port display

A hybrid port can carry multiple VLANs to receive and send traffic for them. Unlike a trunk port, a hybrid port allows traffic of all VLANs to pass through VLAN untagged. You can configure a port connected to a network device or user terminal as a hybrid port.

Select Network-->VLAN and click **Hybrid** to enter the page shown in Figure 4.1-5.

Figure 4.1-5 Hybrid



□	Port	PVID	Permit VLAN	Delete
□	4	1	T: 2-5 U: 1,6-10	Delete

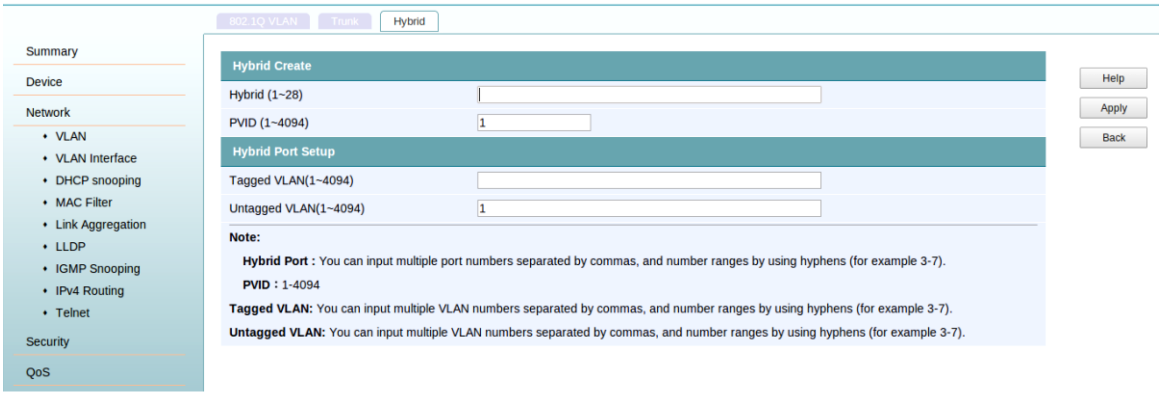
Table 4.1-4 Configuration items of modifying a VLAN

Item	Description
Port	Select the hybrid port to be modified.
PVID	Modify the VID of the selected VLAN.
Permit VLAN	**T:** List of vlans that allowed through the port with Tag; **U:** List of vlans that allowed through without the Tag.
Delete	Delete Hybrid port.

Item	Description
Create	Create Hybrid port.
Del Selected	Delete the selected Hybrid port.

4.1.6 Create Hybrid port

Figure 4.1-6 Create a hybrid port



Hybrid Create

Hybrid (1~28)

PVID (1~4094) 1

Hybrid Port Setup

Tagged VLAN(1~4094)

Untagged VLAN(1~4094) 1

Note:

Hybrid Port : You can input multiple port numbers separated by commas, and number ranges by using hyphens (for example 3-7).

PVID : 1-4094

Tagged VLAN: You can input multiple VLAN numbers separated by commas, and number ranges by using hyphens (for example 3-7).

Untagged VLAN: You can input multiple VLAN numbers separated by commas, and number ranges by using hyphens (for example 3-7).

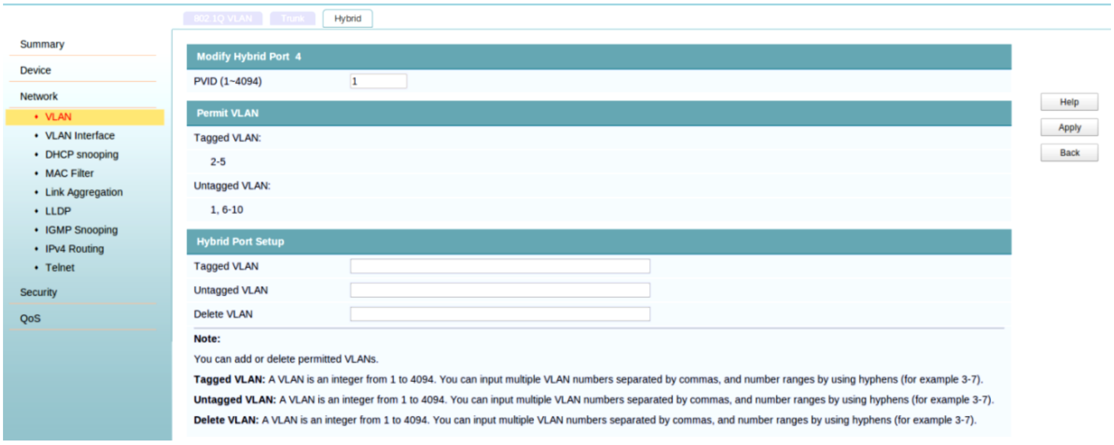
Table 4.1-5 Configuration items of create a VLAN

Item	Description
Hybrid	Create a new Hybrid port number.
PVID	Default port VLAN ID.
Tagged VLAN	List of vlans that allowed through the port with Tag;
Untagged VLAN	List of vlans that allowed through the port without Tag

4.1.7 Modify the Hybrid port configuration

Click the hybrid port to modify the parameter of a hybrid port, as shown in Figure 4.1-7.

Figure 4.1-7 Modify a hybrid port



Modify Hybrid Port 4

PVID (1~4094): 1

Permit VLAN

Tagged VLAN:

2-5

Untagged VLAN:

1, 6-10

Hybrid Port Setup

Tagged VLAN

Untagged VLAN

Delete VLAN

Note:

You can add or delete permitted VLANs.

Tagged VLAN: A VLAN is an integer from 1 to 4094. You can input multiple VLAN numbers separated by commas, and number ranges by using hyphens (for example 3-7).

Untagged VLAN: A VLAN is an integer from 1 to 4094. You can input multiple VLAN numbers separated by commas, and number ranges by using hyphens (for example 3-7).

Delete VLAN: A VLAN is an integer from 1 to 4094. You can input multiple VLAN numbers separated by commas, and number ranges by using hyphens (for example 3-7).

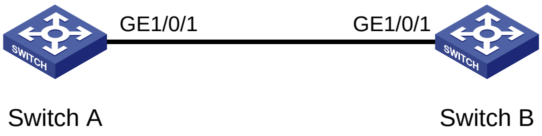
4.1.8 VLAN configuration example

4.1.8.1 Network requirements

Network diagram is as below:

- Trunk port Gigabit Ethernet 1/0/1 of Switch A is connected to trunk port Gigabit Ethernet 1/0/1 of Switch B.
- The PVID of Gigabit Ethernet 1/0/1 is VLAN 100.
- Gigabit Ethernet 1/0/1 permits packets of VLAN 2, VLAN 6 to pass through via VLAN 50and VLAN 100 .

Figure 4.1-8 Network diagram for VLAN configuration



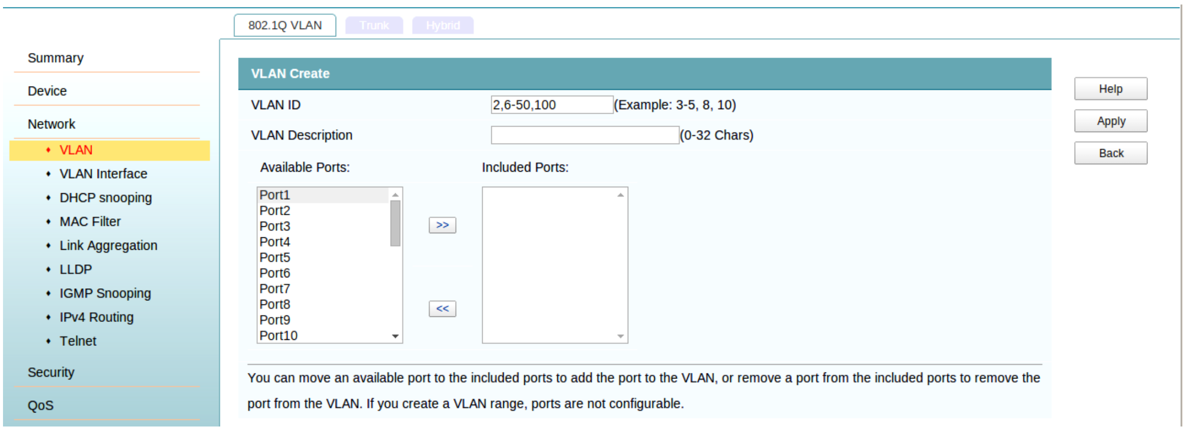
4.1.8.2 Configuration procedure

Configure Switch A

# Create VLAN 2, VLAN 6 through VLAN 50, and VLAN 100.

Select Network-->VLAN, fill in ID in the column of "VLAN ID" as below, and then click "apply".

Figure 4.1-9 Vlan create



VLAN Create

VLAN ID 2,6-50,100 (Example: 3-5, 8, 10)

VLAN Description (0-32 Chars)

Available Ports: Port1 Port2 Port3 Port4 Port5 Port6 Port7 Port8 Port9 Port10

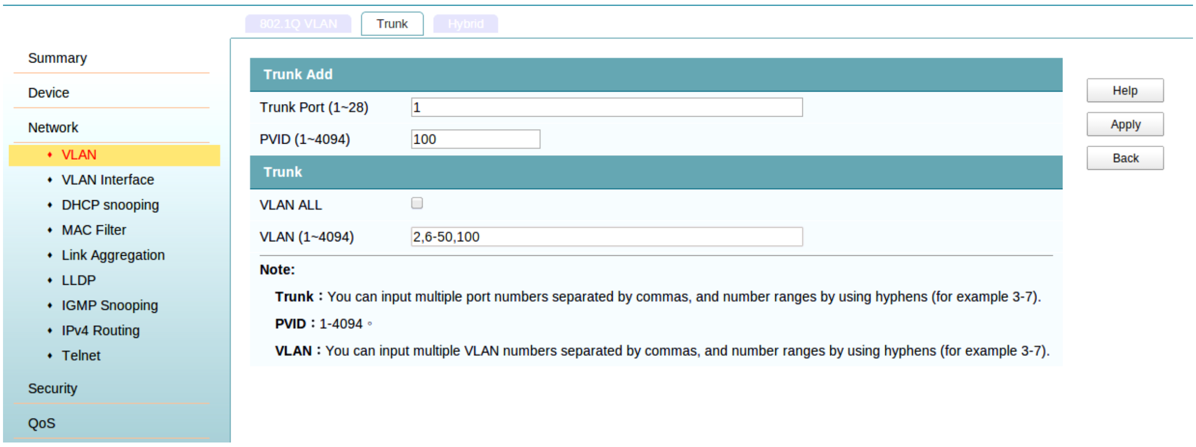
Included Ports:

You can move an available port to the included ports to add the port to the VLAN, or remove a port from the included ports to remove the port from the VLAN. If you create a VLAN range, ports are not configurable.

# Configure GigabitEthernet 1/0/1 as a trunk port and configure VLAN 100 as its PVID.

Select Network-->choose VLAN and select ”Trunk”, choose “1” in the column of “Trunk Port” and fill in “100” in the column of “PVID”. Enter “2,6-50,100” in the column of “trunk vlan” as shown in Figure 4.1-10.

Figure 4.1-10 Trunk port Vlan add



Trunk Add

Trunk Port (1~28) 1

PVID (1~4094) 100

Trunk

VLAN ALL □

VLAN (1~4094) 2,6-50,100

Note:

Trunk : You can input multiple port numbers separated by commas, and number ranges by using hyphens (for example 3-7).

PVID : 1-4094。

VLAN : You can input multiple VLAN numbers separated by commas, and number ranges by using hyphens (for example 3-7).

# Check the configuration.

Click Network -->VLAN, click “trunk” to check the configuration.

4.1.9 Configuration guidelines

When configuring the VLAN function, please conform to following guidelines:

- As the default VLAN, VLAN 1 cannot be created or removed.
- You cannot create or remove VLANs reserved for special purposes.
- Dynamic VLANs cannot be removed on the page for removing VLANs.

4.2 VLAN Interface

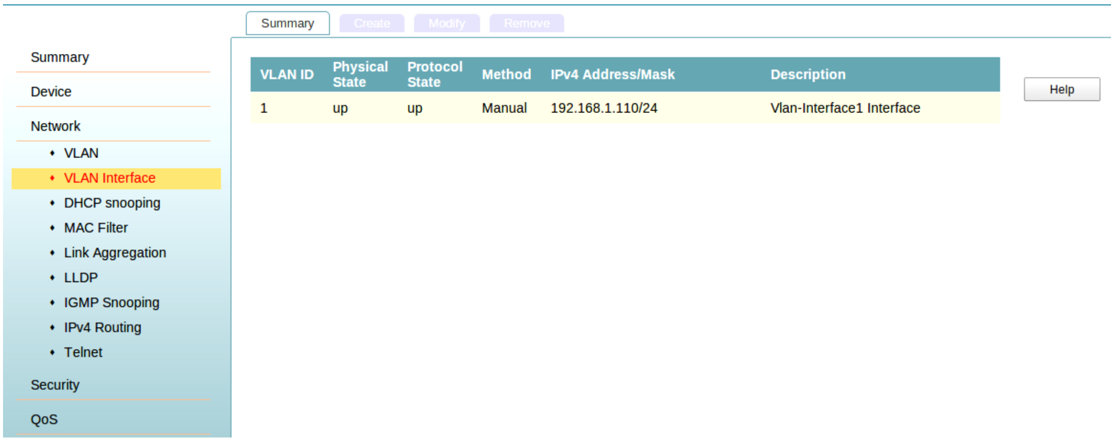
For hosts of different VLANs to communicate, you must use a router or Layer 3 switch to perform layer 3 forwarding. To achieve this, VLAN interfaces are used.

VLAN interfaces are virtual interfaces used for Layer 3 communication between different VLANs. They do not exist as physical entities on devices. For each VLAN, you can create one VLAN interface. You can assign the VLAN interface with an IP address and specify it as the gateway of the VLAN to forward the traffic destined for an IP subnet different from that of the VLAN.

4.2.1 Summary information

This page shows the current VLAN interface information as shown in Figure 4.2-1.

Figure 4.2-1 Summary information



VLAN ID	Physical State	Protocol State	Method	IPv4 Address/Mask	Description
1	up	up	Manual	192.168.1.110/24	Vlan-Interface1 Interface

Table 4.2-1 Configuration of creating a VLAN interface

Item	Description
VLAN ID:	Display a VLAN interface ID .
Physical state	Show the physical state of VLAN interface, as follows: Down: the VLAN management state of virtual interface for open, but physical status to close (it may be because there is no good connection or line fault); Up: the VLAN management of virtual interface states and physical states are open;
Protocol state	Show protocol state of VLAN interface, as follows: Down: the protocol state is closed, usually because there is no configuration IP address; Up: the protocol state is up ;
Method	Manual: configure a static IP address manually; DHCP automatically: access IP addresses dynamically.
IPv4 Address/Mask	Display the IP address of the VLAN virtual interface (if not configured shows "unassigned")

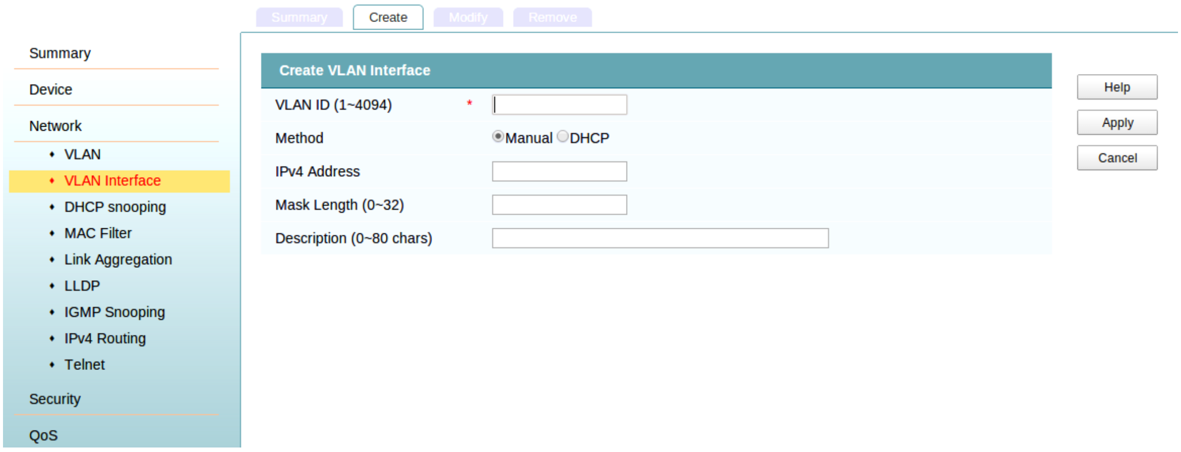
Item	Description
Description	Display the description information of VLAN virtual interface

4.2.2 Creating a VLAN interface

If a VLAN doesn't exist, the system will automatically create the VLAN.

Select Network-->VLAN Interface and click Create to enter the page shown in Figure 4.2-2.

Figure 4.2-2 Create VLAN



Create VLAN Interface

VLAN ID (1~4094) *	
Method	● Manual ○ DHCP
IPv4 Address	
Mask Length (0~32)	
Description (0~80 chars)	

Table 4.2-2 Configuration of creating a VLAN interface

Item	Description
VLAN ID:	Add a VLAN ID
Method	Add VLAN interface IP address manually or automatically. Manual: configure a static IP address manually; DHCP automatically: access IP addresses dynamically
IPv4 Address	add IP address to the VLAN virtual interface, the default is empty
Mask Length	add a subnet mask of VLAN virtual interface, default is empty
Description	Add description for VLAN interface , the default is empty

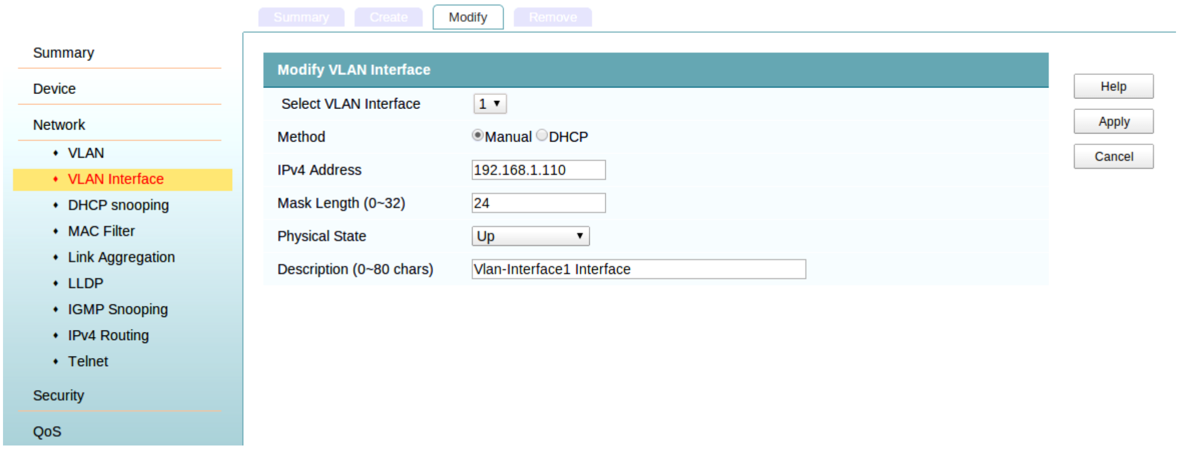
4.2.3 Modifying a VLAN interface

NOTE:

- After modify the IPv4 address for a selected VLAN interface, click Apply to submit the modification.
- After change the IP address which is used to log in to the device, please disconnect with the device firstly and use the changed IP address to re-log in.

Select Network-->VLAN Interface and click Modify to enter the page shown in Figure 4.2-3.

Figure 4.2-3 Modify VLAN



Modify VLAN Interface

Select VLAN Interface	1 ▾
Method	● Manual ○ DHCP
IPv4 Address	192.168.1.110
Mask Length (0~32)	24
Physical State	Up ▾
Description (0~80 chars)	Vlan-Interface1 Interface

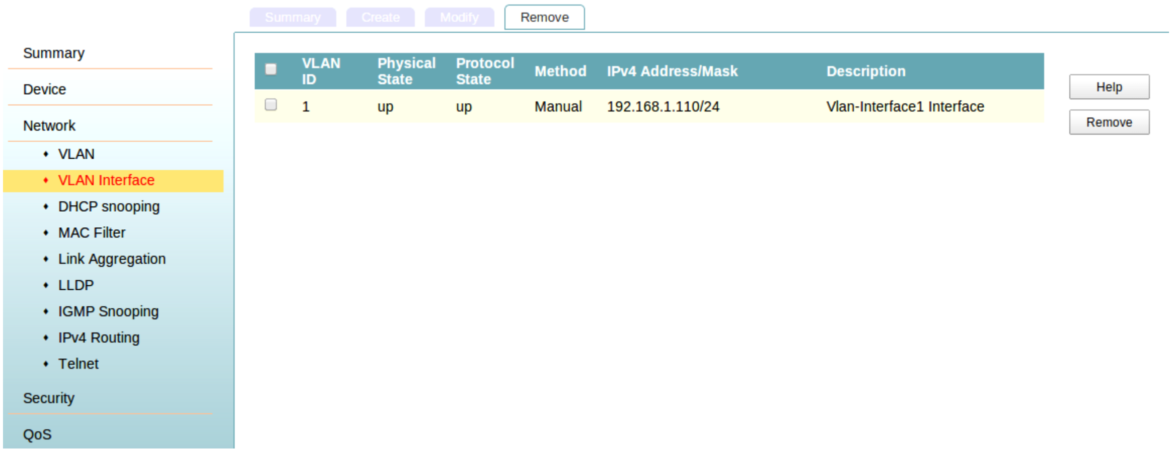
Table 4.2-3 Configuration of modifying a VLAN interface

Item	Description
Select VLAN Interface	Select the VLAN interface to be configured.
Method	Change the IP address of the VLAN virtual interface access method. Manual: configure a static IP address manually ; DHCP automatically: access IP address dynamically.
IPv4 Address	Add IP address to VLAN virtual interface.
Mask Length	Modify the VLAN virtual interface IP address of the corresponding subnet mask
Physical State	Modify the state of the VLAN virtual interface
Description	Add description for VLAN virtual interface

4.2.4 Remove a VLAN interface

Select Network-->VLAN Interface and click Remove to enter the page shown in Figure 4.2-4.

