Zenty | Professional A/V Solution Provider

User Manual [V1.0]

24 Port PoE Gigabit Ethernet Switch

ZT-120 | ZT-IPSP24

48 Port PoE Gigabit Ethernet Switch

ZT-121 | ZT-IPSP48

ZENTY ®
9807 EMILY LANE
STAFFORD, TX 77477
(844) 200-1945
SALES@ZENTY.COM

RoHS compliant

Table of Contents

1. Introduction

1.1 Product Introduction

This series supports IPv4 / IPv6 double stack platform, and supports a variety of senior management functions, including POE management, MAC Table, VLANs, Port Isolation, Loop Protection, IGMP Snooping, MLD Snooping, ERPS, DHCP client, DHCP Snooping, STP/RSTP/MSTP, 802.1 x, QoS, port mirror, LLDP, static routing and NTP etc., 128 static routing and basic QINQ, to provide users with the perfect solution; At the same time the whole series supports SNMP v1 / v2, v3 (Simple Network Management Protocol), CLI command line, Web net tube, TELNET mode of Management, make equipment management more convenient, at the same time, with the ACL control function, attack prevention function, ensuring secure management.

The series complies with FCC and CE standards, and support 1 channel ac power input. Using the mute fan, can adapt to work environment temperature range of - 40 ℃ to 75 ℃, also, it can satisfy the requirements of the various site and provide reliable, economical solution.

1.2 Features

- IEEE802.3, IEEE802.3u, IEEE802.3ab, IEEE802.3z, IEEE802.3ae
- V-Ring looped redundancy technology. Self-healing time for looped network is less than 20ms.
- PoE management, POE load timing restart and on-off.
- IGMP Snooping, Static multicast filtering, MLD Snooping filtering
- DHCP Snooping, protect from ARP attack, attack of illegal DHCP server access
- NTP, easy for real-time synchronization of network time
- Supports SNMP v1/v2/v3
- Supports LLDP
- ACL, enhance the flexibility and safety of network management
- QoS, enhance the stability of network
- Port mirror, convenient for online debug
- Cable testing, convenient for the examining cable length in a project
- STP/RSTP/MSTP, enhance the stability of network

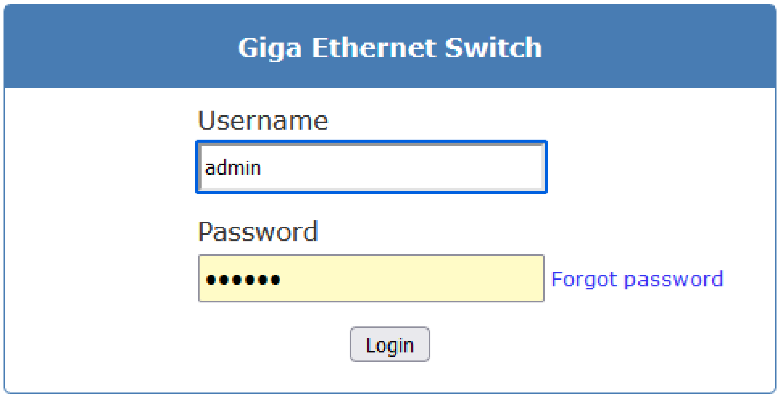
- IEEE802.1Q VLAN, IEEE802.1ad QINQ
- 802.1x authentication to port and MAC
- Static routing L3 switching technology
- Operation temperature range: -40℃ ~ 75℃
- Storage temperature range: -40℃ ~ 85℃

2. Web Configuration

Open installed web browser on your PC, input the switch's IP address like http://xxx.xxx.xxx.xxx, then open that URL to login web management.

Note: IP address of switch is **192.168.2.1** by default. So please input **http://192.168.2.1** in browser. If you cannot access the switches web interface, please make sure that your PC is has a static IP that matches the default IP of the switch (for ex. 192.168.2.11).

When the login window appears, please enter the default username "**admin**" with password "**system**". Then click OK to login.



Giga Ethernet Switch

Username: admin

Password: ●●●●●●

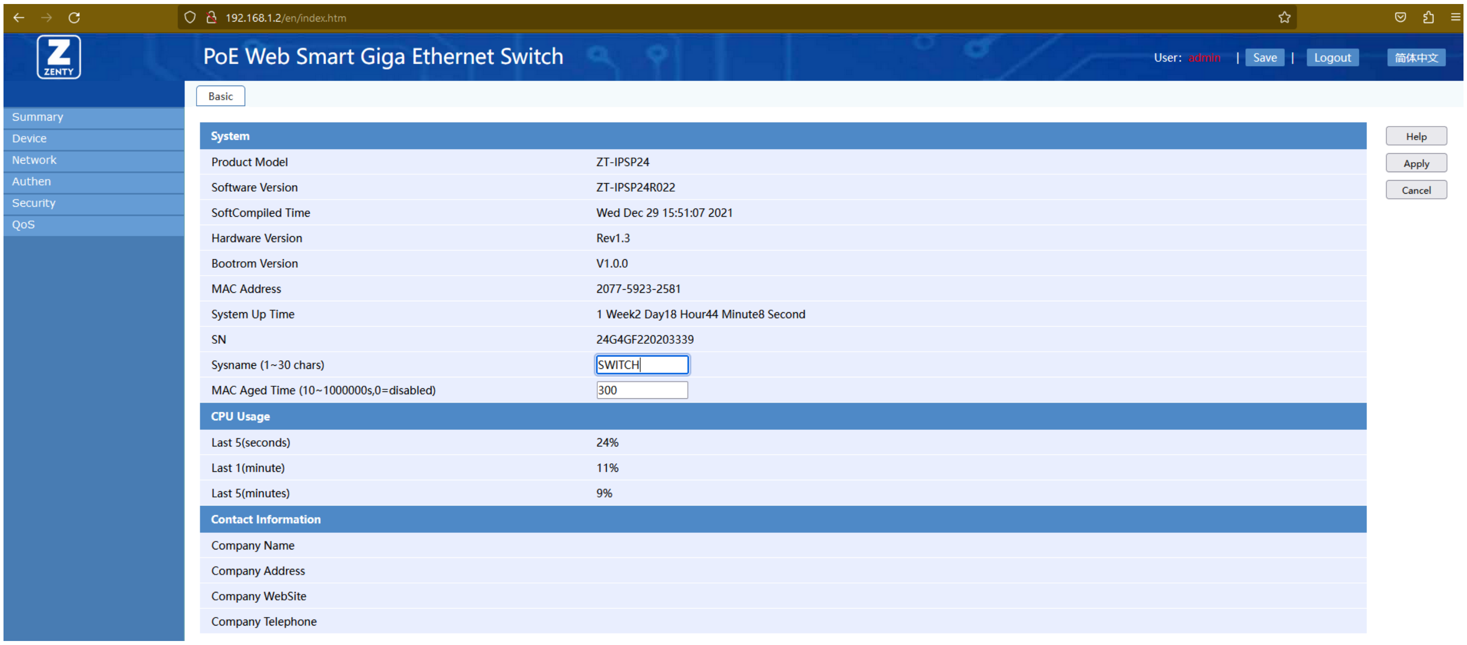
Default User Name: **admin**

Default Password: **system**

2.1 Device Menu Information

2.1.1 Device > Basic

After successfully logging in to the page, the web page directly jumps to the system information page, and you can also select the "Device Overview" or "Device → Basic Information" path to view the switch system information. You can view the device's MAC address, software version, production serial number, etc. on the system information page, modify the system name, MAC address aging time (default 300 seconds).



System	
Product Model	ZT-IPSP24
Software Version	ZT-IPSP24R022
SoftCompiled Time	Wed Dec 29 15:51:07 2021
Hardware Version	Rev1.3
Bootrom Version	V1.0.0
MAC Address	2077-5923-2581
System Up Time	1 Week2 Day18 Hour44 Minute8 Second
SN	24G4GF220203339
Sysname (1~30 chars)	SWITCH
MAC Aged Time (10~1000000s,0=disabled)	300
CPU Usage	
Last 5(seconds)	24%
Last 1(minute)	11%
Last 5(minutes)	9%
Contact Information	
Company Name	
Company Address	
Company WebSite	
Company Telephone	

The meaning of the key items on the page is shown in the table below.

Operation	Explanation
Software Version / Hardware Version / Bootloader Version	Display the software version number, hardware version number, and the bootloader version of the currently running software
MAC Address	Displays the MAC address of the switch
Operation Hours	Displays the switches continuous running time since being powered on
Production Serial Number (SN)	Shows the production serial number of the switch
System Name	Customize the device name so that you can quickly locate it by this name

MAC Address Aging Time	Configure the aging time of the dynamic MAC address entries. The default is 300 seconds.

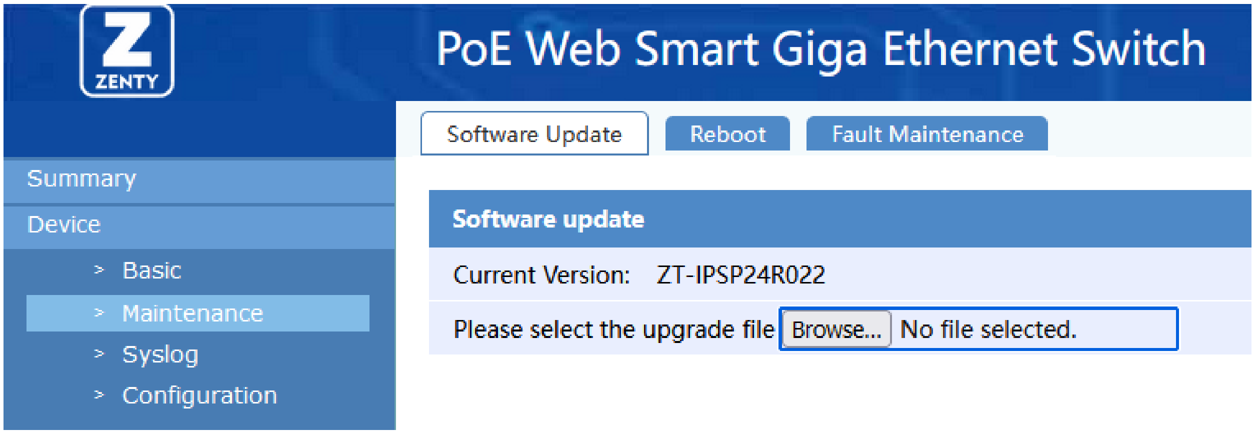
2.1.2 Device > Maintenance

Equipment maintenance includes equipment software update, reboot, and fault maintenance.

Software Update:

Page wizard: Device ⟶ Maintenance ⟶ Software Update, the page is as shown in the figure below. Upgrade the switch software to the latest version, which will make your device more stable and more functional (click the <Browse...> button, select the latest version file, and click the <OK> button to start the upgrade)

Do not power off the device during the upgrade process.



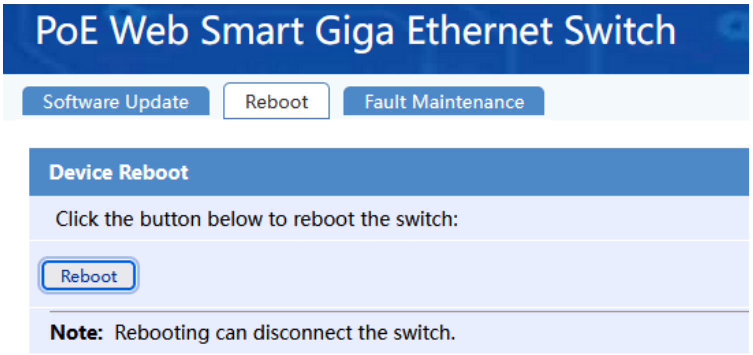
Software update

Current Version: ZT-IPSP24R022

Please select the upgrade file No file selected.

Reboot:

Page wizard: Device ⟶ Maintenance ⟶ Reboot, the page is as shown in the figure below. Select the <Reboot> button to restart.



Device Reboot

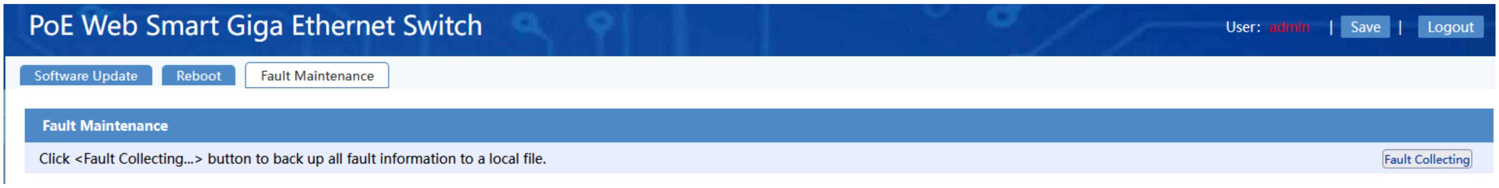
Click the button below to reboot the switch:

Note: Rebooting can disconnect the switch.

Before restarting the device, please save the current configuration. Otherwise, after restarting, unsaved configuration information will be lost.

Fault Maintenance:

Page Wizard: Device → Equipment Maintenance → Fault Maintenance, the page is shown below. Select the <Fault Collecting> button, and all fault maintenance information will be backed up to your PC.



Fault Maintenance

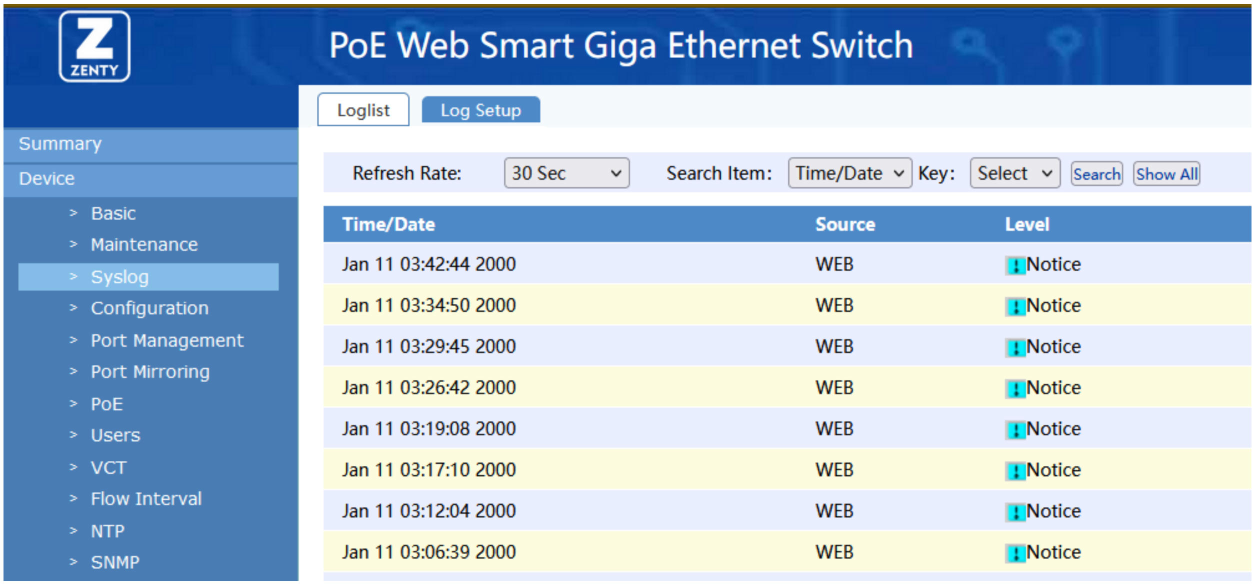
Click <Fault Collecting...> button to back up all fault information to a local file.

2.1.3 Device > Syslog

The system log records information about hardware, software, and system problems in the system. It can also monitor events that occur in the system, providing powerful support for network administrators to monitor network operation and diagnose network faults.

Loglist:

Page Wizard: Device → Syslog → Loglist, the page is shown in the figure below.



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

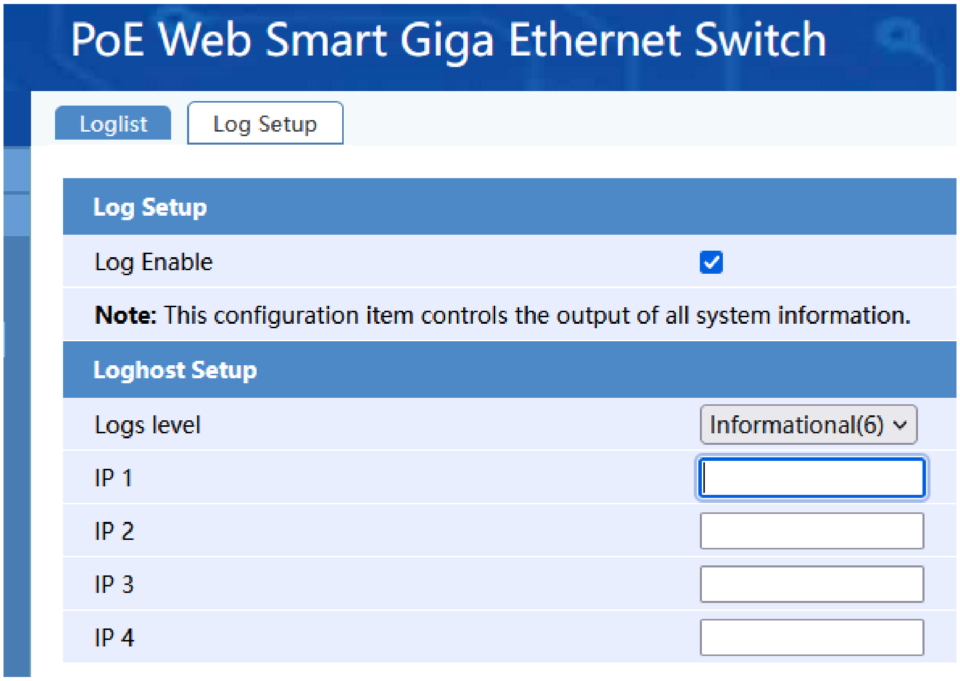
Time/Date	Source	Level
Jan 11 03:42:44 2000	WEB	Notice
Jan 11 03:34:50 2000	WEB	Notice
Jan 11 03:29:45 2000	WEB	Notice
Jan 11 03:26:42 2000	WEB	Notice
Jan 11 03:19:08 2000	WEB	Notice
Jan 11 03:17:10 2000	WEB	Notice
Jan 11 03:12:04 2000	WEB	Notice
Jan 11 03:06:39 2000	WEB	Notice

The meaning of the key items on the page is shown in the table below.

Operation	Explanation
Refresh Rate	Control the refresh rate of the page through the selection of “Refresh Rate” drop down box
Query Item	Query the log information you need to follow through the selection of the “Query Item” drop down box
Positive Sequence Display	Log information is displayed in the order from the first to the last. The reverse display is the opposite
Download	Click the <Download> button to save all log information locally for easy viewing
Refresh	Click the <Refresh> button to manually refresh the log information
Clear	Click the <Clear> button to delete all log information

Log Setup:

Page Wizard: Device → Syslog → Log Setup



Log Enable ☑

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

Logs level: Informational(6)

IP 1

IP 2

IP 3

IP 4

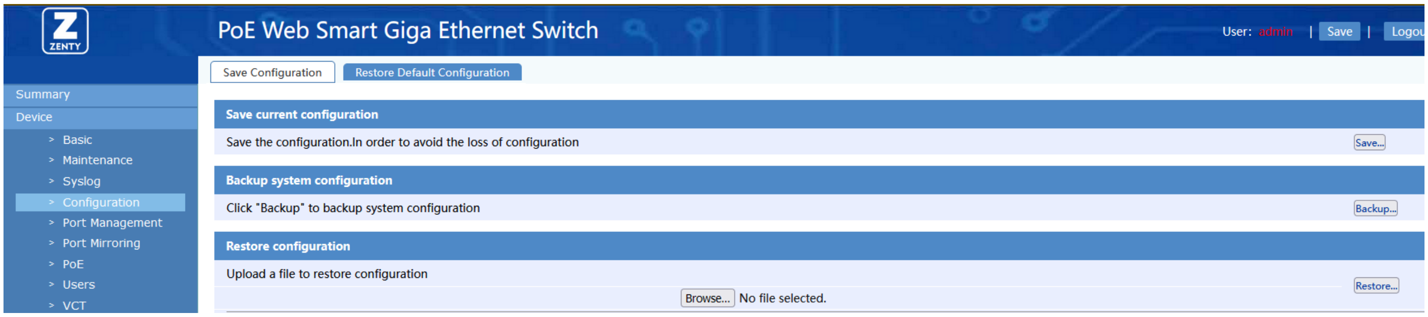
The meaning of the key items on the page is shown in the table below.

Operation	Explanation
Log Enables	Open / close the information center. By default, the information center is turned on
Send Log Level	Only log information no higher than the specified level can be sent to the log host
Log Host IP	Set the IP address of the log host

2.1.4 Device > Configuration

Save Configuration:

Page Wizard: Device ⟶ Configuration ⟶ Save Configuration



Save current configuration

Save the configuration.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

The meaning of the key items on the page is shown in the table below.

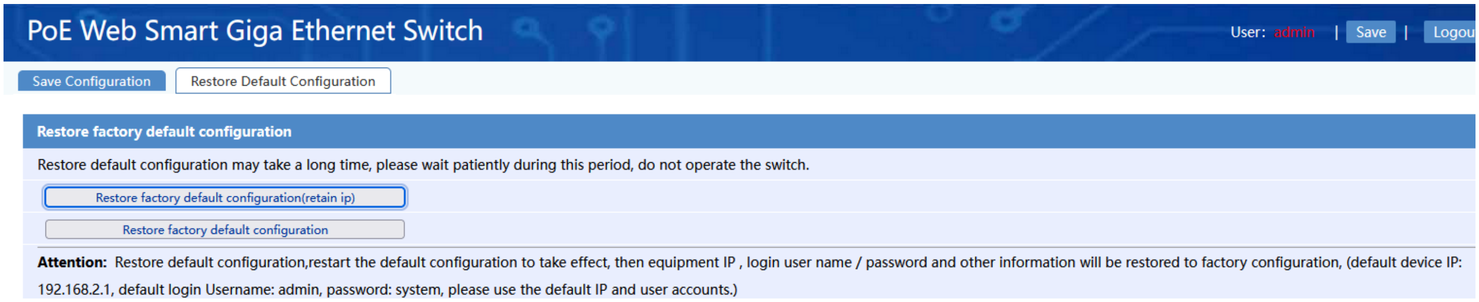
Operation	Explanation
Save current configuration	Click the <Save> button, after confirmation, you can save the configuration information of the current device
Backup system configuration information	Click the <Backup...> button and select the backup path of the configuration file. You can save the current configuration of the device to your computer so that you can use this file (*.cfg) to restore the configuration in the future.
Restore configuration information from a file	Click the <Browse> button, select the previously backed up file (*.cfg), click <Restore Repeat...> button, after confirmation, you can restore the device to the previous configuration (after the

	device is automatically restarted, the configuration takes effect)

After you have configured all items on the configuration page, be sure to save the configuration, otherwise, the unsaved configuration information will be lost due to restarting and other operations.

Restore Default Configuration:

During the process of restoring the factory default configuration, please do not perform other operations on the device, otherwise, the device may not work properly


PoE Web Smart Giga Ethernet Switch
User: admin
Save
Logou
Save Configuration
Restore Default Configuration
Restore factory default configuration(retain ip)
Restore factory default 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: 192.168.2.1, default login Username: admin, password: system, please use the default IP and user accounts.)

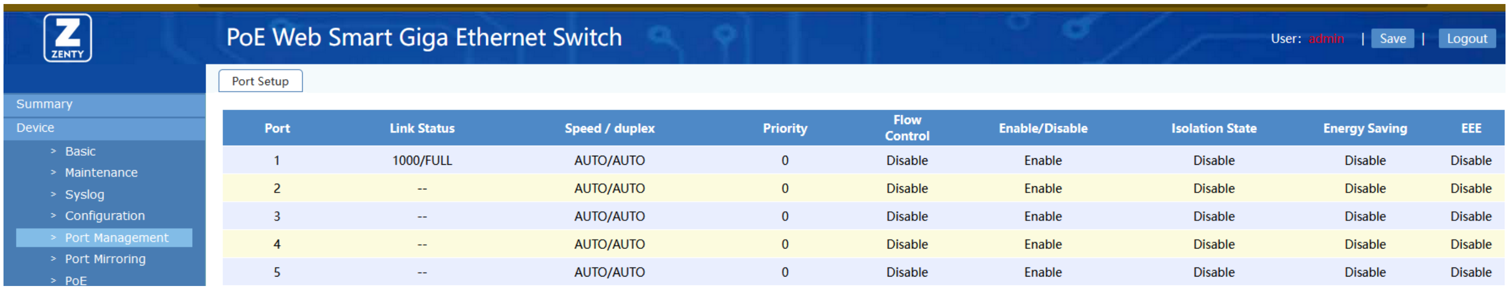
The meaning of the key items on the page is shown in the table below.

Operation	Explanation
Restore configuration, but retain management IP	Select this button, you can continue to use the current IP address to log in to the device for configuration and management
Restore the default configuration	Select this button, you need to use the default IP address to log in to the device for configuration and management

2.1.5 Device > Port Management

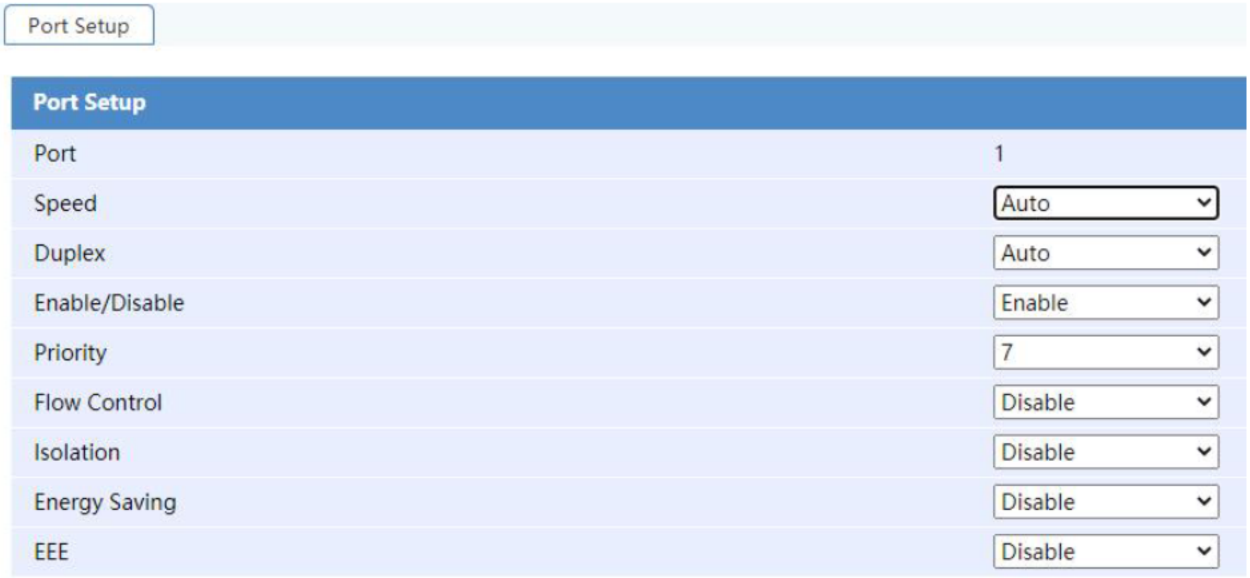
Port Setup:

Page Wizard: Device → Port Management → Port Setup, shows the current port attribute status.



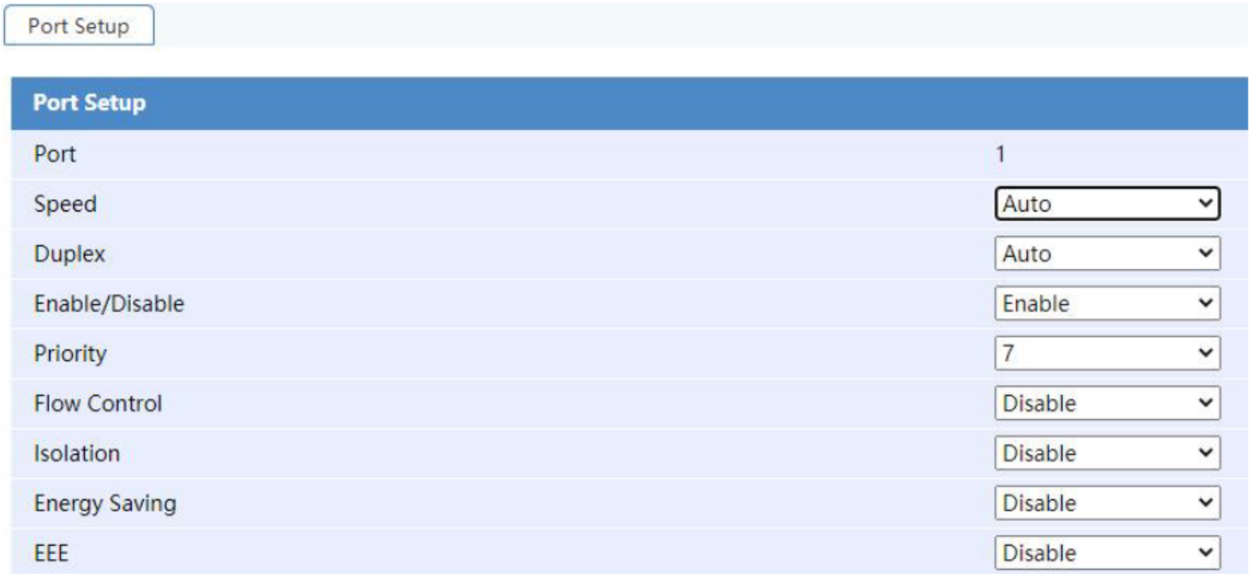
Port	Link Status	Speed / duplex	Priority	Flow Control	Enable/Disable	Isolation State	Energy Saving	EEE
1	1000/FULL	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
2	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
3	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
4	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable
5	--	AUTO/AUTO	0	Disable	Enable	Disable	Disable	Disable

Configure the properties of the specified ports in batches (click the <Batch Configuration> button on the main page to enter the corresponding configuration page).



Port Setup	
Port	1
Speed	Auto
Duplex	Auto
Enable/Disable	Enable
Priority	7
Flow Control	Disable
Isolation	Disable
Energy Saving	Disable
EEE	Disable

Configure the properties of a single port (click the entry corresponding to the port on the main page to enter the corresponding configuration page).



Port Setup	
Port	1
Speed	Auto
Duplex	Auto
Enable/Disable	Enable
Priority	7
Flow Control	Disable
Isolation	Disable
Energy Saving	Disable
EEE	Disable

The meaning of the key items on the page is shown in the table below.

Operation	Explanation
Link status	The actual working speed and mode of the port, if not connected, it will display as "--".
Rate	Configure port rate.
Duplex	There are three situations in the duplex mode of the port: • When you want the port to receive packets while sending packets, you can configure the port to be full-duplex (full) attribute. • When you want the port to only send or receive packets at the same time, you can configure the port to half-duplex (Half) attribute. • When you configure a port to be in auto-negotiation (auto) state, the duplex state of the port is determined by the auto-negotiation between the local port and the peer port. By default, the speed and duplex mode of the port is auto-negotiation.
Open /close	Turn on/off the port. If a port is displayed closed, it cannot forward data. By default, the port is open.
Priority	The priority level of the port is 0 to 7, with 0 being the lowest and 7 being the highest. For packets without the 802.1Q label header, the 48G-4GF will use the port priority as the 802.1p priority for the port to receive packets, and then look up the local priority mapping table based on the priority to mark the packet as a local priority. By default, the port priority is 0.
Flow Control	Turn on or off the port flow control function. If the flow control function is enabled, when the device is congested, it will send a message to the peer switch to notify the peer switch to

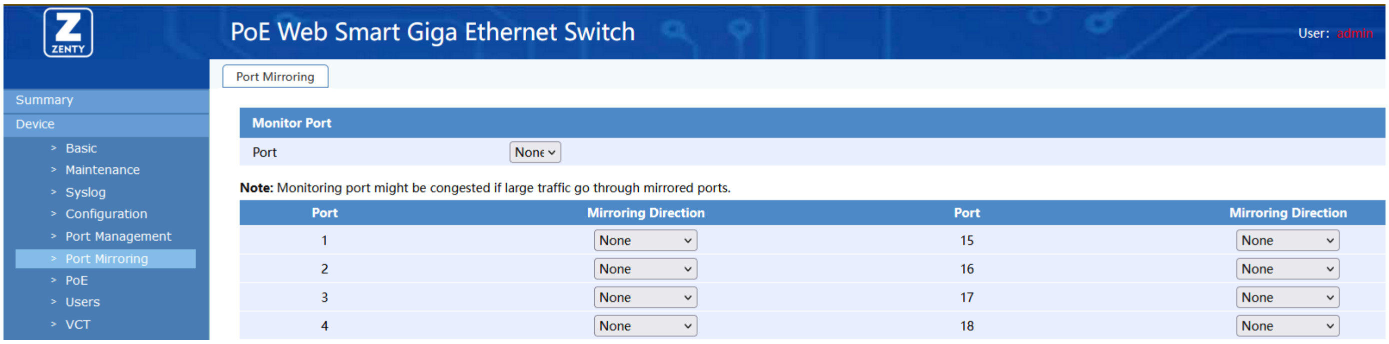
	temporarily stop sending packets or slow down the rate of sending packets, thereby avoiding the occurrence of packet loss and ensuring. The normal operation of the network business. By default, port flow control is disabled.
Isolation	Through the port isolation feature, you can add the ports that need to be controlled to an isolation group ("open" means to join the isolation group; "close" means to exit the isolation group), to achieve the layer 2 data between the ports in the isolation group Isolation not only enhances the security of the network but also provides users with flexible networking solutions. By default, the port is not added to the isolation group.
Energy saving	Turn on or turn off the energy-saving function of the port in the downstate. By default, the function is turned off.
EEE	Enable or disable the EEE (Energy Efficient Ethernet) energy-saving function of the port. By default, the EEE energy-saving function is not enabled.