Figure 4.2-4 Remove VLAN



□	VLAN ID	Physical State	Protocol State	Method	IPv4 Address/Mask	Description
□	1	up	up	Manual	192.168.1.110/24	Vlan-Interface1 Interface

Table 4.2-4 Configuration of removing a VLAN interface

Item	Description
VLAN ID:	Display a VLAN interface ID .
Physical state	Shows the physical state of VLAN interface, as follows: Down: the VLAN management state of virtual interface for open, but physical status to close (it may be because there is no good connection or line fault); Up: the VLAN management of virtual interface states and physical states are open;
Protocol state	Shows protocol state of VLAN interface, as follows: Down: the protocol state is closed, usually because there is no configuration IP address; Up: the protocol state is open;
Method	Manual: configure a static IP address manually; DHCP automatically: access IP addresses dynamically.
IPv4 Address/Mask	Displays the IP address of VLAN virtual interface (if not configured shows "unassigned")
Description	Displays the description of VLAN virtual interface

4.3 DHCP Snooping

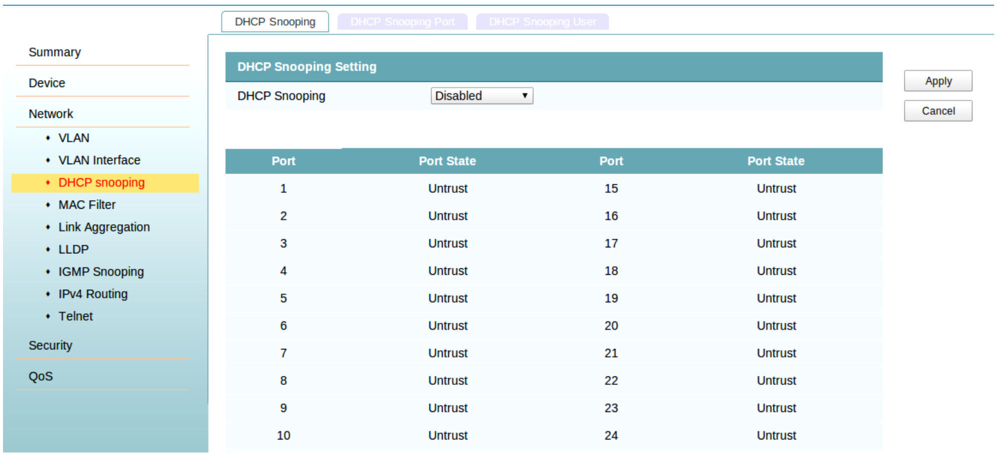
NOTE:

- A DHCP snooping enabled device not to work if it is between the DHCP relay agent and DHCP server, and it can work when it is between the DHCP client and relay agent or between the DHCP client and server.
- It is not recommend you to enable the DHCP client, BOOTP client, and DHCP snooping on the same device. Otherwise, DHCP snooping entries may fail to be generated, or the BOOTP client/DHCP client may fail to obtain an IP address.

4.3.1 Enabling DHCP snooping

Select Network-->DHCP **snooping**, and then click DHCP Snooping to enter the page shown in Figure 4.3-1. You can enable or disable DHCP snooping in the DHCP Snooping field.

Figure 4.3-1 DHCP snooping configuration



DHCP Snooping Setting

DHCP Snooping: Disabled

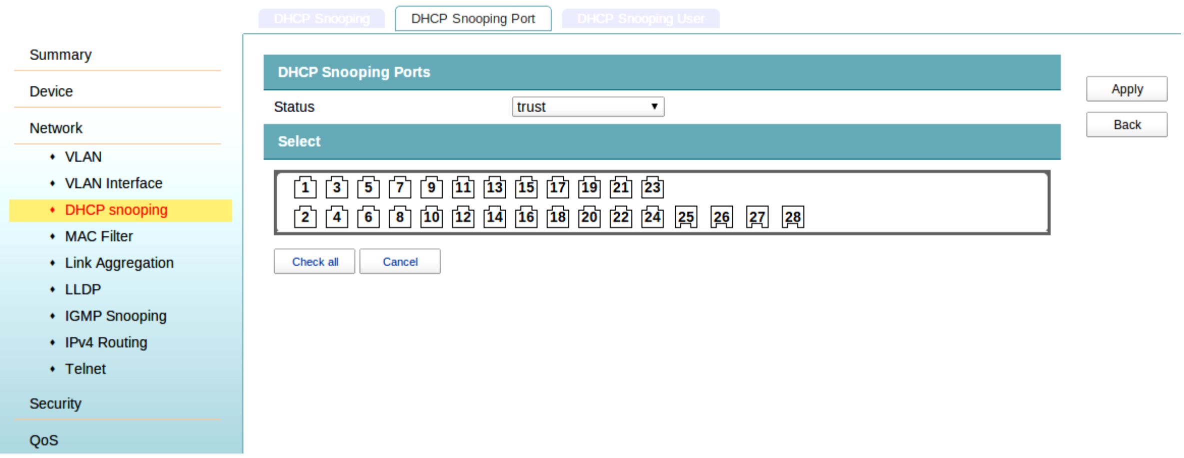
Port	Port State	Port	Port State
1	Untrust	15	Untrust
2	Untrust	16	Untrust
3	Untrust	17	Untrust
4	Untrust	18	Untrust
5	Untrust	19	Untrust
6	Untrust	20	Untrust
7	Untrust	21	Untrust
8	Untrust	22	Untrust
9	Untrust	23	Untrust
10	Untrust	24	Untrust

- Enable DHCP snooping, click Enable in the column of DHCP Snooping.
- Disable DHCP snooping, click Disable in the column of DHCP Snooping.

4.3.2 Configuring DHCP snooping functions on a port

Select Network-->DHCP snooping, and click DHCP Snooping Port to enter the page shown in Figure 4.3-2, where you can configure the port as trusted or untrusted ports, and can check the final configuration via Figure 4.3-1.

Figure 4.3-2 DHCP snooping Port configuration



DHCP Snooping Ports

Status: trust

Select

1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28

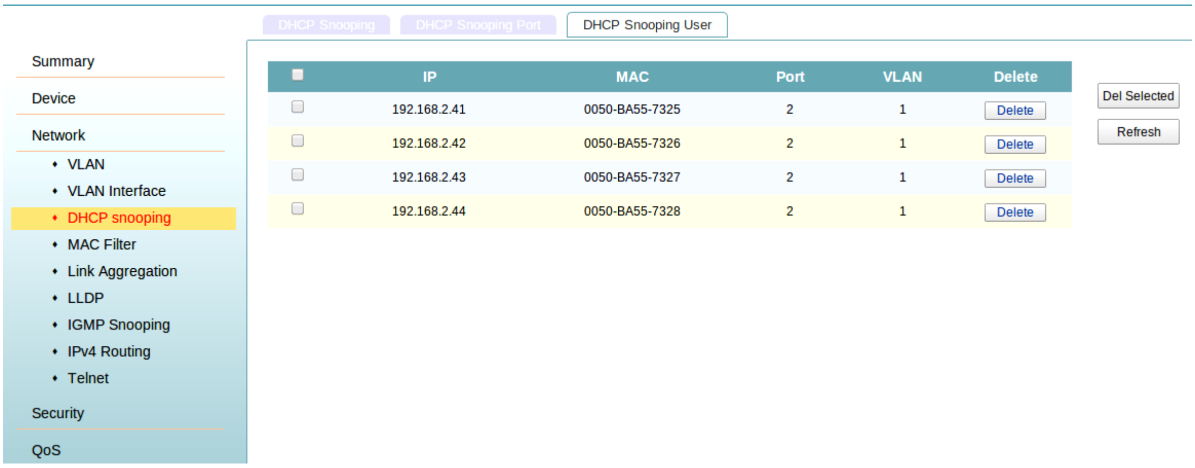
Table 4.3-1 DHCP snooping interface configuration

Item	Description
Port	Displays the name of a specific interface.
Port State	Configure the interface as trusted or untrusted.

4.3.3 Displaying clients' IP-to-MAC bindings

Select Network-->DHCP snooping, and then click DHCP Snooping User to view clients' IP-to-MAC bindings recorded by DHCP snooping, as shown in Figure 4.3-3.

Figure 4.3-3 DHCP snooping user



□	IP	MAC	Port	VLAN	Delete
□	192.168.2.41	0050-BA55-7325	2	1	Delete
□	192.168.2.42	0050-BA55-7326	2	1	Delete
□	192.168.2.43	0050-BA55-7327	2	1	Delete
□	192.168.2.44	0050-BA55-7328	2	1	Delete

Table 4.3-2 DHCP snooping user information configuration

Item	Description
IP	Displays the IP address assigned by the DHCP server to the client.

Item	Description
MAC	Displays the MAC address of the client.
Port	Displays the device interface to which the client is connected.
VLAN	Displays the VLAN to which the device belongs.
Delete	Delete the IP-to-MAC bindings.

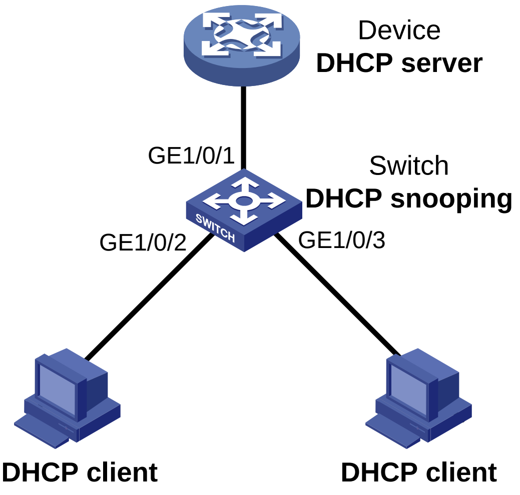
4.3.4 DHCP snooping configuration example

4.3.4.1 Network requirements

As below, a DHCP snooping device (Switch) is connected to a DHCP server through Gigabit Ethernet 1/0/1, and to DHCP clients through Gigabit Ethernet 1/0/2 and Gigabit Ethernet 1/0/3.

- Enable DHCP snooping on Switch and configure DHCP snooping to support Option 82. Configure the handling strategy for DHCP requests containing Option 82 as replace.
- Enable Gigabit Ethernet 1/0/1 to forward DHCP server responses; disable Gigabit Ethernet 1/0/2 and Gigabit Ethernet 1/0/3 from forwarding DHCP server responses.
- Configure Switch to record clients' IP-to-MAC address bindings in DHCP-REQUEST messages and DHCP-ACK messages received from a trusted port.

Figure 4.3-4 Network diagram for DHCP snooping configuration

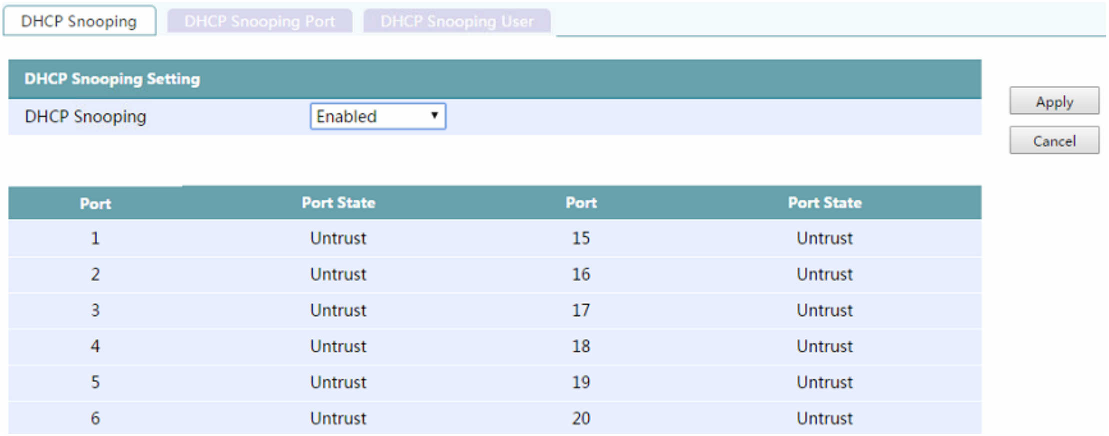


4.3.4.2 Configuration procedure

# Enable DHCP snooping.

1. Select Network-->DHCP, and then click DHCP Snooping to perform the following operation.

Figure 4.3-5 Enable DHCP snooping



DHCP Snooping Setting

DHCP Snooping: Enabled

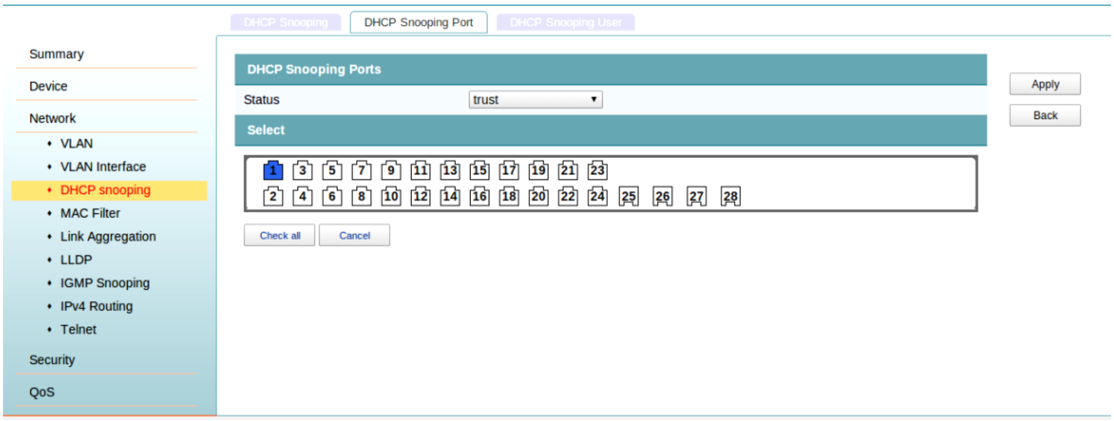
Port	Port State	Port	Port State
1	Untrust	15	Untrust
2	Untrust	16	Untrust
3	Untrust	17	Untrust
4	Untrust	18	Untrust
5	Untrust	19	Untrust
6	Untrust	20	Untrust

2. Choose Enabled in the column of DHCP Snooping.

# Configure DHCP snooping functions on Gigabit Ethernet 1/0/1.

1. Click Network-->DHCP snooping, choose "DHCP Snooping Port" as below.

Figure 4.3-6 Configure DHCP snooping functions on Gigabit Ethernet 1/0/1



DHCP Snooping Ports

Status: trust

Select

2. Choose "trust" in the column of "status".

3. Select "port 1"

4. Click Apply.

4.4 MAC Filter

An Ethernet device uses a MAC address table to forwarding frames through unicast instead of broadcast. This table describes which port a MAC address (or host) can be reached. When forwarding a frame, the device looks up the MAC address of the frame in the MAC address table firstly. If the device finds an entry, it forwards the frame out of the outgoing port in the entry. If the device does not find an entry, it broadcasts the frame out of all but the incoming port.

The device automatically learns entries in the MAC address table, or you can add them manually.

You can configure and display MAC address entries and set its aging time.

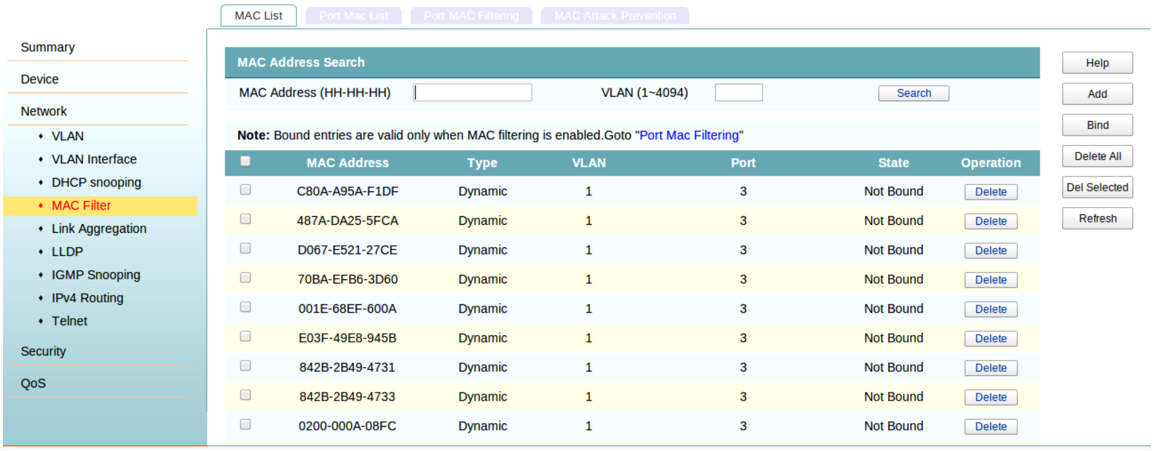
NOTE:

- The MAC address table can contain only Layer 2 Ethernet ports and Layer 2 aggregate interfaces..
- This document covers the configuration of unicast MAC address table entries, including static, dynamic, and blackhole MAC address table entries.

4.4.1 MAC list

Select Network-->MAC Filter. The system automatically displays the MAC List, which shows all the MAC address entries on the device, as shown in Figure 4.44-1.

Figure 4.44-1 MAC List



MAC Address Search

MAC Address (HH-HH-HH) | VLAN (1~4094) | Search

Note: Bound entries are valid only when MAC filtering is enabled.Goto "Port Mac Filtering"

□	MAC Address	Type	VLAN	Port	State	Operation
□	C80A-A95A-F1DF	Dynamic	1	3	Not Bound	Delete
□	487A-DA25-5FCA	Dynamic	1	3	Not Bound	Delete
□	D067-E521-27CE	Dynamic	1	3	Not Bound	Delete
□	70BA-EFB6-3D60	Dynamic	1	3	Not Bound	Delete
□	001E-68EF-600A	Dynamic	1	3	Not Bound	Delete
□	E03F-49E8-945B	Dynamic	1	3	Not Bound	Delete
□	842B-2B49-4731	Dynamic	1	3	Not Bound	Delete
□	842B-2B49-4733	Dynamic	1	3	Not Bound	Delete
□	0200-000A-08FC	Dynamic	1	3	Not Bound	Delete

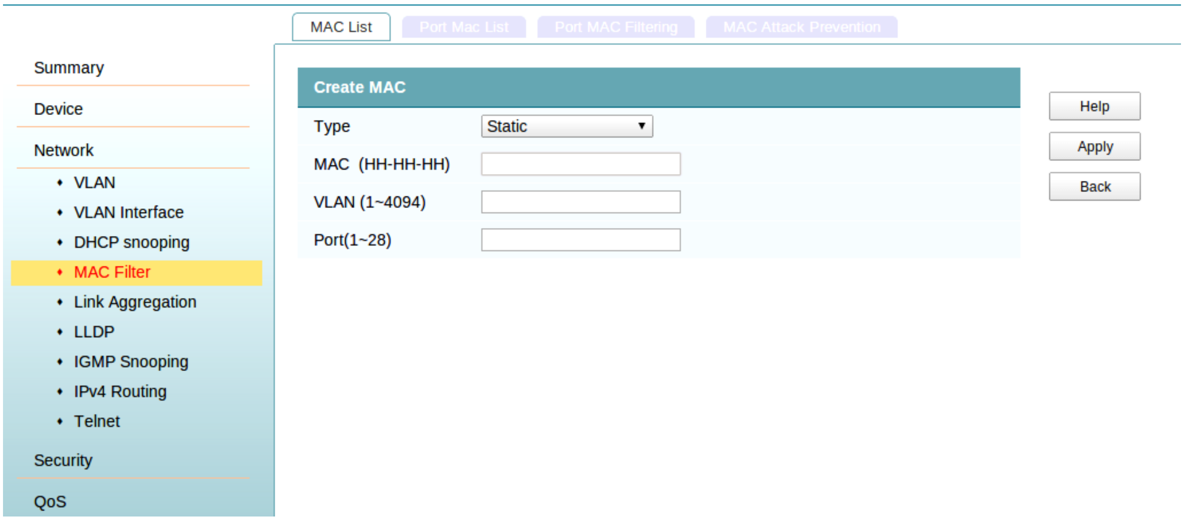
Table 4.4-1 Mac list items

Item	Description
MAC Address search	Enter the MAC address and VLAN ID and click Search
MAC shows	MAC addresses and corresponding VLAN information; click "Bind" to add the binding information
Add	Add MAC address.

Item	Description
Bind	Bind MAC address with IP and port
Delete All	Delete all the MAC address
Del selected	Delete the selected MAC address

Click Add to enter the page as shown in Figure 4.4-2.

Figure 4.4-2 Create a MAC address entry



Create MAC

Type	Static
MAC (HH-HH-HH)	
VLAN (1~4094)	
Port(1~28)	

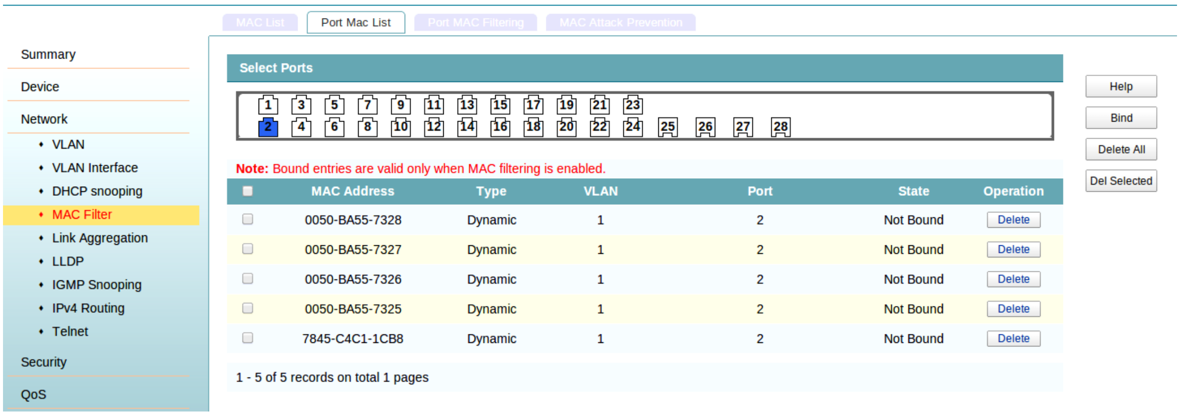
Table 4.4-2 Configuration of creating a MAC address entry

Item	Description
Type	Set the type of the MAC address entry: ● **Static**—Static MAC address entries that never age out. Static Mac address entries manually configured by the users. ● **Dynamic**—Dynamic MAC address entries that will age out. ● **Blackhole**—Blackhole MAC address entries that never age out.
MAC	Set the MAC address to be added.
VLAN	Set the ID of the VLAN to which the MAC address belongs.
Port	Set the port to which the MAC address belongs.

4.4.2 Port MAC List

Select Network-->MAC Filter, and click “Port MAC list”, as shown in Figure 4.4-3.

Figure 4.4-3 Port MAC List



Note: Bound entries are valid only when MAC filtering is enabled.

□	MAC Address	Type	VLAN	Port	State	Operation
□	0050-BA55-7328	Dynamic	1	2	Not Bound	Delete
□	0050-BA55-7327	Dynamic	1	2	Not Bound	Delete
□	0050-BA55-7326	Dynamic	1	2	Not Bound	Delete
□	0050-BA55-7325	Dynamic	1	2	Not Bound	Delete
□	7845-C4C1-1CB8	Dynamic	1	2	Not Bound	Delete

1 - 5 of 5 records on total 1 pages

Table 4.4-3 Port MAC items

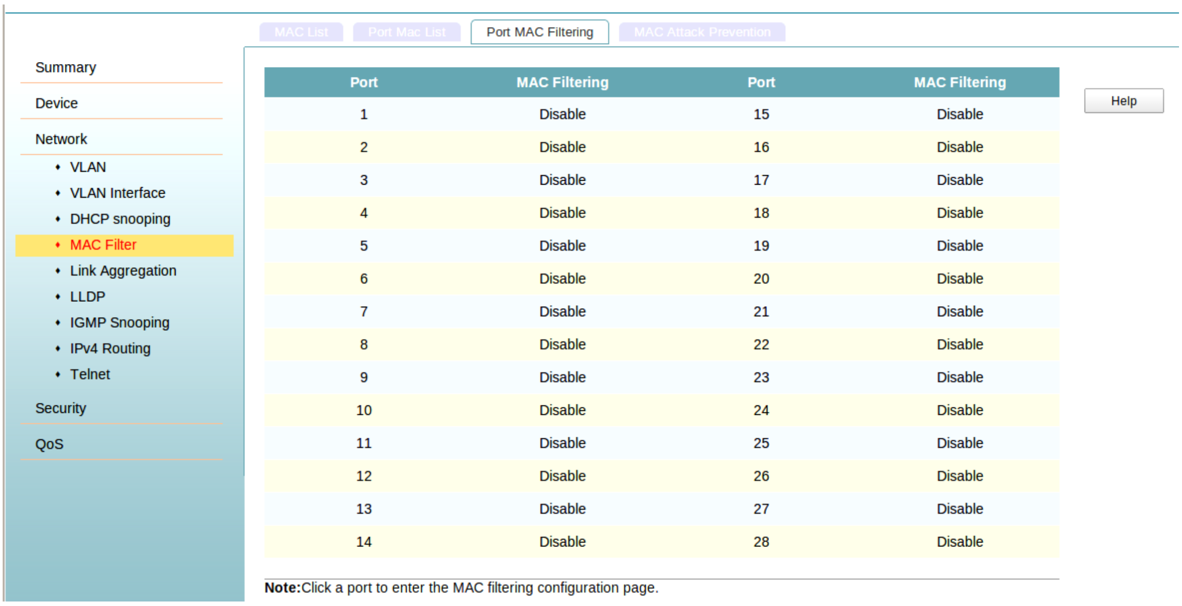
Item	Description
Bind	Add the selected unbounded MAC address to binding list.
Delete All	Delete all MAC address.
Del Selected	Delete the selected MAC address.

4.4.3 Configure a Port MAC Filtering

MAC filtering is used to control network access. Opening the MAC filtering port only allow source address for the binding of MAC address message to pass through so as to achieve the purpose of network access control.

Select Network-->MAC Filter, and click **Port** MAC Filter, as shown in Figure 4.4-4

Figure 4.4-4 Port MAC Filtering



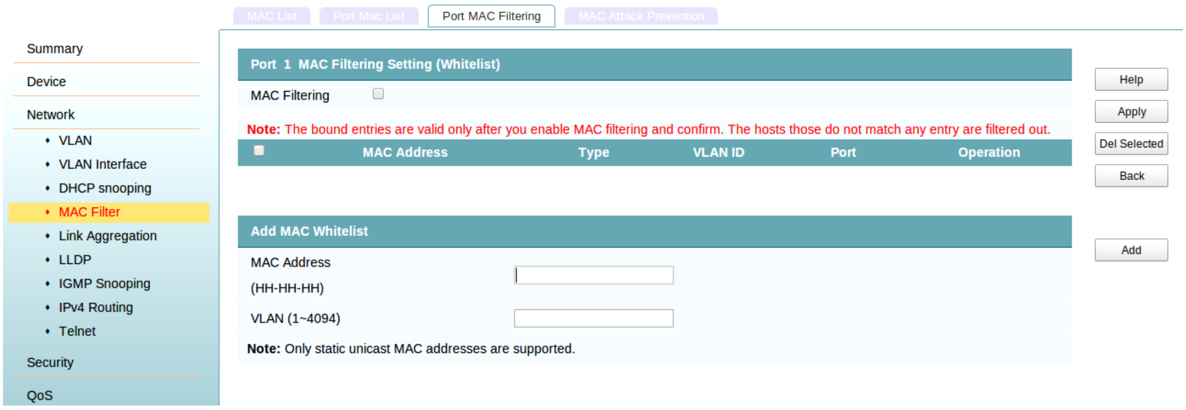
Port	MAC Filtering	Port	MAC Filtering
1	Disable	15	Disable
2	Disable	16	Disable
3	Disable	17	Disable
4	Disable	18	Disable
5	Disable	19	Disable
6	Disable	20	Disable
7	Disable	21	Disable
8	Disable	22	Disable
9	Disable	23	Disable
10	Disable	24	Disable
11	Disable	25	Disable
12	Disable	26	Disable
13	Disable	27	Disable
14	Disable	28	Disable

Note: Click a port to enter the MAC filtering configuration page.

Table 4.4-4 Port MAC Filtering items

Item	Description
Port	Corresponding to port number, click the port number for MAC filter Settings. As shown in Figure 4.4-4
MAC Filtering	Show the state of MAC filtering.

Figure 4.4-5 MAC Filter setting



Port 1 MAC Filtering Setting (Whitelist)

MAC Filtering □

Note: The bound entries are valid only after you enable MAC filtering and confirm. The hosts those do not match any entry are filtered out.

□	MAC Address	Type	VLAN ID	Port	Operation

Add MAC Whitelist

MAC Address (HH-HH-HH)

VLAN (1~4094)

Note: Only static unicast MAC addresses are supported.

Table 4.4-5 Port MAC filtering setting items

Item	Description
MAC Filtering Setting	Open/close the port MAC filtering capabilities. Only enabling this option, white list will take effect.
Add MAC Whitelist	Add a unicast static MAC addresses.

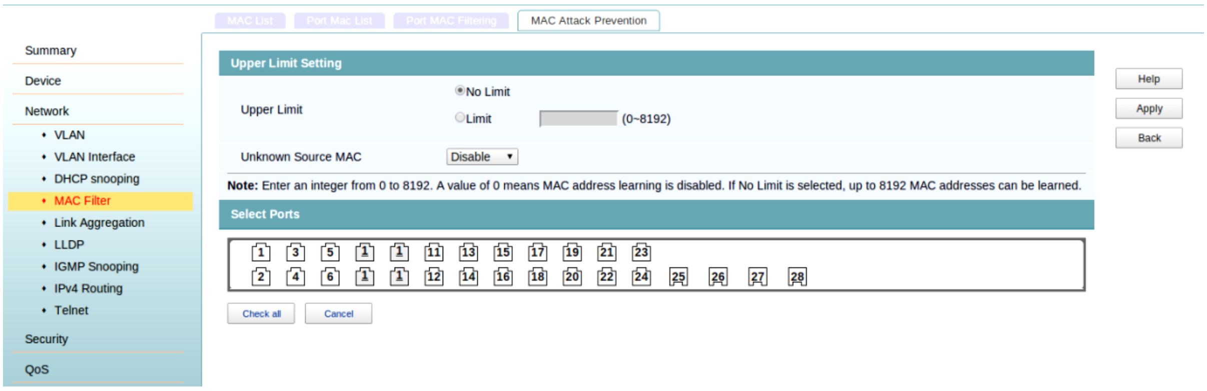
4.4.4 Configure MAC attack prevention

MAC attack prevention ability secure equipment in the local area network (LAN) learning a large number of invalid MAC, which will lower the network performance and stability.

Display the MAC address numbers for a port to learn.

Select Network-->MAC Filter, and click MAC Attack Prevention, as shown in Figure 4.4-6

Figure 4.4-6 MAC Attack Prevention



Upper Limit Setting

Upper Limit ● No Limit ○ Limit (0~8192)

Unknown Source MAC Disable

Note: Enter an integer from 0 to 8192. A value of 0 means MAC address learning is disabled. If No Limit is selected, up to 8192 MAC addresses can be learned.

Select Ports

Table 4.4-6 MAC Attack Prevention items

Item	Description
Port	Corresponding to port number, cannot be set when ports is for polymerization.
Upper Limit	Set the maximum of learned MAC address
Unknown Source MAC	Receive or discard the frame which source MAC address is not in the MAC table

4.5 Link Aggregation

Ethernet link aggregation, or simply link aggregation, combines multiple physical Ethernet ports into one logical link, called an aggregated link. Link aggregation delivers the following benefits:

- Increases bandwidth beyond the limits of any single link. In an aggregated link, traffic is distributed across the member ports.
- Improves link reliability. The member ports dynamically back up other port. When a member port fails, its traffic is automatically switched to other member ports.

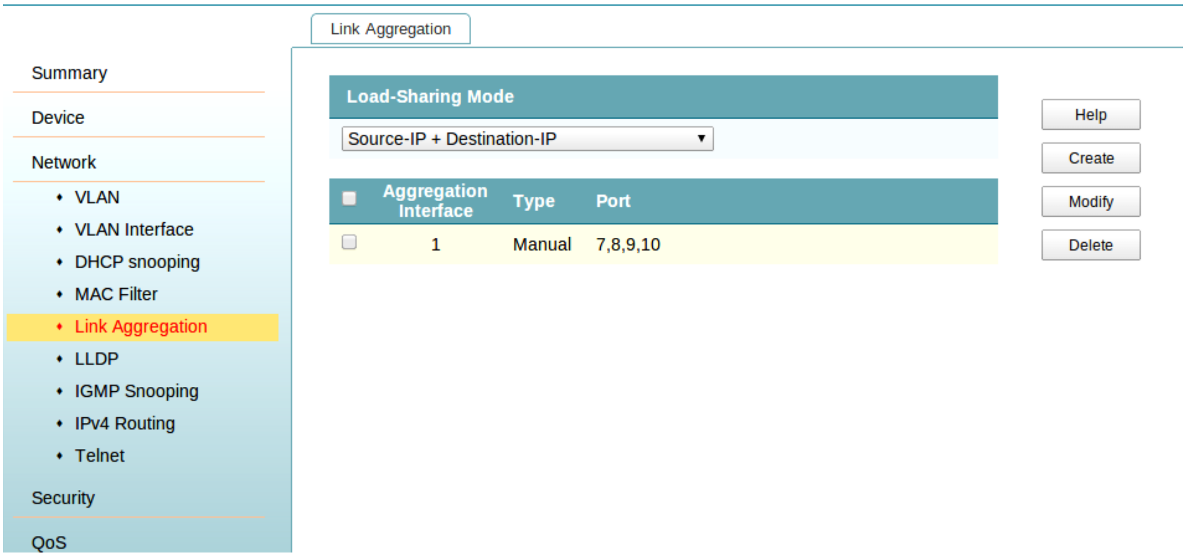
NOTE:

The device supports Layer 2 aggregation interfaces only.

4.5.1 Aggregate interface display

Select Network--> Link Aggregation, as shown in Figure 4.5-1.

Figure 4.5-1 Link aggregation



Load-Sharing Mode: Source-IP + Destination-IP

□	Aggregation Interface	Type	Port
□	1	Manual	7,8,9,10

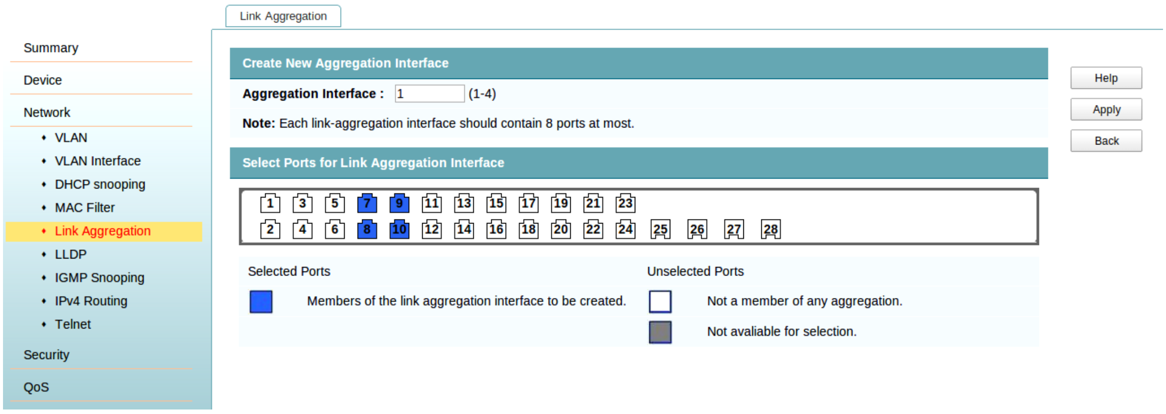
Table 4.5-1 Link aggregation

Items		Description
Load-Sharing mode	Based on the source MAC address	Port in convergence group members according to the source MAC address for load sharing.
	Based on the destination MAC address	Port group said gathering members according to the destination MAC address for load sharing.
	Based on the source MAC address and the destination MAC address	Port in convergence group members according to the source MAC address, the destination MAC address for load sharing.
	Based on the source IP address and destination IP address	Port in convergence group members according to the source IP address, destination IP address for load sharing.
Aggregation Interface		Show aggregation interface
Type		Type of aggregation
Ports		Corresponding port number.

4.5.2 Creating a link aggregation interface

Select Network -->Link Aggregation, and click Create to enter the page as shown in Figure 4.5-1.

Figure 4.5-1 Create new aggregation interface



Create New Aggregation Interface

Aggregation Interface : 1 (1-4)

Note: Each link-aggregation interface should contain 8 ports at most.

Select Ports for Link Aggregation Interface

```
1 3 5 7 9  11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28
```

Selected Ports

🟦 Members of the link aggregation interface to be created.

Unselected Ports

□ Not a member of any aggregation.

■ Not avaliable for selection.

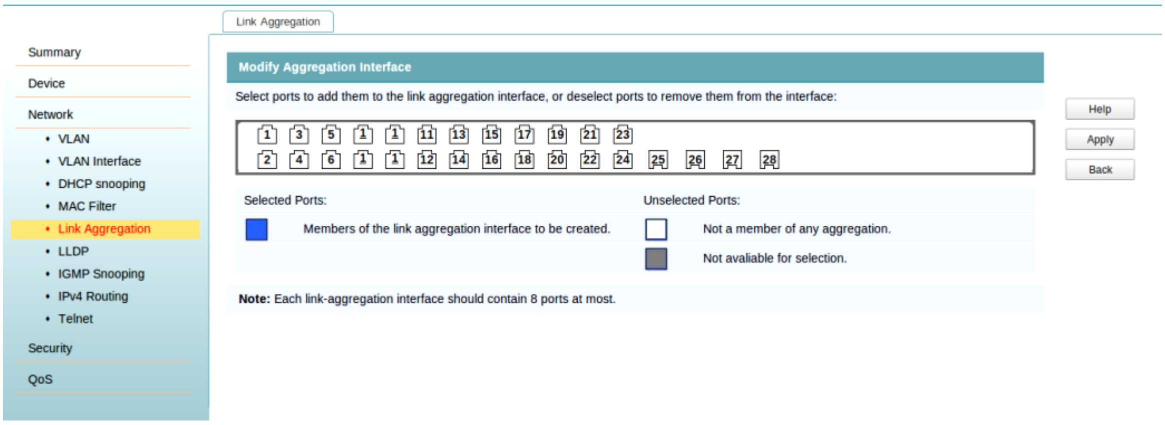
Table 4.5-2 Configuration of creating new link aggregation

Item	Description
Aggregation Interface	Assign an ID to the link aggregation interface to be created.
Select ports for the link aggregation interface	Select one or multiple ports to be assigned to the link aggregation interface from the front panel. You can view the result in the Summary list in the bottom of the page.

4.5.3 Modify the link aggregation interface

Select Network -->Link Aggregation, and click Create to enter the page as shown in Figure 4.5-3.

Figure 4.5-3 Modify Aggregation interface



Modify Aggregation Interface

Select ports to add them to the link aggregation interface, or deselect ports to remove them from the interface:

```
1 3 5 1 1 11 13 15 17 19 21 23
2 4 6 1 1 12 14 16 18 20 22 24 25 26 27 28
```

Selected Ports:

🟦 Members of the link aggregation interface to be created.

Unselected Ports:

□ Not a member of any aggregation.

■ Not avaliable for selection.

Note: Each link-aggregation interface should contain 8 ports at most.

Table 4.5-3 Link Aggregation items

Item	Description
Select ports for the link aggregation interface	Modify one or multiple ports to be assigned to the link aggregation interface from the front panel.

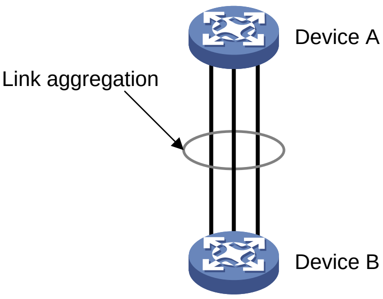
4.5.4 Link aggregation example

4.5.4.1 Network requirements

As shown in Figure 4.5-4, Switch A and Switch B are connected to each other through their Layer 2 Ethernet ports GigabitEthernet 1/0/1 and GigabitEthernet 1/0/3.

Aggregate the ports on each device to form a link aggregation group, thus balance incoming/outgoing traffic across the member ports.

Figure 4.5-4 Network diagram for static link aggregation configuration



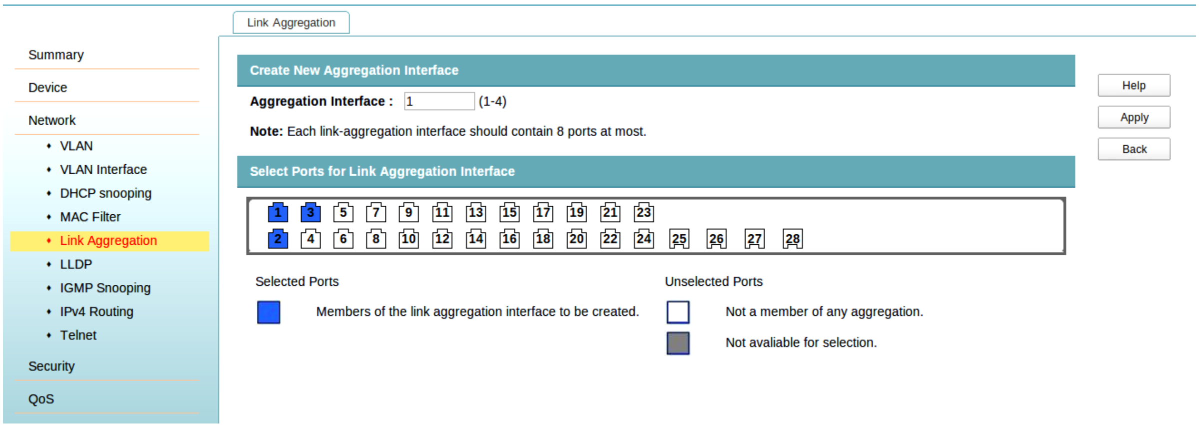
4.5.4.2 Configuration procedure

You can create a dynamic link aggregation group to achieve load balancing.

# Create dynamic link aggregation group 1.

1. Select Network-->Link Aggregation, and click Create to enter the page as shown in Figure 4.5-5.

Figure 4.5-5 Create dynamic link aggregation group



Create New Aggregation Interface

Aggregation Interface : 1 (1-4)

Note: Each link-aggregation interface should contain 8 ports at most.

Select Ports for Link Aggregation Interface

Selected Ports

■ Members of the link aggregation interface to be created.

Unselected Ports

□ Not a member of any aggregation.

▨ Not avaliable for selection.