2.1.6 Device > Port Mirroring

Port mirroring is to copy the mirrored port packets to the monitoring port. The monitoring port is connected to the data detection device. Users use these data detection devices to analyze the packets copied to the monitoring port for network monitoring and troubleshooting.

The switch provides local port mirroring, that is, the mirrored port and monitoring port are on the same device.

Page Wizard: Device → Port Mirroring, click the <No Mirror> button to quickly configure the monitoring port to “None”, and configure the mirroring direction of all ports to “No 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

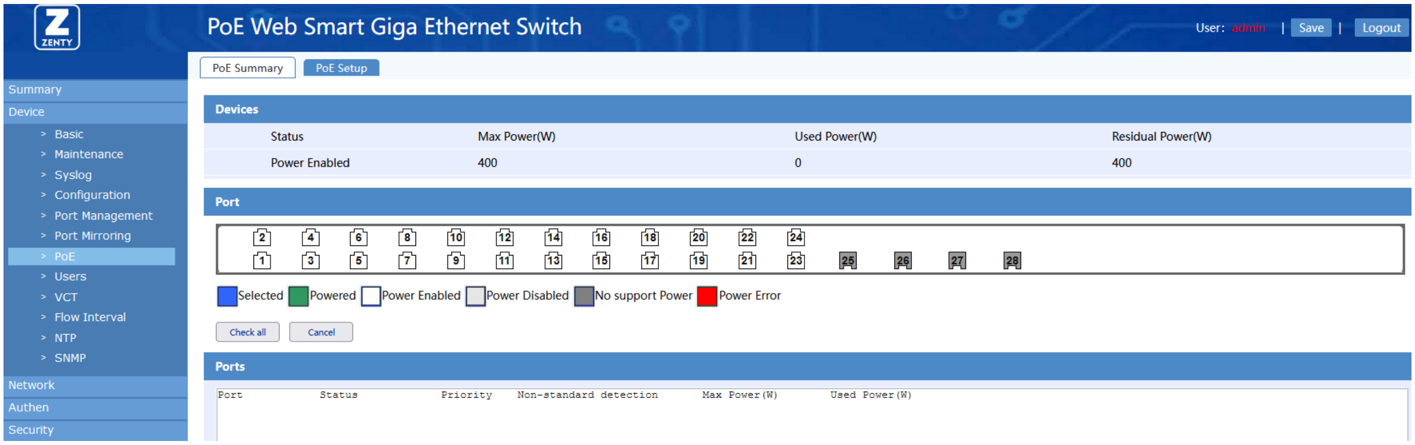
The meaning of the key items on the page is shown in the table below.

Operation	Explanation
Monitoring port	Select the monitoring port, "no mirror" indicates that the port mirroring function of the switch is disabled
Mirroring direction	Select the mirrored port, "no mirror" indicates that the port is not mirrored The meaning of the mirroring direction is as follows: • Mirror incoming port: only the packets received by the port are mirrored to the monitoring port • Mirror out port: only the packets sent by this port are mirrored to the monitoring port • Mirroring in and out ports: packets going in and out of this port are mirrored to the monitoring port

2.1.7 Device > PoE

PoE Summary:

Page Wizard: Device ⟶ PoE ⟶ PoE Summary. Shows the current PoE status for all available ports.



Devices

Status	Max Power(W)	Used Power(W)	Residual Power(W)
Power Enabled	400	0	400

Port

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

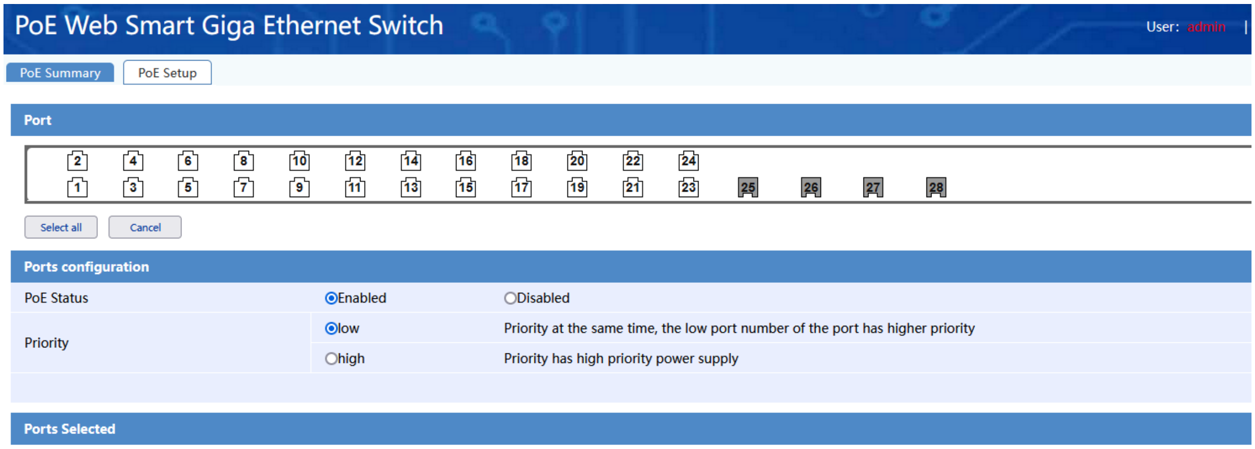
🟦 Selected 🟩 Powered □ Power Enabled □ Power Disabled ■ No support Power 🟥 Power Error

Ports

```
Port          Status          Priority    Non-standard detection      Max Power(W)       Used Power(W)
```

PoE Setup:

Page Wizard: Device ⟶ PoE ⟶ PoE Setup. Allows you to set the PoE status and priority of single or multiple ports.



Port

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

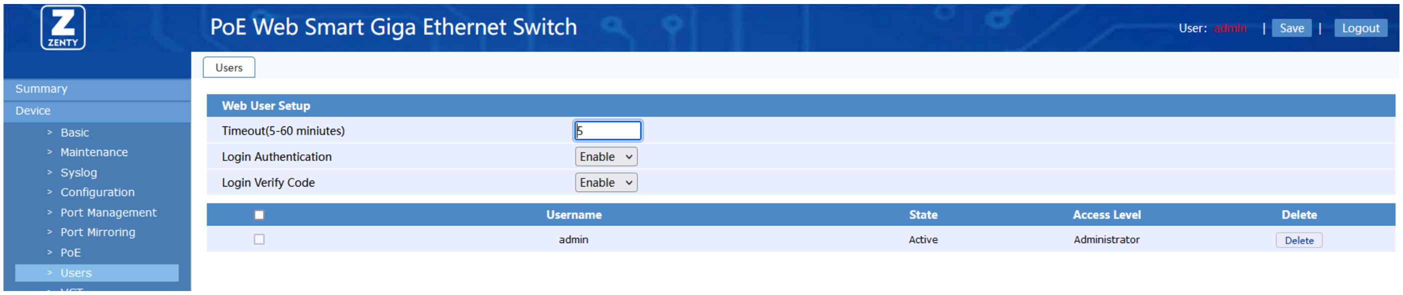
Ports configuration

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

Ports Selected

2.1.8 Device > Users

Page Wizard: Device ⟶ Users. On this page, you can configure the user timeout time, turn on/off the WEB authentication function, and turn on/off the WEB verification code function.



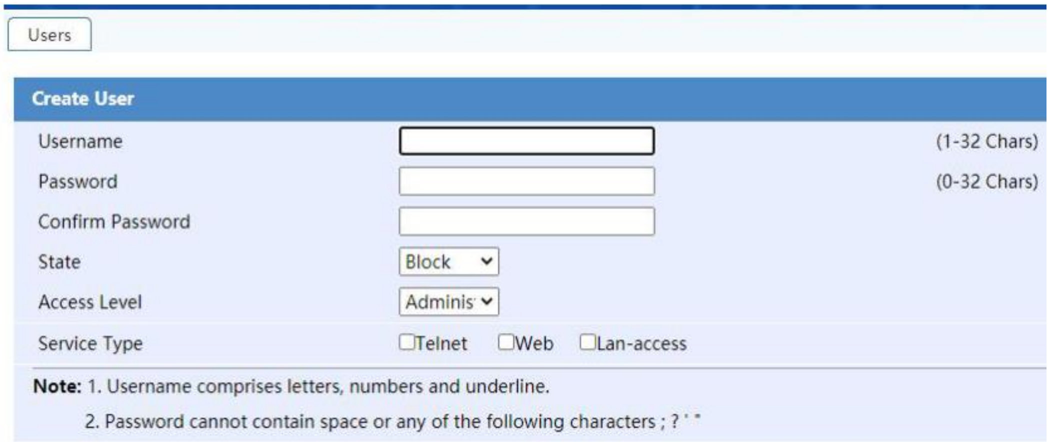
Web User Setup

Timeout(5-60 minitutes)	5
Login Authentication	Enable
Login Verify Code	Enable

■	Username	State	Access Level	Delete
□	admin	Active	Administrator	Delete

Steps to add a local user:

Click the <New> button on the main page, set the new user-related information on the "Add Local User" page, and click the <OK> button to take effect.



Create User

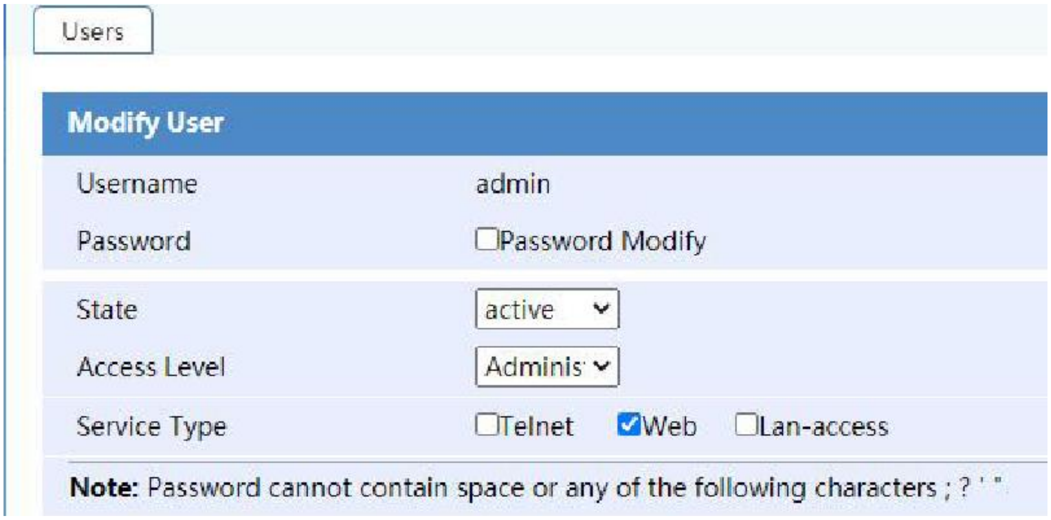
Username		(1-32 Chars)
Password		(0-32 Chars)
Confirm Password		
State	Block	
Access Level	Adminis	
Service Type	□Telnet □Web □Lan-access	

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

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

Steps to modify local users:

Click on the local user entry to be modified on the main page to enter the "Modify Local User" page for modification.



Modify User

Username	admin
Password	□Password Modify
State	active
Access Level	Adminis
Service Type	□Telnet ☑Web □Lan-access

Note: Password cannot contain space or any of the following characters ; ? ' "

The meaning of the key items on the page is shown in the table below.

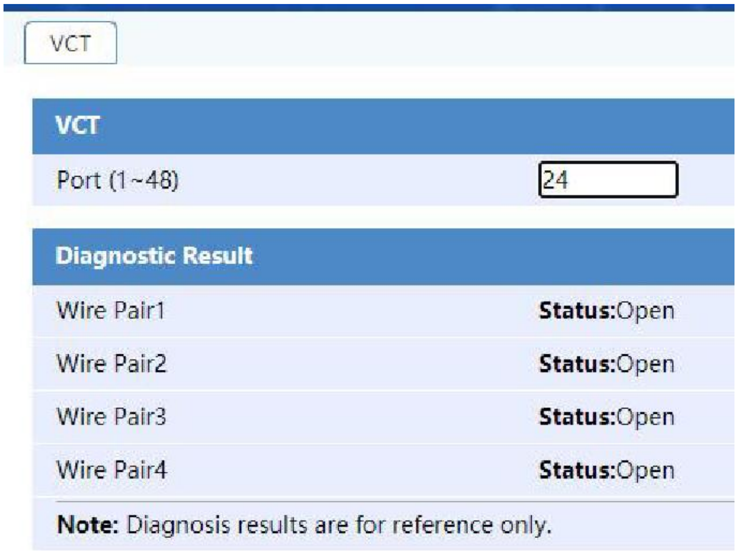
Operation	Explanation
Overtime time	Configure the timeout time of the web settings page, the default is 5 minutes
WEB user authentication	Turn on/off the user authentication function. After closing, the user does not need to verify

	when logging in
WEB login verification code	Turn on/off the WEB login verification code function. After opening, you need to enter the verification code when logging in to WEB
Username	Set the local username to be added
Confirm password	Set local user password
State	Set the status of local users
Rank	Set the level of local users

2.1.9 Device > VCT

When the line is faulty, you can diagnose the cable connected to the port, which is convenient for you to check the working condition of the cable in the network.

Page Wizard: Device → VCT. Enter the port number to be diagnosed in the "Port" text box and click the <OK> button to complete the cable diagnosis of the port.



VCT

Port (1~48) 24

Diagnostic Result

Wire Pair1 **Status:**Open

Wire Pair2 **Status:**Open

Wire Pair3 **Status:**Open

Wire Pair4 **Status:**Open

Note: Diagnosis results are for reference only.

The meaning of the key items on the page is shown in the table below.

Operation	Explanation
State	Display the connection status of the port. The display as "normal" indicates that the port is connected; the display as "open" indicates that the port is not connected; the display as "short circuit" indicates that a pair of differential lines

	have a short circuit.
Length	- When the cable status is "normal", the length of the connecting cable is not reflected in the displayed information. - When the cable status is "short circuit or open circuit", the length in the displayed information refers to the length from the port to the abnormal position.

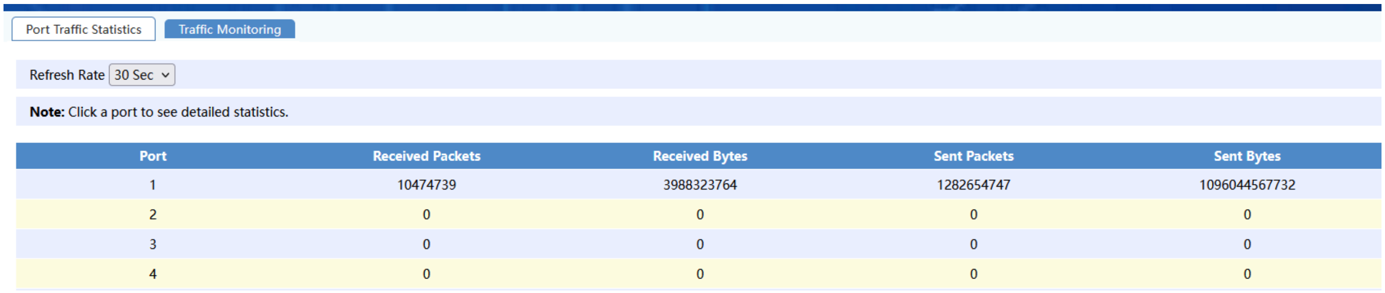
- During the cable diagnosis process, please do not plug or unplug the port network cable, and the diagnosed port cannot be in the shutdown state.

- The cable diagnosis is only valid when there is no device connection at the other end of the network cable or the network cable is abnormal. When both ends of the network cable is connected, the diagnosis result may be invalid. For normal network cable quality testing, please use professional network cable testing.

2.1.10 Device > Flow Interval

Port Traffic Statistics:

Page Wizard: Device ⟶ Flow Interval ⟶ Port Traffic Statistics. The port statistics page can view the number of data packets received/sent by each port of the switch.

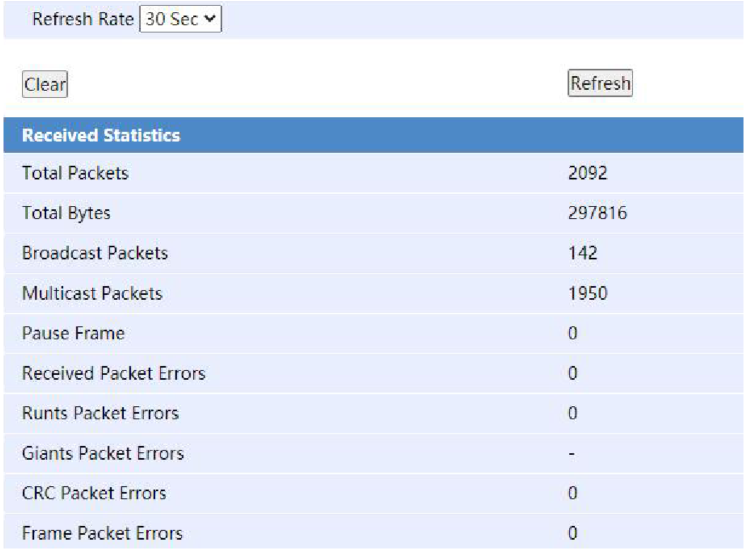


Refresh Rate 30 Sec

Note: Click a port to see detailed statistics.

Port	Received Packets	Received Bytes	Sent Packets	Sent Bytes
1	10474739	3988323764	1282654747	1096044567732
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0

To view, the number of various types of error packets received/sent on the designated port of the 48G-4GF device (click the entry corresponding to the port on the main page to enter the corresponding statistical information page).



Refresh Rate: 30 Sec

Received Statistics	
Total Packets	2092
Total Bytes	297816
Broadcast Packets	142
Multicast Packets	1950
Pause Frame	0
Received Packet Errors	0
Runts Packet Errors	0
Giants Packet Errors	-
CRC Packet Errors	0
Frame Packet Errors	0

The meaning of the key items on the page is shown in the table below.

Operation	Explanation
Refresh rate	You can select the refresh rate to automatically update the statistics of the current page regularly.
Statistics reset	You can click this button to clear the statistics of the current page.
Statistics refresh	You can click this button to immediately update the statistics of the current page.

Description of the packets received/sent on the port:

Message	Explanation
Receive Statistics	
Total packet	Total number of received messages.
Total bytes	Total bytes of received messages.
Broadcast package	Total number of broadcast messages received.
Multicast package	Total number of multicast messages received.
Receive error packets	The total number of received error packets.
Runts error package	Number of packets with correct CRC and data

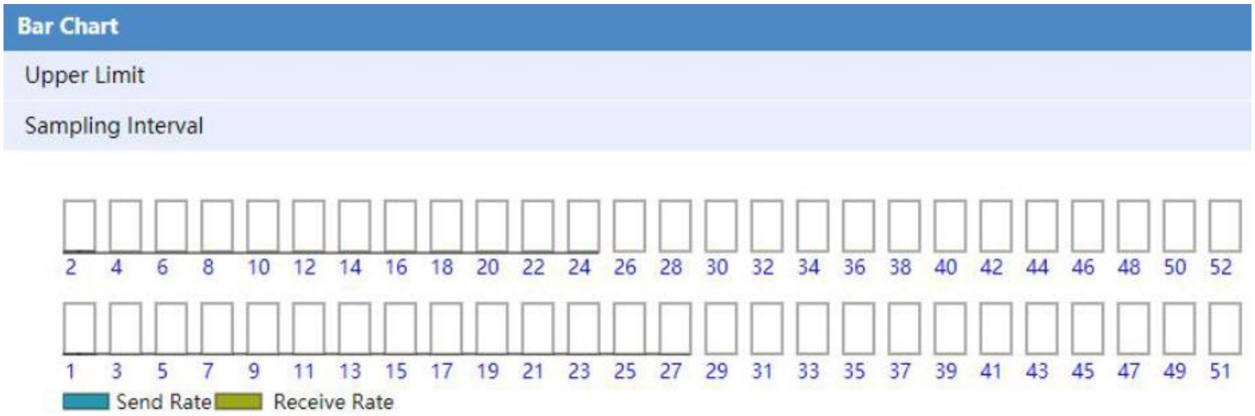
	frame length less than 64 bytes.
Giants error package	Number of packets with correct CRC and data frame length greater than 1518 bytes.
CRC error packet	Number of packets with CRC error and data frame length between 64 and 1518 bytes.
Frame error packet	The length of the data frame is between 64 and 1518 bytes, and the number of FCS (Frame Check Sequence) bytes of the message is a non-integer message.
Aborts error package	The total number of illegal packets received. The illegal packets include: • Message fragmentation: frames with a length less than 64 bytes (the length can be an integer or non-integer) and the CRC check error. • Jabber frame: greater than 1518 or 1522 bytes, and CRC check error (message bytes can be an integer or non-integer). • Symbol error frame: the message contains at least one erroneous symbol. • Length error frame: The 802.3 length field in the message does not match the actual length of the message (46 to 1500 bytes).
Ignored error package	Number of packets discarded due to insufficient receive buffers on the port.
Send Statistics	
Total packet	Total number of messages sent.
Total bytes	Total number of bytes sent.
Broadcast package	Total number of broadcast messages sent.
Multicast package	Total number of multicast messages sent.
Send error packet	Total number of error messages sent.

Aborts error package	The total number of packets that failed to send, that is, the packets have been sent, but due to various reasons (such as conflict).
Deferred error packet	Number of packets delayed by the first transmission request due to a busy network.
Collisions error package	Number of conflicting packets generated by the port during packet transmission.
Late collisions error package	The number of delayed collision frames. The delayed collision frame means that the first 512 bits of the frame has been sent. Due to the detection of a collision, the frame is delayed.

Traffic Monitoring

Page Wizard: Device → Flow Interval → Traffic Monitoring. Through port traffic monitoring, users can graphically monitor the current traffic of each port of the device and the changes in traffic over a specified period of time. Flow monitoring consists of flow monitoring histogram and flow monitoring line chart:

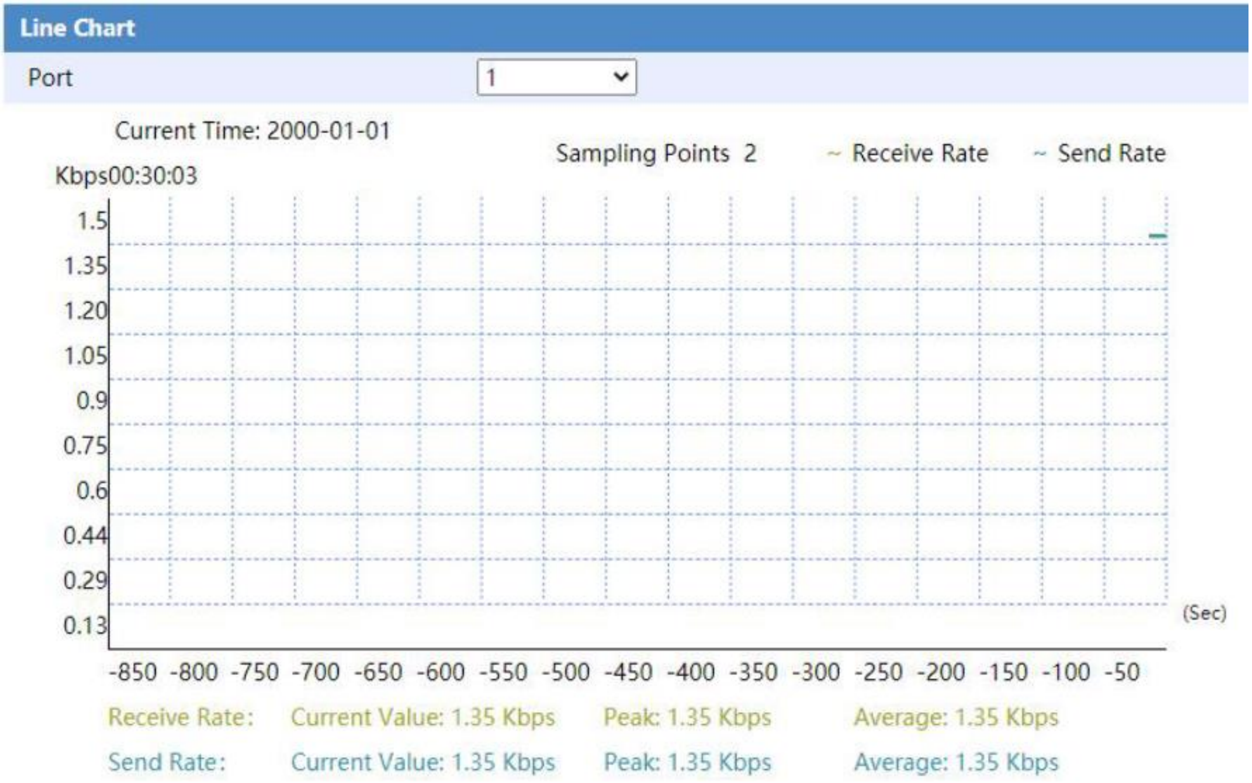
- Flow monitoring histogram: Use the histogram to display the status of each port's current receiving rate and sending rate.
- Flow monitoring line chart: display the flow change of a specified port over a period of time in a line fluctuation manner.



Bar Chart

Upper Limit

Sampling Interval

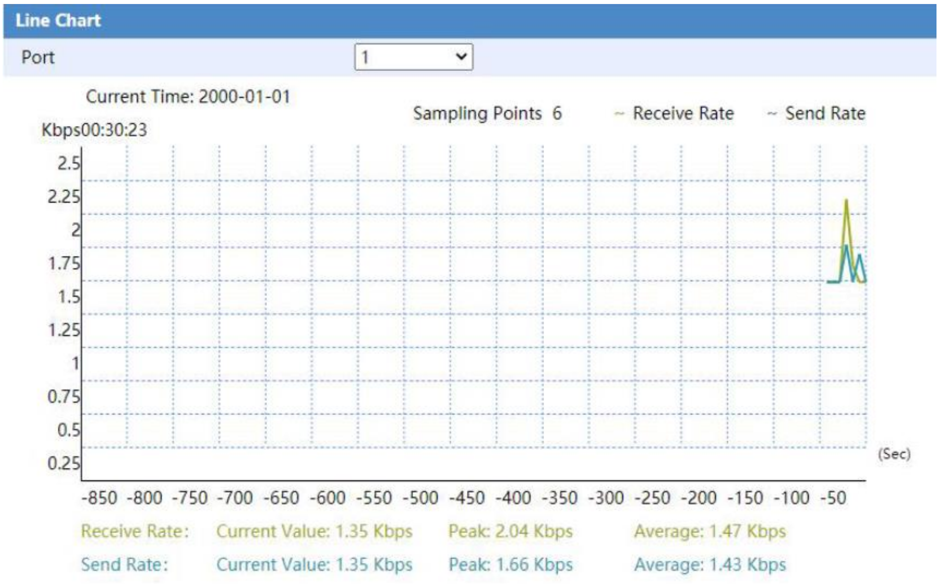


Receive Rate: Current Value: 1.35 Kbps Peak: 1.35 Kbps Average: 1.35 Kbps

Send Rate: Current Value: 1.35 Kbps Peak: 1.35 Kbps Average: 1.35 Kbps

The flow monitoring histogram page can realize the following functions:

- Monitoring port traffic through rate histogram.
- Select the upper limit of the histogram in the drop-down box of “Traffic Upper Limit”, you can observe the proportion of each port's receive/send rate relative to the upper limit. When the proportion exceeds 95%, the histogram border will have a red warning.
- Select the time interval in the "Sampling interval" drop-down box, you can make the page refresh at this time interval.
- Move the mouse to a port histogram, and a yellow text box will appear, showing the port number, receiving rate, and sending rate. Click the histogram, you can observe the line rate chart of the port.
- Click the <Stop Monitoring> button on the page to pause the traffic monitoring; click the <Resume Monitoring> button to resume the traffic monitoring.



Line Chart

Port: 1

Current Time: 2000-01-01 00:30:23

Sampling Points 6

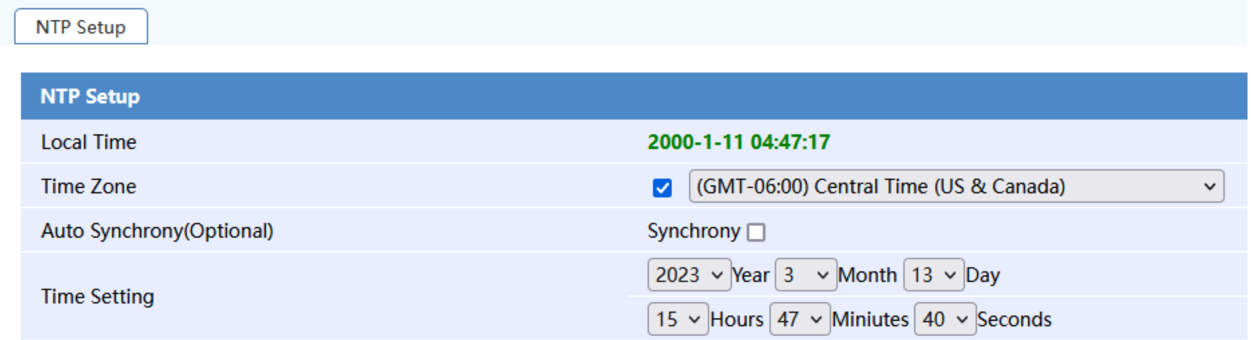
Receive Rate:	Current Value: 1.35 Kbps	Peak: 2.04 Kbps	Average: 1.47 Kbps
Send Rate:	Current Value: 1.35 Kbps	Peak: 1.66 Kbps	Average: 1.43 Kbps

The flow monitoring line chart page can realize the following functions:

- Monitor port traffic through rate line chart.
- Click the port number in the histogram or select the specified port in the "Port Number" drop-down box, you can observe the rate change of the port in real-time.
- The current value, peak value and average value of the receiving rate and sending rate are displayed at the bottom of the line chart.

2.1.11 Device > NTP

Page Wizard: Device ⟶ NTP Setup. NTP is an acronym for Simple Network Time Protocol, a network protocol for synchronizing the clocks of computer systems. You can specify NTP Servers and set GMT Time zone.