2. Set the link aggregation interface IDas1.

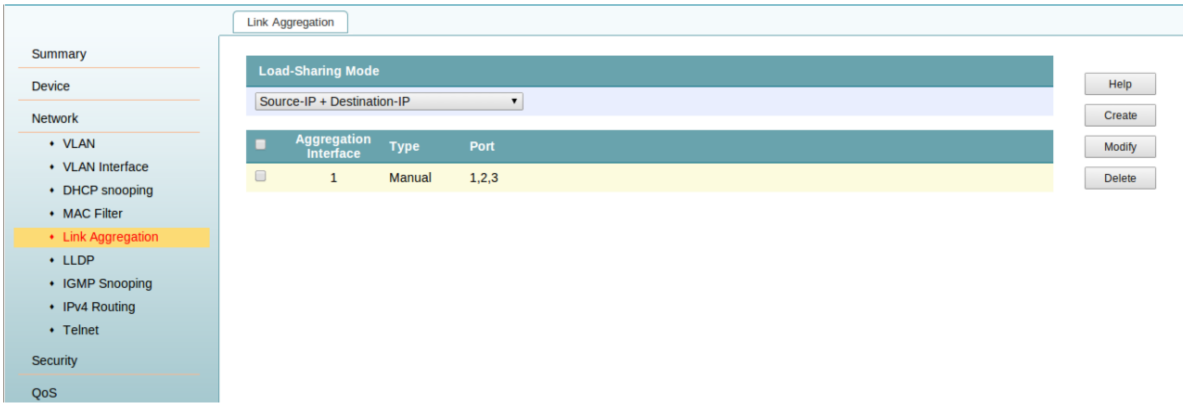
3. Select GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 on the chassis front panel.

4. Click Apply.

5. Checking configuration

6. Select Network-->Link Aggregation, as shown in Figure 4.5-6.

Figure 4.5-6 Link Aggregation



Load-Sharing Mode

Source-IP + Destination-IP

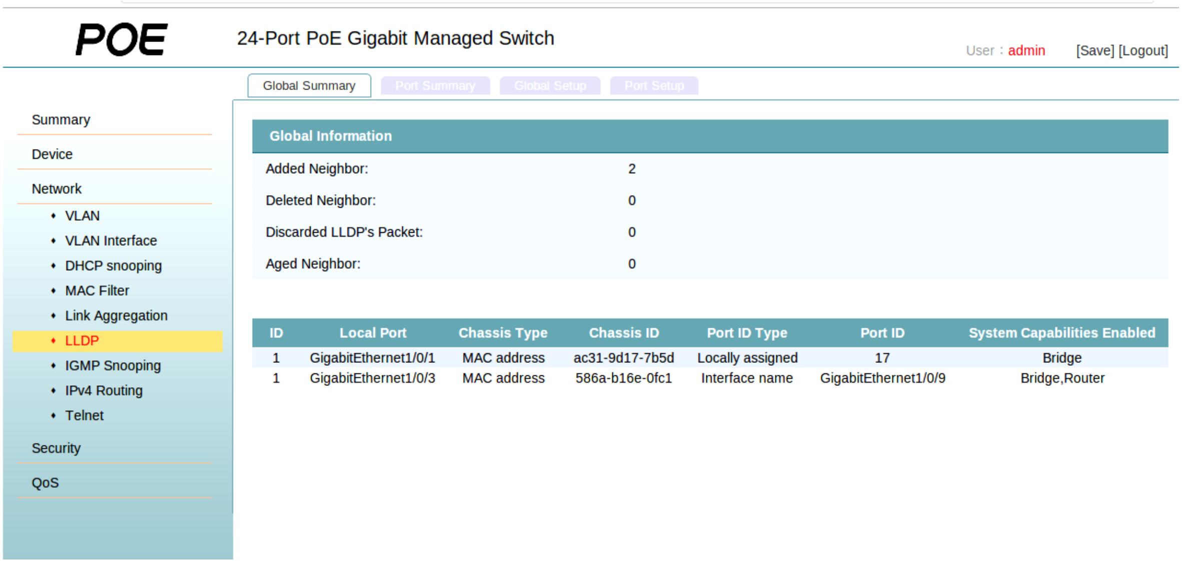
□	Aggregation Interface	Type	Port
□	1	Manual	1,2,3

4.6 LLDP

4.6.1 Global LLDP information summary

Select Network-->LLDP, and click Global Summary to display global local LLDP information and statistics, as shown in Figure 4.6-1.

Figure 4.6-1 Global Summary



Global Information

Added Neighbor:	2
Deleted Neighbor:	0
Discarded LLDP's Packet:	0
Aged Neighbor:	0

ID	Local Port	Chassis Type	Chassis ID	Port ID Type	Port ID	System Capabilities Enabled
1	GigabitEthernet1/0/1	MAC address	ac31-9d17-7b5d	Locally assigned	17	Bridge
1	GigabitEthernet1/0/3	MAC address	586a-b16e-0fc1	Interface name	GigabitEthernet1/0/9	Bridge,Router

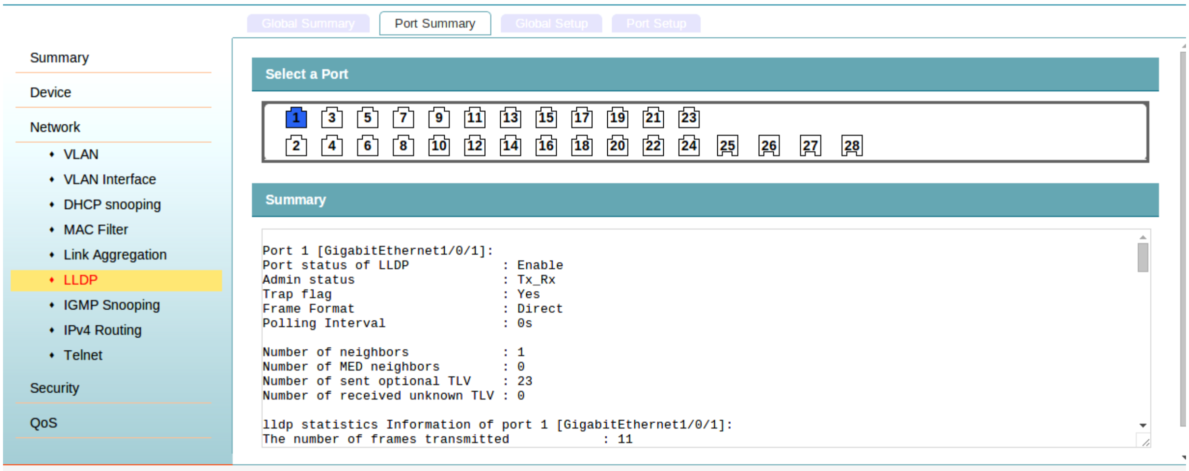
Table 4.6-1 Filed description

Item	Description
Chassis ID	The local chassis ID depending on the chassis type defined.
System capabilities enabled	The enabled network function advertised by the local device: ● Bridge ● Router

4.6.2 Displaying LLDP information for a port

Select Network-->LLDP, and click Port Summary, as shown in Figure 4.6-2.

Figure 4.6-2 Port summary



```
Port 1 [GigabitEthernet1/0/1]:
Port status of LLDP            : Enable
Admin status                   : Tx_Rx
Trap flag                      : Yes
Frame Format                   : Direct
Polling Interval               : 0s

Number of neighbors            : 1
Number of MED neighbors        : 0
Number of sent optional TLV    : 23
Number of received unknown TLV : 0

lldp statistics Information of port 1 [GigabitEthernet1/0/1]:
The number of frames transmitted            : 11
```

On the port list, select a port to display its LLDP information at the lower half of the page. The detail information is shown in Table 4.6-1 and Table 4.6-2.

Table 4.6-2 The local information

Item	Description
Port ID subtype	Port ID type: ● Interface alias ● Port component ● MAC address ● Network address ● Interface name ● Agent circuit ID ● Locally assigned—Locally-defined port ID type other than those listed above.

Item	Description
Power port class	The power over Ethernet port class: ● PSE—A power supply device. ● PD—A powered device.
Port power classification	Port power classification of the PD: ● Unknown ● Class 0 ● Class 1 ● Class 2 ● Class 3 ● Class 4
Media policy type	Available options include: ● Unknown ● Voice ● Voice signaling ● Guest voice ● Guest voice signaling ● Soft phone voice ● Videoconferencing ● Streaming video ● Video signaling
PoE PSE power source	The type of PSE power source advertised by the local device: ● Primary ● Backup
Port PSE priority	Available options include: ● Unknown—The PSE priority of the port is unknown. ● Critical—The priority level 1. ● High—The priority level 2. ● Low—The priority level 3.

Table 4.6-3 LLDP neighbor information of an LLDP-enabled port

Item	Description
Chassis type	Chassis ID type: ● Chassis component ● Interface alias ● Port component ● MAC address ● Network address ● Interface name ● Locally assigned—Local configuration.
Chassis ID	Chassis ID depending on the chassis type, which can be a MAC address of the device.
Port ID type	The port ID value.
System capabilities supported	The primary network function of the system: ● Repeater ● Bridge ● Router
System capabilities enabled	The network function enabled on the system: ● Repeater ● Bridge ● Router
Auto-negotiation supported	The support of the neighbor for auto negotiation.
Auto-negotiation enabled	The enable status of auto negotiation on the neighbor.
OperMau	Current speed and duplex mode of the neighbor.
Link aggregation supported	The neighbor supports link aggregation.
Link aggregation enabled	Link aggregation is enabled on the neighbor.
Aggregation port ID	Link aggregation group ID. It is 0 if the neighbor port is not assigned to any link aggregation group.
Maximum frame Size	The maximum frame size supported on the neighbor port.

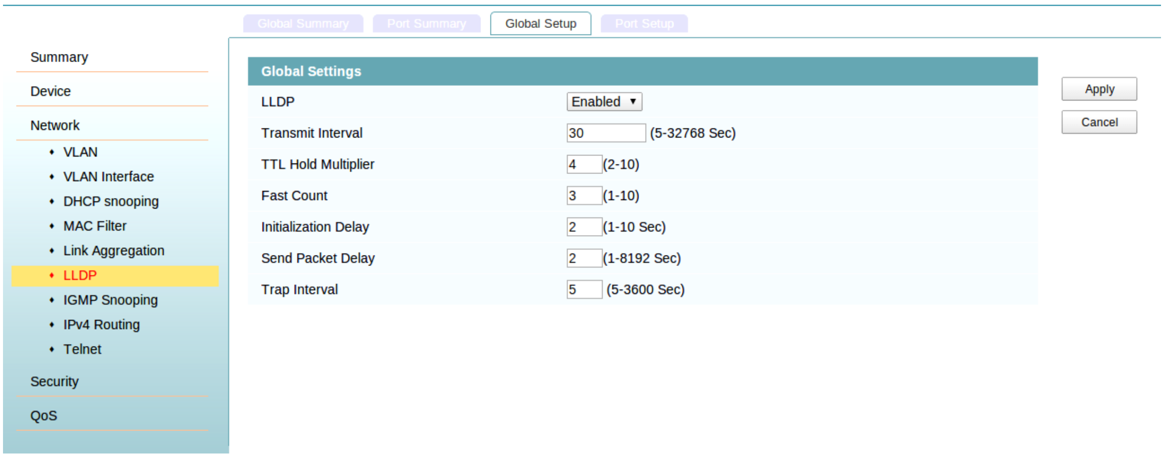
Item	Description
Device class	MED device type: • Connectivity device—An intermediate device that provide network connectivity. • Class I—a generic endpoint device. All endpoints that require the discovery service of LLDP belong to this category. • Class II—A media endpoint device. The class II endpoint devices support the media stream capabilities in addition to the capabilities of generic endpoint devices. • Class III—A communication endpoint device. The class III endpoint devices directly support end users of the IP communication system. Providing all capabilities of generic and media endpoint devices, Class III endpoint devices are used directly by end users.
Media policy type	Available options include: • Unknown • Voice • Voice signaling • Guest voice • Guest voice signaling • Soft phone voice • Videoconferencing • Streaming video • Video signaling
Unknown Policy	Indicates whether or not the media policy type is unknown.
VLAN tagged	Indicates whether or not packets of the media VLAN are tagged.
Media policy VlanID	ID of the media VLAN.
Media policy L2 priority	Layer 2 priority.
Media policy Dscp	DSCP precedence.
HardwareRev	Hardware version of the neighbor.
FirmwareRev	Firmware version of the neighbor.
SoftwareRev	Software version of the neighbor.
SerialNum	The serial number advertised by the neighbor.
Manufacturer name	The manufacturer name advertised by the neighbor.
Model name	The model name advertised by the neighbor.
Asset tracking identifier	Asset ID advertised by the neighbor. This ID is used for the purpose of inventory management and asset tracking.

Item	Description
PoE PSE power source	The type of PSE power source advertised by the neighbor: ● Primary ● Backup
Port PSE priority	Available options include: ● Unknown—The PSE priority of the port is unknown. ● Critical—The priority level 1. ● High—The priority level 2. ● Low—The priority level 3.

4.6.3 Configuring global LLDP setup

Select Network-->LLDP and click Global Setup to enter the page shown in Figure 4.6-3.

Figure 4.6-3 Global Setup



Global Settings

LLDP	Enabled ▾	
Transmit Interval	30	(5-32768 Sec)
TTL Hold Multiplier	4	(2-10)
Fast Count	3	(1-10)
Initialization Delay	2	(1-10 Sec)
Send Packet Delay	2	(1-8192 Sec)
Trap Interval	5	(5-3600 Sec)

Table 4.6-4 Global LLDP setup configuration

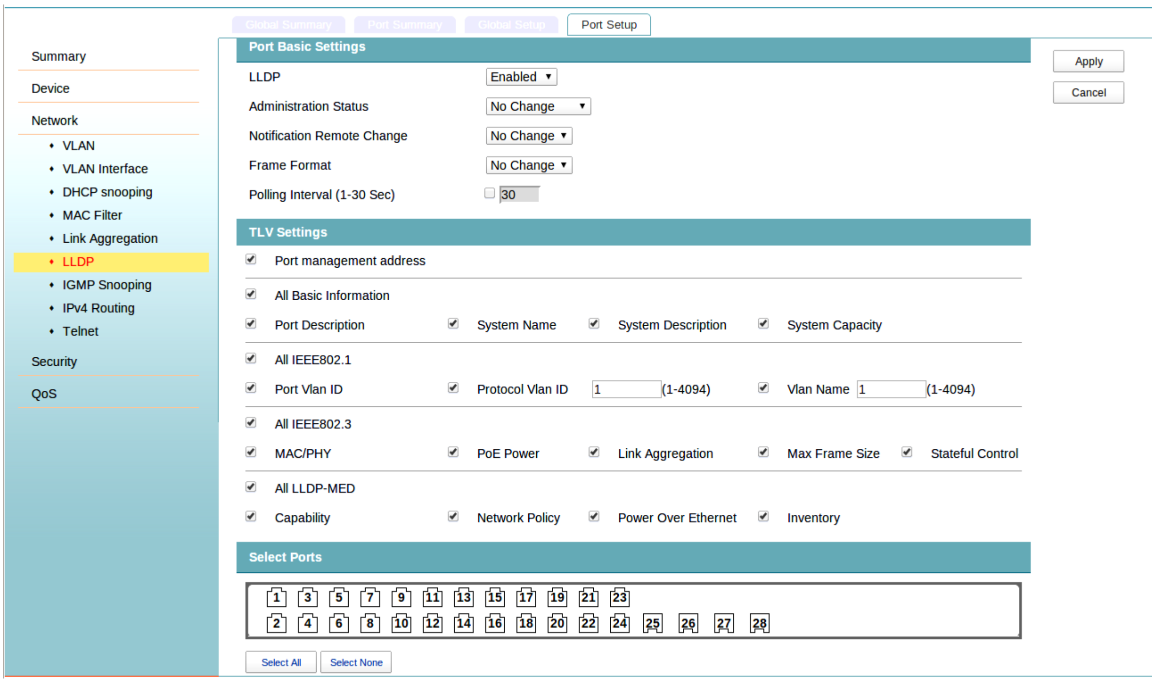
Item	Description
LLDP	Enable or disable global LLDP.
Transmit Interval	Set transmit interval.

Item	Description
TTL Hold Multiplier	Set TTL multiplier. The TTL TLV carried in an LLDPDU determines how long the device information carried in the LLDPDU can be saved on a recipient device. You can configure the TTL of locally sent LLDPDUs to determine how long information about the local device can be saved on a neighbor device by setting the TTL multiplier. The TTL is expressed as *TTL multiplier* × *LLDPDU transit interval*. ⓘIMPORTANT: ● If the product of the TTL multiplier and the LLDPDU transmit interval is greater than 65535, the TTL carried in transmitted LLDPDUs takes 65535 seconds. ● As the maximum TTL allowed by CDP is 255 seconds, please ensure the product of the TTL multiplier and the LLDPDU transmit interval is less than 255 seconds for CDP-compatible LLDP to work properly with Cisco IP phones.
Fast Count	Set the number of LLDPDUs sent each time fast LLDPDU transmission is triggered.
Initialization Delay	Set initialization delay for LLDP-enabled ports. Each time the LLDP operating mode of a port changes, its LLDP protocol state machine re-initializes. To prevent LLDP from being initialized too frequently at times of frequent operating mode change, initialization delay is introduced. With this delay mechanism, a port must wait for the specified interval before it can initialize LLDP after the LLDP operating mode changes.
Send Packet Delay	Set LLDPDU transmit delay. With LLDP enabled, a port advertises LLDPDUs to its neighbors both periodically and when the local configuration changes. To avoid excessive number of LLDPDUs caused by frequent local configuration changes, an LLDPDU transmit delay is introduced. Thus, after sending an LLDPDU, the port must wait for the specified interval before it sends another one. ⓘIMPORTANT: LLDPDU transmit delay must be less than the TTL to ensure the LLDP neighbors can receive LLDPDUs to update information about the device you are configuring before it is aged out.
Trap Interval	Set the minimum interval for sending traps. With the LLDP trapping function enabled on a port, traps are sent out the port to advertise the topology changes detected over the trap interval to neighbors. By tuning this interval, you can prevent excessive traps from being sent when topology is instable.

4.6.4 Configuring LLDP settings on ports

Select Network-->LLDP, and click Port Setup, as shown in Figure 4.6-4.You can configure LLDP settings on ports individually or in batch.

Figure 4.6-4 Port Setup



Port Basic Settings

LLDP: Enabled

Administration Status: No Change

Notification Remote Change: No Change

Frame Format: No Change

□ Polling Interval (1-30 Sec): 30

TLV Settings

☑ Port management address

☑ All Basic Information

☑ Port Description ☑ System Name ☑ System Description ☑ System Capacity

☑ All IEEE802.1

☑ Port Vlan ID ☑ Protocol Vlan ID 1 (1-4094) ☑ Vlan Name 1 (1-4094)

☑ All IEEE802.3

☑ MAC/PHY ☑ PoE Power ☑ Link Aggregation ☑ Max Frame Size ☑ Stateful Control

☑ All LLDP-MED

☑ Capability ☑ Network Policy ☑ Power Over Ethernet ☑ Inventory

Select Ports

1 3 5 7 9 11 13 15 17 19 21 23

2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28

Table 4.6-5 Basic Settings for port

Item		Description
Basic Settings	LLDP	Enable or disable LLDP.
	Administration Status	Set the LLDP operating mode on the port or ports you are configuring: ● TxRx—Sends and receives LLDPDUs. ● Tx—Sends but not receives LLDPDUs. ● Rx—Receives but not sends LLDPDUs ● Disable—Neither sends nor receives LLDPDUs.
	Notification Remote Change	Enable or disable remote notification.

Item		Description
	Frame Format	Set the encapsulation for LLDPDUs: ● ETHII—Encapsulates outgoing LLDPDUs in Ethernet II frames and processes an incoming LLDPDU only if its encapsulation is Ethernet II. ● SNAP—Encapsulates outgoing LLDPDUs in Ethernet II frames and processes an incoming LLDPDU only if its encapsulation is Ethernet II. IMPORTANT: LLDP-CDP PDUs use only SNAP encapsulation.
	Polling Interval	Enable LLDP polling and set the polling interval. If no polling interval is set, LLDP polling is disabled. With the polling mechanism, LLDP periodically detects local configuration changes. If a configuration change is detected, an LLDPDU is sent to inform the LLDP neighbors of the change.

Table 4.6-6 TLV Settings items

Item		**Description**
Port management address setting		Select to include the management address TLV in transmitted LLDPDUs and in addition, set the management address and its format (a numeric or character string in the TLV). If no management address is specified, the main IP address of the lowest VLAN carried on the port is used. If no main IP address is assigned to the VLAN, 127.0.0.1 is used.
All Basic Information setting	Port Description	Select to include the port description TLV in transmitted LLDPDUs.
	System Name	Select to include the system name TLV in transmitted LLDPDUs.
	System Description	Select to include the system description TLV in transmitted LLDPDUs.
	System Capabilities	Select to include the system capabilities TLV in transmitted LLDPDUs.
All IEEE802.1 setting	Port VLAN ID	Select to include the PVID TLV in transmitted LLDPDUs.
	Protocol VLAN ID	Select to include port and protocol VLAN ID TLVs in transmitted LLDPDUs and specify the VLAN IDs to be advertised. If no VLAN is specified, the lowest protocol VLAN ID is transmitted.
	VLAN Name	Select to include VLAN name TLVs in transmitted LLDPDUs and specify the VLAN IDs to be advertised. If no VLAN is specified, the lowest VLAN carried on the port is advertised.
All IEE802.3 setting	MAC/PHY Configuration/Status	Select to include the MAC/PHY configuration/status TLV in transmitted LLDPDUs.

Item		Description
	POE Power	Select to include the POE power TLV in transmitted LLDPDUs.
	Link Aggregation	Select to include the link aggregation TLV in transmitted LLDPDUs.
	Maximum Frame Size	Select to include the maximum frame size TLV in transmitted LLDPDUs.
	Stateful Control	Select to include the state control TLV in transmitted LLDPDUs
ALL LLDP-MED Setting	Capabilities	Select to include the LLDP-MED capabilities TLV in transmitted LLDPDUs.
	Network Policy	Select to include the network policy TLV in transmitted LLDPDUs.
	Power Over Ethernet	Select to include the extended POEI TLV in transmitted LLDPDUs.
	Inventory	Select to include the hardware revision TLV, firmware revision TLV, software revision TLV, serial number TLV, manufacturer name TLV, model name TLV and asset ID TLV in transmitted LLDPDUs.

4.6.5 Configuration guidelines

When configuring LLDP, follow these guidelines:

To make LLDP take effect, you must enable it both globally and on ports.

When selecting TLVs to send in LLDPDUs, note the following:

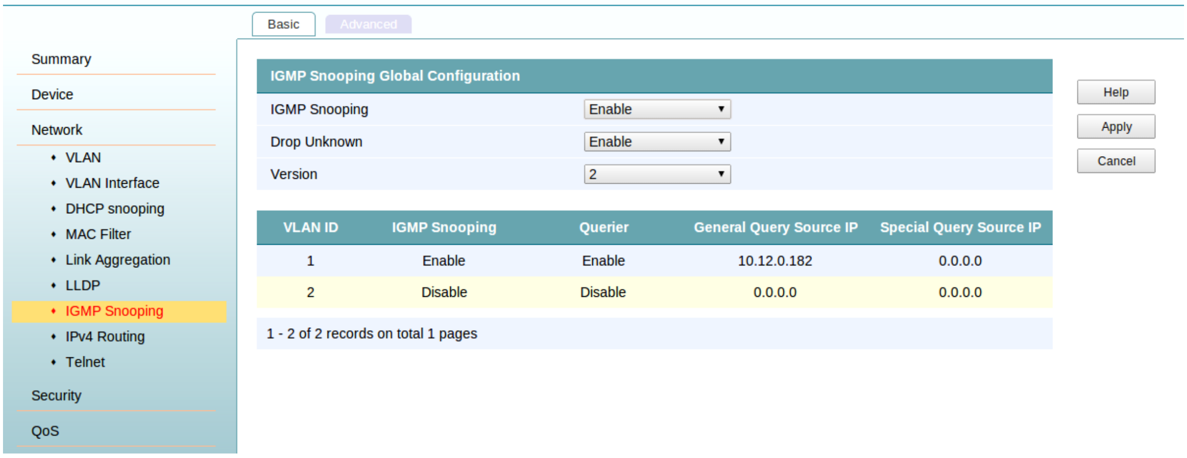
- To advertise LLDP-MED TLVs, you must include the LLDP-MED capabilities set TLV.
- To remove the LLDP-MED capabilities set TLV, you must remove all other LLDP-MED TLVs.
- To remove the MAC/PHY configuration TLV, remove the LLDP-MED capabilities set TLV first.
- If the LLDP-MED capabilities set TLV is included, the MAC/PHY configuration/status TLV is included automatically.

4.7 IGMP Snooping

4.7.1 Enabling IGMP snooping globally

Select Network -->IGMP Snooping to enter the basic configuration page shown in Figure 4.7-1.

Figure 4.7-1 Basic IGMP snooping configurations



IGMP Snooping Global Configuration

IGMP Snooping	Enable
Drop Unknown	Enable
Version	2

VLAN ID	IGMP Snooping	Querier	General Query Source IP	Special Query Source IP
1	Enable	Enable	10.12.0.182	0.0.0.0
2	Disable	Disable	0.0.0.0	0.0.0.0

1 - 2 of 2 records on total 1 pages

Table 4.7-1 IGMP snooping configuration items

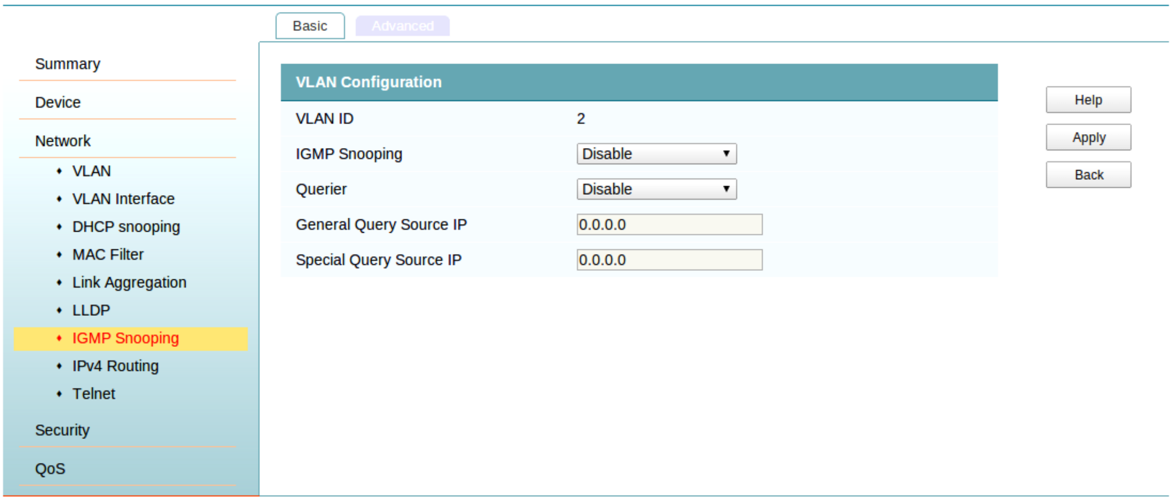
Item	Description
IGMP snooping	Globally enable or disable IGMP snooping.
Drop Unknown	Enable or disable the function of dropping unknown multicast packets. Unknown multicast data refer to multicast data for which no entries exist in the IGMP snooping forwarding table. ● With the function of dropping unknown multicast data enabled, the switch drops all the received unknown multicast data. ● With the function of dropping unknown multicast data disabled, the switch floods unknown multicast data in the VLAN to which the unknown multicast data belong.
Version	By configuring an IGMP snooping version, you actually configure the versions of IGMP messages that IGMP snooping can process. ● IGMP snooping version 2 can process IGMPv1 and IGMPv2 messages, but not IGMPv3 messages, which will be flooded in the VLAN. ● IGMP snooping version 3 can process IGMPv1, IGMPv2, and IGMPv3 messages.

4.7.2 Configuring IGMP snooping in a VLAN

Select Network -->IGMP Snooping to enter the basic configuration page shown in Figure 4.7-1.

Select VLAN ID corresponding to the VLAN to enter the page you can configure IGMP snooping in the VLAN, as shown in Figure 4.7-2.

Figure 4.7-2 VLAN configuration



VLAN Configuration

VLAN ID	2
IGMP Snooping	Disable
Querier	Disable
General Query Source IP	0.0.0.0
Special Query Source IP	0.0.0.0

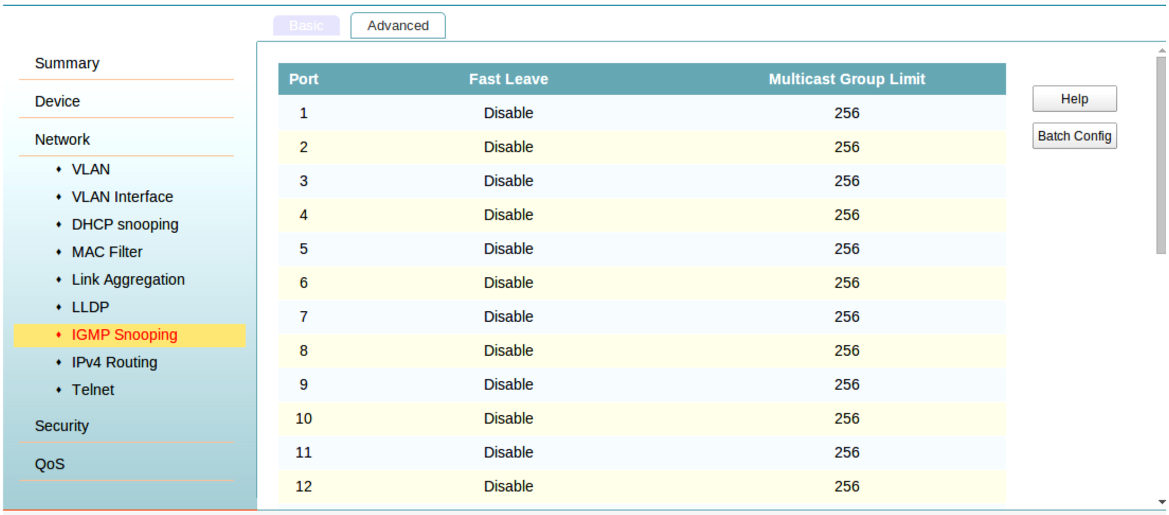
Table 4.7-2 Configuring IGMP snooping in a VLAN

Item	**Description**
VLAN ID	Displays the ID of the VLAN to be configured.
IGMP Snooping	Enable or disable IGMP snooping in the VLAN. You can proceed with the subsequent configurations only if Enable is selected here.
Querier	Enable or disable the IGMP snooping querier function. On a network without Layer 3 multicast devices, no IGMP querier-related function can be implemented because a Layer 2 device does not support IGMP. To address this issue, please enable IGMP snooping querier on a Layer 2 device so that the device can generate and maintain multicast forwarding entries at data link layer, thereby implementing IGMP querier-related functions.
General Query Source IP	Specify the source IP address of general queries. HP recommends you to configure a non-all-zero IP address as the source IP address of IGMP queries.
Special Query Source IP	Specify the source IP address of group-specific queries. HP recommends you to configure a non-all-zero IP address as the source IP address of IGMP queries

4.7.3 Display IGMP snooping port functions

Select Network -->IGMP Snooping to enter the basic configuration page and then click Advanced to enter the page shown in Figure 4.7-3.

Figure 4.7-3 Display port information

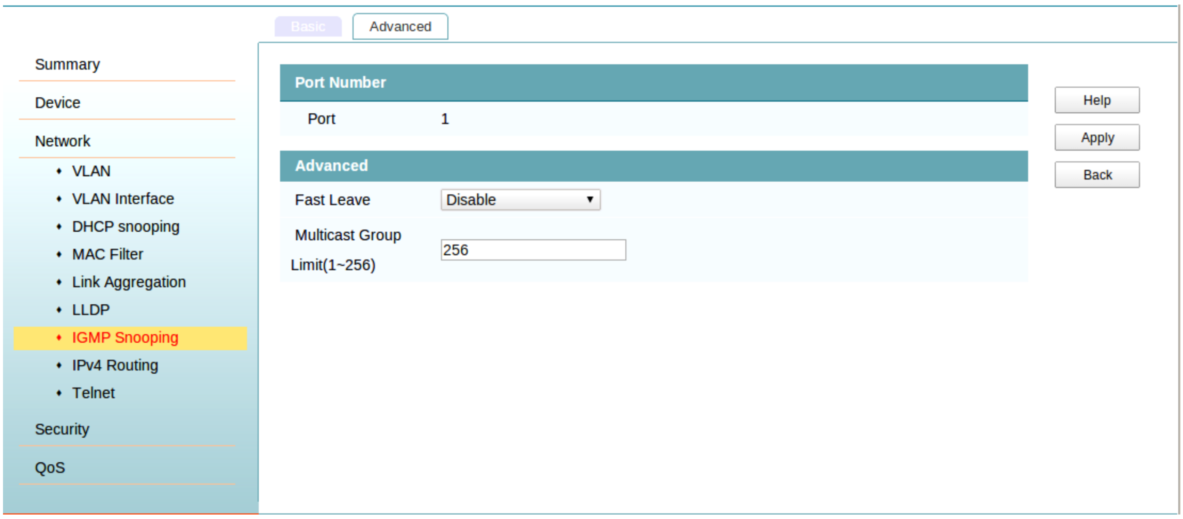


Port	Fast Leave	Multicast Group Limit
1	Disable	256
2	Disable	256
3	Disable	256
4	Disable	256
5	Disable	256
6	Disable	256
7	Disable	256
8	Disable	256
9	Disable	256
10	Disable	256
11	Disable	256
12	Disable	256

4.7.4 Configuring IGMP snooping port

Select Network -->IGMP Snooping to enter the basic configuration page and then click Advanced, and select the port to enter the page shown in Figure 4.7-4. Of course, you can also refer to the configuration select the Batch Config tab as shown Figure 4.7-5.

Figure 4.7-4 Advanced configuration



Port Number

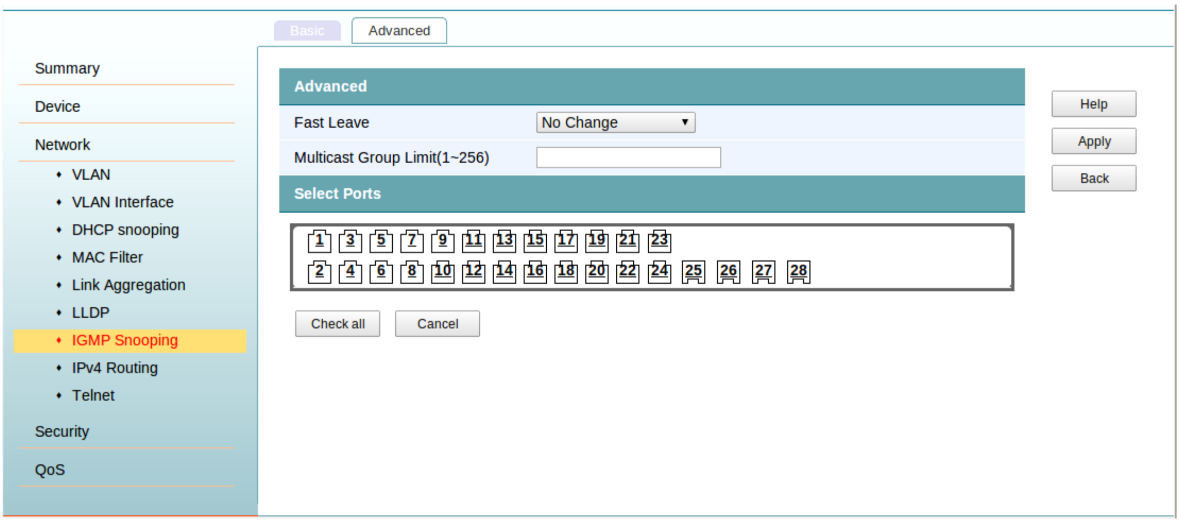
Port 1

Advanced

Fast Leave: Disable

Multicast Group Limit(1~256): 256

Figure 4.7-5 Batch configuration



Advanced

Fast Leave: No Change

Multicast Group Limit(1~256):

Select Ports

1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28

Table 4.7-3 Configuration for advanced IGMP snooping features

Item	Description
Port	Select the port on which advanced IGMP snooping features are to be configured. The port can be an Ethernet port or Layer-2 aggregate port. After a port is selected, advanced features configured on this port are displayed at the lower part of this page. ⓘIMPORTANT: Advanced IGMP snooping features configured on a Layer 2 aggregate port do not interfere with features configured on its member ports, nor do they take part in aggregation calculations; features configured on a member port of the aggregate group will not take effect until it leaves the aggregate group
Fast Leave	Enable or disable the fast leave function for the port. With the fast leave function enabled on a port, the switch, when receiving an IGMP leave message on the port, immediately deletes that port from the outgoing port list of the corresponding forwarding table entry. Then, when receiving IGMP group-specific queries for that multicast group, the switch does not forward them to that port. In VLANs where only one host is attached to each port, the fast leave function helps improve bandwidth and resource usage. ⓘIMPORTANT: If fast leave is enabled for a port to which more than one host is attached, when one host leaves a multicast group, the other hosts listening to the same multicast group fails to receive multicast data.

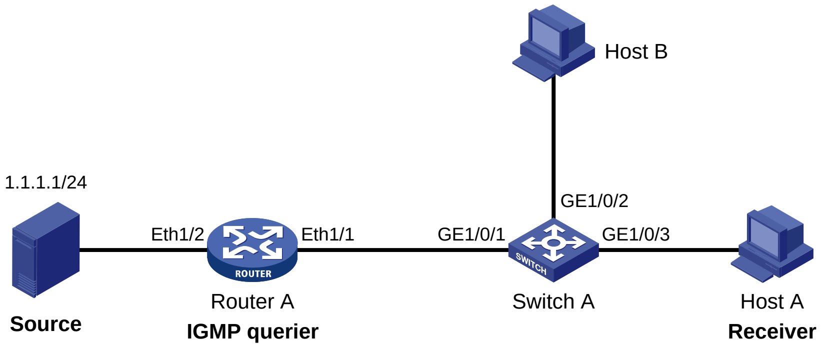
Item	Description
Group Limit	Configure the maximum number of multicast groups that the port can join. With this feature, you can regulate multicast traffic on the port. ❗IMPORTANT: When the number of multicast groups a port has joined reaches the configured threshold, the system deletes all the forwarding entries persistent on that port from the IGMP snooping forwarding table, and the hosts on this port need to join the multicast groups again.

4.7.5 IGMP snooping configuration example

4.7.5.1 Network requirements

- As shown in Figure 4.7-6, Router A connects to a multicast source (Source) through Ethernet 1/2, and to Switch A through Ethernet 1/1.
- The multicast source sends multicast data to group 224.1.1.1. Host A is a receiver of the multicast group.
- IGMPv2 runs on Router A and IGMP snooping version 2 runs on Switch A.
- The function of dropping unknown multicast packets is enabled on Switch A to prevent Switch A from flooding multicast packets in the VLAN if no corresponding Layer 2 forwarding entry exists.
- The fast leave function is enabled for Gigabit Ethernet 1/0/3 on Switch A to improve bandwidth and resource usage.

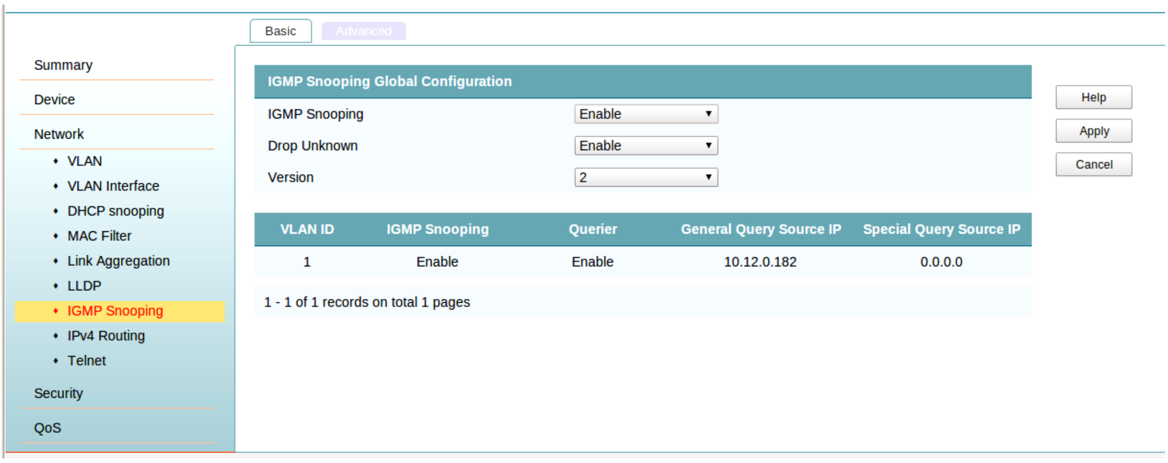
Figure 4.7-6 Network diagram for IGMP snooping configuration



4.7.5.2 Configuration procedure

1. Select Network -->IGMP snooping to enter the basic configuration page as shown in Figure 4.7-7.

Figure 4.7-7 Enable IGMP snooping globally



IGMP Snooping Global Configuration

IGMP Snooping: Enable

Drop Unknown: Enable

Version: 2

VLAN ID	IGMP Snooping	Querier	General Query Source IP	Special Query Source IP
1	Enable	Enable	10.12.0.182	0.0.0.0

1 - 1 of 1 records on total 1 pages

2. Select Enable in the column of “IGMP Snooping”

3. Select Enable in the column of “Drop Unknown”.

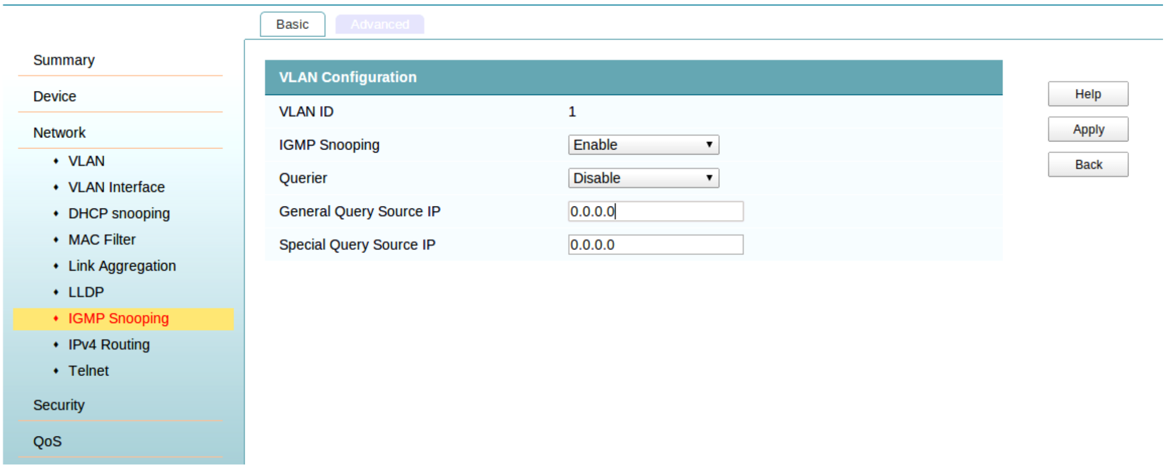
4. Select 2 for IGMP Version.

5. Click Apply.

# In VLAN 1, enable IGMP snooping .

1. Click VLAN ID corresponding to VLAN 1 to enter its configuration page and perform the following configurations, as shown in Figure 4.7-8.