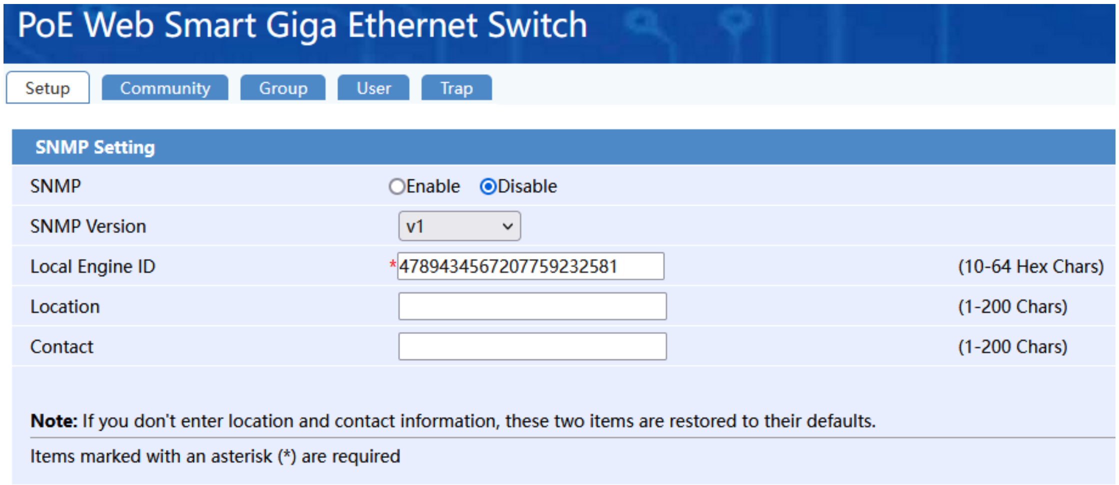
NTP Setup

Local Time	2000-1-11 04:47:17
Time Zone	☑ (GMT-06:00) Central Time (US & Canada)
Auto Synchrony(Optional)	Synchrony □
Time Setting	2023 Year 3 Month 13 Day 15 Hours 47 Miniutes 40 Seconds

2.1.12 Device > SNMP

Setup:

Page Wizard: Device → SNMP → Setup. On this page you can configure SNMP agent enable, SNMP version, local engine ID, physical location information, contact information.



SNMP Setting

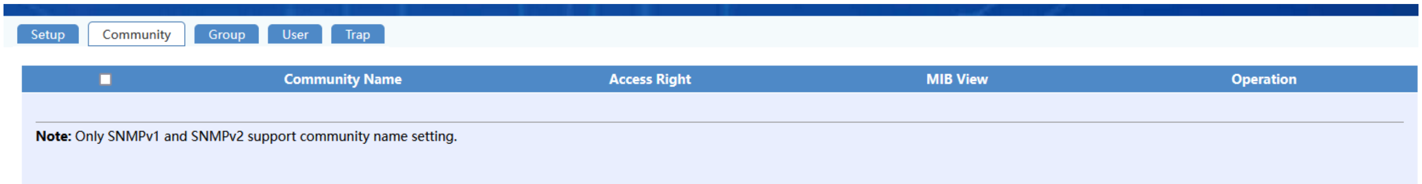
SNMP	○Enable ●Disable	
SNMP Version	v1	
Local Engine ID	*4789434567207759232581	(10-64 Hex Chars)
Location		(1-200 Chars)
Contact		(1-200 Chars)

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

Community:

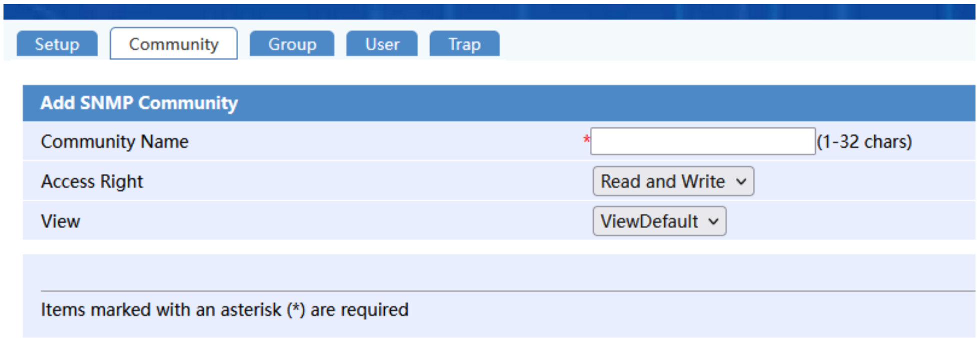
Page Wizard: Device → SNMP → Community. On this page you can display or create a new SNMP community.



□	Community Name	Access Right	MIB View	Operation

Note: Only SNMPv1 and SNMPv2 support community name setting.

Click the "New" button to enter the new SNMP community page. The user can configure the name of the newly created community, the access rights, and views of the community. The configuration page is shown in the following figure:



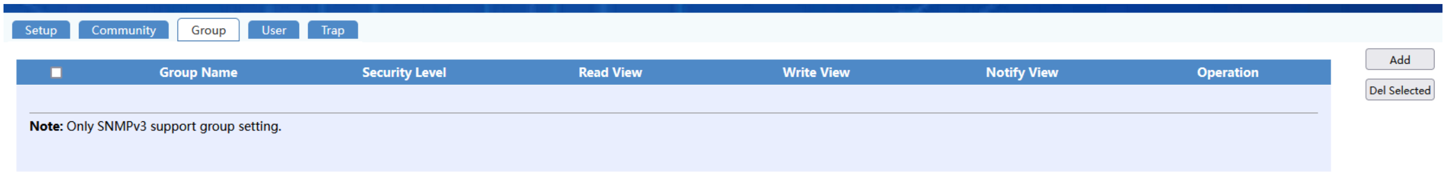
Add SNMP Community

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

Items marked with an asterisk (*) are required

Group:

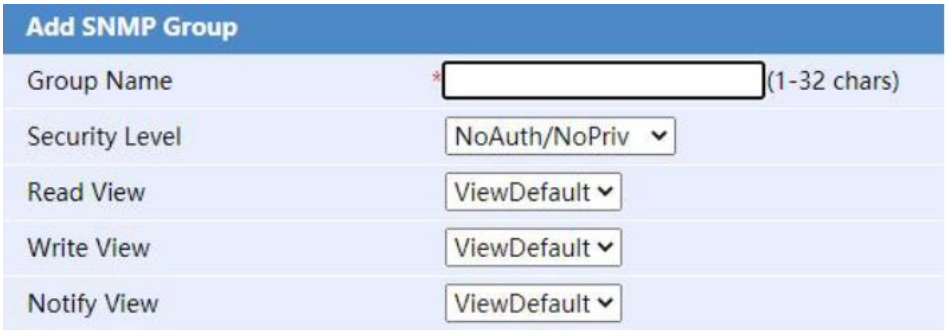
Page Wizard: Device ⟶ SNMP ⟶ Group. On this page you can display or create a new SNMP group.



□	Group Name	Security Level	Read View	Write View	Notify View	Operation

Note: Only SNMPv3 support group setting.

Click "New" to enter the new SNMP group page, the user can configure the group name, security level and view permissions of the newly created group.

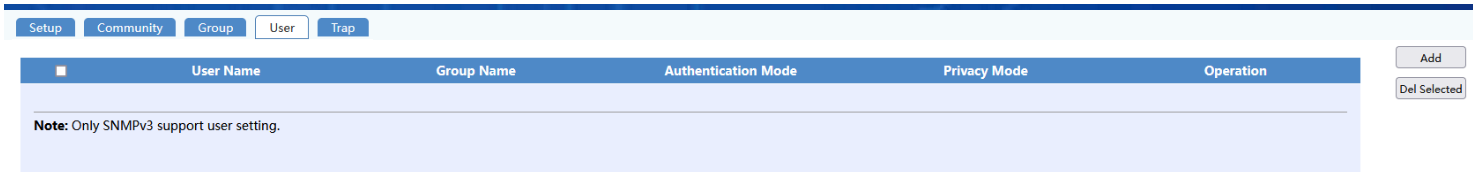


Add SNMP Group

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

User:

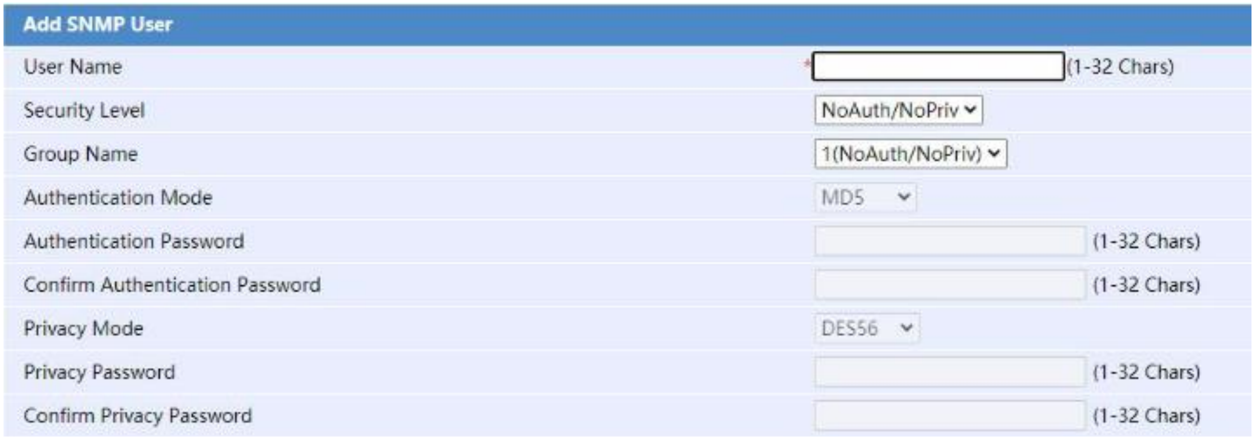
Page Wizard: Device ⟶ SNMP ⟶ User. On this page, can display or create new SNMP users.



□	User Name	Group Name	Authentication Mode	Privacy Mode	Operation

Note: Only SNMPv3 support user setting.

Click "New" to enter the new user page, the user can configure the user-name, security level, and authentication mode of the new user and other relevant information.

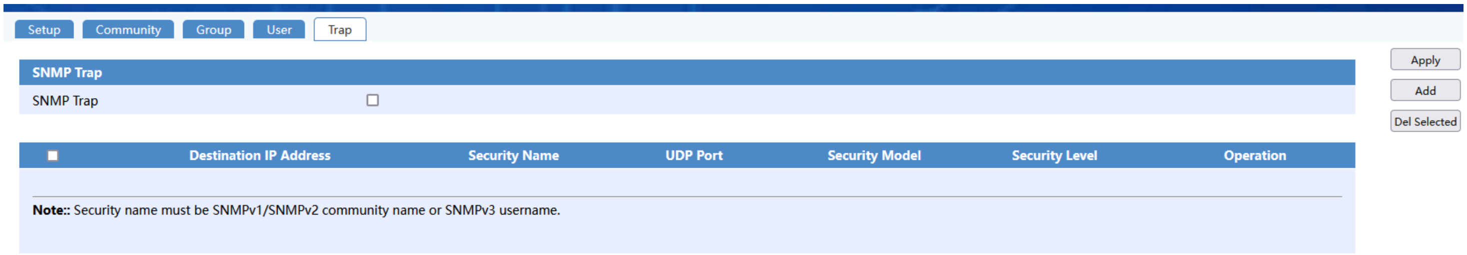


Add SNMP User

User Name	* (1-32 Chars)
Security Level	NoAuth/NoPriv
Group Name	1(NoAuth/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)

Trap:

Page Wizard: Device ⟶ SNMP ⟶ Trap. On this page you can configure to turn on/off the SNMP trap function, display trap host information, and create a new trap host.



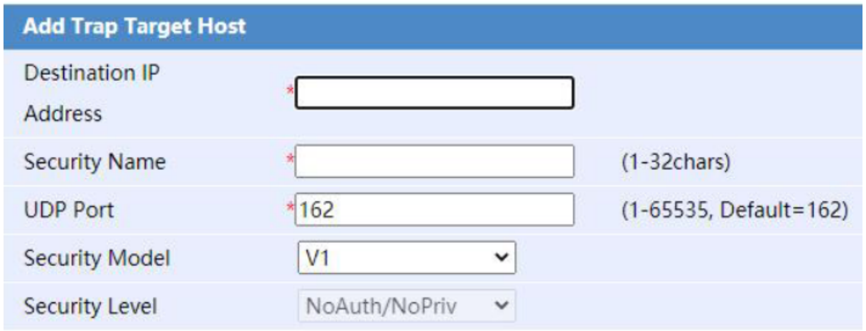
SNMP Trap

SNMP Trap □

□	Destination IP Address	Security Name	UDP Port	Security Model	Security Level	Operation

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

Click "New" to enter the new Trap host page, the user can configure the IP address, security name, UDP port, security model, the security level of the new Trap host.



Add Trap Target Host

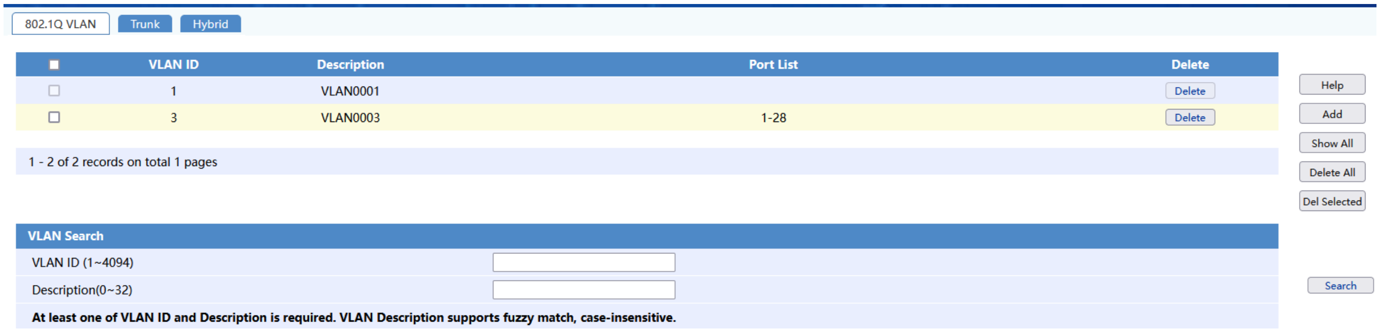
Destination IP Address	*	
Security Name	*	(1-32chars)
UDP Port	* 162	(1-65535, Default=162)
Security Model	V1	
Security Level	NoAuth/NoPriv	

2.2 Network Menu Information

2.2.1 Network > VLAN

802.1Q VLAN:

Page Wizard: Network ⟶ VLAN ⟶ 802.1Q VLAN. This page can display and query the VLAN information and the ports it contains (the main page. VLAN 1 includes all ports by default).



□	VLAN ID	Description	Port List	Delete
□	1	VLAN0001		Delete
□	3	VLAN0003	1-28	Delete

1 - 2 of 2 records on total 1 pages

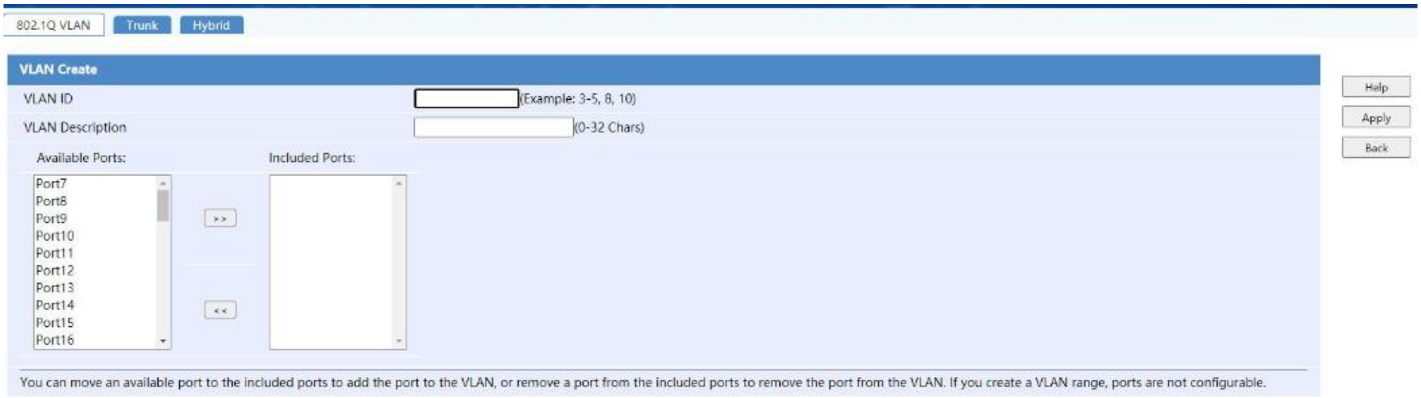
VLAN Search

VLAN ID (1~4094)

Description(0~32)

At least one of VLAN ID and Description is required. VLAN Description supports fuzzy match, case-insensitive.

Create a new VLAN (click the <New> button on the main page to enter the corresponding page, as shown below. Enter the VLAN you want to create in the "VLAN ID" text box and click the <OK> button to take effect), and create a new Access port (Click on the main page Select the port to be added to the VLAN, and click the <OK> button to take effect).



VLAN Create

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

VLAN Description (0-32 Chars)

Available Ports: Port7, Port8, Port9, Port10, Port11, Port12, Port13, Port14, Port15, Port16

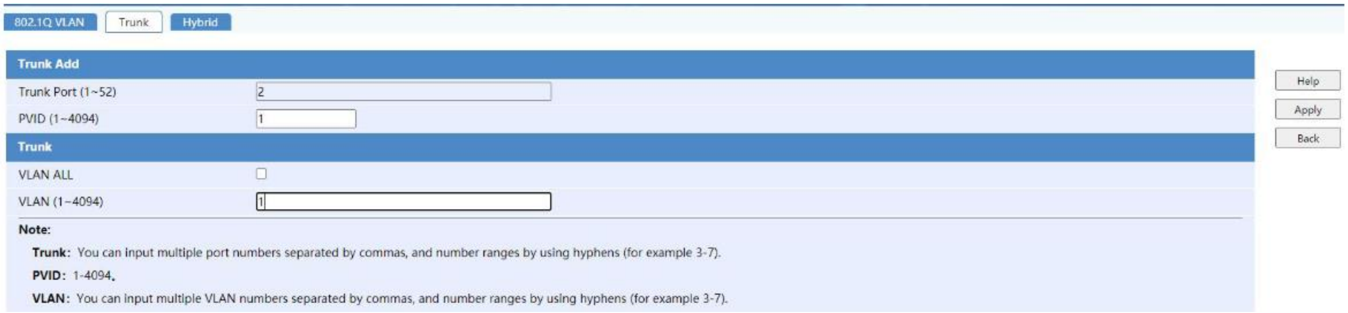
Included Ports:

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.

Trunk:

Page Wizard: Network → VLAN → Trunk. Displays the current port information.

Steps to create a new trunk port: Click the <New> button on the main page to enter the corresponding page. Specify the trunk port, configure the PVID and the port to allow the VLAN, and click the <OK> button to take effect.



Trunk Add

Trunk Port (1~52)	2
PVID (1~4094)	1

Trunk

VLAN ALL	□
VLAN (1~4094)	1

Note:

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

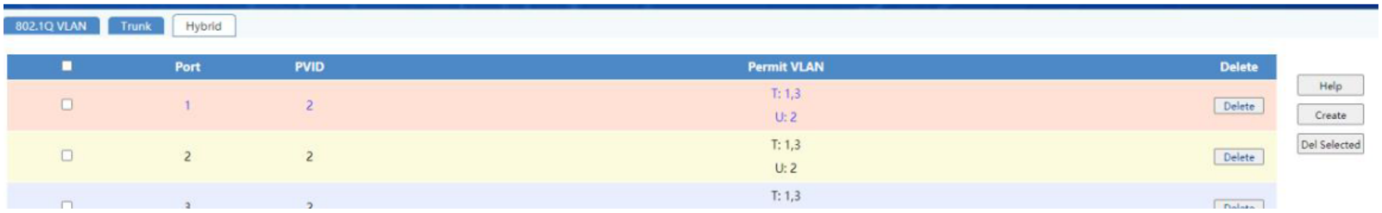
PVID: 1-4094.

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

Steps to modify Trunk port: Click the entry corresponding to the port on the main page to enter the corresponding page. Modify the PVID and port allowed to pass VLAN, click <OK> button to take effect.

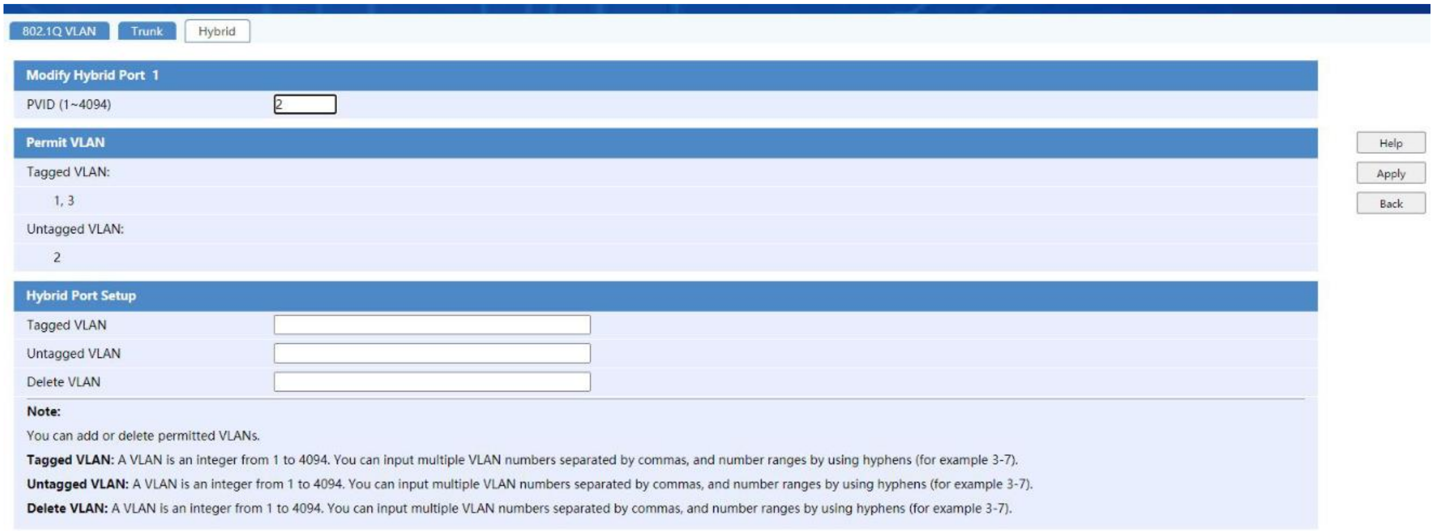
Hybrid:

Page Wizard: Network → VLAN → Hybrid. The page is shown in the figure below, showing the current Hybrid port information of the switch.



■	Port	PVID	Permit VLAN	Delete
□	1	2	T: 1,3 U: 2	Delete
□	2	2	T: 1,3 U: 2	Delete
□	3	2	T: 1,3	Delete

Steps to create a new Hybrid port: Click the <New> button on the main page to enter the corresponding page. Specify the Hybrid port, and configure the PVID and port to pass through the VLAN. Click the <OK> button to take effect.



Modify Hybrid Port 1

PVID (1~4094) 2

Permit VLAN

Tagged VLAN:

1, 3

Untagged VLAN:

2

Hybrid Port Setup

Tagged VLAN

Untagged VLAN

Delete VLAN

Note:

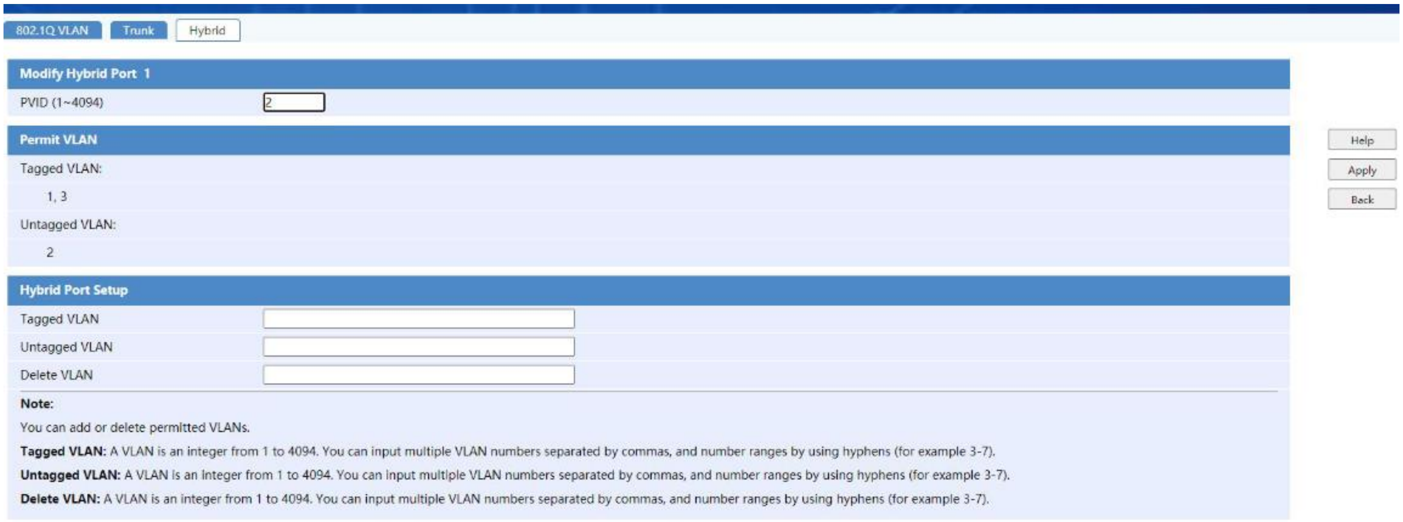
You can add or delete permitted VLANs.

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).

Steps to modify Hybrid port: Click the entry corresponding to the port on the main page to enter the corresponding page. Modify the PVID and port allowed to pass VLAN, click <OK> button to take effect.



Modify Hybrid Port 1

PVID (1~4094) 2

Permit VLAN

Tagged VLAN:

1, 3

Untagged VLAN:

2

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).

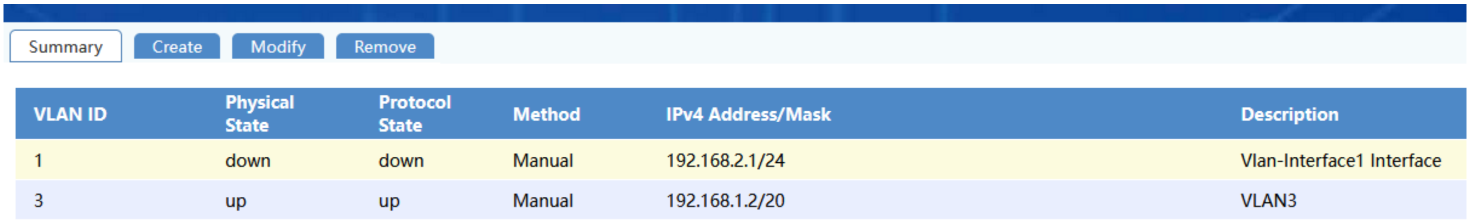
- PVID: number, the value range is 1-4094.
- Tagged VLAN: number, the value range is 1-4094, you can enter multiple values, separated by commas. A short line can be used to indicate a range.
- Untagged VLAN: number, the value range is 1-4094, you can enter multiple values, separated by commas. A short line can be used to indicate a range.
- Delete VLAN: number, the value range is 1-4094, you can enter multiple values, separated by commas. A short line can be used to indicate a range.

2.2.2 Network > VLAN Interface

The VLAN interface menu is mainly used to configure and manage Layer 3 VLAN interfaces of the device, including interface display, new interface creation, interface modification, and interface deletion.

Summary:

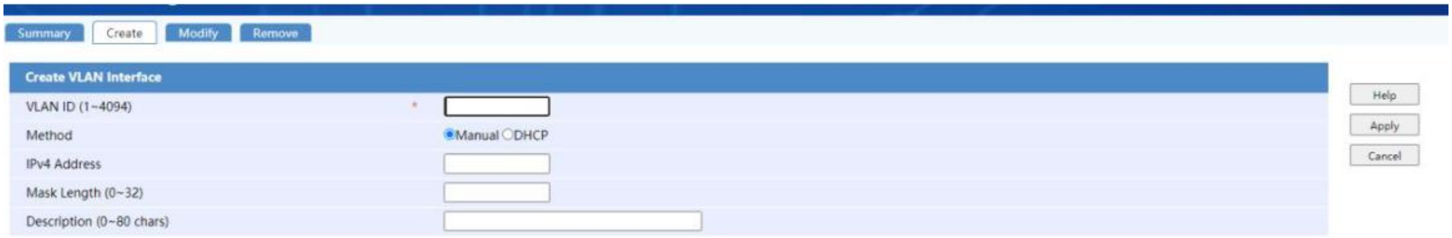
Page Wizard: Network ⟶ VLAN Interface ⟶ Summary. Users can query the interface, interface status and interface information of the current device through this page.



VLAN ID	Physical State	Protocol State	Method	IPv4 Address/Mask	Description
1	down	down	Manual	192.168.2.1/24	Vlan-Interface1 Interface
3	up	up	Manual	192.168.1.2/20	VLAN3

Create:

Page Wizard: Network ⟶ VLAN Interface ⟶ Create. Users can create a new Layer 3 VLAN interface through this page and configure the address acquisition method of the interface. If it is a static acquisition method, you can also configure specific interface address information.

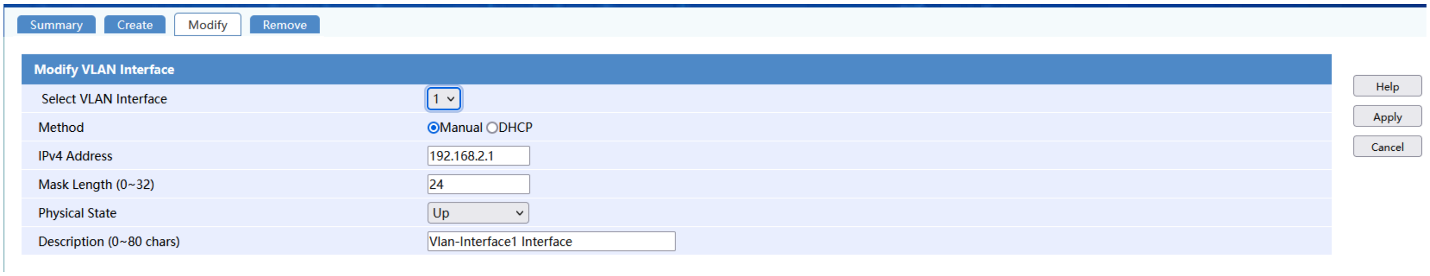


Create VLAN Interface

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

Modify:

Page Wizard: Network ⟶ VLAN Interface ⟶ Modify. The user can modify the three-layer VLAN interface through this page and can modify the IP address of the interface. If it is a static IP acquisition method, the interface address information can also be modified.