Figure 4.7-8 Configure IGMP snooping in the VLAN



VLAN Configuration

VLAN ID	1
IGMP Snooping	Enable
Querier	Disable
General Query Source IP	0.0.0.0
Special Query Source IP	0.0.0.0

2. Select Enable in the column of IGMP snooping .

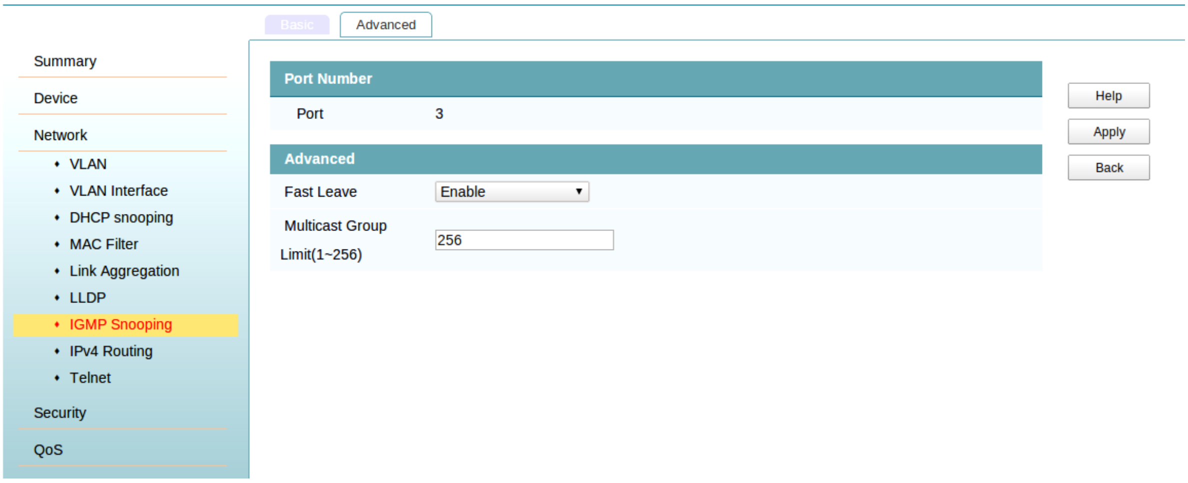
3. Select Disable in the column of Querier.

4. Click Apply

# Enable the fast leave function for Gigabit Ethernet 1/0/3.

1. Click Advanced, as shown in Figure 4.7-9.

Figure 4.7-9 Configure IGMP snooping on Gigabit Ethernet 1/0/3



Port Number

Port	3

Advanced

Fast Leave	Enable
Multicast Group Limit(1~256)	256

2. Select Gigabit Ethernet 1/0/3from the Port drop-down list.

3. Select Enable in the column of Fast Leave.

4. Click Apply to complete the operation.

4.8 IPv4 Routing

Static routes are manually configured. If a network’s topology is simple, only need to configure static routes for the network to work properly. The proper configuration and usage of static routes can improve network performance and ensure bandwidth for important network applications.

The disadvantage of using static routes is that they cannot adapt to network topology changes. If a fault or a topological change occurs in the network, the routes will be unreachable. The network administrator has to modify the static routes manually.

While configuring a static route, specify either the output interface or the next hop address as needed. The next hop address cannot be a local interface IP address; otherwise, the route configuration will not take effect.

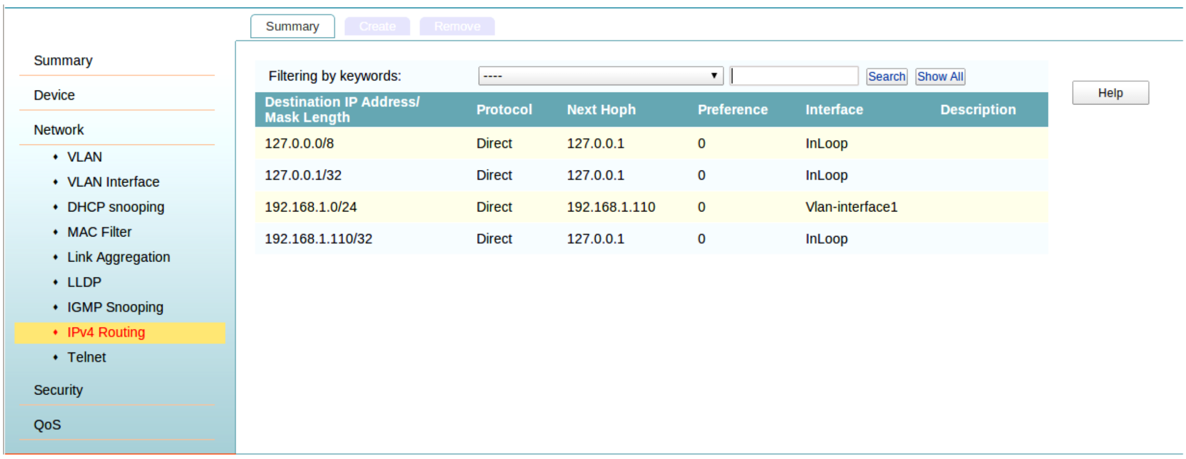
It is necessary to identify next hop addresses for all route entries because the router needs to use the next hop address of a matching entry to resolve the corresponding link layer address.

4.8.1 The IPv4 active route summary information

The page for viewing of an effective IP routing table of all the items, including manual configuration and effect of static routing and background issued by the default route.

Select Network --> IPv4 Routing to enter the page shown in Figure 4.8-1.

Figure 4.8-1 Active route table



Filtering by keywords: ----

Destination IP Address/ Mask Length	Protocol	Next Hoph	Preference	Interface	Description
127.0.0.0/8	Direct	127.0.0.1	0	InLoop	
127.0.0.1/32	Direct	127.0.0.1	0	InLoop	
192.168.1.0/24	Direct	192.168.1.110	0	Vlan-interface1	
192.168.1.110/32	Direct	127.0.0.1	0	InLoop	

Table 4.8-1 Description of the fields of the active route table

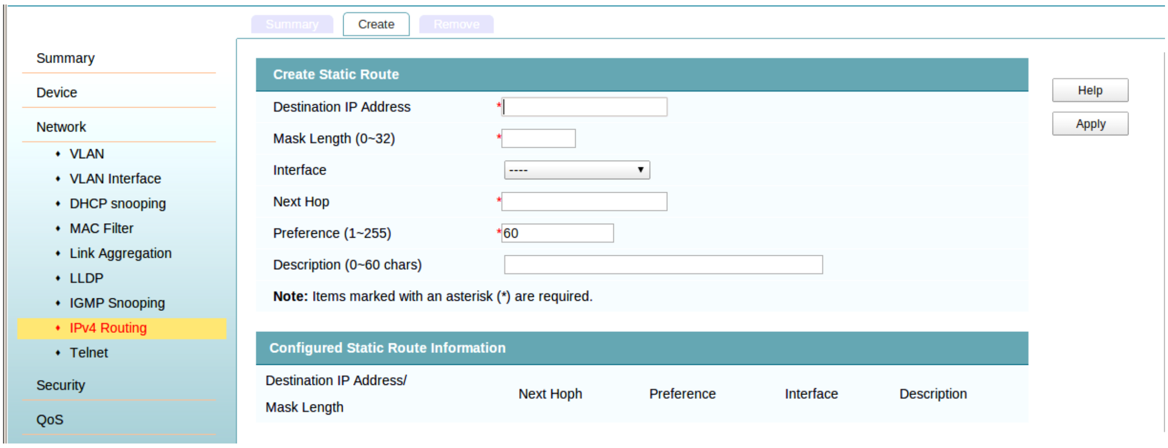
Field	Description
Destination IP Address/ Mask Length	Destination IP address of the route/ Mask length of the destination IP address

Field	Description
Protocol	Protocol that discovered the route
Next Hop	Next hop IP address of the route
Preference	Preference value for the route The smaller the number, the higher the preference.
Interface	Output interface of the route. Packets destined for the destination IP address will be forwarded out the interface.
Description	Description of the destination IP address.

4.8.2 Creating an IPv4 static route

Select Network --> IPv4 Routing and click Create to enter IPv4 static route configuration page, as shown in Figure 4.8-2.

Figure 4.8-2 Create an IPv4 static route



Create Static Route

Destination IP Address	*
Mask Length (0~32)	*
Interface	----
Next Hop	*
Preference (1~255)	*60
Description (0~60 chars)	

Note: Items marked with an asterisk (*) are required.

Configured Static Route Information

Destination IP Address/ Mask Length	Next Hoph	Preference	Interface	Description

Table 4.8-2 IPv4 static route configuration items

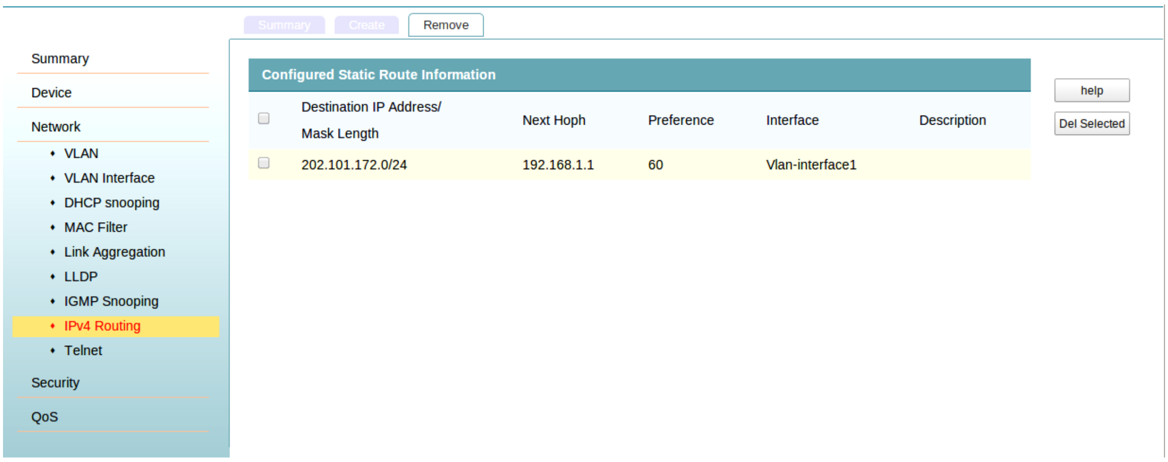
Item	Description
Destination IP Address	Type the destination IP address of the static route, in dotted decimal notation.
Mask Length	Specify the mask of the destination IP address. Type in the length of the mask.
Interface	Select the output interface. You can select any available interface, for example, a virtual interface, of the device. If select NULL 0, the destination IP address is unreachable.
Next Hop	Type the next hop IP address, in dotted decimal notation.
Preference	To add a static routing priority. For different static routing, can be configured with different priority, which is more flexible for routing management.

Item	Description
Next Hop	Type the next hop IP address, in dotted decimal notation.
Description	Add description for static routing, the default is empty

4.8.3 Remove an IPv4 static route

Select Network --> IPv4 Routing and click Create to enter the IPv4 static route configuration page, as shown in Figure 4.8-3.

Figure 4.8-3 Remove an IPv4 static route



Configured Static Route Information

□	Destination IP Address/ Mask Length	Next Hoph	Preference	Interface	Description
□	202.101.172.0/24	192.168.1.1	60	Vlan-interface1	

Table 4.8-3 IPv4 static route configuration items

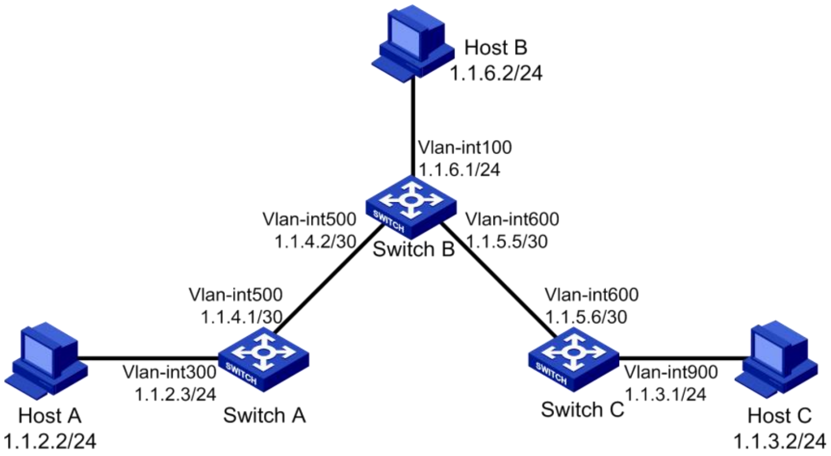
Item	Description
Select All	Select all the static routing entries in the table
Select None	Uncheck all has been selected in the table of static routing table entry
Delete	Delete all selected static routing table entry

4.8.4 Static route configuration example

4.8.4.1 Network requirements

The IP addresses of devices are shown in Figure 4.8-4. Configure IPv4 static routes on Switch A, Switch B, and Switch C so that any two hosts can communicate with each other.

Figure 4.8-4 Network diagram for IPv4 static route configuration



4.8.4.2 Configuration outlines

Table 1 On Switch A, configure a default route with Switch B as the next hop.

Table 2 On Switch B, configure one static route with Switch A as the next hop and the other with Switch C as the next hop.

Table 3 On Switch C, configure a default route with Switch B as the next hop.

Table 4 Configure the IP addresses of the interfaces (omitted)

Table 5 Configure IPv4 static routes

4.8.4.3 Configuration procedure

# Configure a default route to Switch B on Switch A.

1. Select Network --> IPv4 Routing from the navigation tree of Switch A, and then click the Create tab to enter the page shown in Figure 4.8-5.

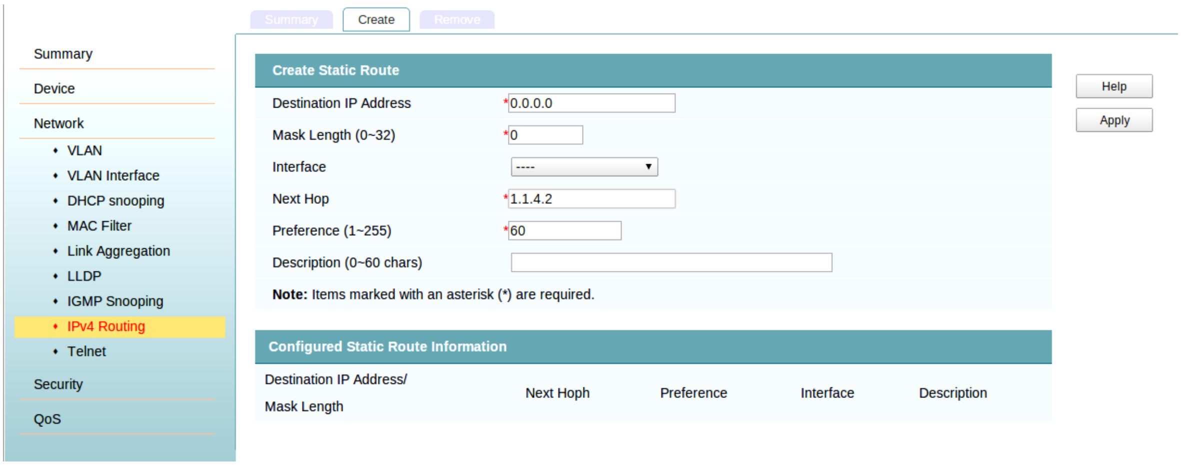
2. Type 0.0.0.0 for Destination IP Address.

3. Select 0 (0.0.0.0) from the Mask drop-down list.

4. Type 1.1.4.2 for Next Hop.

5. Click Apply.

Figure 4.8-5 Configure a default route



Create Static Route

Destination IP Address	*0.0.0.0
Mask Length (0~32)	*0
Interface	----
Next Hop	*1.1.4.2
Preference (1~255)	*60
Description (0~60 chars)	

Note: Items marked with an asterisk (*) are required.

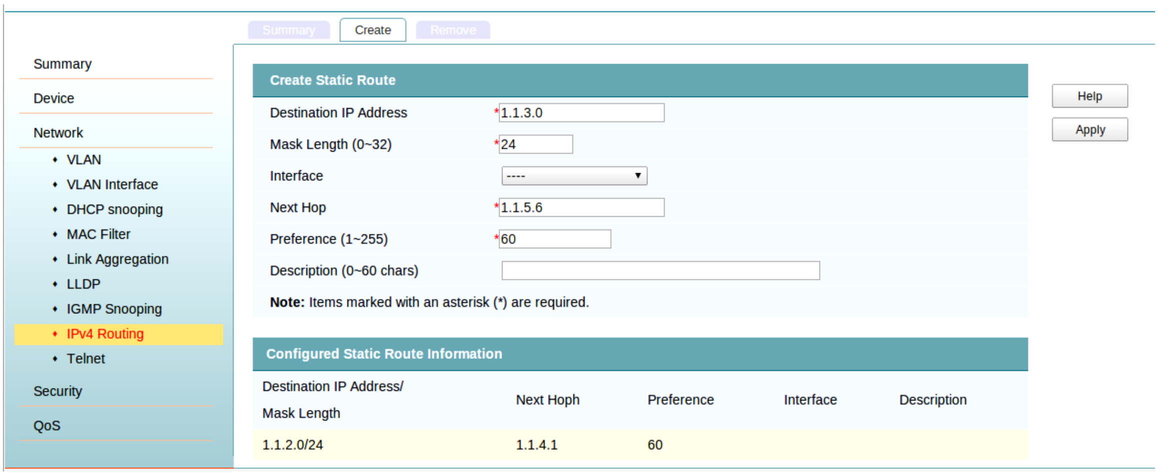
Configured Static Route Information

Destination IP Address/ Mask Length	Next Hoph	Preference	Interface	Description

# Configure a static route to Switch A and Switch C respectively on Switch B.

1. Select Network --> IPv4 Routing from the navigation tree of Switch B, and then click the Create tab to enter the page shown in Figure 4.8-6.
2. Type 1.1.2.0 for Destination IP Address.
3. Select 24 (255.255.255.0) from the Mask drop-down list.
4. Type 1.1.4.1 for Next Hop.
5. Click Apply.
6. Type 1.1.3.0 for Destination IP Address.
7. Select 24 (255.255.255.0) from the Mask drop-down list.
8. Type 1.1.5.6 for Next Hop.
9. Click Apply.

Figure 4.8-6 Configure a static route



Create Static Route

Destination IP Address	*1.1.3.0
Mask Length (0~32)	*24
Interface	----
Next Hop	*1.1.5.6
Preference (1~255)	*60
Description (0~60 chars)	

Note: Items marked with an asterisk (*) are required.

Configured Static Route Information

Destination IP Address/ Mask Length	Next Hoph	Preference	Interface	Description
1.1.2.0/24	1.1.4.1	60		

# Configure a default route to Switch B on Switch C.

1. Select Network --> IPv4 Routing from the navigation tree of Switch C, and then click the Create tab to enter the page as shown in Figure 4.8-7.

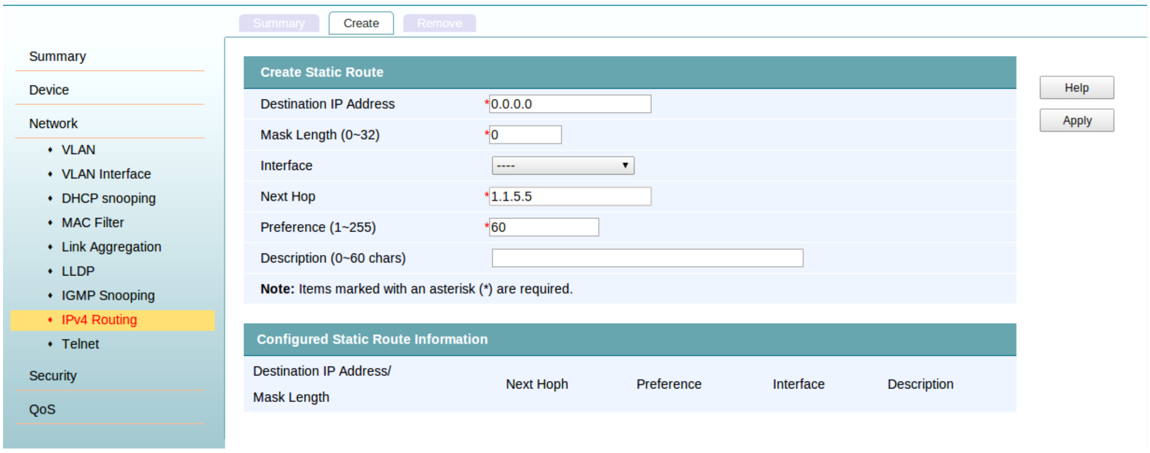
2. Type 0.0.0.0 for Destination IP Address.

3. Select 0 (0.0.0.0) from the Mask drop-down list.

4. Type 1.1.5.5 for Next Hop.

5. Click Apply.

Figure 4.8-7 Configure a default route



Create Static Route

Destination IP Address	*0.0.0.0
Mask Length (0~32)	*0
Interface	----
Next Hop	*1.1.5.5
Preference (1~255)	*60
Description (0~60 chars)	

Note: Items marked with an asterisk (*) are required.

Configured Static Route Information

Destination IP Address/ Mask Length	Next Hoph	Preference	Interface	Description

4.8.4.4 Configuration verification

# Display the active route table.

Enter the IPv4 route page of Switch A, Switch B, and Switch C respectively to verify that the newly configured static routes are displayed in the active route table.

# Ping Host B from Host A (assuming both hosts run Windows XP).

```
C:\Documents and Settings\Administrator-->ping 1.1.3.2

Pinging 1.1.3.2 with 32 bytes of data:

Reply from 1.1.3.2: bytes=32 time=1ms TTL=128
Reply from 1.1.3.2: bytes=32 time=1ms TTL=128
Reply from 1.1.3.2: bytes=32 time=1ms TTL=128
Reply from 1.1.3.2: bytes=32 time=1ms TTL=128

Ping statistics for 1.1.3.2:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
   Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

4.8.5 Precautions

When configuring a static route, note the followings:

- If you do not specify the preference when configuring a static route, the default preference will be used. Reconfiguration of the default preference applies only to newly created static routes. The web interface does not support configuration of the default preference.
- The static route does not take effect if you specify the next hop address first and then configure it as the IP address of a local interface, such as a VLAN interface.
- If Null 0 interface is specified as the output interface, the next hop address is not required. If you want to specify a broadcast interface (such as a VLAN interface) as the output interface, which may have multiple next hops, specify the next hop at the same time.
- You can delete only static routes on the Remove tab.

4.9 Telnet

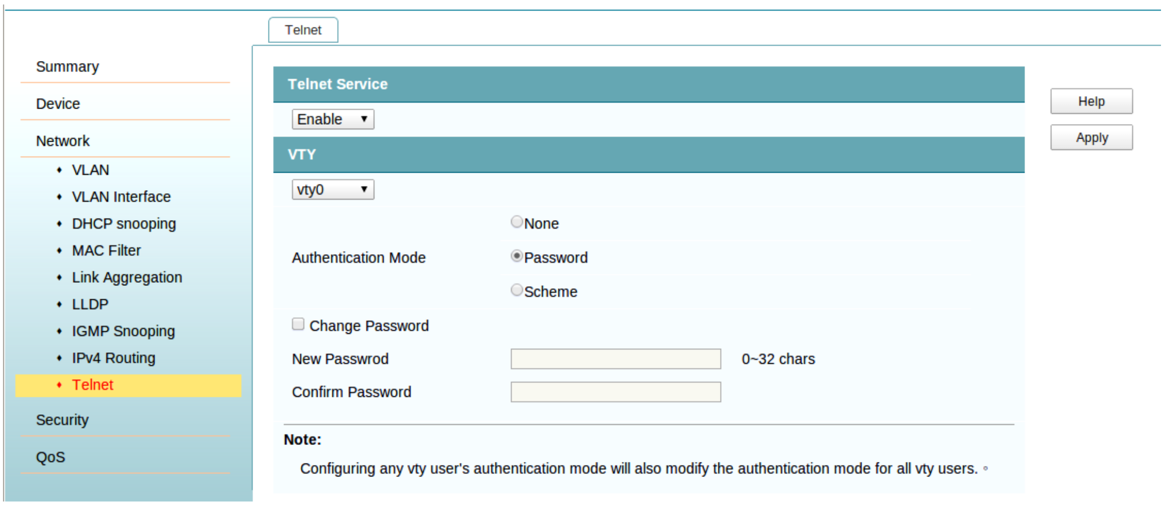
The Telnet protocol is an application layer protocol that provides remote login and virtual terminal functions on the network.

This page is used to configure a Telnet server of opening and closing, and configure a Telnet terminal vty user attributes.

4.9.1 Configuring telnet service

Select Network-->Telnet to enter the service management configuration page, as shown in Figure 4.9-1.

Figure 4.9-1 Configure Telnet service



Telnet Service

Enable

VTY

vty0

Authentication Mode ○None ●Password ○Scheme

□ Change Password

New Passwrod 0~32 chars

Confirm Password

Note:

Configuring any vty user's authentication mode will also modify the authentication mode for all vty users. 。

Table 4.9-1 Service management configuration

Item		Description
Telnet Service	Enable Telnet service	Specify whether to enable the Telnet service. The Telnet service is disabled by default.
Authentication Mode	None	No certification is required for the end user login
	Password	login password authentication
	Scheme	Require user name and password authentication to login
Change Password		Modify vty user login password authentication way need password, when the authentication is password authentication, must be a vty user profile password

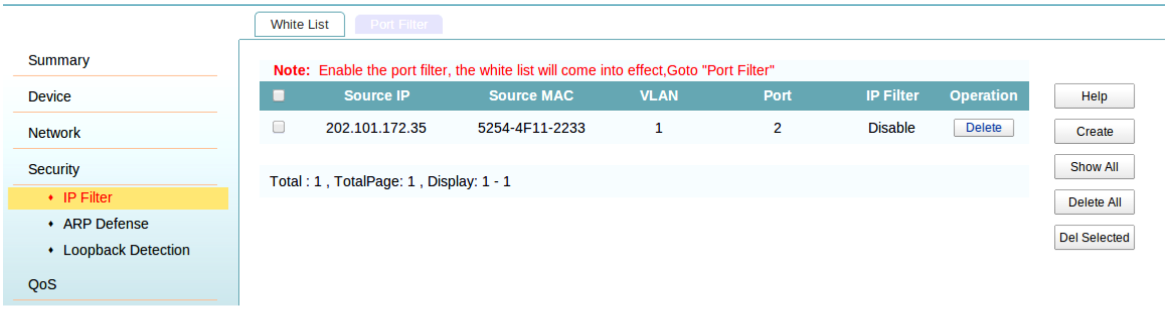
5 Security management

5.1 IP Filter

This page is used to display the current configuration on the switch port IP filtering white list, and allows you to add the white list.

Select Security-->**IP Filter** to enter the default page as shown in Figure 5.1-1.

Figure 5.1-1 The White list



Note: Enable the port filter, the white list will come into effect,Goto "Port Filter"

□	Source IP	Source MAC	VLAN	Port	IP Filter	Operation
□	202.101.172.35	5254-4F11-2233	1	2	Disable	Delete

Total : 1 , TotalPage: 1 , Display: 1 - 1

5.1.1 The White list

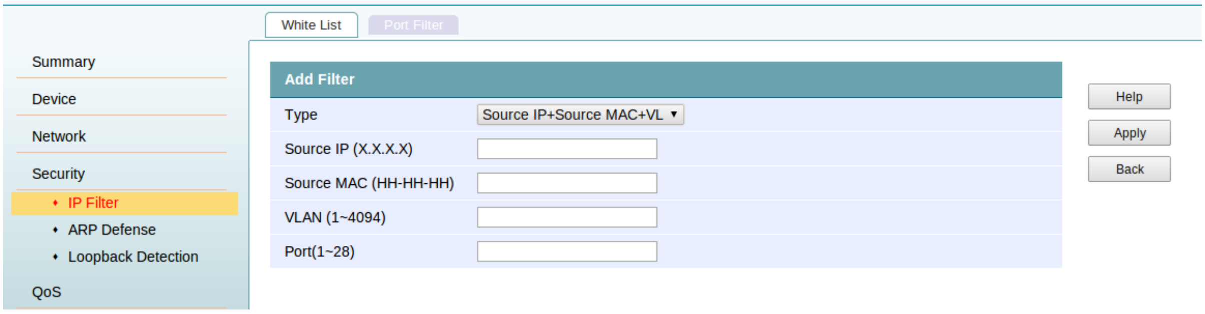
Table 5.1-1 White List items

Item	Description
Port	White list table in port
IP Filter	Open IP filtering capabilities according to corresponding items in white list table port
Create	Add white list page
Show all	Show all white list information
Delete all	Delete all the white list of devices
Delete Selected	By clicking on the "batch delete" to delete the selected white list

5.1.1.1 Add a White List

Click **Create** to add a white list as shown in Figure 5.1-2.

Figure 5.1-2 Add White list



Add Filter

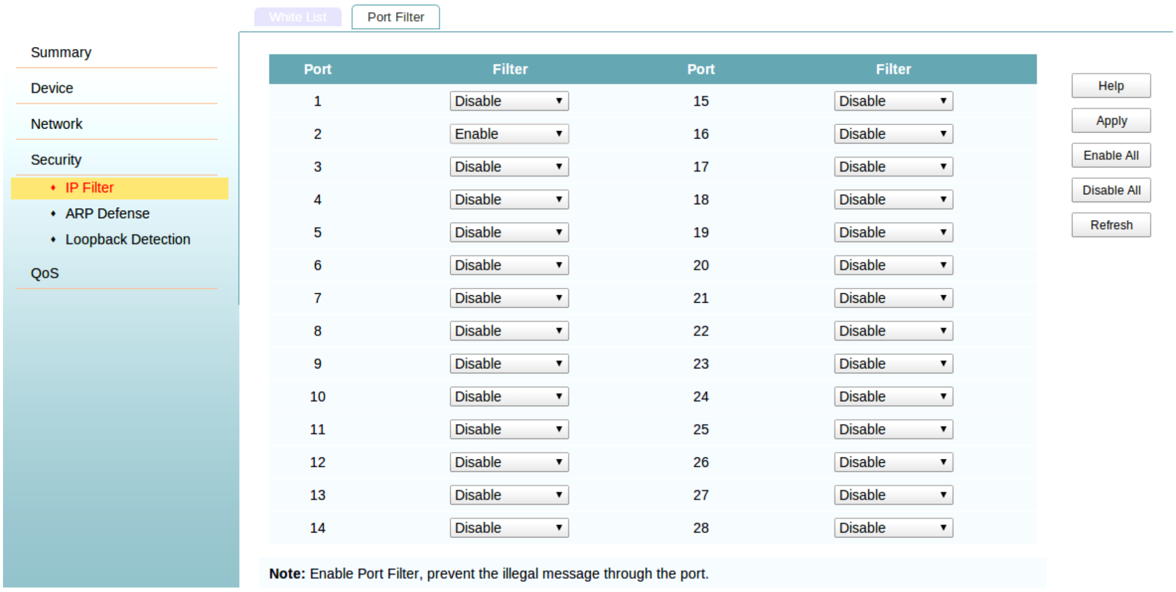
Type	Source IP+Source MAC+VL
Source IP (X.X.X.X)	
Source MAC (HH-HH-HH)	
VLAN (1~4094)	
Port(1~28)	

Table 5.1-2 Add filter

Item	Description
Type	Add the type of white list table, including: the source IP address, the source MAC address, the source IP address + source of VLAN, MAC address, VLAN, source IP address + source MAC address + VLAN
Source IP	White list table of source IP address
Source MAC	White list of the source MAC address table entries
VLAN	White list in the VLAN
Port	White list in port

5.1.2 Port Filter

Figure 5.1-3 configuration of port filter



Port	Filter	Port	Filter
1	Disable	15	Disable
2	Enable	16	Disable
3	Disable	17	Disable
4	Disable	18	Disable
5	Disable	19	Disable
6	Disable	20	Disable
7	Disable	21	Disable
8	Disable	22	Disable
9	Disable	23	Disable
10	Disable	24	Disable
11	Disable	25	Disable
12	Disable	26	Disable
13	Disable	27	Disable
14	Disable	28	Disable

Note: Enable Port Filter, prevent the illegal message through the port.

Table 5.1-3 Port filter summary

Item	Description
Filter	Select to enable or disable port filtering capability
Enable All	Click "Enable All" and then click "Apply" to enable all ports filtering capabilities
Disable All	Click "Disable All" and then click "Apply" to close all port IP filtering capabilities

5.2 ARP Defense

The Address Resolution Protocol (ARP) resolves IP addresses into physical addresses such as MAC addresses. On an Ethernet LAN, a device uses ARP to get the MAC address of the target device for a packet.

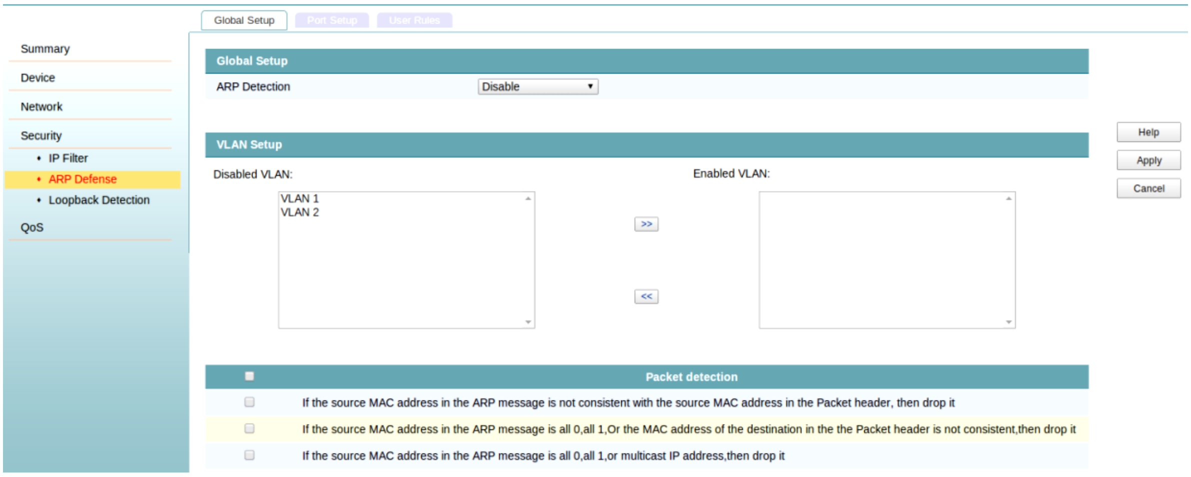
5.2.1 Global Setup

NOTE:

If both ARP packet validity check and user validity check are enabled, the former one applies first, and then the latter applies.

Select Network-->ARP Defense to enter the default Global Setup page as shown in Figure 5.2-1.

Figure 5.2-1 ARP Detection summary



Global Setup

ARP Detection: Disable

VLAN Setup

Disabled VLAN:
VLAN 1
VLAN 2

Enabled VLAN:

□ Packet detection

□ If the source MAC address in the ARP message is not consistent with the source MAC address in the Packet header, then drop it

□ If the source MAC address in the ARP message is all 0,all 1,Or the MAC address of the destination in the the Packet header is not consistent,then drop it

□ If the source MAC address in the ARP message is all 0,all 1,or multicast IP address,then drop it

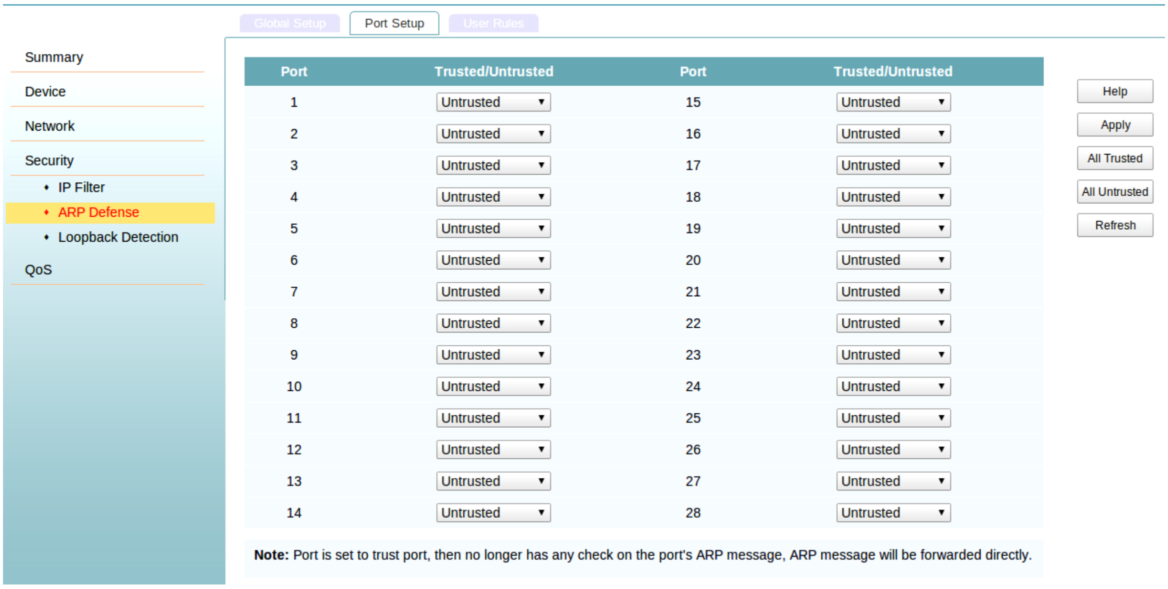
Table 5.2-1 ARP Detection configuration items

Item	Description
Global Setup	Enable/Disable ARP detection.

Item	Description
VLAN Setup	Select VLANs on which ARP detection is to be enabled. add VLANs to the Enabled VLAN list box, select one or multiple VLANs from the Disabled VLAN list box and click the >>button. Remove VLANs from the Enabled VLAN list box, select one or multiple VLANs from the list box and click the << button.
Trusted Ports	Select trusted ports. add ports to the Trusted Ports list box, select one or multiple ports from the Untrusted Ports list box and click the << button. Remove ports from the Trusted Ports list box, select one or multiple ports from the list box and click the >> button.
Packet Validation	If the source MAC address in the ARP message is not consistent with the source MAC address in the Packet header, drop it; If the source MAC address in the ARP message is all 0, all 1, or the MAC address of the destination in the Packet header is not consistent, drop it; 1. If the source MAC address in the ARP message is all 0, all 1, or multicast IP address, drop it; 2. If none of the above is selected, the system does not check the validity of ARP packets.

5.2.2 Port Setup

Figure 5.2-2 Port Setup



Port	Trusted/Untrusted	Port	Trusted/Untrusted
1	Untrusted ▾	15	Untrusted ▾
2	Untrusted ▾	16	Untrusted ▾
3	Untrusted ▾	17	Untrusted ▾
4	Untrusted ▾	18	Untrusted ▾
5	Untrusted ▾	19	Untrusted ▾
6	Untrusted ▾	20	Untrusted ▾
7	Untrusted ▾	21	Untrusted ▾
8	Untrusted ▾	22	Untrusted ▾
9	Untrusted ▾	23	Untrusted ▾
10	Untrusted ▾	24	Untrusted ▾
11	Untrusted ▾	25	Untrusted ▾
12	Untrusted ▾	26	Untrusted ▾
13	Untrusted ▾	27	Untrusted ▾
14	Untrusted ▾	28	Untrusted ▾

Note: Port is set to trust port, then no longer has any check on the port's ARP message, ARP message will be forwarded directly.

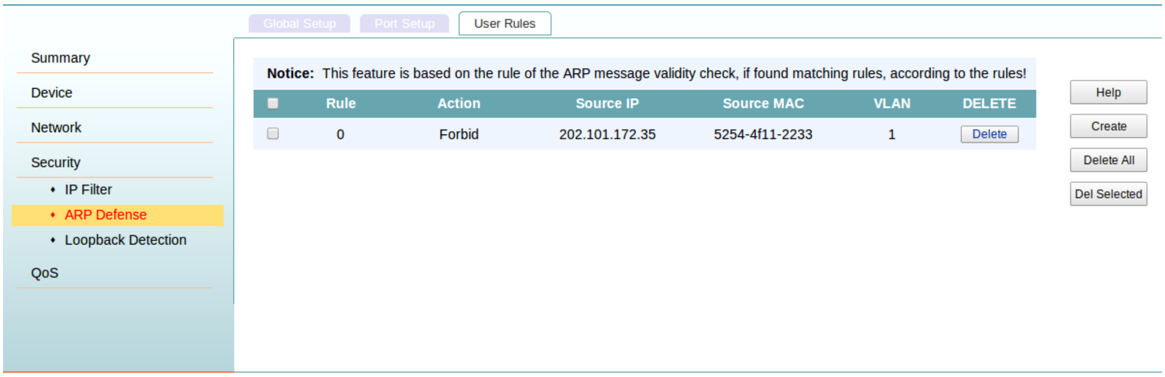
There is no any check on the port’s ARP message for Trusted port, ARP message will be forwarded directly.

5.2.3 Displaying ARP entries

Select Security-->ARP Defense to enter the User Rules Table page as shown in Figure 5.2-3.

All ARP entries are displayed on the page.

Figure 5.2-3 User Rules



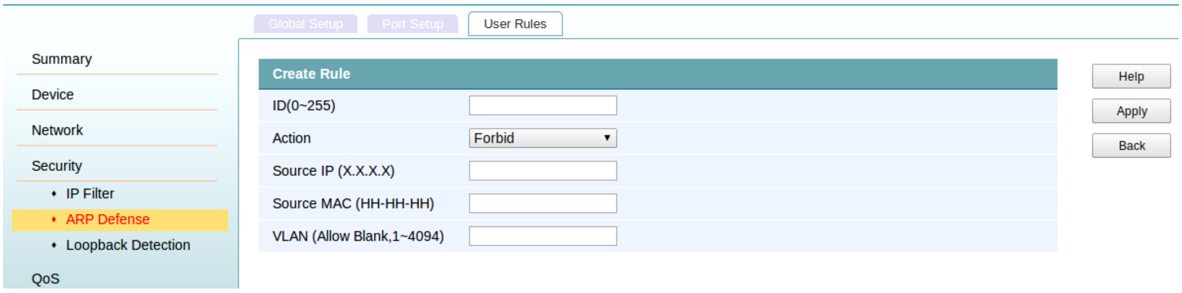
Notice: This feature is based on the rule of the ARP message validity check, if found matching rules, according to the rules!

□	Rule	Action	Source IP	Source MAC	VLAN	DELETE
□	0	Forbid	202.101.172.35	5254-4f11-2233	1	Delete

5.2.4 Creating a static ARP entry

Select Security-->ARP Defense to enter the default User Rules Table page as shown in Figure 5.2-3. Click Create to enter the Create Rule page, as shown in Figure 5.2-4.

Figure 5.2-4 Add a static ARP entry



Create Rule

ID(0~255)

Action: Forbid

Source IP (X.X.X.X)

Source MAC (HH-HH-HH)

VLAN (Allow Blank,1~4094)

Table 5.2-2 Static ARP entry configuration

Item	Description
Source IP	Type an IP address for the static ARP entry.
Source MAC	Type a MAC address for the static ARP entry.