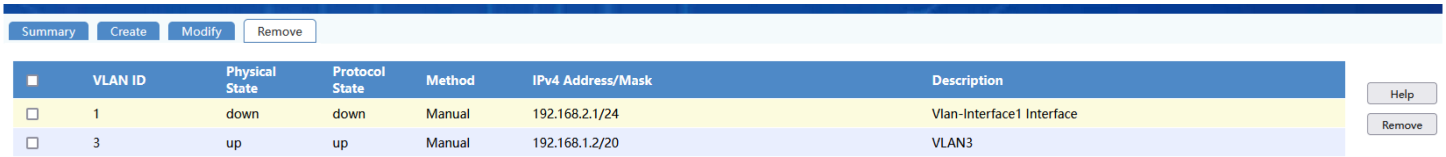


Modify VLAN Interface

Select VLAN Interface	1
Method	● Manual ○ DHCP
IPv4 Address	192.168.2.1
Mask Length (0~32)	24
Physical State	Up
Description (0~80 chars)	Vlan-Interface1 Interface

Remove:

Page Wizard: Network ⟶ VLAN Interface ⟶ Remove. Users can delete the specified Layer 3 VLAN interface through this page. The configuration page is as follows:

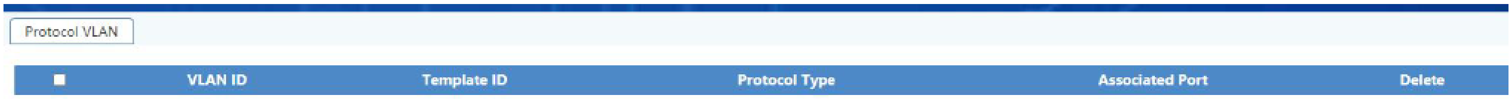


□	VLAN ID	Physical State	Protocol State	Method	IPv4 Address/Mask	Description
□	1	down	down	Manual	192.168.2.1/24	Vlan-Interface1 Interface
□	3	up	up	Manual	192.168.1.2/20	VLAN3

2.2.3 Network > Protocol VLAN

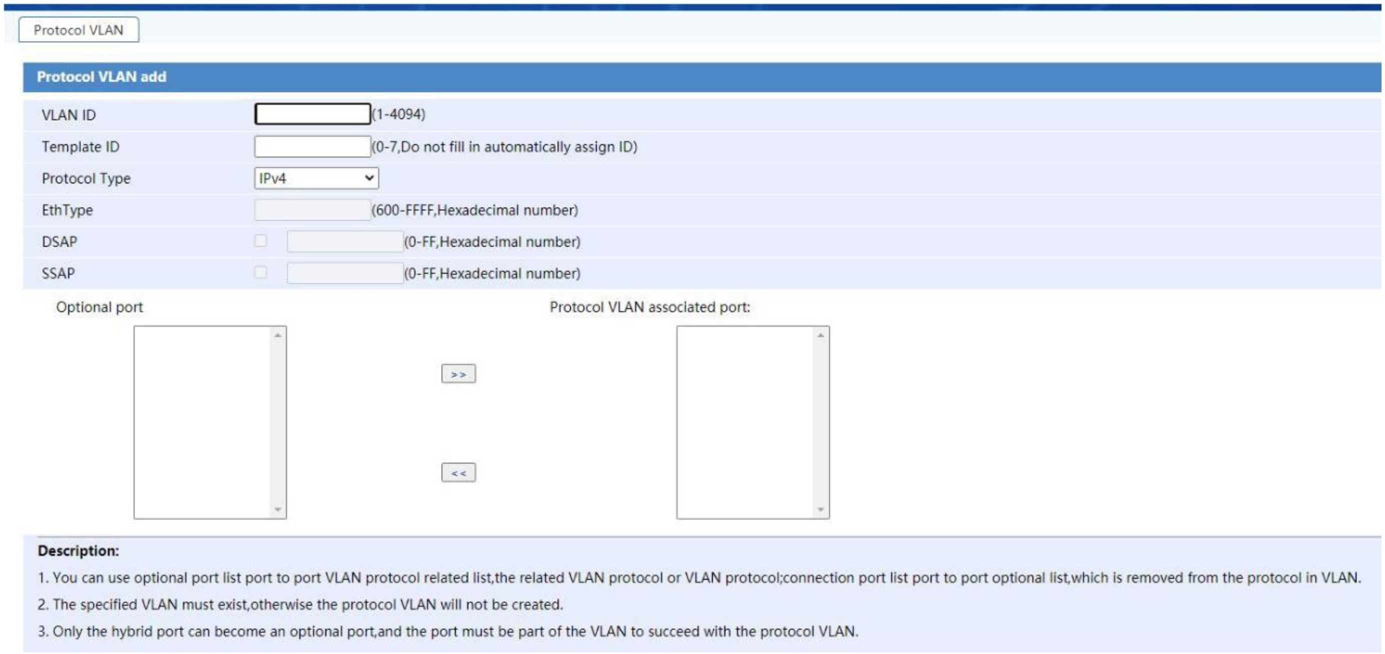
Protocol VLAN, also known as protocol-based VLAN, is another VLAN division method to distinguish port-based VLAN. By configuring protocol-based VLAN, the switch can analyze the packets received without VLAN information on the port, and match the packets with the protocol template set by the user according to the different encapsulation formats and the values of special fields, and automatically Successful packets are added with the VLAN tag configured in the protocol template to automatically distribute data belonging to the specified protocol to the corresponding VLAN for transmission.

Page Wizard: Network ⟶ Protocol VLAN, on this page you can view the configured protocol VLAN information.



□	VLAN ID	Template ID	Protocol Type	Associated Port	Delete

Click the <New> button on the protocol VLAN display page to create a protocol VLAN:



VLAN ID	(1-4094)
Template ID	(0-7,Do not fill in automatically assign ID)
Protocol Type	IPv4
EthType	(600-FFFF,Hexadecimal number)
DSAP	□ (0-FF,Hexadecimal number)
SSAP	□ (0-FF,Hexadecimal number)

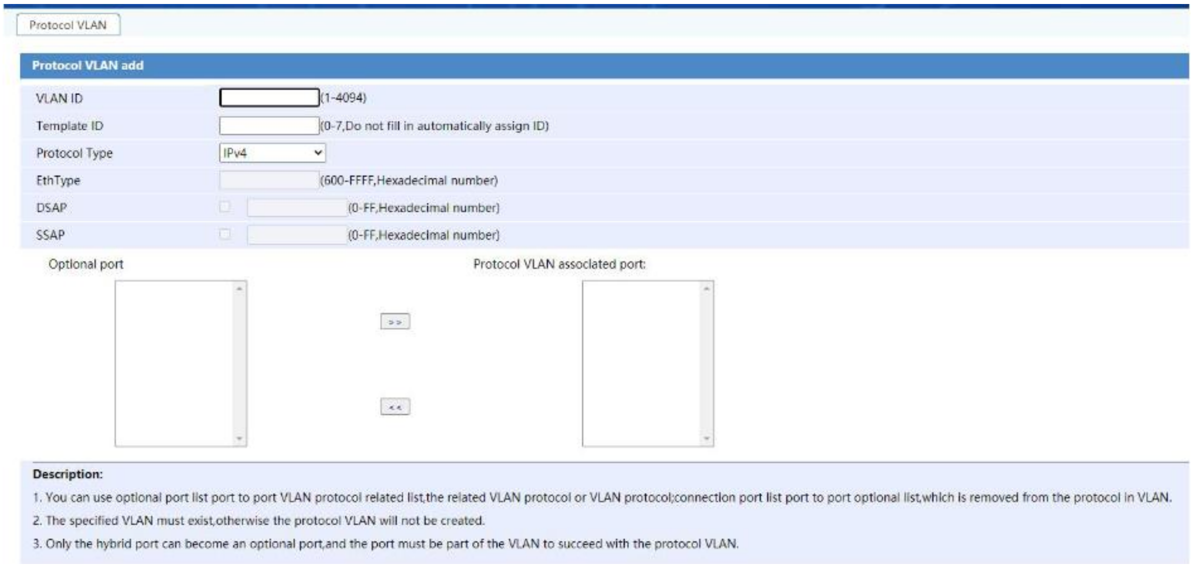
Description:

1. You can use optional port list port to port VLAN protocol related list,the related VLAN protocol or VLAN protocol;connection port list port to port optional list,which is removed from the protocol in VLAN.
2. The specified VLAN must exist,otherwise the protocol VLAN will not be created.
3. Only the hybrid port can become an optional port,and the port must be part of the VLAN to succeed with the protocol VLAN.

The meaning of the key items on the page is shown in the table below.

Operation	Explanation
VLAN ID	VLAN ID of the newly created protocol VLAN
Template ID	Template ID of the protocol VLAN
Protocol type	Protocol type of protocol VLAN, support IPv4, IPv6, AT (appletalk), IPx ethernetii, IPx LLC, IPx raw, IPx snap, MODE ethernetii, MODE LLC, MODE snap
Eth Type	Ethernet protocol type value when the protocol type is MODE ethernetii or MODE snap
DSAP	Destination service access point when the protocol type is MODE snap
SSAP	Source service access point when the protocol type is MODE snap

Click the protocol VLAN entry on the protocol VLAN display page to enter the corresponding protocol VLAN modification page, which can modify the protocol VLAN associated port configuration.



VLAN ID	(1-4094)
Template ID	(0-7,Do not fill in automatically assign ID)
Protocol Type	IPv4
EthType	(600-FFFF,Hexadecimal number)
DSAP	□ (0-FF,Hexadecimal number)
SSAP	□ (0-FF,Hexadecimal number)

Description:

1. You can use optional port list port to port VLAN protocol related list,the related VLAN protocol or VLAN protocol;connection port list port to port optional list,which is removed from the protocol in VLAN.
2. The specified VLAN must exist,otherwise the protocol VLAN will not be created.
3. Only the hybrid port can become an optional port,and the port must be part of the VLAN to succeed with the protocol VLAN.

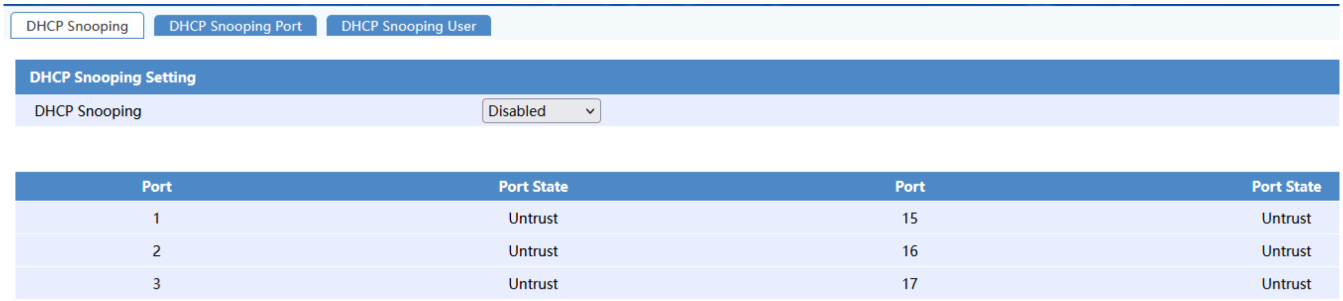
2.2.4 Network > DHCP Snooping

DHCP Snooping technology is a DHCP security feature. Untrusted DHCP information is filtered by establishing and maintaining a DHCP Snooping binding table. This information refers to DHCP information from untrusted areas. The DHCP Snooping binding table contains information such as the MAC address, IP address, lease period, and VLAN-ID interface of users in the untrusted zone.

- The main function of DHCP-snooping is to isolate illegal DHCP server by configuring untrusted ports.
- Cooperate with the switch DAI to prevent the spread of the ARP virus.
- Establish and maintain a DHCP-snooping binding table. This table is generated by the IP and MAC addresses in the DHCP ack package, and the second is manually specified. This table is the basis for subsequent DAI (dynamic arp inspect) and IP Source Guard. These two similar technologies use this table to determine whether the IP or MAC address is legal and restrict users from connecting to the network.

DHCP Snooping:

Page Wizard: Network ⟶ DHCP Snooping. On this page you can turn on/off the DHCP Snooping function.



DHCP Snooping Setting

DHCP Snooping	Disabled

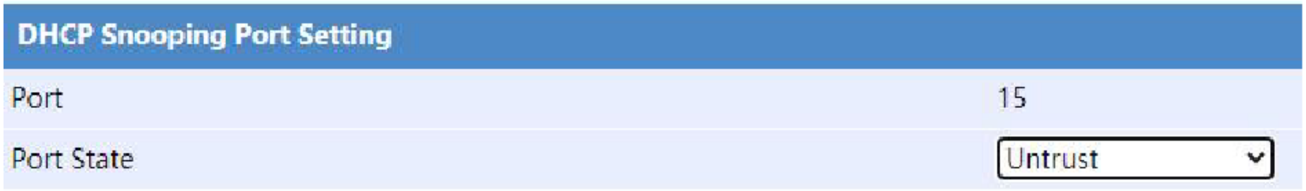
Port	Port State	Port	Port State
1	Untrust	15	Untrust
2	Untrust	16	Untrust
3	Untrust	17	Untrust

DHCP Snooping Port:

Page Wizard: Network ⟶ DHCP Snooping Port.

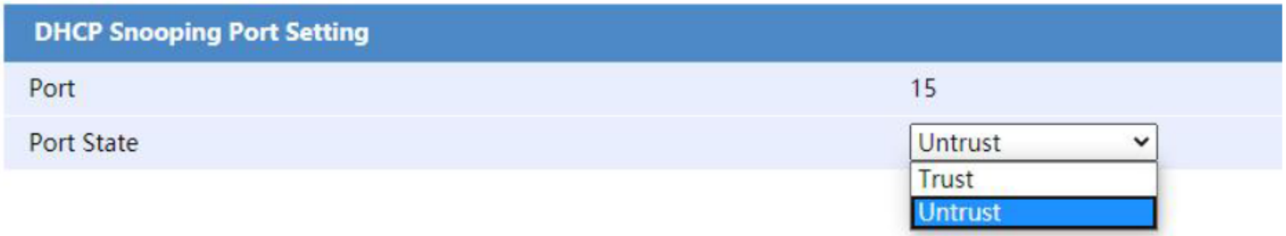
1. Configure a single port:

Click the corresponding entry in the port trust status bar on the page. Enter the corresponding configuration page and select the trust status of the port.



DHCP Snooping Port Setting

Port	15
Port State	Untrust

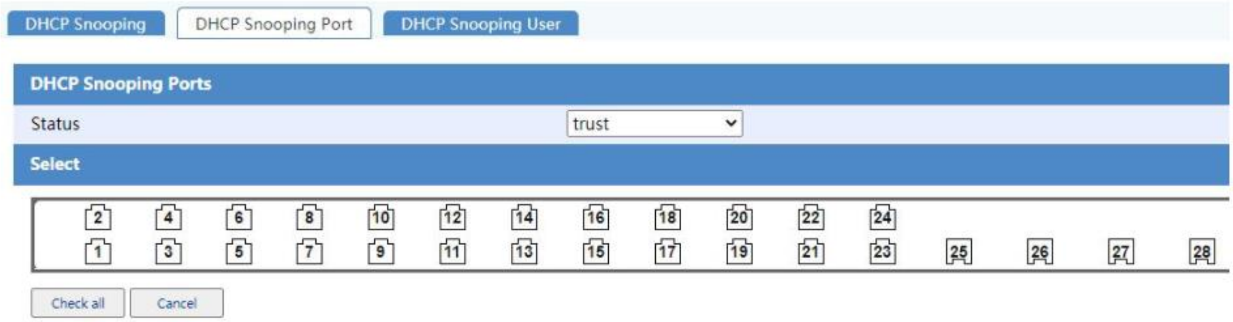


DHCP Snooping Port Setting

Port	15
Port State	Untrust

2. Set ports in batches:

Select the trust status of the port under the Port Batch Settings column.

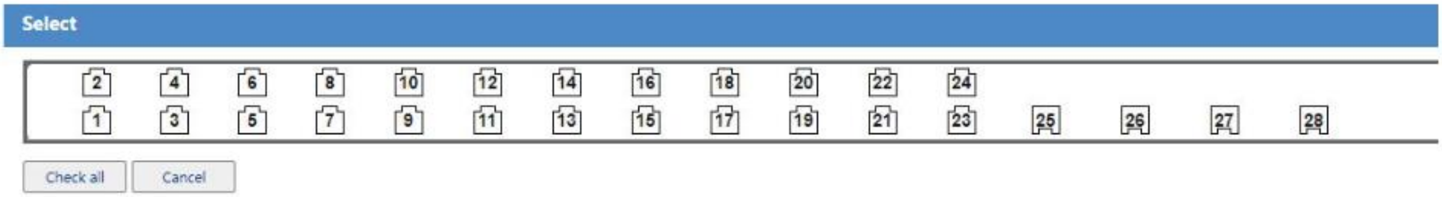


DHCP Snooping Ports

Status	trust

Select

In the Select Port column, you can select ports in batches.



DHCP Snooping User:

Page Wizard: Network ⟶ DHCP Snooping User. On this page, you can view the user MAC address, IP address, VLAN-ID interface, and other information of the untrusted zone in the DHCP Snooping binding table.

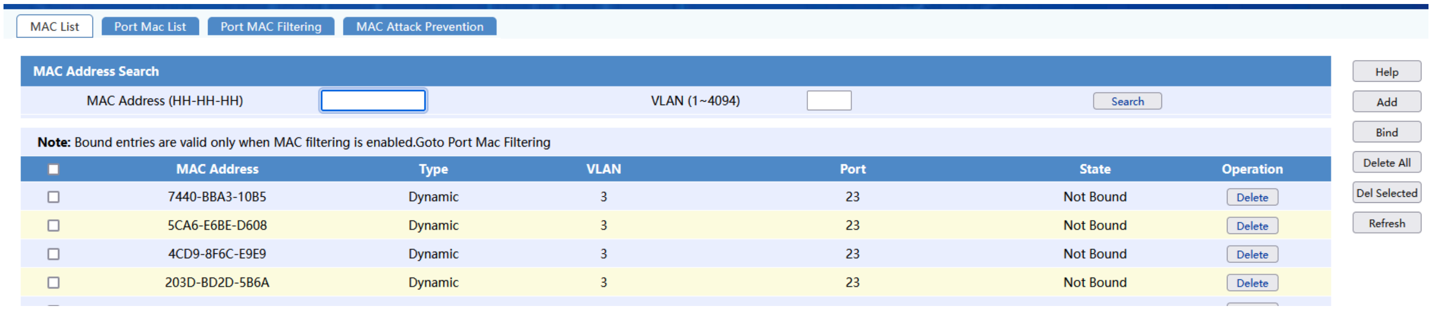
2.2.5 Network > MAC Filter

This switch supports the following three types of MAC address entries:

- Static: added manually, and the MAC address entry will not be aged. After you add it, the entry is in the "bound" state (multicast MAC address entries do not support binding operations).
- Dynamic: automatically learn or add manually, and the MAC address entry will be aged. When you add it, the entry is in the "unbound" state; if you perform a binding operation on it, it becomes a static entry.
- Blackhole: Manually added, all packets whose destination address is the MAC address will be discarded (for example, for security reasons, a user can be blocked from receiving packets), and does not support the binding operation.

MAC List:

Page Wizard: Network ⟶ MAC Filter ⟶ MAC List. The page is as shown in the figure below, you can display and query (through the combination of MAC address and VLAN conditions) all the MAC address table information of the device and the specified MAC address table item Bind (select the entry to be bound on the main page, and click the <Binding> button to take effect).



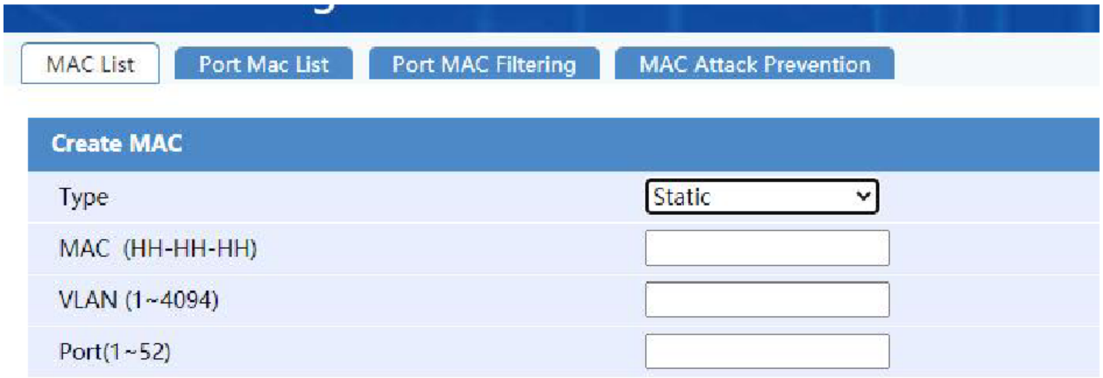
MAC Address Search

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
□	7440-BBA3-10B5	Dynamic	3	23	Not Bound	Delete
□	5CA6-E6BE-D608	Dynamic	3	23	Not Bound	Delete
□	4CD9-8F6C-E9E9	Dynamic	3	23	Not Bound	Delete
□	203D-BD2D-5B6A	Dynamic	3	23	Not Bound	Delete

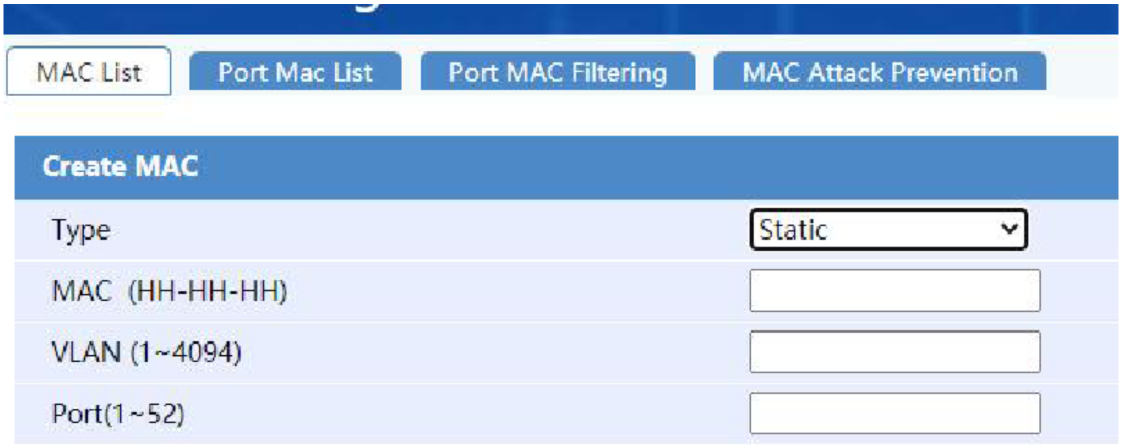
Steps to add a new MAC address entry: Click the <Add> button on the main page, configure the relevant parameters of the MAC address entry on the page that is jumped to, and click the <OK> button to take effect.



Create MAC

Type	Static
MAC (HH-HH-HH)	
VLAN (1~4094)	
Port(1~52)	

Modify static or blackhole MAC address entries (click the corresponding MAC address entry on the main page to modify the entry), dynamic MAC address entries cannot be modified.



Create MAC

Type	Static
MAC (HH-HH-HH)	
VLAN (1~4094)	
Port(1~52)	

The meaning of the key items on the page is shown in the table below.

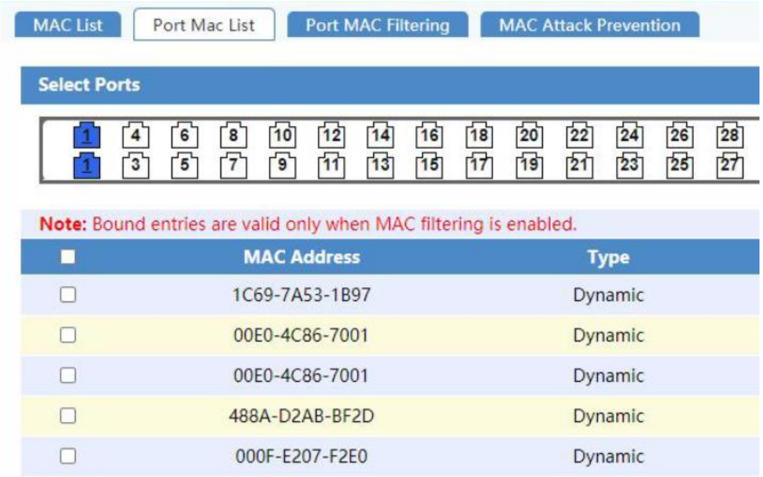
Operation	Explanation
MAC address query	You can enter MAC and VLAN ID for query and display, in which MAC address must be entered.
MAC display	Display the MAC address and its corresponding VLAN in the switch. User can select MAC with status "unbound" Address, and add the corresponding MAC to the binding list by clicking the <Binding> button.
State	Display MAC address binding status • Not supported: The MAC is not allowed to be added to the binding list, such as black hole MAC, multicast MAC; • Bound: The MAC has been added to the binding list; • Unbound: The MAC is not in the binding list, but it is allowed to be added.
Add	Open the Add MAC Address page.
Binding	Add the selected MAC address that can be bound to the binding list.
Delete	Click the <Delete> button after the item to be deleted to delete the related content.
Delete all	Delete all MAC addresses on the device.
Batch deletion	Delete selected MAC addresses in batches and delete them.

Port MAC List:

Page Wizard: Network → MAC Filter → Port MAC List. This page mainly provides the following functions:

- Display the MAC address table information under the specified port

- Bind the unbound MAC address entries under the port (select the corresponding port number, and select the unbound MAC address entries under the port, click the <Binding> button to take effect).

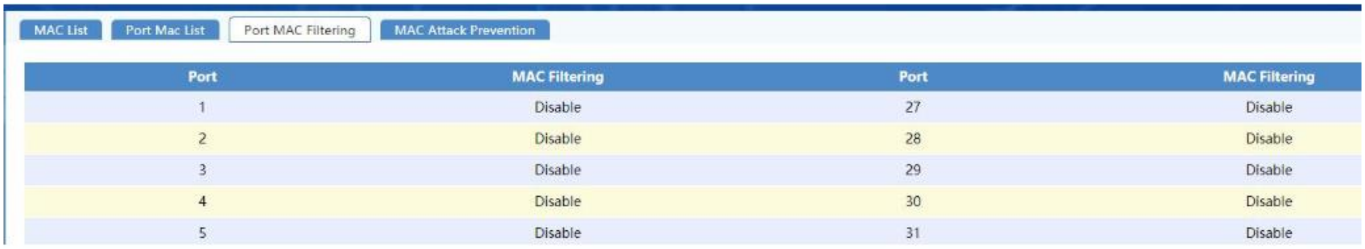


Note: Bound entries are valid only when MAC filtering is enabled.

☐	MAC Address	Type
☐	1C69-7A53-1B97	Dynamic
☐	00E0-4C86-7001	Dynamic
☐	00E0-4C86-7001	Dynamic
☐	488A-D2AB-BF2D	Dynamic
☐	000F-E207-F2E0	Dynamic

Port MAC Filtering:

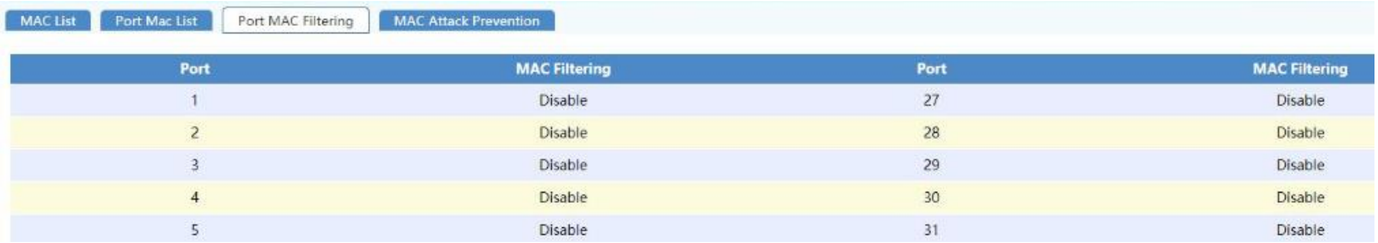
Page Wizard: Network → MAC Filter → Port MAC Filtering. Displays the status of the MAC address filter function of each port.



Port	MAC Filtering	Port	MAC Filtering
1	Disable	27	Disable
2	Disable	28	Disable
3	Disable	29	Disable
4	Disable	30	Disable
5	Disable	31	Disable

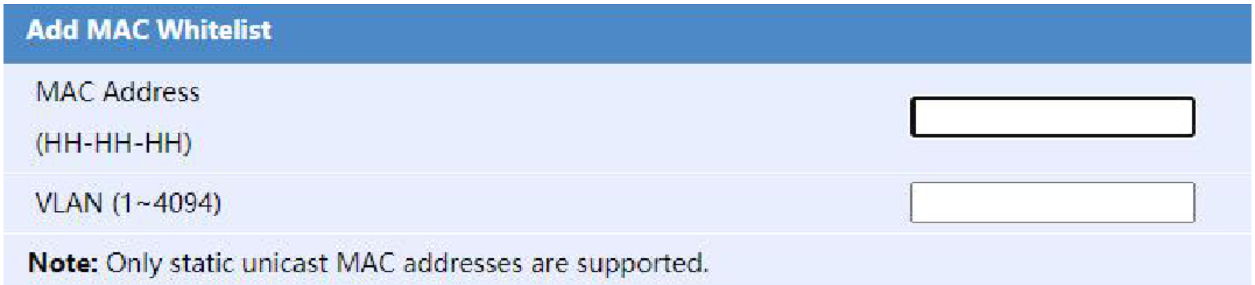
Configuration steps:

1. Turn on the MAC address filtering function of the specified port, click the entry corresponding to the port on the main page, select the "MAC filtering enabled" checkbox, and click the <OK> button to take effect.



Port	MAC Filtering	Port	MAC Filtering
1	Disable	27	Disable
2	Disable	28	Disable
3	Disable	29	Disable
4	Disable	30	Disable
5	Disable	31	Disable

2. Add the static MAC address entry of the specified port, click the entry corresponding to the port on the main page, enter the corresponding parameters in the "MAC address" and "VLAN" text boxes, and click the <Add> button to take effect.



Add MAC Whitelist

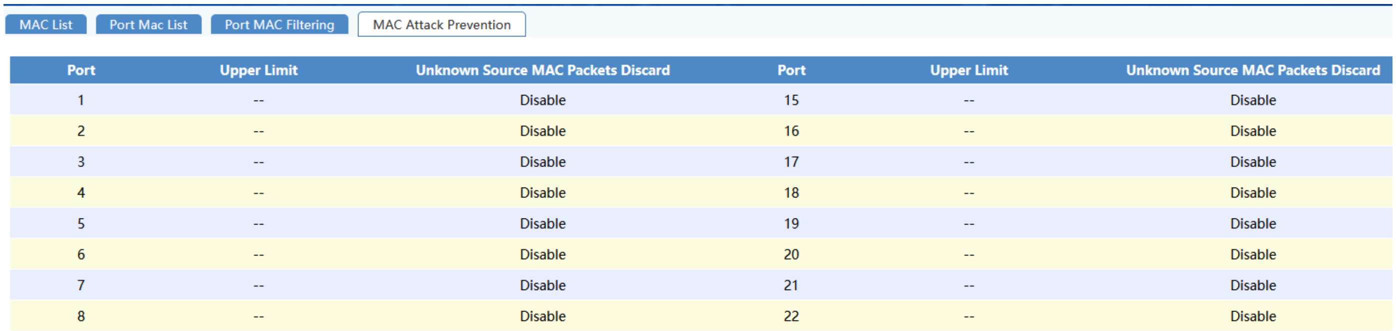
MAC Address (HH-HH-HH)	
VLAN (1~4094)	

Note: Only static unicast MAC addresses are supported.

MAC Attack Prevention:

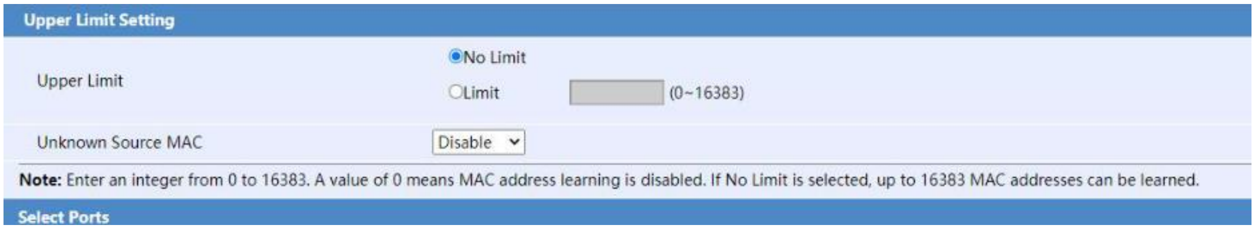
Page Wizard: Network → MAC Filter → MAC Attack Prevention. The anti-MAC address attack function mainly prevents the device from continuously learning the MAC address of a large number of invalid packets in the local area network, making the device's MAC address forwarding table too large, resulting in a sharp decline in its forwarding performance.

The switch achieves the function of preventing MAC address attacks by limiting the number of MAC addresses learned on the port.



Port	Upper Limit	Unknown Source MAC Packets Discard	Port	Upper Limit	Unknown Source MAC Packets Discard
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

Configure the number of MAC addresses that can be learned by a single port. Click the entry corresponding to the port on the main page to enter the corresponding page.



Upper Limit Setting

Upper Limit	● No Limit ○ Limit (0~16383)
Unknown Source MAC	Disable

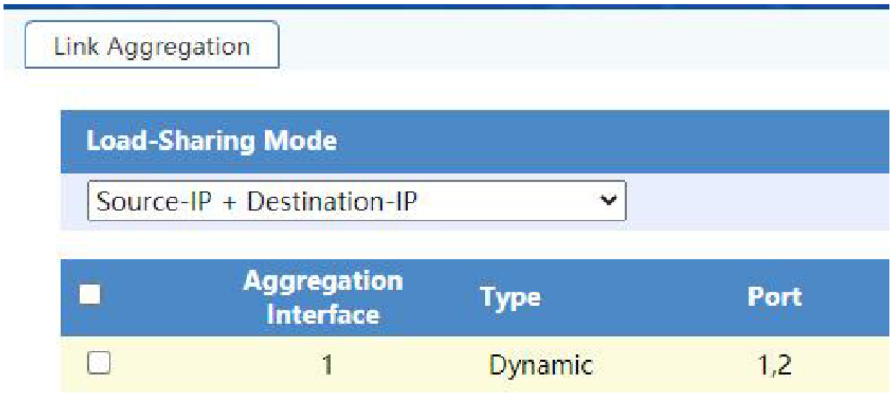
Note: Enter an integer from 0 to 16383. A value of 0 means MAC address learning is disabled. If No Limit is selected, up to 16383 MAC addresses can be learned.

Select Ports

Batch configure the number of MAC addresses that can be learned by the specified port.
Click the <Batch Configuration> button on the main page to enter the corresponding page.

2.2.6 Network > Link Aggregation

Page Wizard: Network ⟶ Link Aggregation. You can view the current link aggregation status and configure the aggregation algorithm on this page.



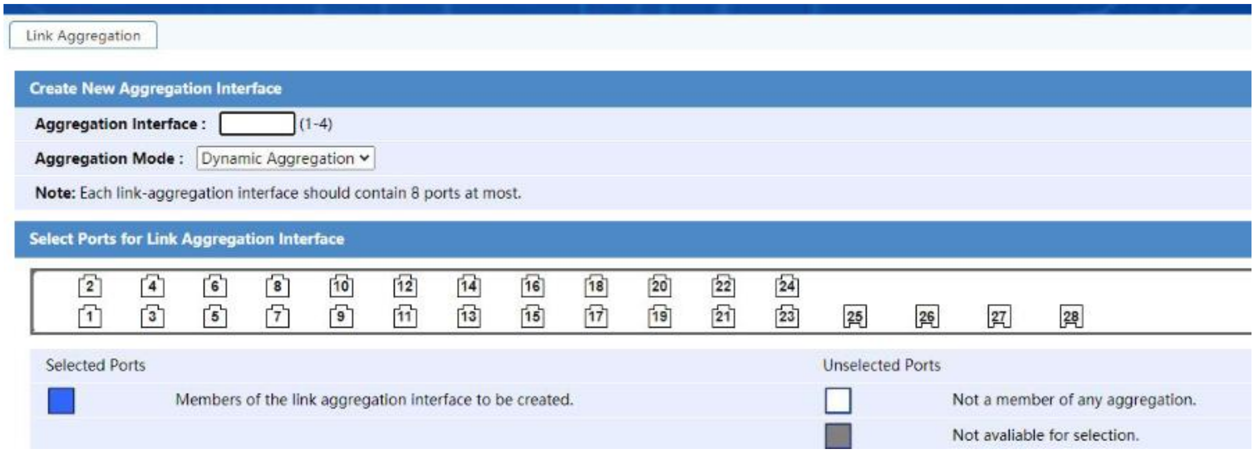
Link Aggregation

Load-Sharing Mode

Source-IP + Destination-IP

□	Aggregation Interface	Type	Port
□	1	Dynamic	1,2

Create a new link aggregation: Click the <New> button on the main page to enter the corresponding page.



Link Aggregation

Create New Aggregation Interface

Aggregation Interface : (1-4)

Aggregation Mode : Dynamic Aggregation

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

Select Ports for Link Aggregation Interface

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

Selected Ports		Unselected Ports	
🟦	Members of the link aggregation interface to be created.	□	Not a member of any aggregation.
		▨	Not avaliable for selection.

Modify the created link aggregation: select an entry on the main page, double-click it or click the <modify> button to enter the corresponding page.

The meaning of the key items on the page is shown in the table below.

Operation	Explanation
Aggregation algorithm	Select the aggregation algorithm of the switch: Based on source MAC address: indicates that each member port in the aggregation group performs load sharing based on the source MAC address Based on destination MAC address: indicates that each member port in the aggregation group performs load sharing based on the destination MAC address Based on source MAC address and destination MAC address: indicates that each member port in the aggregation group performs load sharing based on the source MAC address and destination MAC address Based on source IP address and destination IP address: indicates that each member port in the aggregation group performs load sharing based on the source IP address and destination IP address By default, each member port in the aggregation group performs load sharing based on the source IP address + destination IP address
Aggregate interface number	Display aggregate interface number
Type	Show aggregation type
Port	Port numbers included in the aggregation group

Ports in the following situations cannot join the aggregation group:

- Mirror monitoring port
- Port with MAC address filtering enabled

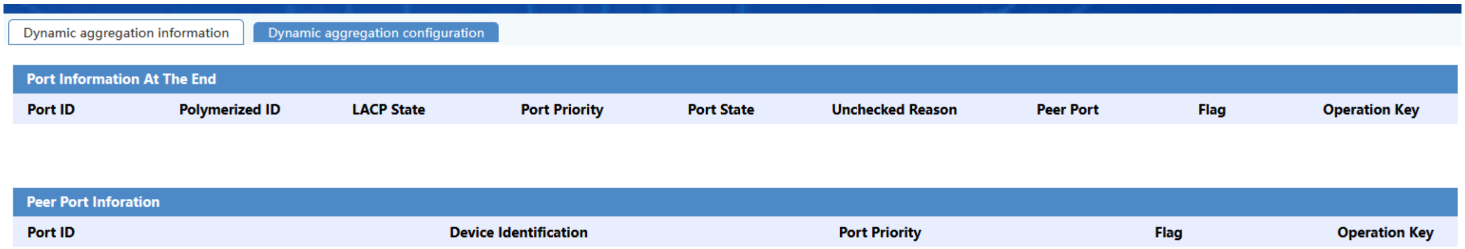
- Ports configured with MAC address learning limit

2.2.7 Network > LACP

Link Aggregation Control Protocol (LACP) provides a standardized means for exchanging information between Partner Systems that require high-speed redundant links. Link aggregation lets you group up to eight consecutive ports into a single dedicated connection. This feature can expand bandwidth to a device on the network. LACP operation requires full-duplex mode. For more detailed information, refer to the IEEE 802.3ad standard.

Dynamic Aggregation Information:

Page Wizard: Network ⟶ LACP ⟶ Dynamic Aggregation Information. On this page, users can view the dynamic aggregation information.


Dynamic aggregation information
Dynamic aggregation configuration

Port Information At The End

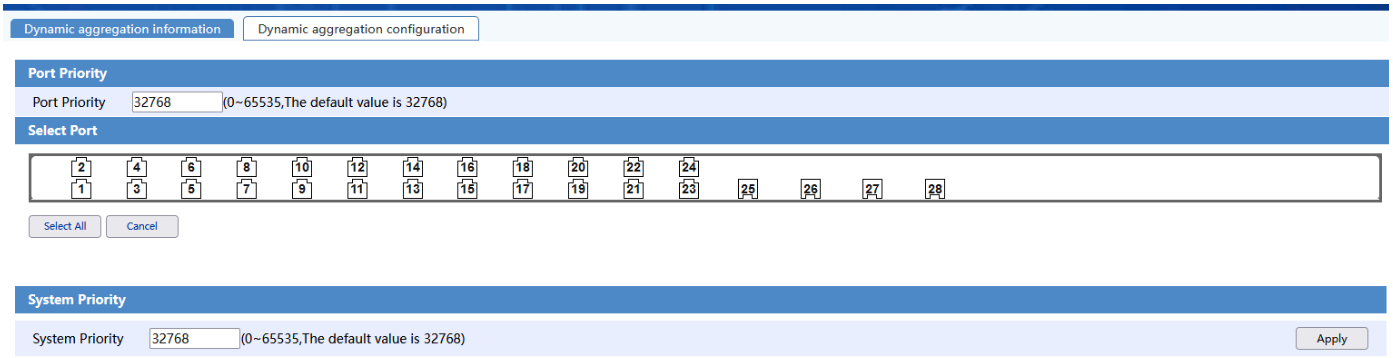
Port ID	Polymerized ID	LACP State	Port Priority	Port State	Unchecked Reason	Peer Port	Flag	Operation Key

Peer Port Inforation

Port ID	Device Identification	Port Priority	Flag	Operation Key

Dynamic Aggregation Configuration:

Page Wizard: Network ⟶ LACP ⟶ Dynamic Aggregation Configuration. Users can create dynamic aggregation group for switches.



Port Priority

Port Priority 32768 (0~65535,The default value is 32768)

Select Port

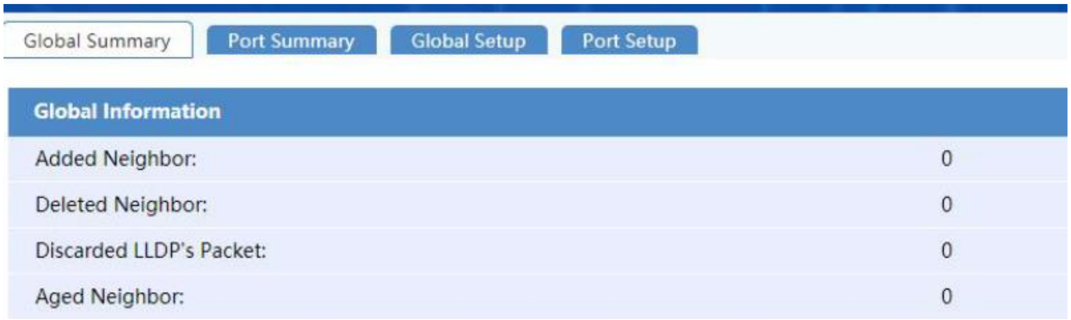
System Priority

System Priority 32768 (0~65535,The default value is 32768)

2.2.8 Network > LLDP

Global Summary:

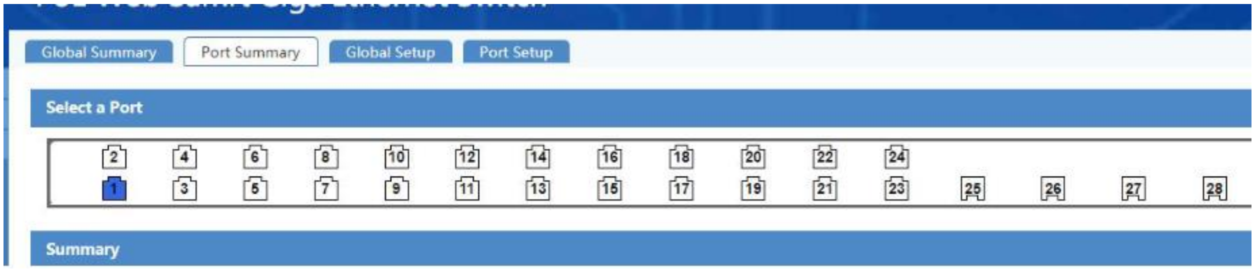
Page Wizard: Network → LLDP → Global Summary. On this page, you can view added neighbor devices, deleted neighbor devices, dropped LLDP packets, and aged neighbor devices.



Global Information	
Added Neighbor:	0
Deleted Neighbor:	0
Discarded LLDP's Packet:	0
Aged Neighbor:	0

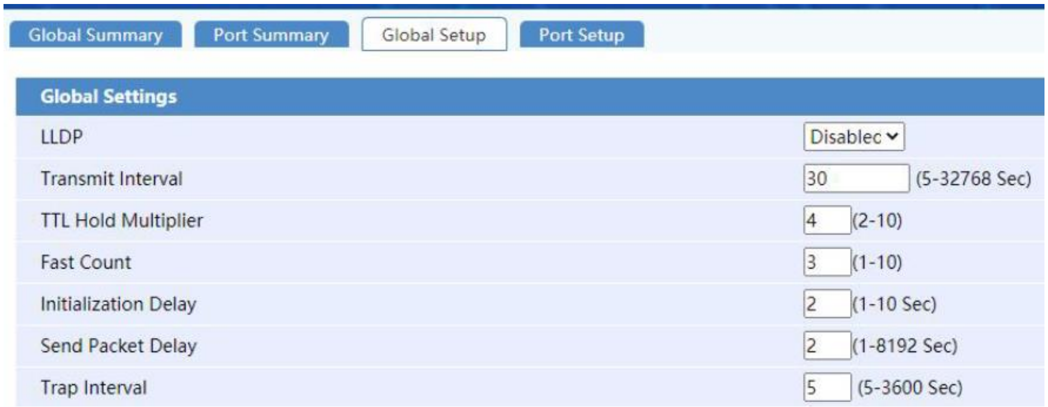
Port Summary:

Page Wizard: Network → LLDP → Port Summary. On this page, you can select a port such as port 2 and the LLDP packet statistics of port 2 will be displayed in the Summary column.



Global Setup:

Page Wizard: Network → LLDP → Global Setup.



Global Settings	
LLDP	Disablec
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)

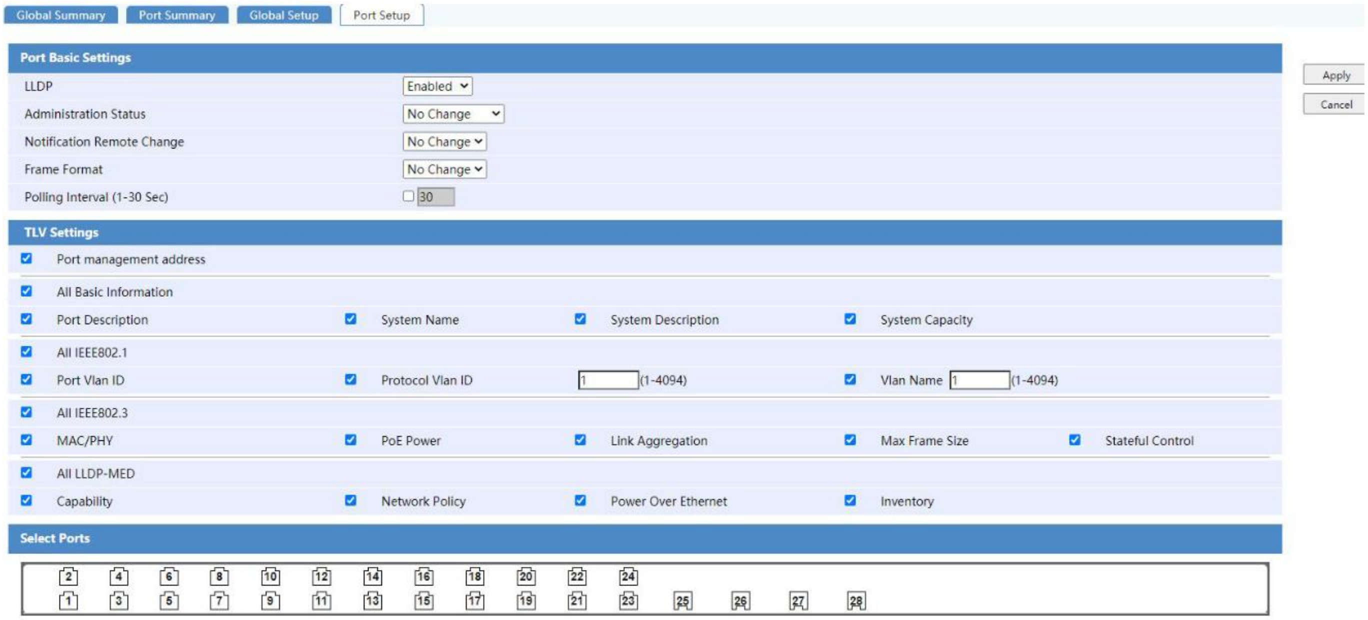
The meaning of the key items on the page is shown in the table below.

Operation	Explanation
LLDP	Select disabled in the drop-down box to turn off the LLDP function, select enabled even if the LLDP function is enabled.
Transmit Interval	LLDP packet transmission interval.
TTL Hold Multiplier	TTL multiplier.
Fast Count	Number of LLDP packets sent quickly.
Initialization Delay	Initialization delay time.
Send Packet Delay	Delay in sending LLDP packets.
Trap Interval	Trap information sending interval.

After configuring the above information, select the <Apply> button to apply.

Port Setup:

Page Wizard: Network ⟶ LLDP ⟶ 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

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

The meaning of the key items on the page is shown in the table below.

Operation	Explanation
LLDP	Select disabled in the drop-down box to turn off the LLDP function, select enabled even if the LLDP function is enabled.
Administration Status	Port LLDP working mode: • send&receive: indicates that both LLDP packets are sent and received. • receive_Only: indicates that only LLDP packets are received and not sent. • send_Only: indicates that only LLDP packets are not sent. • disabled: indicates that neither LLDP packets are sent nor received.
Notification Remote Change	For remote change notification, select disabled in the drop-down box to turn off the remote notification function, select enabled even if you can remote change notification function.
Frame Format	Choose frame format.
Polling Interval (1-30 Sec)	The value of the polling interval, 0 means the polling function is off.

The meaning of the key items in the TLV setting page is shown in the table below.

Operation	Explanation
Port management address	Port management address.
All Basic Information	Check to select all options under the basic information, including port description, system name, system description, and system capacity.
All IEEE802.1	Check to select all options under IEEE802.1, including port VLAN ID, protocol VLAN ID, and VLAN name.
All IEEE802.3	Check to select all options under IEEE802.3, including MAC, POE power supply, link aggregation, longest frame,

	and status control.
All LLDP-MED	Check to select all options under LLDP MED, including performance, network strategy, power over Ethernet, and equipment MED asset information.

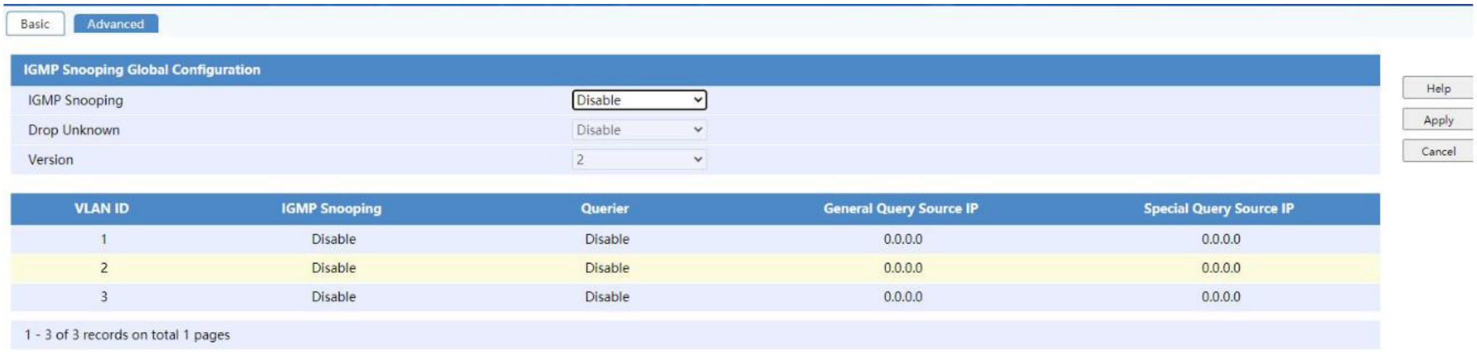
After configuring the above information, select the <Apply> button to apply.

2.2.9 Network > IGMP Snooping

The Layer 2 device running IGMP Snooping analyzes the received IGMP messages to establish a mapping relationship between the port and the MAC multicast address, and forwards the multicast data based on this mapping relationship.

Basic:

Page Wizard: Network → IGMP Snooping → Basic. You can turn on/off the IGMP Snooping function, turn on/off the location multicast drop, and set the version. After enabling the IGMP Snooping function, after pressing the <OK> button, the page will pop up the prompt box "Enable IGMP snooping will clear the IP multicast MAC address in the MAC address table, are you sure?"



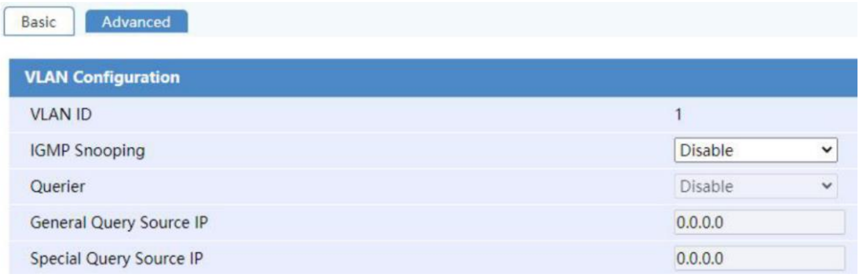
IGMP Snooping Global Configuration

IGMP Snooping	Disable
Drop Unknown	Disable
Version	2

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

1 - 3 of 3 records on total 1 pages

VLAN configuration: Click the entry corresponding to VLAN on the main page to enter the VLAN configuration page.

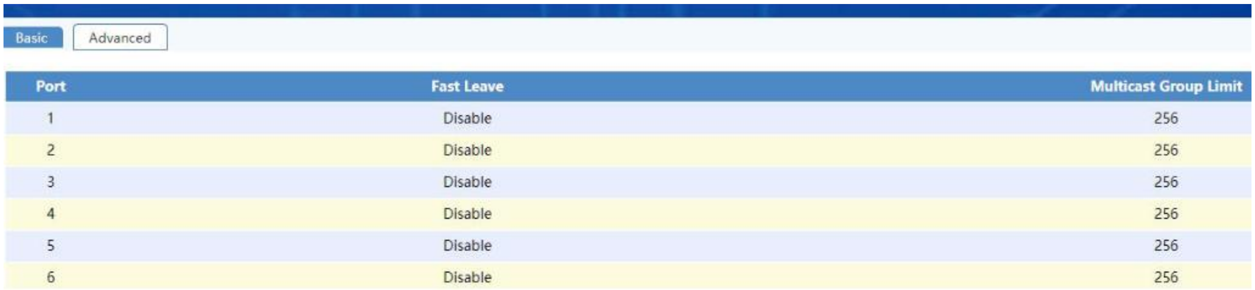


VLAN Configuration

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

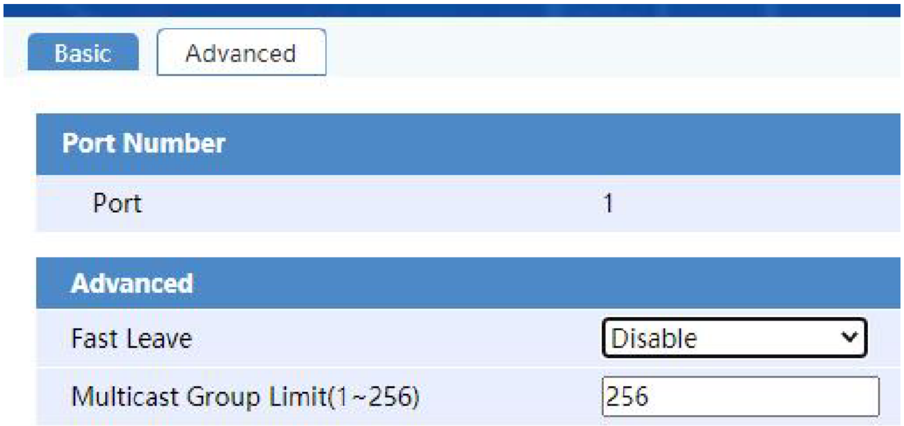
Advanced:

Page Wizard: Network ⟶ IGMP Snooping ⟶ Advanced. Single port configuration: click the entry corresponding to the port on the main page to enter the corresponding page, open/close the port and leave quickly, and configure the maximum number of multicast groups (the maximum number of multicast groups is 256).



Port	Fast Leave	Multicast Group Limit
1	Disable	256
2	Disable	256
3	Disable	256
4	Disable	256
5	Disable	256
6	Disable	256

Batch configuration: Click the <Batch configuration> button on the main page to enter the corresponding page.



Port Number

Port	1

Advanced

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

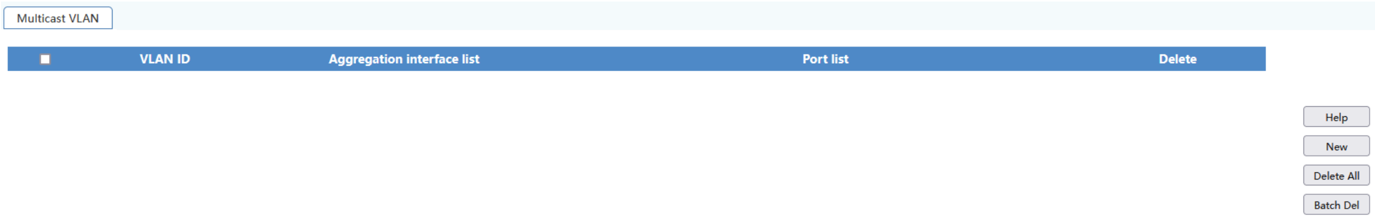
2.2.10 Network > Multicast VLAN

Page Wizard: Network ⟶ Multicast VLAN. Users can create, edit, and delete multicast VLAN ports on this page.

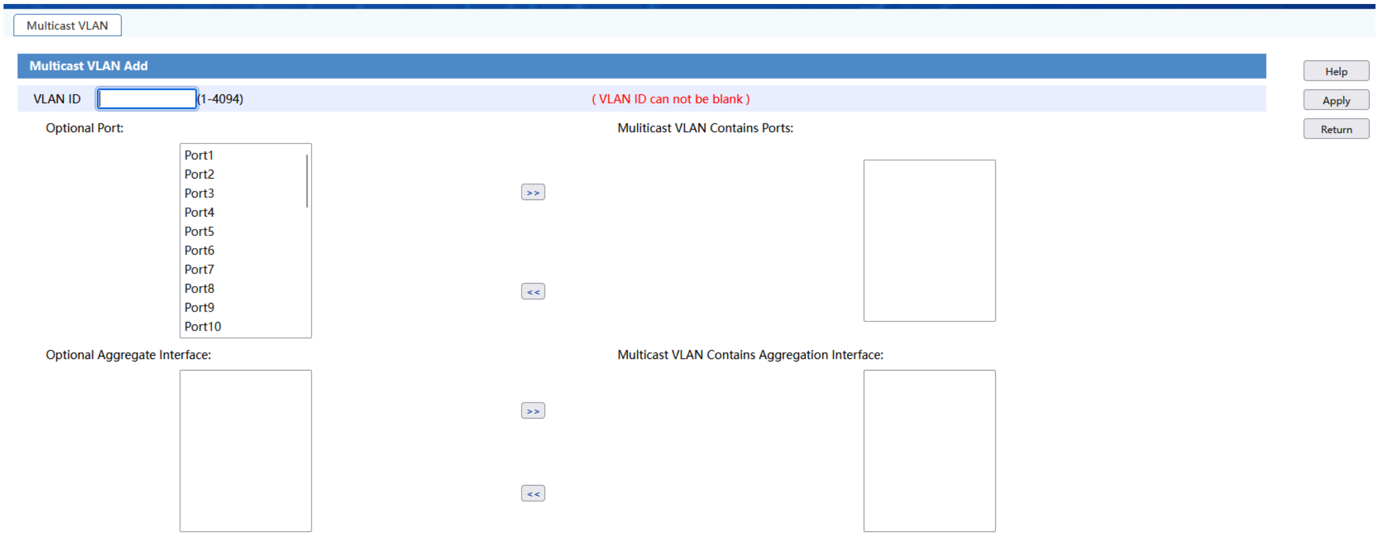
- You can move the ports in the optional port list to the multicast VLAN to include the port list to join the multicast VLAN or move the ports in the ports in the multicast VLAN containing port list to the optional port list from the multicast VLAN delete.
- You can move interfaces in the list of optional aggregation interfaces to the multicasts VLAN to include the aggregation interface list to join the multicast VLAN, or move the ports in the

multicast VLAN containing the aggregation interface list to the list of optional aggregation interfaces. Remove from multicast VLAN.

- The specified VLAN must exist, otherwise the multicast VLAN cannot be created.
- Only the aggregated interfaces that have been created can become optional aggregation interfaces.



□	VLAN ID	Aggregation interface list	Port list	Delete



VLAN ID (1-4094) (VLAN ID can not be blank)

Optional Port: Port1 Port2 Port3 Port4 Port5 Port6 Port7 Port8 Port9 Port10

Muliticast VLAN Contains Ports:

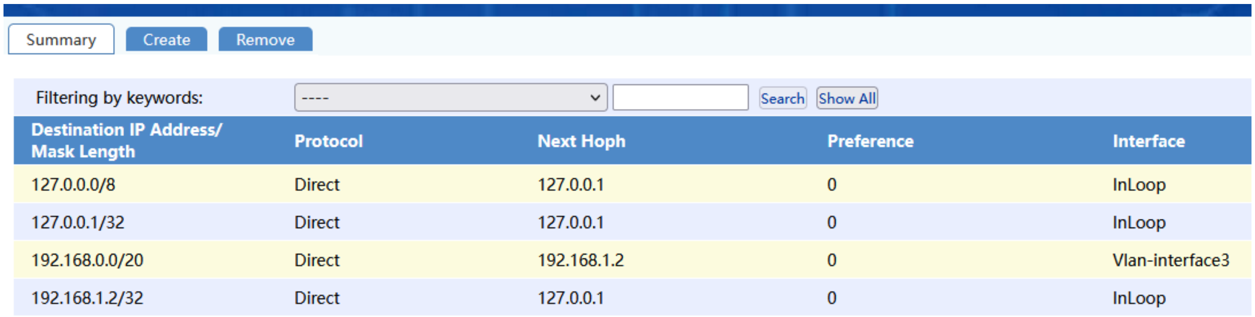
Optional Aggregate Interface:

Multicast VLAN Contains Aggregation Interface:

2.2.11 Network > IPv4 Routing

Summary:

Page Wizard: Network ⟶ IPv4 Routing ⟶ Summary. Users can view summary of destination IP addresses on this page.

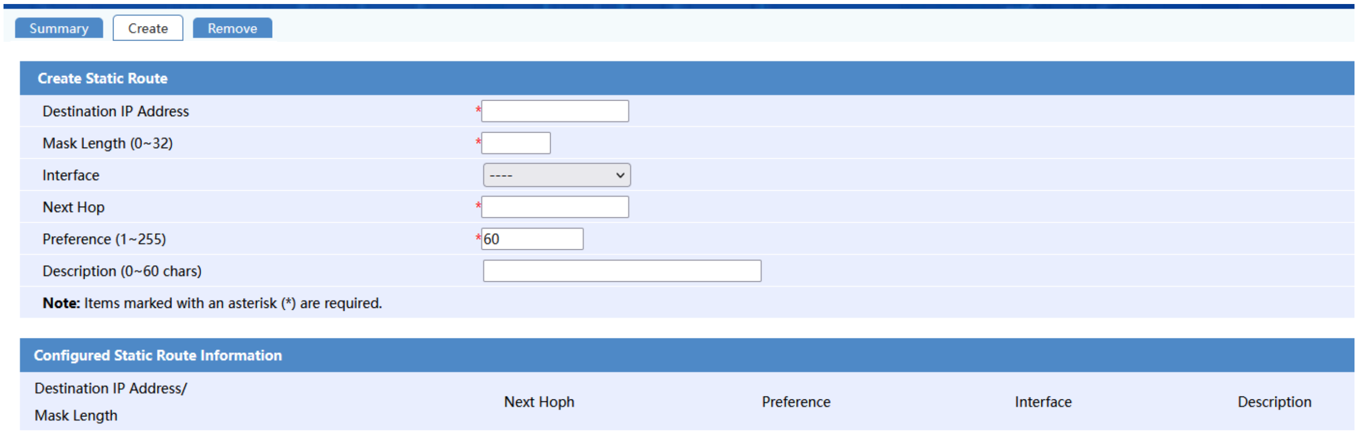


Filtering by keywords: ----

Destination IP Address/ Mask Length	Protocol	Next Hoph	Preference	Interface
127.0.0.0/8	Direct	127.0.0.1	0	InLoop
127.0.0.1/32	Direct	127.0.0.1	0	InLoop
192.168.0.0/20	Direct	192.168.1.2	0	Vlan-interface3
192.168.1.2/32	Direct	127.0.0.1	0	InLoop

Create:

Page Wizard: Network ⟶ IPv4 Routing ⟶ Create. Users can create static routes via this page. After inputting the information, click on apply to save the settings.



Create Static Route

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

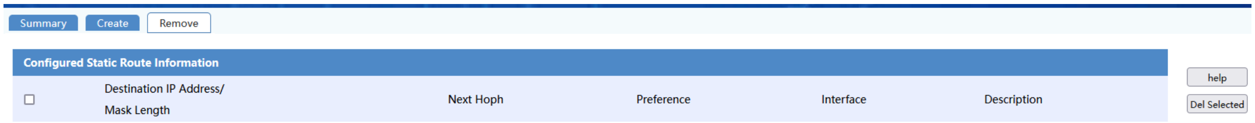
Note: Items marked with an asterisk (*) are required.

Configured Static Route Information

Destination IP Address/ Mask Length	Next Hoph	Preference	Interface	Description

Remove:

Page Wizard: Network ⟶ IPv4 Routing ⟶ Remove. Users can remove configured static route information via this page.