VLAN	Type a VLAN ID and specify a port for the static ARP entry. ❗IMPORTANT: VLAN ID must be the ID of the VLAN that has already been created, and the port must belong to the VLAN. The corresponding VLAN interface must have been created.

5.3 Loopback Detection

Check the Ethernet port whether can work normally or not by performing loopback test, during which the port cannot forward data packets normally.

Ethernet port loopback test can be an internal loopback test or an external loopback test.

- In an internal loopback test, self-loop is established in the switching chip to check whether there is a chip failure related to the functions of the port.
- In an external loopback test, a loopback plug is used on the port. Packets forwarded by the port will be received by itself through the loopback plug. The external loopback test can be used to check whether there is a hardware failure on the port.

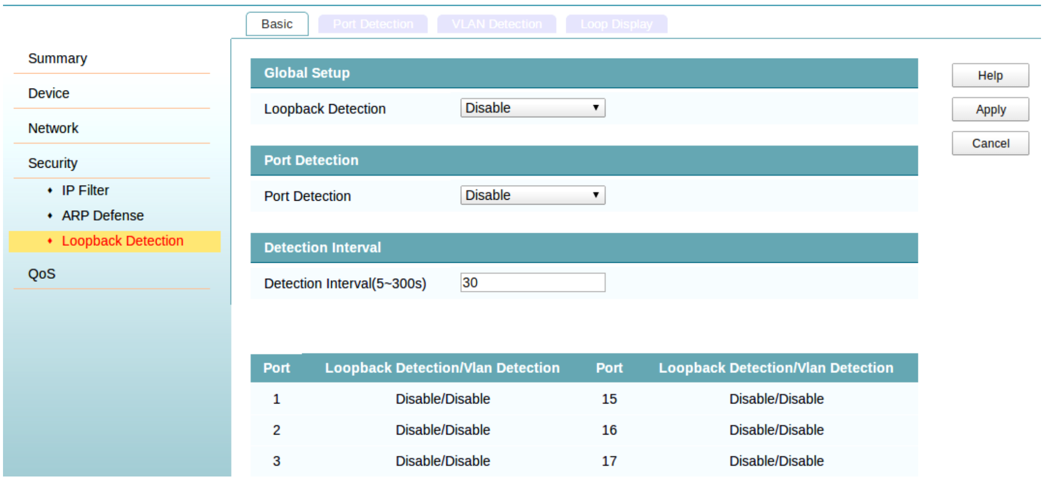
5.3.1 Loopback operation

Table 5.3-1 Loopback operation steps

Step	Remark
Configuring loopback detection globally	Required. By default, loopback detection is disabled globally.
Configuring loopback detection on a port	Required. By default, loopback detection is disabled on a port.

Select Device-->Loopback Detection to enter the basic page, as shown in Figure 5.3-1.

Figure 5.3-1 Loopback detection setup



Global Setup

Loopback Detection: Disable

Port Detection

Port Detection: Disable

Detection Interval

Detection Interval(5~300s): 30

Port	Loopback Detection/Vlan Detection	Port	Loopback Detection/Vlan Detection
1	Disable/Disable	15	Disable/Disable
2	Disable/Disable	16	Disable/Disable
3	Disable/Disable	17	Disable/Disable

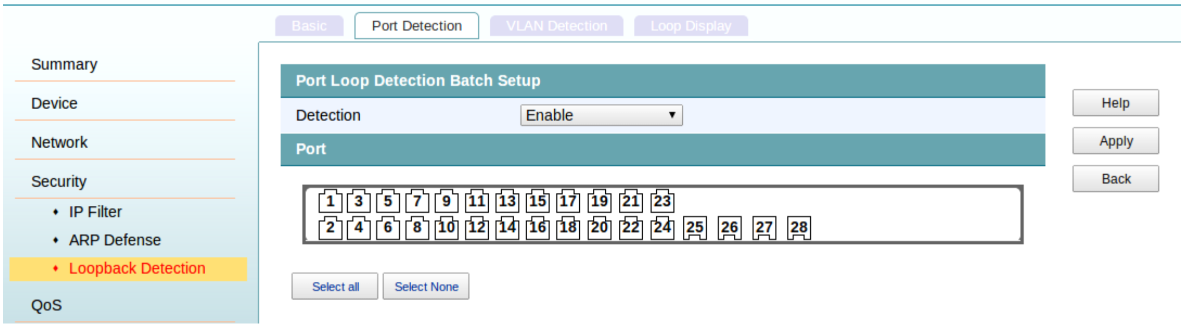
Table 5.3-2 configuration items

Item	Description
Loopback Detection	Enable or disable loopback detection globally.
Port Detection	Enable or disable loopback detection on ports.
Detection Interval	Set detection interval

5.3.2 Configuring loopback detection on a port

Select Device-->Loopback Detection to enter the Port Detection page, as shown in Figure 5.3-2.

Figure 5.3-2 Port Detection setup



Port Loop Detection Batch Setup

Detection: Enable

Port

1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28

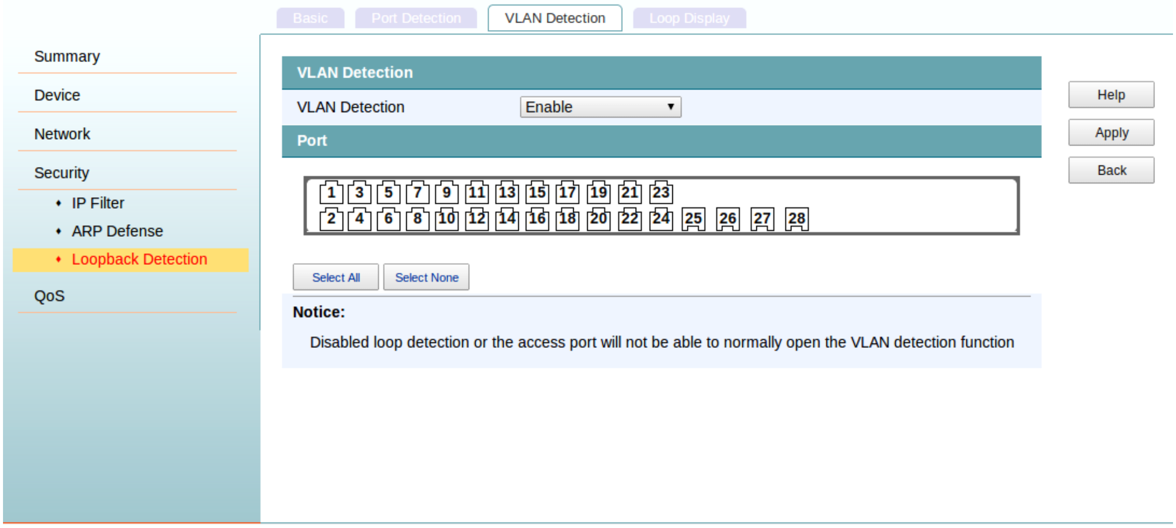
Table 5.3-3 Configuration items

Item	Description
Port Loop Detection Batch Setup	Enable or disable loopback detection on the target port.
Port	Select port for loopback detection configuration.

5.3.3 Configuring loopback detection on VLAN

Select Device-->Loopback Detection to enter VLAN Detection, as shown in Figure 5.3-3.

Figure 5.3-3 VLAN Detection



VLAN Detection

VLAN Detection: Enable

Port

1 3 5 7 9 11 13 15 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28

Notice:

Disabled loop detection or the access port will not be able to normally open the VLAN detection function

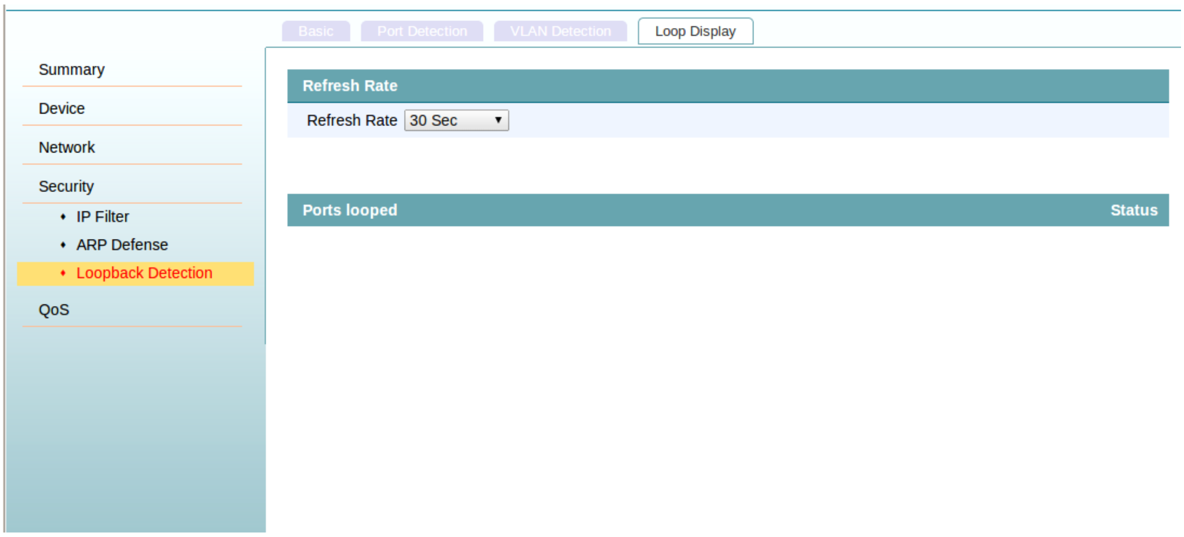
Table 5.3-4 Configuration items

Item	Description
VLAN Detection	Enable: the system performs loopback detection in all VLANs for the target trunk or hybrid port. Disable: the system performs loopback detection only in the default VLAN of the target trunk or hybrid port. This configuration item is available only for a trunk or hybrid port.
Port	Select port for loopback detection configuration.

5.3.4 Displaying loopback detection information

Select Device-->Loopback Detection to enter Loop Display, as shown in Figure 5.3-4.

Figure 5.3-4 Loop Display



Refresh Rate: 30 Sec

Table 5.3-5 Configuration items

Item	Description
Refresh rate	Sets refresh rate of loopback detection.

5.3.5 Configuration guidelines

Note the followings when performing a loopback test:

- You can perform an internal loopback test but not an external loopback test on a port that is physically down, but you can perform neither test on a port that is manually shut down.

- The system does not allow Rate, Duplex, Cable Type and Port Status configuration on a port under a loopback test.

An Ethernet port works in full duplex mode when the loopback test is performed, and restores its original duplex mode after the loopback test.

6 QOS

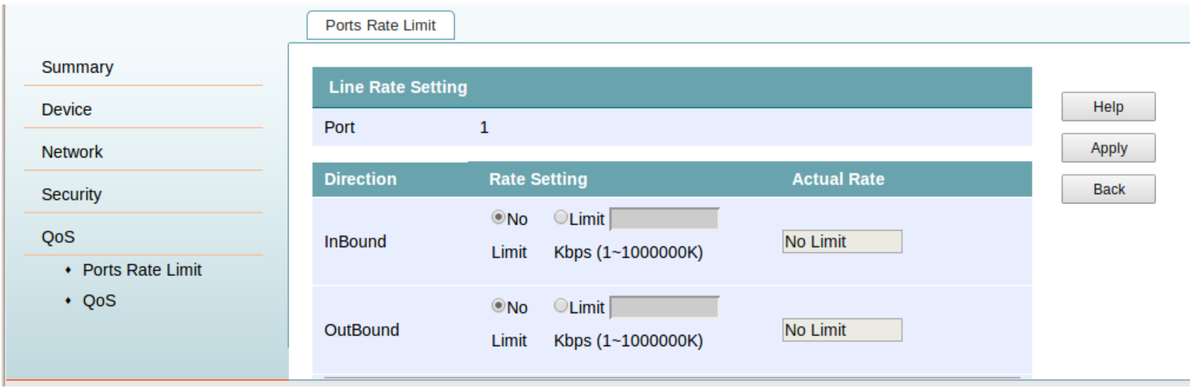
Quality of Service (QoS) reflects the ability of a network to meet customer needs, and evaluates the ability of forwarding packets of different services.

The evaluation can be based on different criteria because the network may provide various services. Generally, QoS performance is measured with respect of bandwidth, delay, jitter, and packet loss ratio during packet forwarding process.

6.1 Ports Rate Limit

Select QoS-->Ports rate Limit and select the port to enter the port rate configuration page, as shown in Figure 6.1-1.

Figure 6.1-1 Port rate Limit



Line Rate Setting

Port 1

Direction	Rate Setting	Actual Rate
InBound	● No Limit ○ Limit Kbps (1~1000000K)	No Limit
OutBound	● No Limit ○ Limit Kbps (1~1000000K)	No Limit

Table 6.1-1 Configuration items

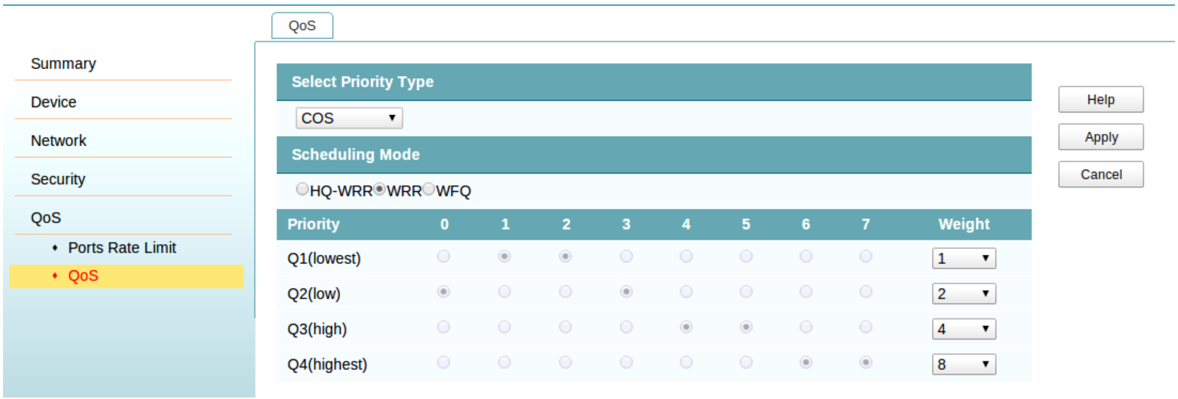
Item	Description
Rate Limit	Enable or disable line rate on the specified port.
Direction	Select a direction in which the line rate is to be applied. Inbound—Limits the rate of packets received on the specified port. Outbound—Limits the rate of packets sent by the specified port.

Item	Description
Select port(s)	Specify the ports to be configured with line rate Click the ports to be configured with line rate in the port list or click **Bacth config** . You can select one or more ports.

6.2 QOS

6.2.1 Configuring priority mapping tables

Figure 6.22-1 Qos setting



Select Priority Type

COS

Scheduling Mode

○HQ-WRR ●WRR ○WFQ

Priority	0	1	2	3	4	5	6	7	Weight
Q1(lowest)	○	●	●	○	○	○	○	○	1
Q2(low)	●	○	○	●	○	○	○	○	2
Q3(high)	○	○	○	○	●	●	○	○	4
Q4(highest)	○	○	○	○	○	○	●	●	8

Switches to realize the function of simple QoS, in the network congestion occurs, the system will set the switch priority queue and queue scheduling algorithm to control the packet forwarding order. There are 4 queue switches, 1 is the lowest priority queue, queue 4 is the highest priority. The priority of the switches support for: COS priority, DSCP priority; Switches support queue scheduling algorithm for: high-priority weighted round robin scheduling (HQ - WRR), weighted round robin scheduling (WRR), weighted fair queuing (WFQ) dispatching.

COS priority is determined by the VLAN Tag message, its mapping relationship with scheduling queue for queue for VLAN Tag priority 1, 2, 1; VLAN Tag 0 and 3 for the queue priority 2; VLAN Tag 4, 5 for the queue priority 3; VLAN Tag priority for queue in June and July 4.

DSCP is in accordance with the TOS field in IP packet priority after six DSCP priority mapping for 4 queue, each group of 16 and corresponding to a scheduling priority queue, and scheduling priority queue corresponding relation is: 0-15 corresponding queue priority 1;16-31 corresponding priority queue 2;32-47 corresponding queue priority 3;48-63 corresponding queue priority 4.

6.2.2 QOS configuration Example

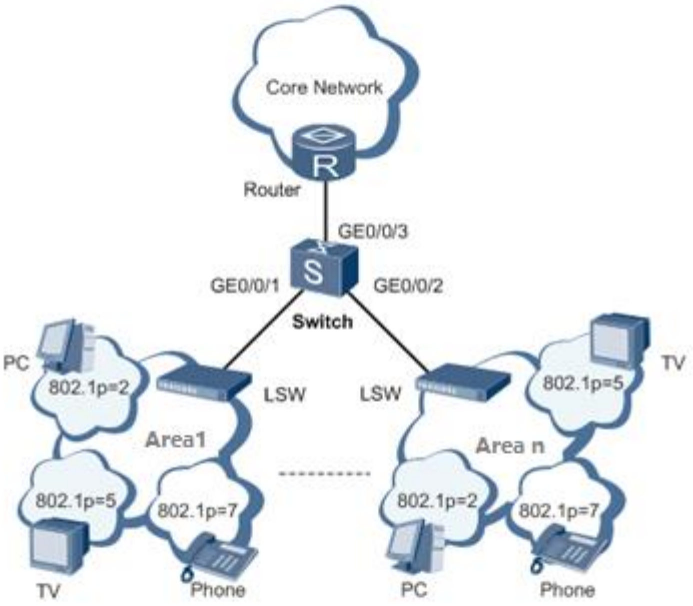
6.2.2.1 Networking requirement

Switch would connect with router via GE0/0/3 interface. Internet service includes voice, video and data and the 802.1p priority is 7,5,2.all these service can arrive in user side via router and Switch as shown in Figure 6.2-2. In order to weaken the effect caused by network congestion and ensure the service requirement of high priority & low-delay, the configuration is as below.

Table 6.2-1 Service type

Service type	**Service level**
voice	CS7(Q4 queue, absolute priority)
video	EF（Q3 queue，second priority）
data	AF2（Q1 queue, lowest priority）

Figure 6.2-2 Networking diagram



6.2.2.2 Data preparation

In order to complete above configuration example, the following data should be prepared：

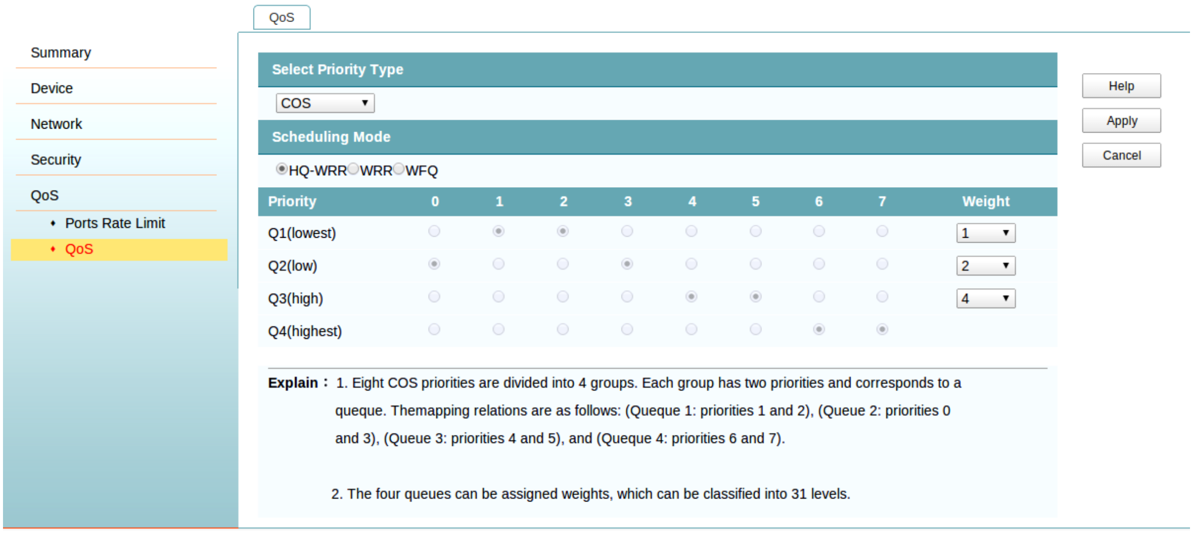
- VLAN of data, video and voice is 10,20,30 respectively.

- 802.1p priority of data, video and voice is 2, 5,7 respectively.
- Scheduler parameters of each service level.

6.2.2.3 Operation procedures

1. Create VLAN 10,VLAN 20,VLAN 30 according to vlan configuration instruction.
2. Set SwitchGE0/0/1 GE0/0/2 GE0/0/3 as Trunk port, and allow VLAN 10 VLAN20 VLAN 30 to pass through. For more details, refer to vlan configuration instruction.
3. Click QOS-->QOS as shown in Figure 6.2-3.

Figure 6.2-3 Qos operation



Select Priority Type

COS ▾

Scheduling Mode

● HQ-WRR ○ WRR ○ WFQ

Priority	0	1	2	3	4	5	6	7	Weight
Q1(lowest)	○	●	●	○	○	○	○	○	1 ▾
Q2(low)	●	○	○	●	○	○	○	○	2 ▾
Q3(high)	○	○	○	○	●	●	○	○	4 ▾
Q4(highest)	○	○	○	○	○	○	●	●	

Explain： 1. Eight COS priorities are divided into 4 groups. Each group has two priorities and corresponds to a queque. Themapping relations are as follows: (Queque 1: priorities 1 and 2), (Queue 2: priorities 0 and 3), (Queue 3: priorities 4 and 5), and (Queque 4: priorities 6 and 7).

2. The four queues can be assigned weights, which can be classified into 31 levels.

4. Choose "COS" in the column of "select priority type"
5. Select "HQ-WRR" in the column of "Sheduling Mode"
6. Click "Apply"

6.2.3 Configuration guidelines

When an ACL is referenced to implement QoS, the actions defined in the ACL rules, deny or permit, do not take effect; actions to be taken on packets matching the ACL depend on the traffic behavior definition in QoS.