Configured Static Route Information

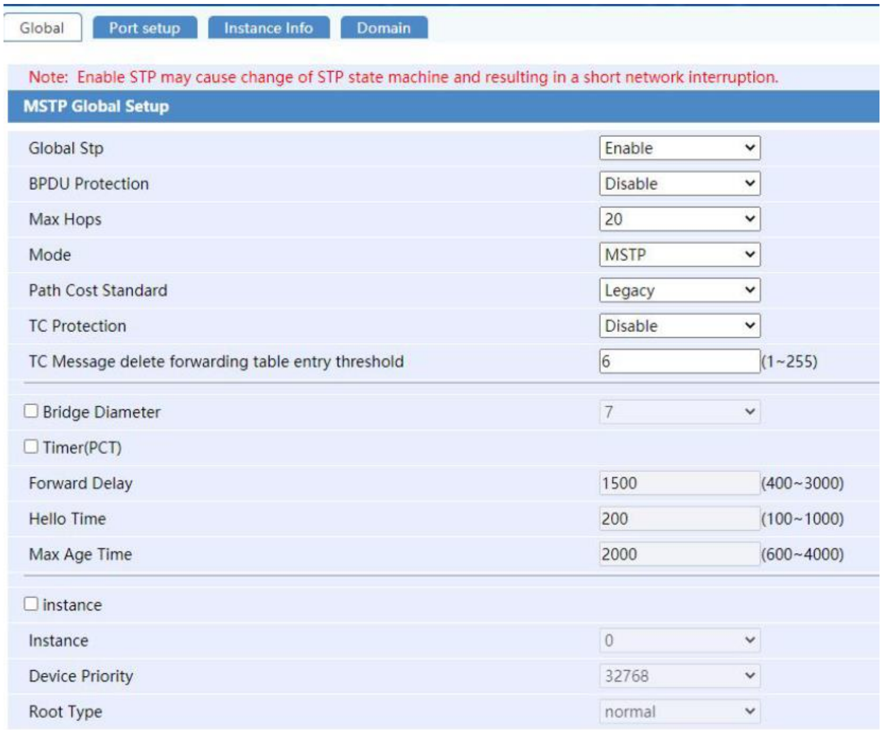
☐	Destination IP Address/ Mask Length	Next Hoph	Preference	Interface	Description

2.2.12 Network > MSTP

Spanning Tree Protocol is a Layer 2 management protocol that eliminates Layer 2 loops by selectively blocking redundant links in the network, and also has the function of the link backup.

Global:

Page Wizard: Network → MSTP → Global. This page can be set to turn on/off the MSTP function and related parameters.



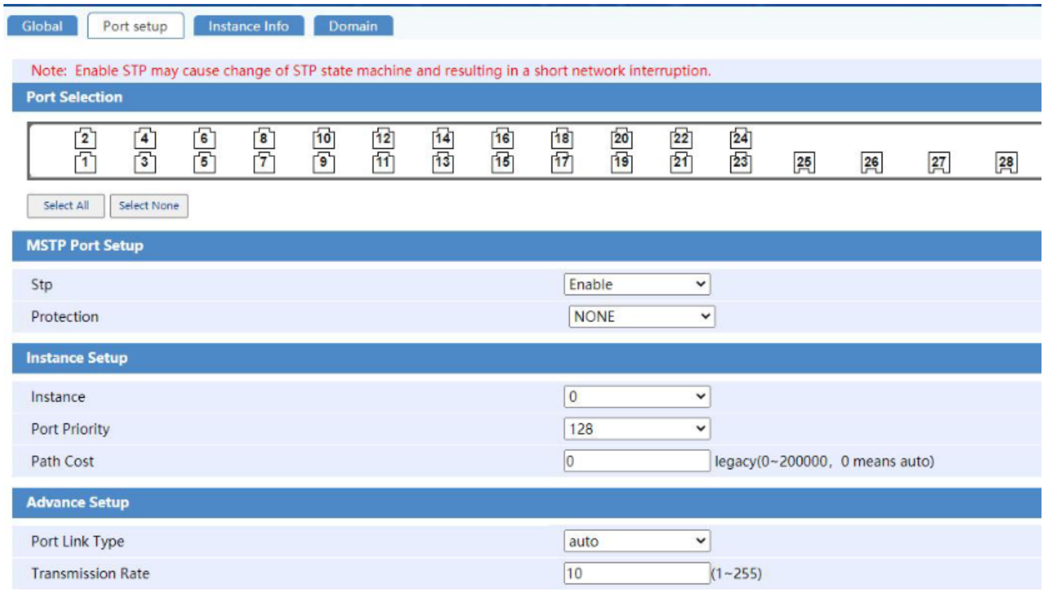
Note: Enable STP may cause change of STP state machine and resulting in a short network interruption.

MSTP Global Setup

Global Stp	Enable
BPDU Protection	Disable
Max Hops	20
Mode	MSTP
Path Cost Standard	Legacy
TC Protection	Disable
TC Message delete forwarding table entry threshold	6 (1~255)
□ Bridge Diameter	7
□ Timer(PCT)	
Forward Delay	1500 (400~3000)
Hello Time	200 (100~1000)
Max Age Time	2000 (600~4000)
□ instance	
Instance	0
Device Priority	32768
Root Type	normal

Port Setup:

Page Wizard: Network → MSTP → Port Setup. this page can be configured to open/close the port MSTP function and related attributes of MSTP under the port, as shown in the following figure:



Note: Enable STP may cause change of STP state machine and resulting in a short network interruption.

Port Selection

MSTP Port Setup

Stp	Enable
Protection	NONE

Instance Setup

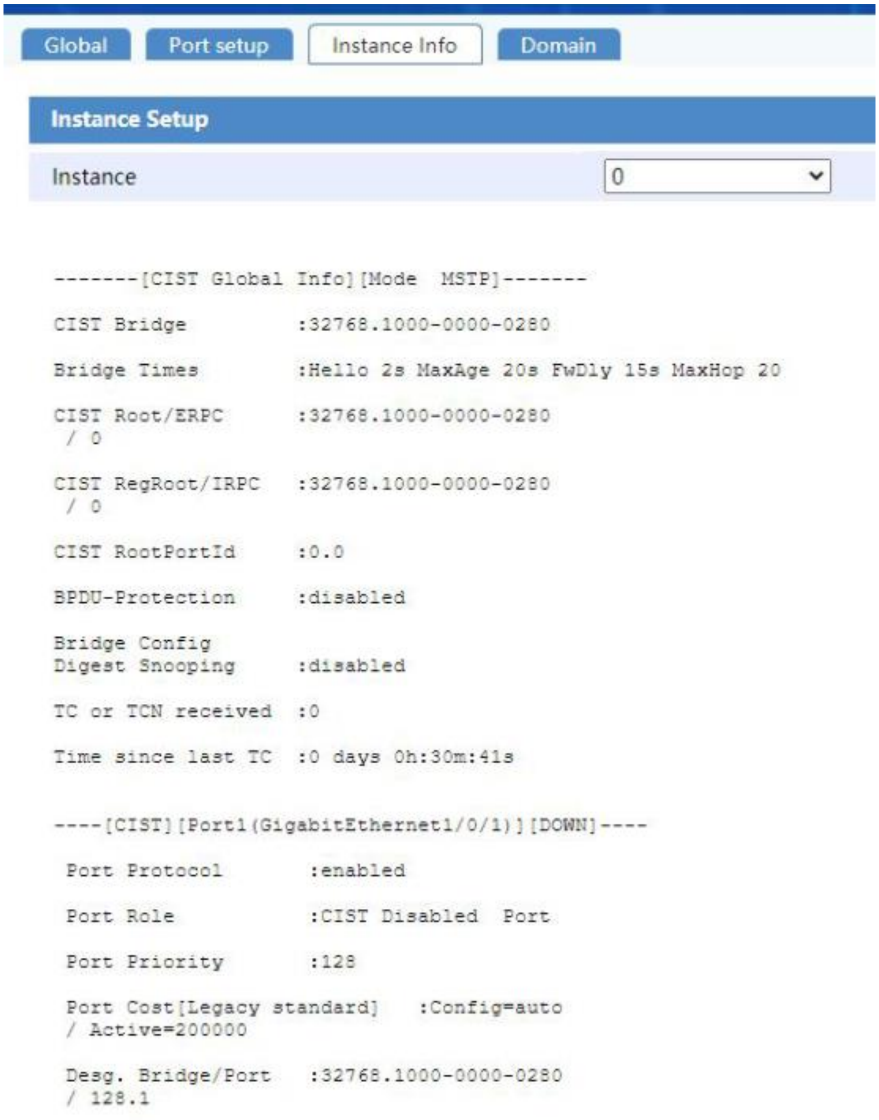
Instance	0
Port Priority	128
Path Cost	0 legacy(0~200000, 0 means auto)

Advance Setup

Port Link Type	auto
Transmission Rate	10 (1~255)

Instance Info:

Page Wizard: Network ⟶ MSTP ⟶ Instance Info. This page can display MSTP instance information.



Instance Setup

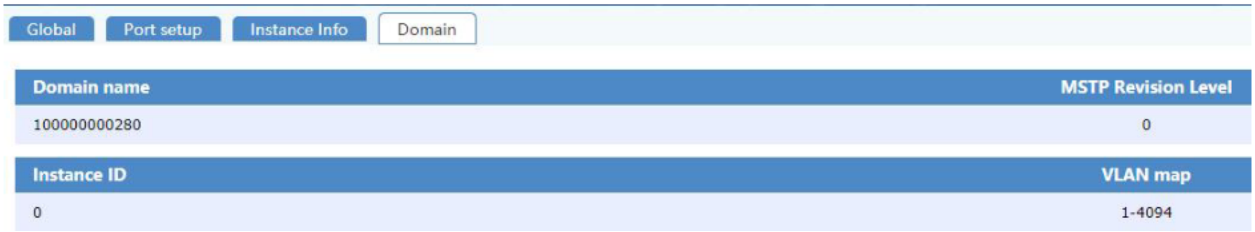
Instance: 0

```
-------[CIST Global Info][Mode MSTP]-------

CIST Bridge         :32768.1000-0000-0280

Bridge Times        :Hello 2s MaxAge 20s FwDly 15s MaxHop 20

CIST Root/ERPC      :32768.1000-0000-0280
 / 0

CIST RegRoot/IRPC   :32768.1000-0000-0280
 / 0

CIST RootPortId     :0.0

BPDU-Protection     :disabled

Bridge Config
Digest Snooping     :disabled

TC or TCN received  :0

Time since last TC  :0 days 0h:30m:41s

----[CIST][Port1(GigabitEthernet1/0/1)][DOWN]----

 Port Protocol       :enabled

 Port Role           :CIST Disabled  Port

 Port Priority       :128

 Port Cost[Legacy standard]   :Config=auto
 / Active=200000

 Desg. Bridge/Port   :32768.1000-0000-0280
 / 128.1
```

Domain:

Page Wizard: Network ⟶ MSTP ⟶ Domain. this page can display MSTP domain configuration effective information.

Click the <Modify> button to modify the domain configuration information, and the modified domain configuration information will take effect immediately.



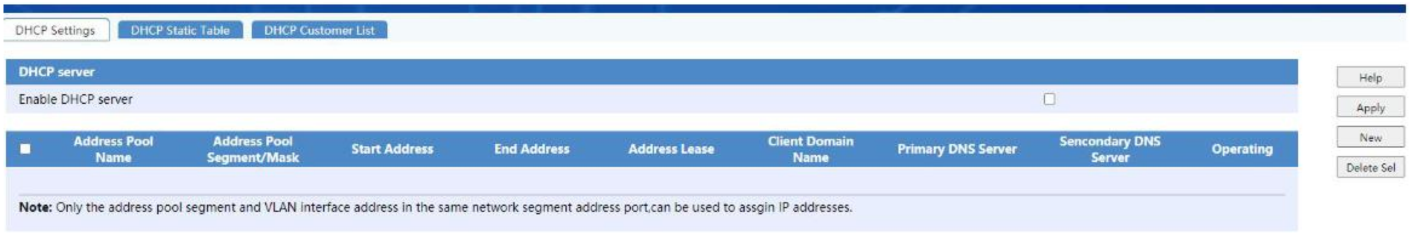
Domain name	MSTP Revision Level
100000000280	0

Instance ID	VLAN map
0	1-4094

2.2.13 Network > DHCP

DHCP Settings:

Page Wizard: Network → DHCP → DHCP Settings. This page can globally turn on/off the DHCP server function, and display address pool information.



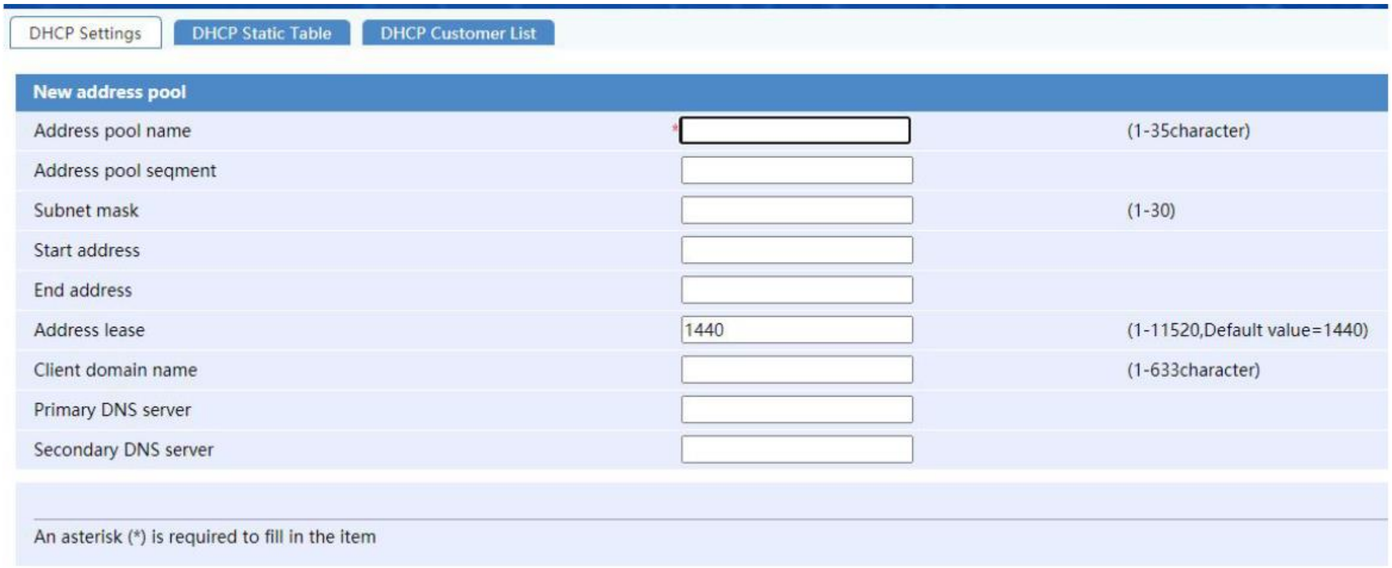
DHCP server	
Enable DHCP server	□

■	Address Pool Name	Address Pool Segment/Mask	Start Address	End Address	Address Lease	Client Domain Name	Primary DNS Server	Sencondary DNS Server	Operating

Note: Only the address pool segment and VLAN interface address in the same network segment address port,can be used to assgin IP addresses.

Click the <New> button on the page to create a new DHCP server address pool.

Click the corresponding address pool entry on the DHCP setting page to enter the corresponding address pool modification page.

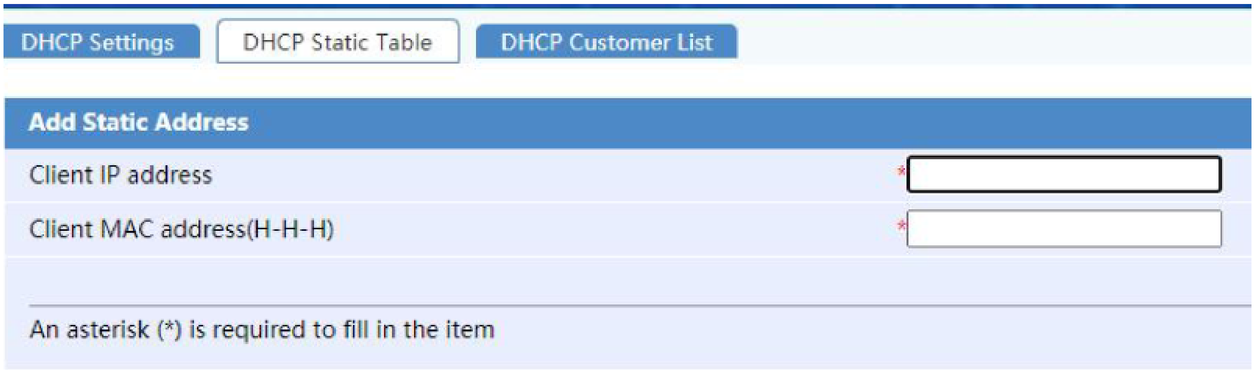


New address pool		
Address pool name	*	(1-35character)
Address pool seqment		
Subnet mask		(1-30)
Start address		
End address		
Address lease	1440	(1-11520,Default value=1440)
Client domain name		(1-633character)
Primary DNS server		
Secondary DNS server		

An asterisk (*) is required to fill in the item

DHCP Static Table:

Page Wizard: Network ⟶ DHCP ⟶ DHCP Static Table. This page can display the currently configured DHCP client static table entries, or click the <New> button to add a DHCP client static list.



Add Static Address

Client IP address	*
Client MAC address(H-H-H)	*

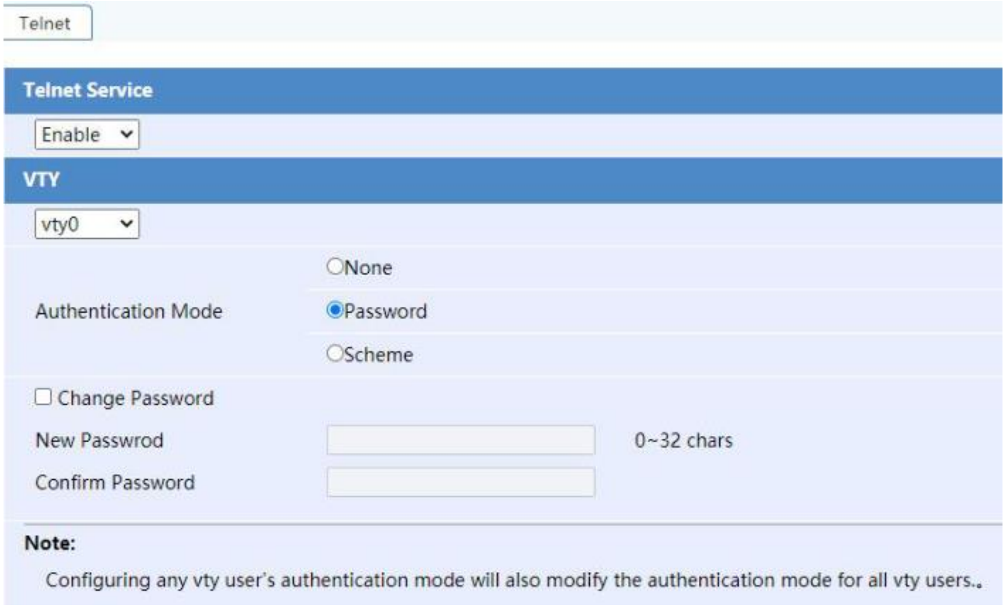
An asterisk (*) is required to fill in the item

DHCP Customer List:

Page Wizard: Network ⟶ DHCP ⟶ DHCP Customer List. This page can display the list of currently online DHCP clients.

2.2.14 Network > Telnet

Page Wizard: Network ⟶ Telnet. Under Telnet service, you can choose to turn on/off the Telnet function.



Telnet Service

Enable

VTY

vty0

Authentication Mode ○None ●Password ○Scheme

□ Change Password

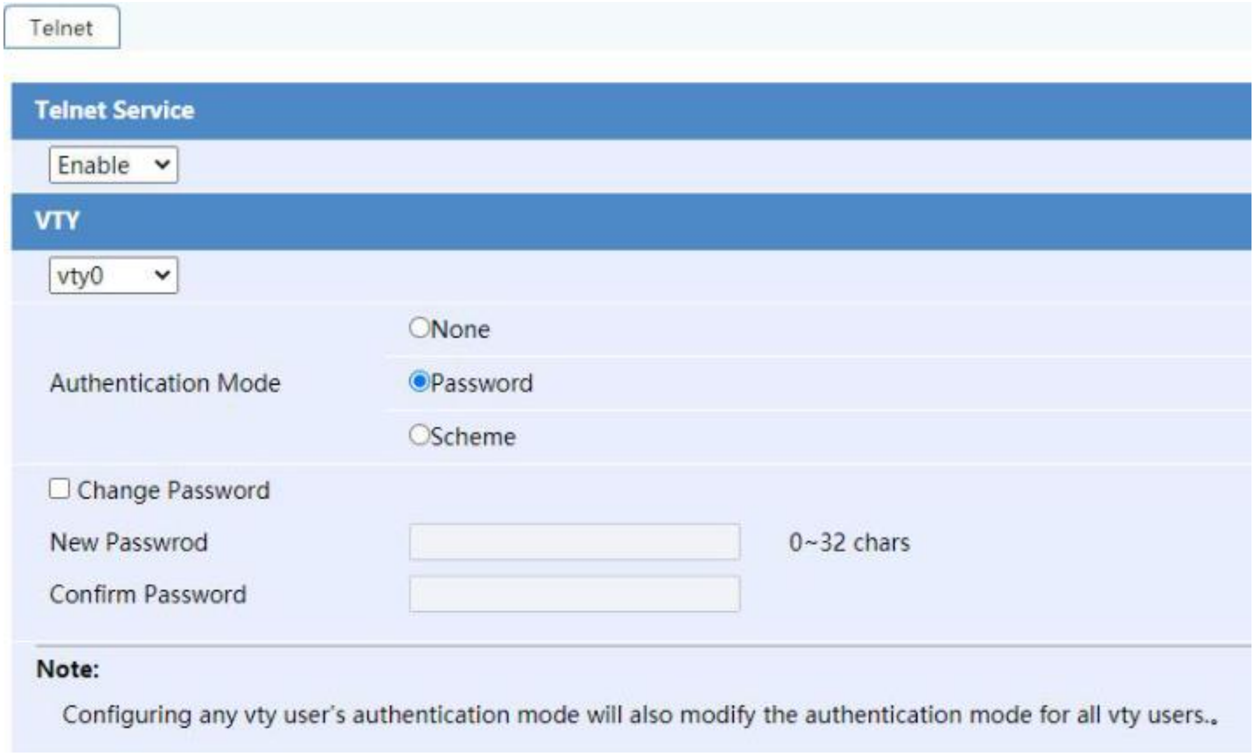
New Passwrod 0~32 chars

Confirm Password

Note:

Configuring any vty user's authentication mode will also modify the authentication mode for all vty users., Page Wizard: Network → Telnet → VTY configuration. In the VTY configuration page, you can select Telnet authentication mode, which is none, password, and scheme. You can set and change the password when you select a password or scheme mode.

- The authentication method is none: indicates that the next time you log in to the device using Telnet, no user name and password authentication is required, and anyone can log in to the device through Telnet. This situation may bring hidden security risks.
- The authentication method is password: indicates that the next time you log in to the device using Telnet, password authentication is required. Only when the password authentication succeeds can the user log in to the device.
- The authentication method is scheme: indicates that the next time you log in to the device using Telnet, you need to authenticate the username and password. If the username or password is incorrect, the login will fail. User authentication is divided into local authentication and remote authentication. If local authentication is used, local users and corresponding parameters need to be configured. If remote authentication is used, user names and passwords need to be configured on the remote authentication server.



Telnet Service

Enable

VTY

vty0

Authentication Mode ○None ●Password ○Scheme

□ Change Password

New Passwrod 0~32 chars

Confirm Password

Note:

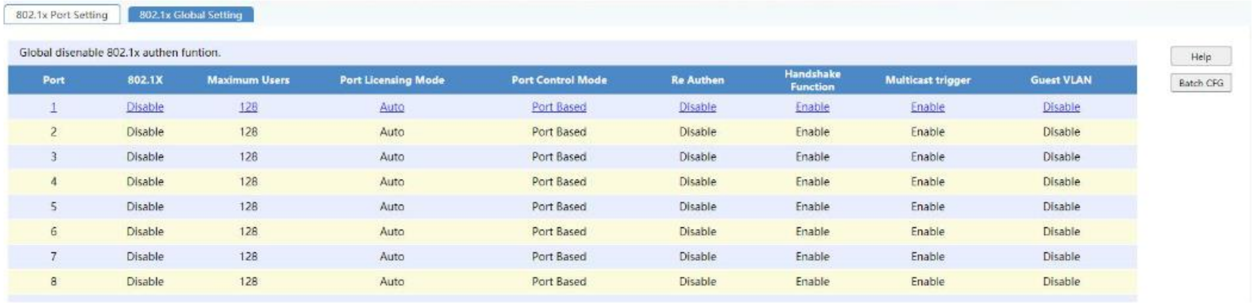
Configuring any vty user's authentication mode will also modify the authentication mode for all vty users.,

2.3 Authentication Menu Information

2.3.1 Authen > 802.1x

802.1x Port Setting:

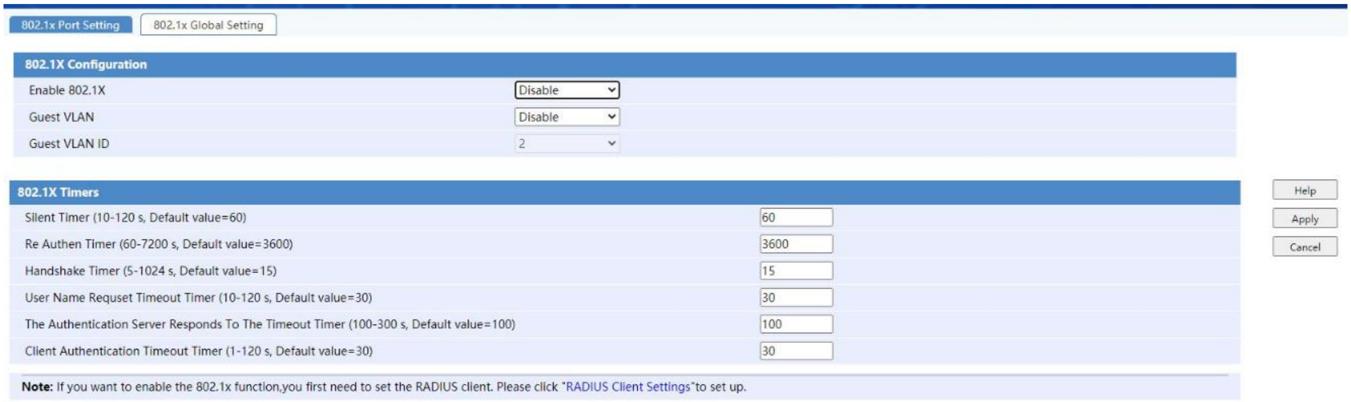
Page Wizard: Authen → 802.1x → Port Setting. This page shows the global on/off status of 802.1x and the configuration information of 802.1x under the port. Click the corresponding port entry to configure the 802.1x function of a single port, and click the <Batch Configuration> button to configure the port 802.1X function in batches.



Global disenable 802.1x authen funtion.

Port	802.1X	Maximum Users	Port Licensing Mode	Port Control Mode	Re Authen	Handshake Function	Multicast trigger	Guest VLAN
1	Disable	128	Auto	Port Based	Disable	Enable	Enable	Disable
2	Disable	128	Auto	Port Based	Disable	Enable	Enable	Disable
3	Disable	128	Auto	Port Based	Disable	Enable	Enable	Disable
4	Disable	128	Auto	Port Based	Disable	Enable	Enable	Disable
5	Disable	128	Auto	Port Based	Disable	Enable	Enable	Disable
6	Disable	128	Auto	Port Based	Disable	Enable	Enable	Disable
7	Disable	128	Auto	Port Based	Disable	Enable	Enable	Disable
8	Disable	128	Auto	Port Based	Disable	Enable	Enable	Disable

Click the corresponding port to enter the port configuration page:



802.1X Configuration

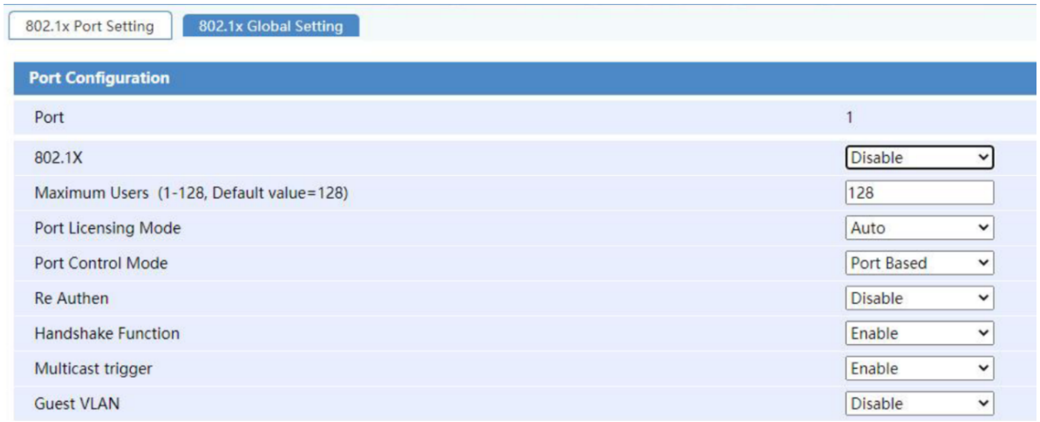
Enable 802.1X	Disable
Guest VLAN	Disable
Guest VLAN ID	2

802.1X Timers

Silent Timer (10-120 s, Default value=60)	60
Re Authen Timer (60-7200 s, Default value=3600)	3600
Handshake Timer (5-1024 s, Default value=15)	15
User Name Requset Timeout Timer (10-120 s, Default value=30)	30
The Authentication Server Responds To The Timeout Timer (100-300 s, Default value=100)	100
Client Authentication Timeout Timer (1-120 s, Default value=30)	30

Note: If you want to enable the 802.1x function,you first need to set the RADIUS client. Please click "RADIUS Client Settings"to set up.

Click the <Batch Configuration> button to configure the port 802.1X functions in batches:

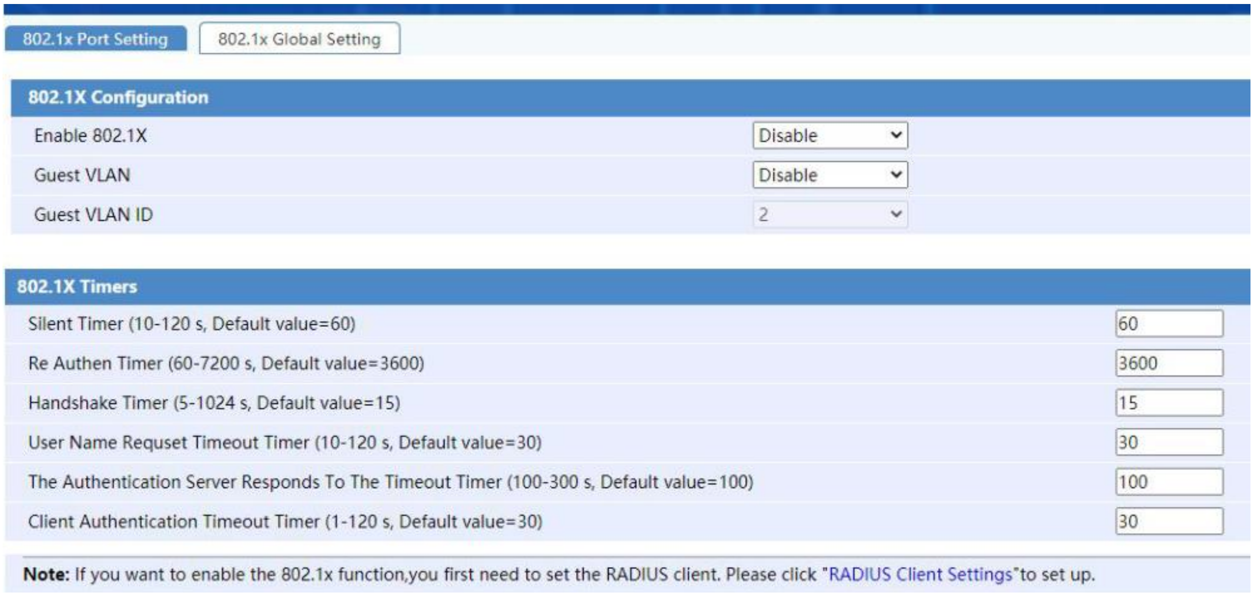


Port Configuration

Port	1
802.1X	Disable
Maximum Users (1-128, Default value=128)	128
Port Licensing Mode	Auto
Port Control Mode	Port Based
Re Authen	Disable
Handshake Function	Enable
Multicast trigger	Enable
Guest VLAN	Disable

802.1x Global Setting:

Page Wizard: Authen ⟶ 802.1x ⟶ Global Setting. This page can configure 802.1x global function.



802.1X Configuration

Enable 802.1X	Disable
Guest VLAN	Disable
Guest VLAN ID	2

802.1X Timers

Silent Timer (10-120 s, Default value=60)	60
Re Authen Timer (60-7200 s, Default value=3600)	3600
Handshake Timer (5-1024 s, Default value=15)	15
User Name Requset Timeout Timer (10-120 s, Default value=30)	30
The Authentication Server Responds To The Timeout Timer (100-300 s, Default value=100)	100
Client Authentication Timeout Timer (1-120 s, Default value=30)	30

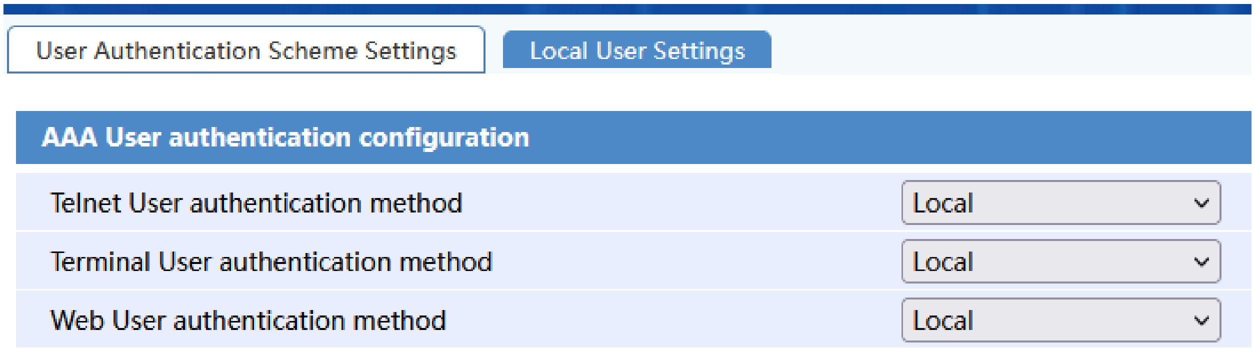
Note: If you want to enable the 802.1x function,you first need to set the RADIUS client. Please click "RADIUS Client Settings"to set up.

2.3.2 Authen > AAA

AAA is short for Authentication, Authorization, and Accounting (authentication, authorization, and accounting). It is a management mechanism for network security and provides three security functions: authentication, authorization, and accounting.

User Authentication Scheme Settings:

Page Wizard: Authen ⟶ AAA ⟶ User Authentication Scheme Settings. This page is mainly used to configure the authentication scheme for login users. Telnet users and Terminal users can configure non-authentication, local authentication, and remote authentication. Web users can only configure non-authentication and local authentication schemes.

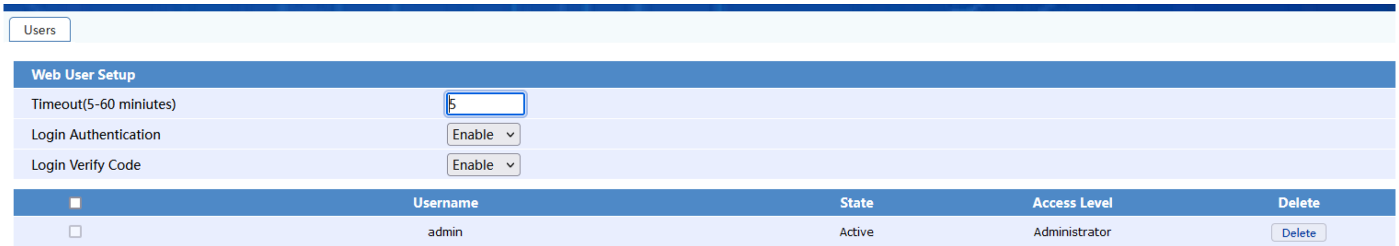


AAA User authentication configuration

Telnet User authentication method	Local
Terminal User authentication method	Local
Web User authentication method	Local

Local User Settings:

Page Wizard: Authen ⟶ AAA ⟶ Local User Settings. This page is mainly used to configure local users (Lan-access users or login users) when using the local authentication scheme. After clicking <Local User Settings>, they actually jump to the "Device -> User Management" page for configuration. For details, please refer to the "Device -> User Management" configuration page.



Web User Setup

Timeout(5-60 miniutes)	5
Login Authentication	Enable
Login Verify Code	Enable

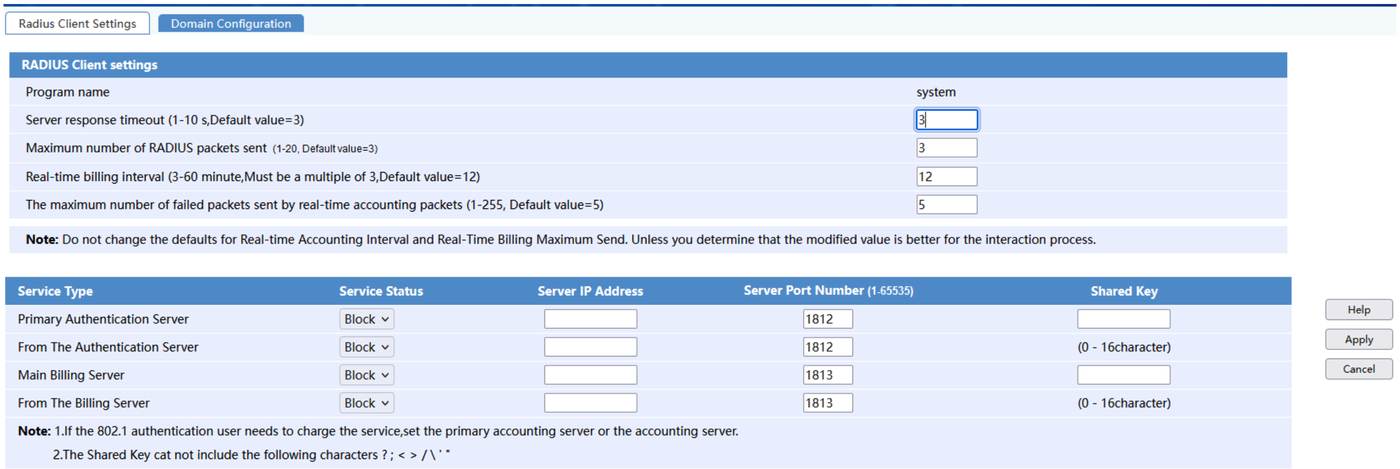
□	Username	State	Access Level	Delete
□	admin	Active	Administrator	Delete

2.3.3 Authen > Radius

RADIUS (Remote Authentication Dial-In User Service, Remote Authentication Dial-In User Service) is a distributed, client/server structure information interaction protocol that can protect the network from unauthorized access. It is often used in both various network environments with high security and allowing remote users to access. The protocol defines the RADIUS message format and message transmission mechanism and specifies the use of UDP as the transport layer protocol to encapsulate RADIUS messages (UDP ports 1812 and 1813 are used as authentication and accounting ports, respectively).

Radius Client Settings:

Page Wizard: Authen ⟶ Radius ⟶ Radius Client Settings. This page is mainly used to configure the RADIUS scheme.



RADIUS Client settings

Program name	system
Server response timeout (1-10 s,Default value=3)	3
Maximum number of RADIUS packets sent (1-20, Default value=3)	3
Real-time billing interval (3-60 minute,Must be a multiple of 3,Default value=12)	12
The maximum number of failed packets sent by real-time accounting packets (1-255, Default value=5)	5

Note: Do not change the defaults for Real-time Accounting Interval and Real-Time Billing Maximum Send. Unless you determine that the modified value is better for the interaction process.

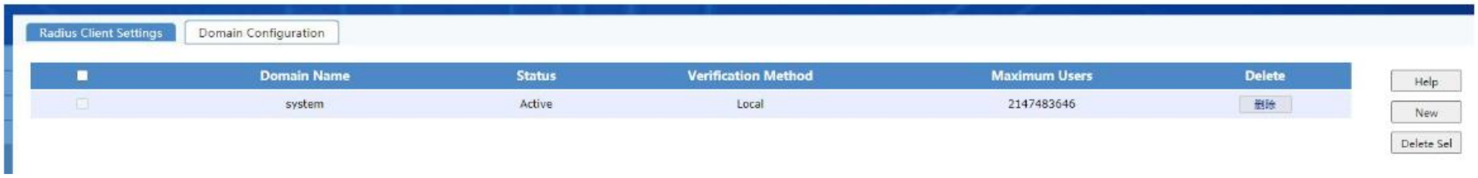
Service Type	Service Status	Server IP Address	Server Port Number (1-65535)	Shared Key
Primary Authentication Server	Block		1812	
From The Authentication Server	Block		1812	(0 - 16character)
Main Billing Server	Block		1813	
From The Billing Server	Block		1813	(0 - 16character)

Note: 1.If the 802.1 authentication user needs to charge the service,set the primary accounting server or the accounting server.

2.The Shared Key cat not include the following characters ? ; < > / \ ' "

Domain Configuration:

Page Wizard: Authen → Radius → Domain Configuration. This page is mainly used to configure the domain in the Radius scheme.
Click the <New> button on the page to create a new domain.



■	Domain Name	Status	Verification Method	Maximum Users	Delete
□	system	Active	Local	2147483646	删除

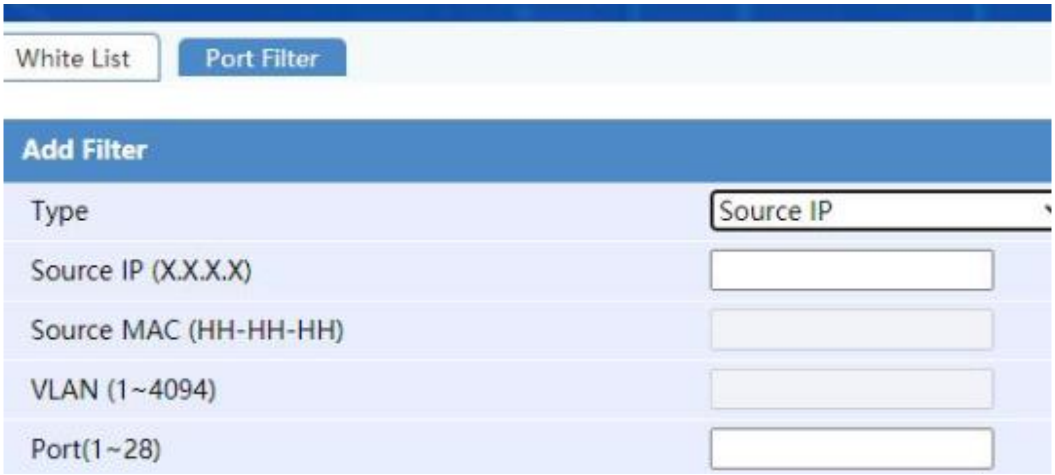
2.4 Security Menu Information

Enable the IP filter function on the port connected to the user side of the device, which can filter the packets received on the port to prevent illegal packets from passing through the port, thereby limiting the illegal use of network resources (such as illegal hosts spoofing legitimate users IP access network), which improves port security.

2.4.1 Security > IP Filter

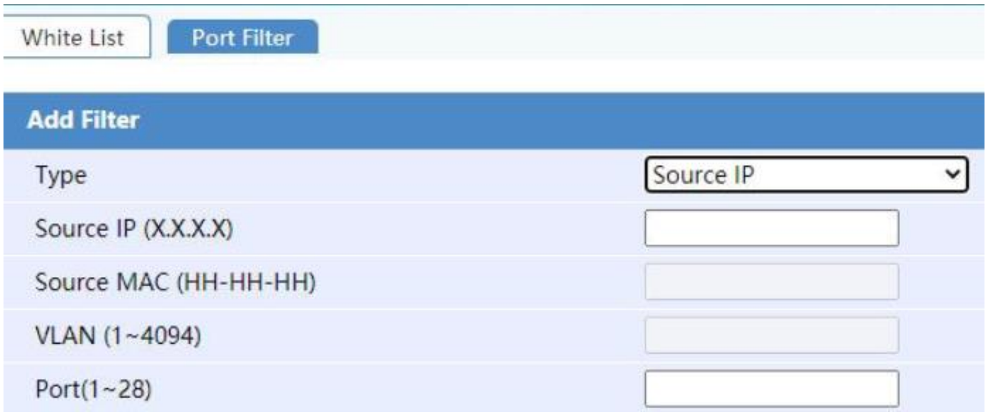
White List:

Page Wizard: Security → IP Filter → White List. on this page you can view and add white list users.



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

Before enabling the port filtering function, add the IP address and MAC address of the management device to the white list in the "White List Display Page" Device Information.



Add Filter

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

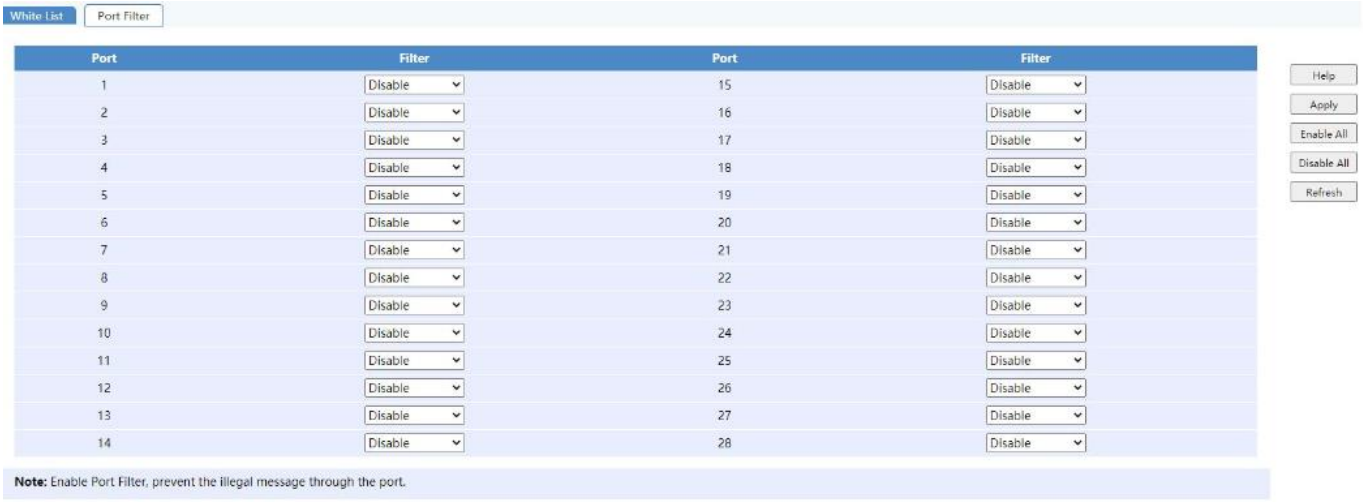
The meaning of the key items in the TLV setting page is shown in the table below.

Operation	Explanation
Type	Available types are • Source IP address: just enter the IP address and port number. • Source MAC address: just enter the MAC address and port number. • Source IP address + VLAN: IP address and VLAN ID need to be entered. • Source MAC address + VLAN: need to input MAC address and VLAN ID. • Source IP address + MAC address + VLAN: IP address, MAC address, and VLAN ID need to be entered.
Source IP address	Enter the IP address of the management device.
Source MAC address	Enter the MAC address of the management device.
VLAN	Enter VLAN ID.
Port	Select the port number to be whitelisted.

Port Filter:

Page Wizard: Security → IP Filter → Port Filter. On this page, you can choose to turn on/off the port IP filtering function and select off/on in the drop-down box of IP filtering. You can select <All On> or

<All Off> for batch setting.



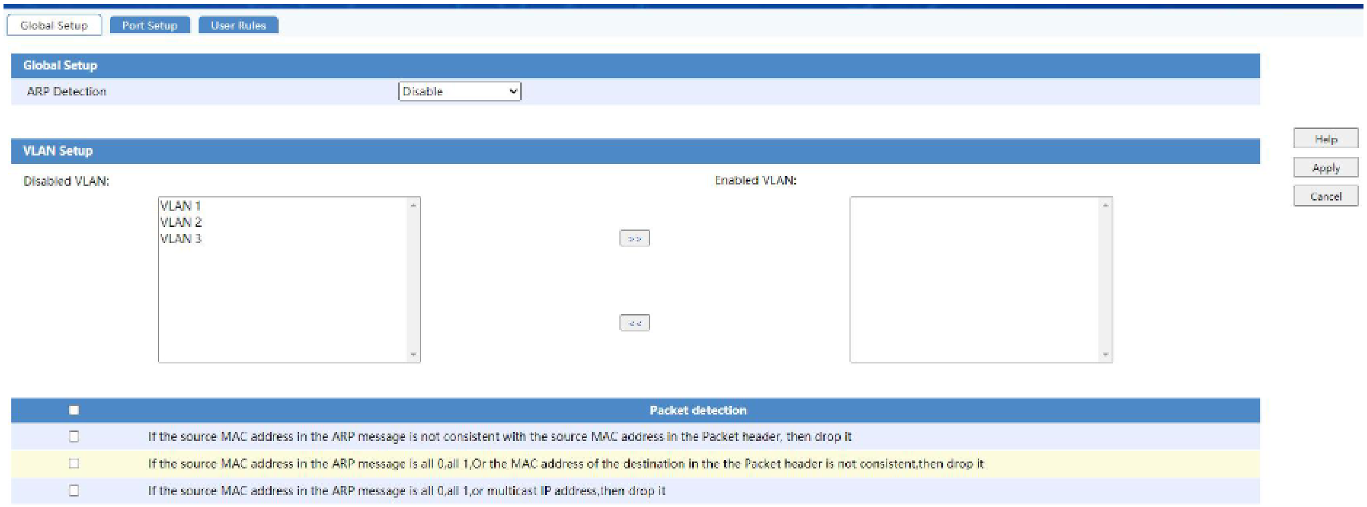
Port	Filter	Port	Filter
1	Disable	15	Disable
2	Disable	16	Disable
3	Disable	17	Disable
4	Disable	18	Disable
5	Disable	19	Disable
6	Disable	20	Disable
7	Disable	21	Disable
8	Disable	22	Disable
9	Disable	23	Disable
10	Disable	24	Disable
11	Disable	25	Disable
12	Disable	26	Disable
13	Disable	27	Disable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

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

2.4.2 Security > ARP Attack Defense

Global Setup:

Page Wizard: Security → ARP Defense → Global Setup. This page can be configured to enable/disable ARP detection globally. The VLAN setting box can be configured to enable/disable ARP detection by VLAN. It can also be configured to enable or disable the validity check of different ARP packets.



Global Setup

ARP Detection: Disable

VLAN Setup

Disabled VLAN:

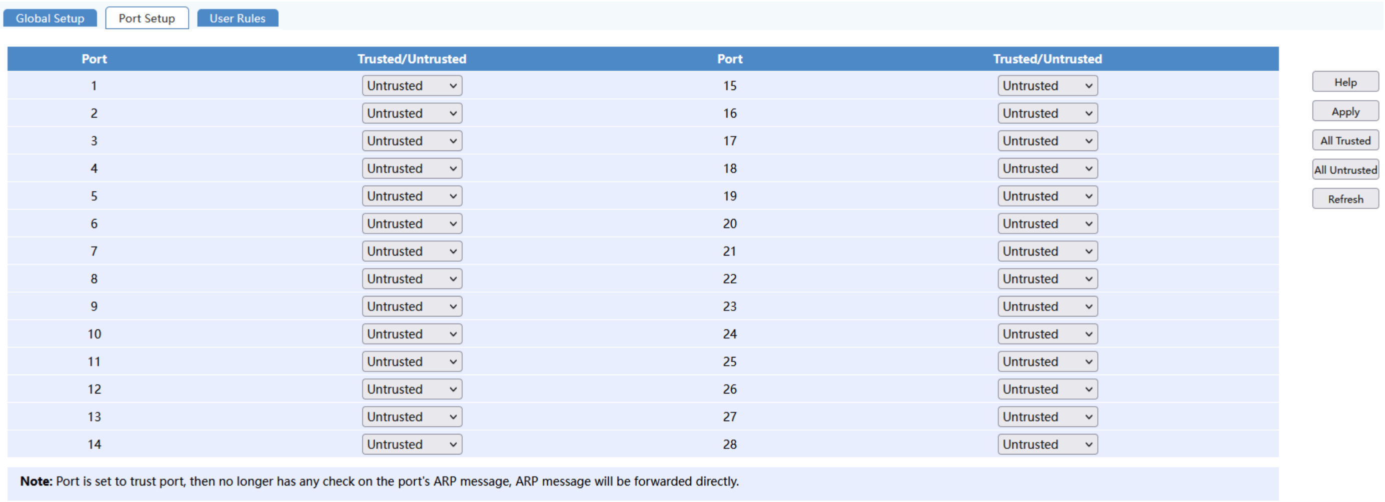
VLAN 1
VLAN 2
VLAN 3

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

Port Setup:

Page Wizard: Security → ARP Defense → Port Setup. On this page, you can configure whether the port is a trusted port for ARP packets.

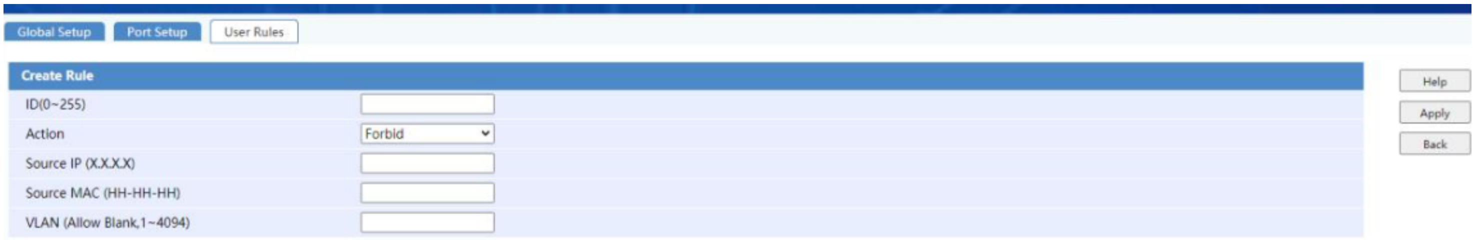


Port	Trusted/Untrusted	Port	Trusted/Untrusted
1	Untrusted	15	Untrusted
2	Untrusted	16	Untrusted
3	Untrusted	17	Untrusted
4	Untrusted	18	Untrusted
5	Untrusted	19	Untrusted
6	Untrusted	20	Untrusted
7	Untrusted	21	Untrusted
8	Untrusted	22	Untrusted
9	Untrusted	23	Untrusted
10	Untrusted	24	Untrusted
11	Untrusted	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.

User Rules:

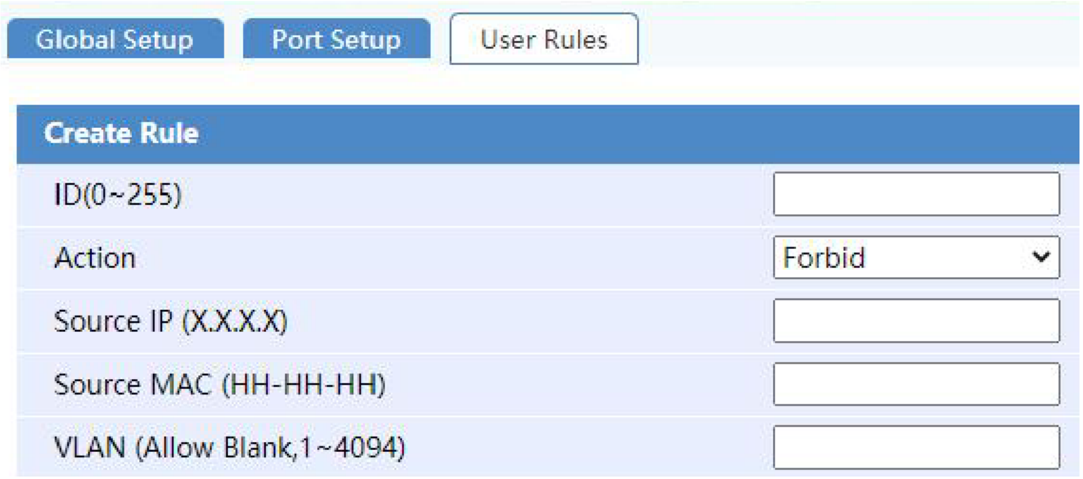
Page Wizard: Security ⟶ ARP Defense ⟶ User Rules. On this page, you can view and add ARP inspection user rules. After enabling ARP inspection, you can configure the rules to control ARP packet forwarding behavior.



Create Rule

ID(0~255)	
Action	Forbid
Source IP (X.X.X.X)	
Source MAC (HH-HH-HH)	
VLAN (Allow Blank,1~4094)	

By clicking the "Add" button on the page above, you can add ARP inspection rules based on user configuration. The configuration page is shown below:



Create Rule

ID(0~255)	
Action	Forbid
Source IP (X.X.X.X)	
Source MAC (HH-HH-HH)	
VLAN (Allow Blank,1~4094)	

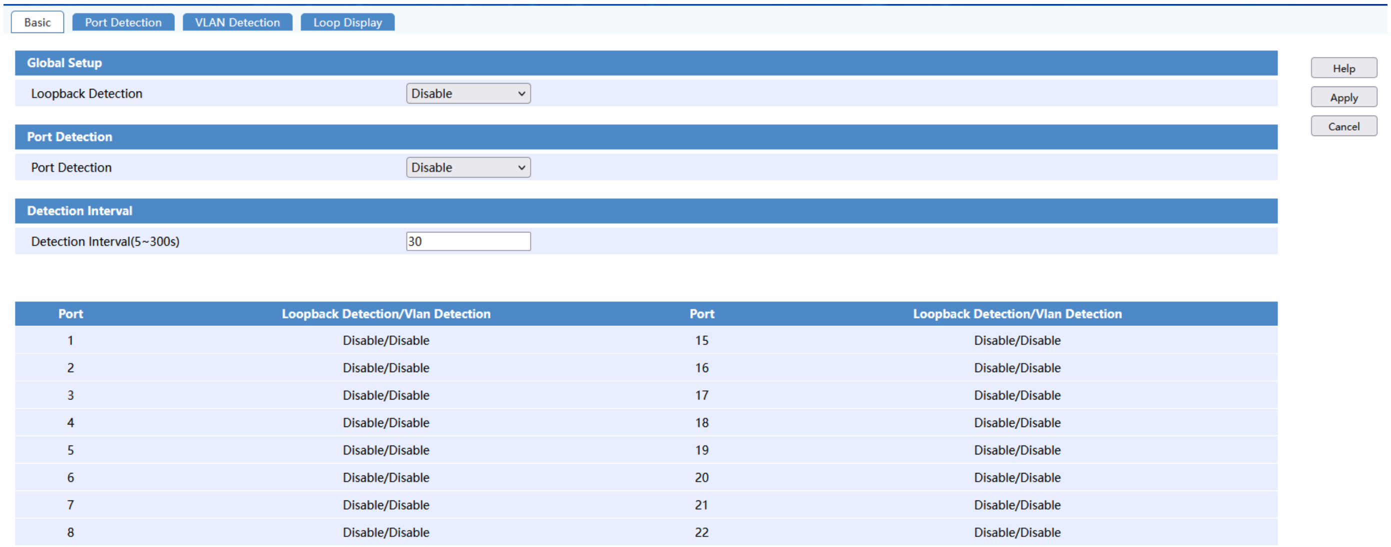
The meaning of the key items in the TLV setting page is shown in the table below.

Operation	Explanation
ID	User rule ID, value range 0~255
Behavior	Rule behavior, the action to be performed when the rule is matched
Source IP address	Source IP address of ARP protocol
Source MAC address	Source MAC address of ARP protocol
VLAN	Enter VLAN ID

2.4.3 Security > Loopback Detection

Basic:

Page Wizard: Security ⟶ Loopback Detection ⟶ Basic. This page can be configured with global on/off loop detection function, multi-port loop detection on/off function, loop detection time interval, and display port loop detection and on/off status by VLAN detection. After moving the mouse to the port state, you can also click to enter the single port configuration mode.



Global Setup

Loopback Detection: Disable

Port Detection

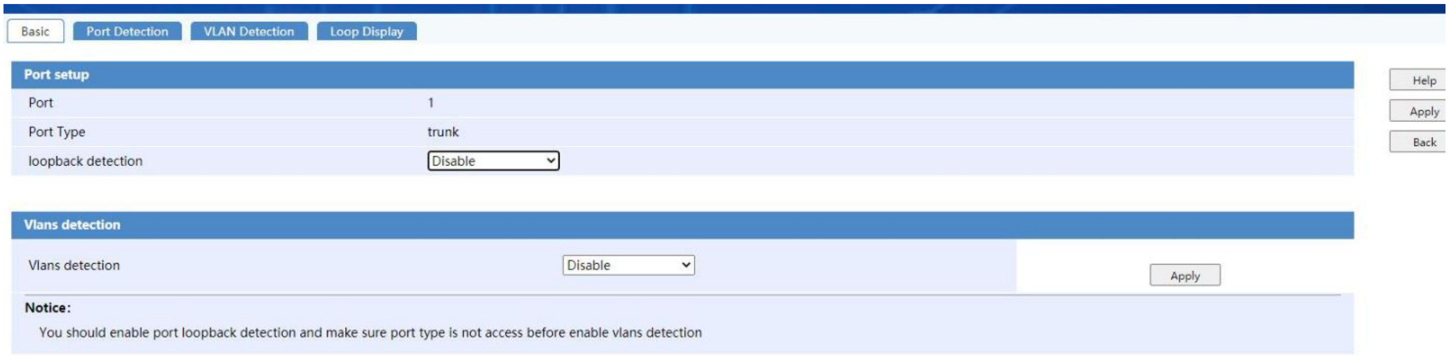
Port Detection: Disable

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
4	Disable/Disable	18	Disable/Disable
5	Disable/Disable	19	Disable/Disable
6	Disable/Disable	20	Disable/Disable
7	Disable/Disable	21	Disable/Disable
8	Disable/Disable	22	Disable/Disable

On the single port configuration page, you can configure whether to enable loop detection on the port and whether to enable the VLAN detection function.



Port setup

Port	1
Port Type	trunk
loopback detection	Disable

Vlans detection

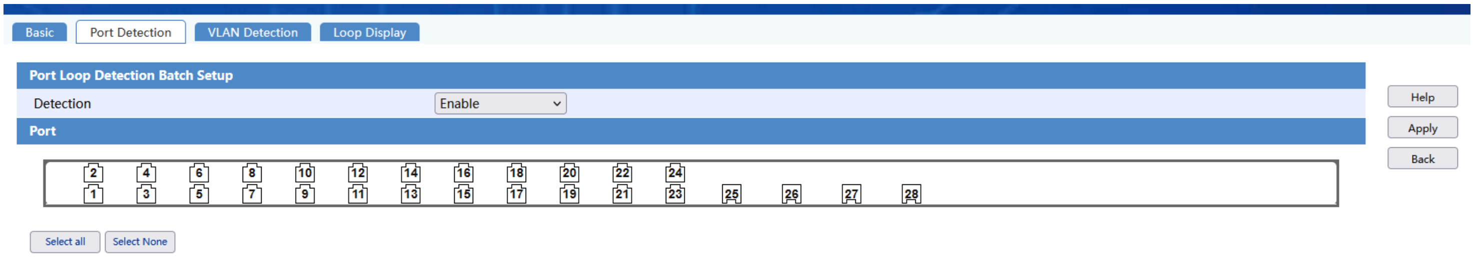
Vlans detection	Disable

Notice:

You should enable port loopback detection and make sure port type is not access before enable vlans detection

Port Detection:

Page Wizard: Security ⟶ Loopback Detection ⟶ Port Detection. This page is used to configure the port open/close loop detection function in batches.

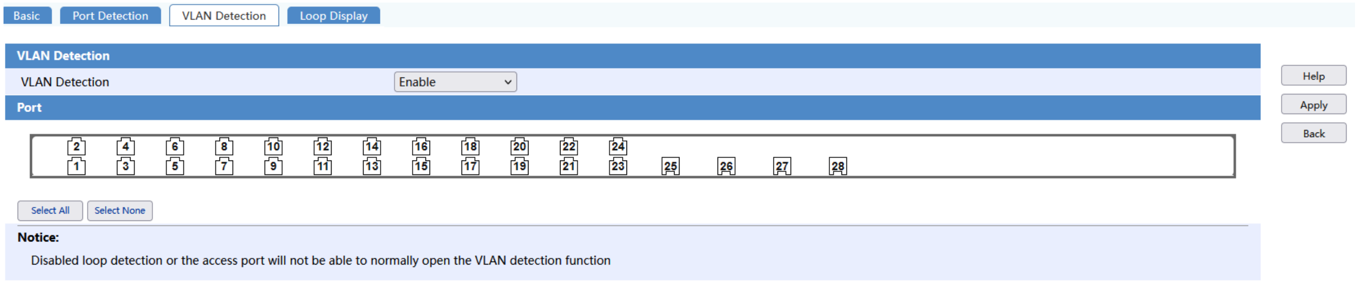


Port Loop Detection Batch Setup

Detection	Enable

VLAN Detection:

Page Wizard: Security ⟶ Loopback Detection ⟶ VLAN Detection. This page can configure the port opening/closing by VLAN detection function in batches.



VLAN Detection

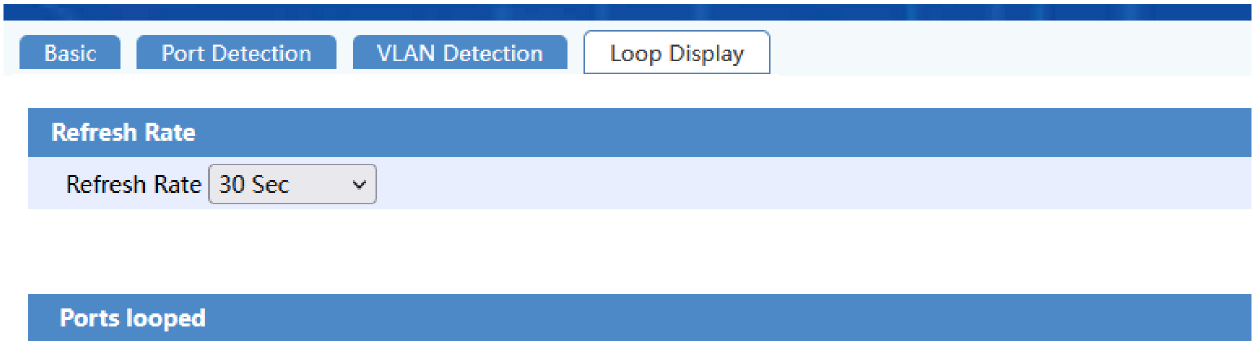
VLAN Detection	Enable

Notice:

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

Loop Display:

Page Wizard: Security ⟶ Loopback Detection ⟶ Loop Display. This page can be configured to display the web page refresh rate of the loop status, and at the same time, you can check whether the port has a loop and the current status of the port through the port with the loop.



Refresh Rate

Refresh Rate 30 Sec

Ports looped

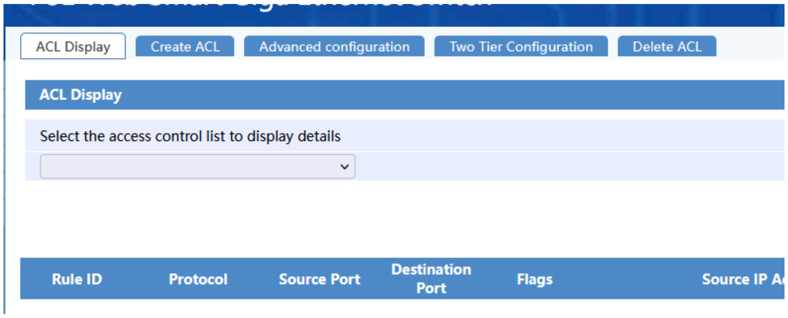
2.5 QoS Menu Information

2.5.1 QoS > ACL IPv4

ACL (Access Control List, access control list) is a collection of one or more rules used to identify the packet flow. The so-called rules refer to the judgment statements describing the matching conditions of the packet. These conditions may be the source address, a destination address, port number, etc. of the packet. The network device recognizes specific messages in accordance with these rules and processes them according to a preset policy.

ACL Display:

Page Wizard: QoS → ACL IPV4 → ACL Display. On this page, users are able to select the access control list to view their details.



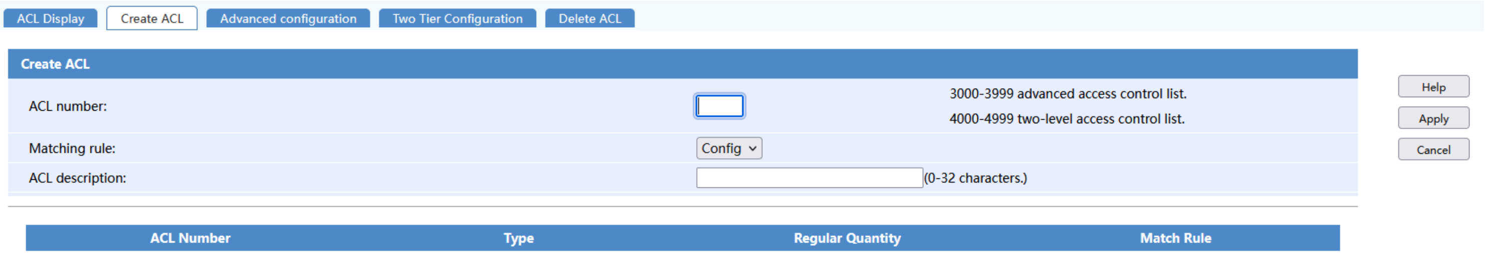
ACL Display

Select the access control list to display details

Rule ID	Protocol	Source Port	Destination Port	Flags	Source IP A

Create ACL:

Page Wizard: QoS → ACL IPV4 → Create ACL. When creating an ACL, the user must assign a number to it. Different numbers correspond to different types of ACLs. At the same time, in order to facilitate memory and identification, the user can also choose whether to set a name for the ACL when creating it. Once the ACL is created, users are not allowed to set names, modify or delete their original names. After the ACL is created, the user can specify the ACL by specifying the number or name in order to operate it.



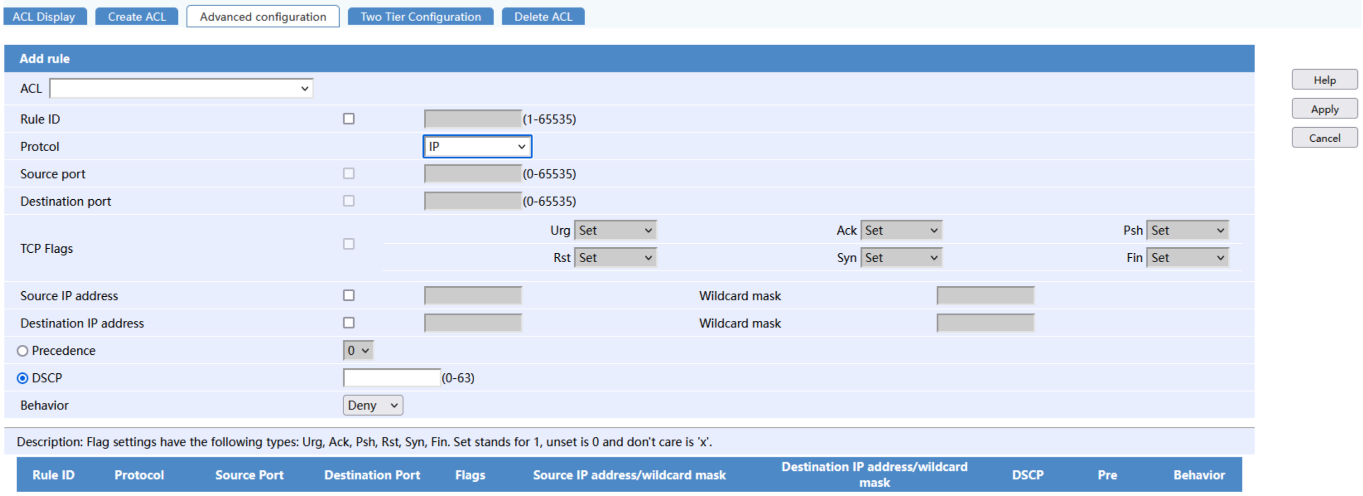
Create ACL

ACL number:		3000-3999 advanced access control list. 4000-4999 two-level access control list.
Matching rule:	Config	
ACL description:		(0-32 characters.)

ACL Number	Type	Regular Quantity	Match Rule

Advanced Configuration:

Page Wizard: QoS ⟶ ACL IPV4 ⟶ Advanced Configuration. IPv4 advanced ACL can be based on the source IP address, destination IP address, packet priority, protocol type and characteristics of IP bearer (such as TCP/UDP source port and destination port, TCP packet identification, ICMP protocol message type, and message codes, etc.) to formulate rules to match IPv4 packets. Users can use IPv4 advanced ACL to formulate more accurate, rich, and flexible rules than IPv4 basic ACL.



Add rule

ACL				
Rule ID	□	(1-65535)		
Protcol		IP		
Source port	□	(0-65535)		
Destination port	□	(0-65535)		
TCP Flags	□	Urg Set Rst Set	Ack Set Syn Set	Psh Set Fin Set
Source IP address	□		Wildcard mask	
Destination IP address	□		Wildcard mask	
○ Precedence	0			
● DSCP	(0-63)			
Behavior	Deny			

Description: Flag settings have the following types: Urg, Ack, Psh, Rst, Syn, Fin. Set stands for 1, unset is 0 and don't care is 'x'.

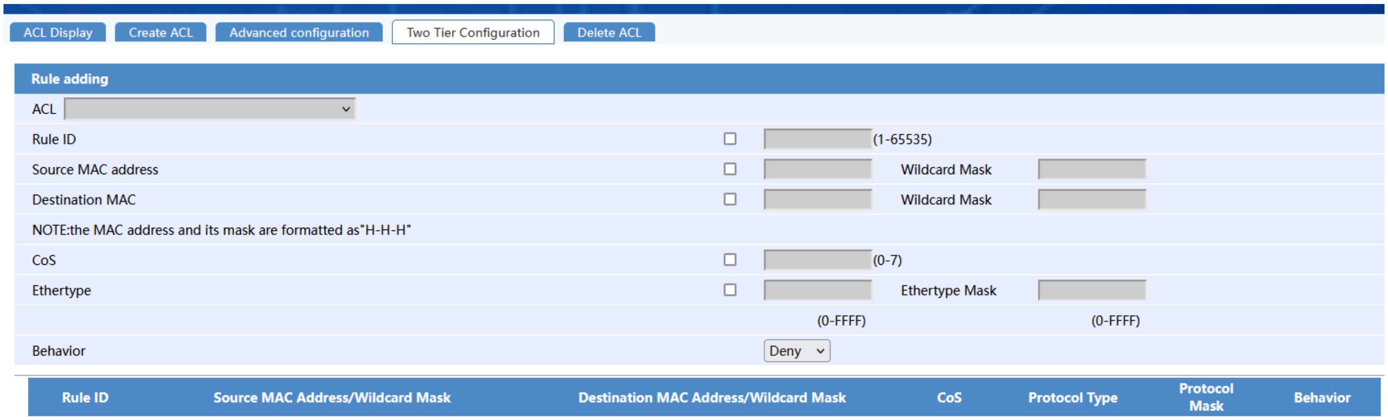
Rule ID	Protocol	Source Port	Destination Port	Flags	Source IP address/wildcard mask	Destination IP address/wildcard mask	DSCP	Pre	Behavior

Operation	Command	Explanation
Enter superuser view	**super**	-----
Create an IPv4 advanced ACL and enter IPv4 advanced ACL view	**acl number***acl-number*	Required. By default, no ACL exists Ipv4 advanced ACL number range 3000~3999
Configure ACL description	**description** text	Optional, by default, ACL does not have any
	rule [*rule-id*] **{ deny | permit } {gre |**	By default, there are no rules in the IPv4

Create a rule	**icmp**| **igmp**| **ip**| **ipinip**| **ospf**| **tcp**| **udp**} { {**destination** { *dest-addr dest wildcard* }|**dscp**dscp|***precedence****precedence*|**source***sour-addr sour-wildcard* | **source-port***operator port1* [*port2*] | **destination-port***operator port1* [*port2*]|{**ack***ack-value* | **fin***fin value* |**psh***psh-value* |**rst***rst-value* |**syn***syn-value* |**urg***urg-value* } *}	advanced ACL

Two Tier Configuration:

Page Wizard: QoS → ACL IPV4 → Two Tier Configuration. On this page, users are able to two tier ACL configuration.



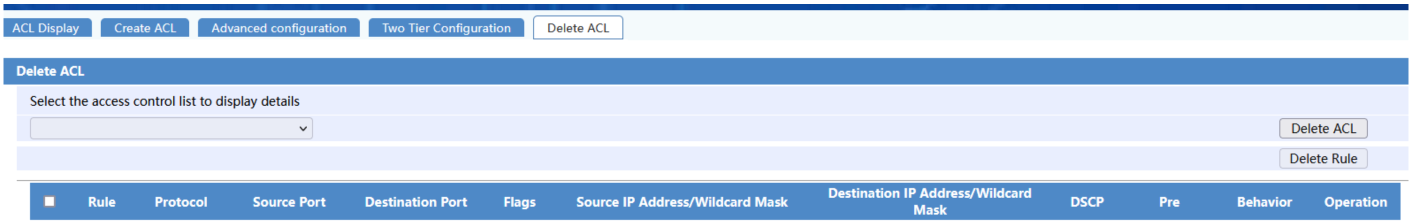
Rule adding

ACL				
Rule ID	□	(1-65535)		
Source MAC address	□		Wildcard Mask	
Destination MAC	□		Wildcard Mask	
NOTE:the MAC address and its mask are formatted as"H-H-H"				
CoS	□	(0-7)		
Ethertype	□		Ethertype Mask	
		(0-FFFF)		(0-FFFF)
Behavior		Deny		

Rule ID	Source MAC Address/Wildcard Mask	Destination MAC Address/Wildcard Mask	CoS	Protocol Type	Protocol Mask	Behavior

Delete ACL:

Page Wizard: QoS → ACL IPV4 → Delete ACL. On this page, users are able to delete ACL and rules by selecting the desired one through the drop-down menu.



Delete ACL

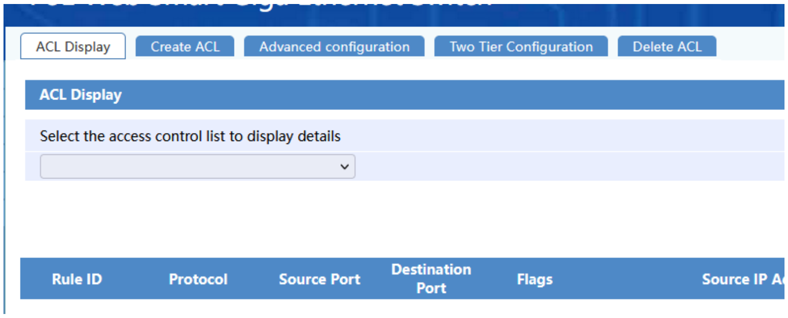
Select the access control list to display details

□	Rule	Protocol	Source Port	Destination Port	Flags	Source IP Address/Wildcard Mask	Destination IP Address/Wildcard Mask	DSCP	Pre	Behavior	Operation

2.5.2 QoS > ACL IPv6

ACL Display:

Page Wizard: QoS ⟶ ACL IPV6 ⟶ ACL Display. On this page, users are able to select the access control list to view their details.



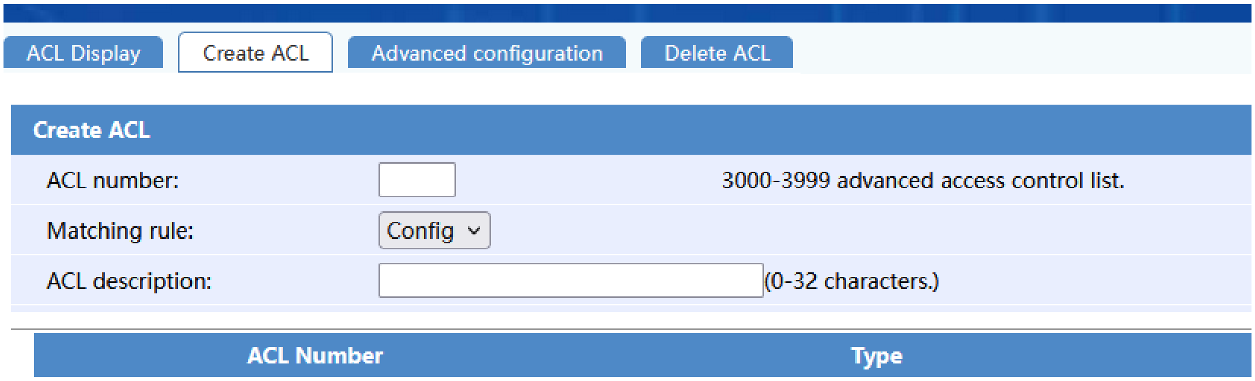
ACL Display

Select the access control list to display details

Rule ID	Protocol	Source Port	Destination Port	Flags	Source IP A

Create ACL:

Page Wizard: QoS ⟶ ACL IPV6 ⟶ Create ACL. When creating an ACL, the user must assign a number to it. Different numbers correspond to different types of ACLs. At the same time, in order to facilitate memory and identification, the user can also choose whether to set a name for the ACL when creating it. Once the ACL is created, users are not allowed to set names, modify or delete their original names. After the ACL is created, the user can specify the ACL by specifying the number or name in order to operate it.



Create ACL

ACL number:		3000-3999 advanced access control list.
Matching rule:	Config	
ACL description:		(0-32 characters.)

ACL Number	Type

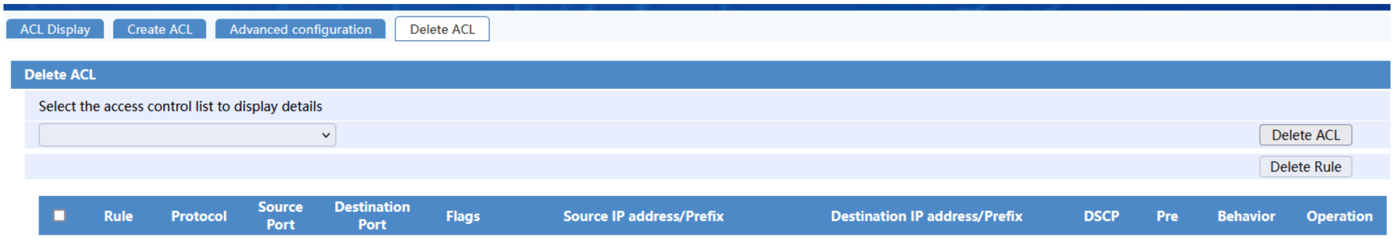
Advanced Configuration:

Page Wizard: QoS ⟶ ACL IPV6 ⟶ Advanced Configuration. IPv6 advanced ACL can be based on the source IPv6 address of the packet, the destination IPv6 address, the priority of the packet, the protocol type and characteristics of the IPv6 bearer (such as the source and destination ports of TCP/UDP, the TCP message identifier, and the message type of the ICMPv6 protocol and message codes, etc.) to formulate rules to match IPv6 packets. Users can use IPv6 advanced ACL to formulate more accurate, rich, and flexible rules than IPv6 basic ACL.

Operation	Command	Explanation
Enter superuser view	**super**	-----
Create an IPv6 advanced ACL and enter IPv6 advanced ACL view	**Aclipv6 number** *num-adv-v6* **[match-order {auto | config}]**	Required, by default, no ACL exists Ipv6 advanced ACL number range 3000~3999
Configure ACL description information	**description** text	Optional, by default, ACL does not have any description information
Create a rule	**rule {deny | permit** | *priority* **{deny | permit}** }{*protocol* **| gre | icmpv6 | ipv6 | ipv6-ah | ipv6-esp | ospf} [destination** *dest-ip* **prefix | dscp** *dscp-val* **| precedence** *precedence-val* **| source** *src-ipprefix*] **rule {deny | permit** | *priority* **{deny | permit} } tcp [destination** *dest-ipprefix* **| dscp** *dscp-val* **| precedence** *precedence-val* **| source** *src-ip* **prefix | destination-port eq** *port-number* | **source-port eq** *port-number* |**ack** *val* | **fin** *val* **| psh** *val* **| rst** *val* **| syn** *val* **| urg** *val*] **rule {deny | permit** | *priority* **{deny | permit} } udp [destination** *dest-ipprefix* **| dscp** *dscp-val* **| precedence** *precedence-val* **| source** *src-ipprefix* **| destination-port eq** *port-number* | **source-port eq** *port-number*]	By default, there are no rules in the IPv6 advanced ACL

Delete ACL:

Page Wizard: QoS → ACL IPV6 → Delete ACL. On this page, users are able to delete ACL and rules by selecting the desired one through the drop-down menu.



Delete ACL

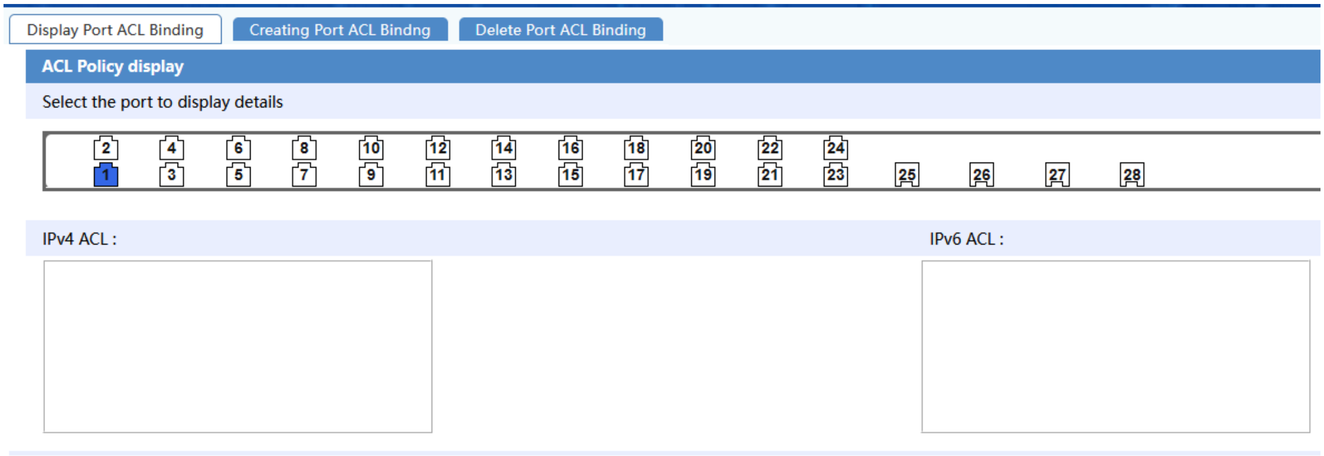
Select the access control list to display details

□	Rule	Protocol	Source Port	Destination Port	Flags	Source IP address/Prefix	Destination IP address/Prefix	DSCP	Pre	Behavior	Operation

2.5.3 QoS > ACL Policy

Display Port ACL Binding:

Page Wizard: QoS → ACL Policy → Display Port ACL Binding. View the ACL IPv4 and IPv6 policies for each port in detail.



ACL Policy display

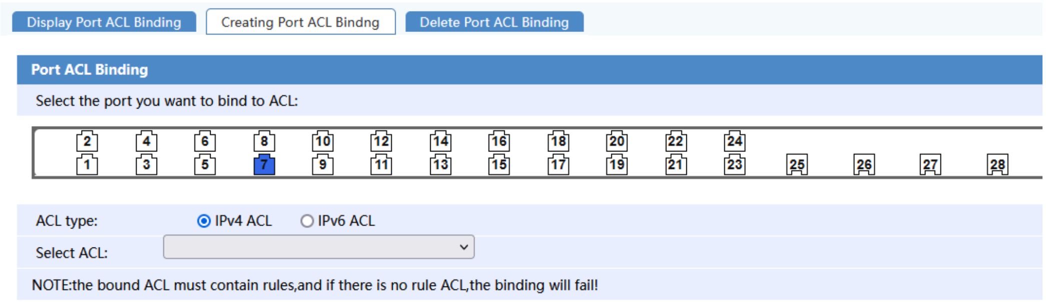
Select the port to display details

IPv4 ACL :

IPv6 ACL :

Create Port ACL Binding:

Page Wizard: QoS → ACL Policy → Create Port ACL Binding. Select ports that you want to bind to ACL. Users can select IPv4 or IPv6 ACL types. The bound ACL must contain rules, and if there is no rule ACL, the binding will fail.



Port ACL Binding

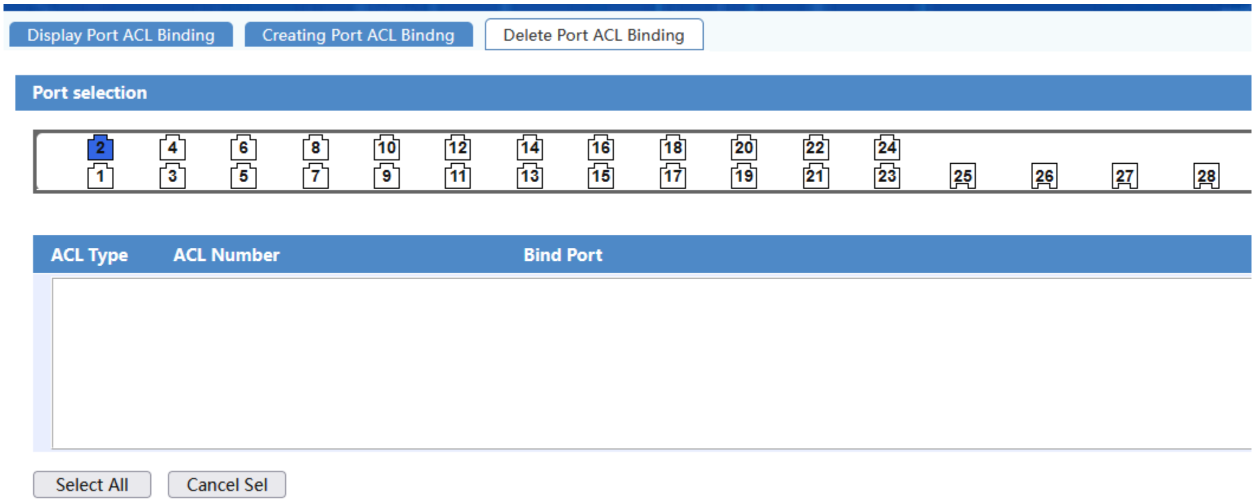
Select the port you want to bind to ACL:

ACL type: ● IPv4 ACL ○ IPv6 ACL

Select ACL:

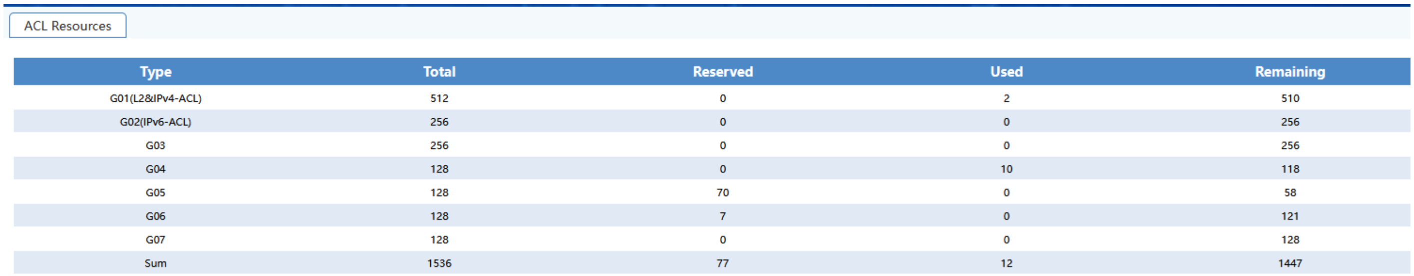
NOTE:the bound ACL must contain rules,and if there is no rule ACL,the binding will fail!

Page Wizard: QoS ⟶ ACL Policy ⟶ Delete Port ACL Binding. Select individual or multiple bind ports, and delete the ACL binding via this page.



2.5.4 QoS > ACL Resource

Page Wizard: QoS ⟶ ACL Resources. View the type, total, reserved, used, and remaining ACL resources via this page.

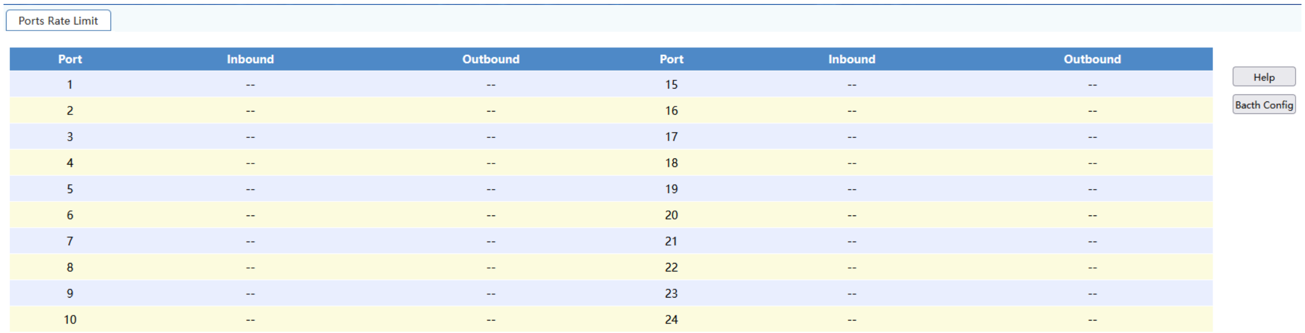


Type	Total	Reserved	Used	Remaining
G01(L2&IPv4-ACL)	512	0	2	510
G02(IPv6-ACL)	256	0	0	256
G03	256	0	0	256
G04	128	0	10	118
G05	128	70	0	58
G06	128	7	0	121
G07	128	0	0	128
Sum	1536	77	12	1447

2.5.5 QoS > Ports Rate Limit

Page Wizard: QoS ⟶ Port Rate Limit. On this page, you can check the speed limit status of each port's in/out ports ("--" means that no speed limit is applied.)

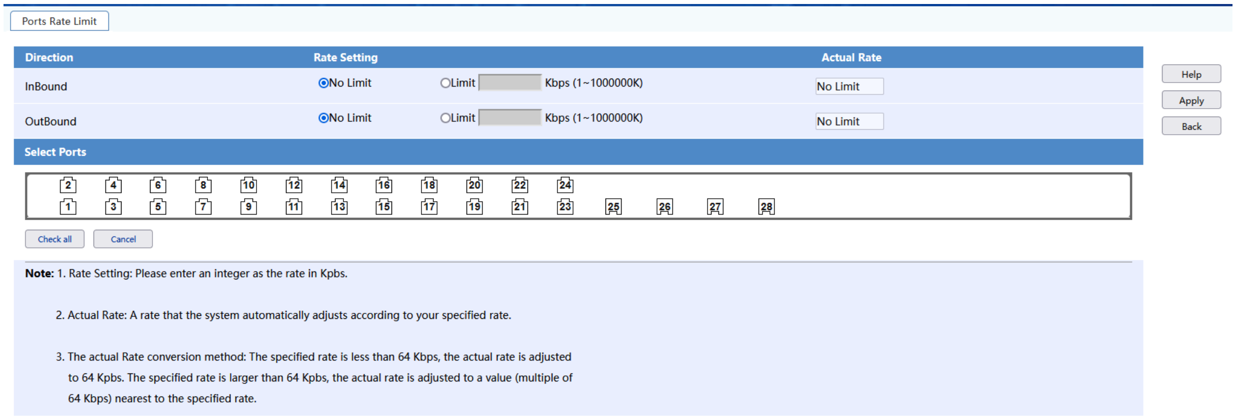
The Port rate limit refers to the rate limit based on the port. It uses token buckets to control packet traffic. The token bucket can be regarded as a container for storing a certain number of tokens. The system puts tokens into the bucket at a set rate. When the tokens in the bucket are full, the extra tokens overflow and the tokens in the bucket no longer increase. The port rate limit supports both inbound and outbound directions. For the convenience of description, the outbound port rate-limiting process is used as an example: All packets sent through the port must first be processed through the token bucket. When a token is stored in the token bucket, the packet can be sent according to the token; otherwise, the packet will enter the port cache for congestion management. In this way, you can control the packet flow through the port.



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

Configure the inbound/outbound port speed limit of a single port: click the entry corresponding to the port on the main page to enter the corresponding page.

Configure the inbound/outbound port speed limit of the specified port in batches: Click the <Batch Configuration> button on the main page to enter the corresponding page.



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

Note: 1. Rate Setting: Please enter an integer as the rate in Kpbs.

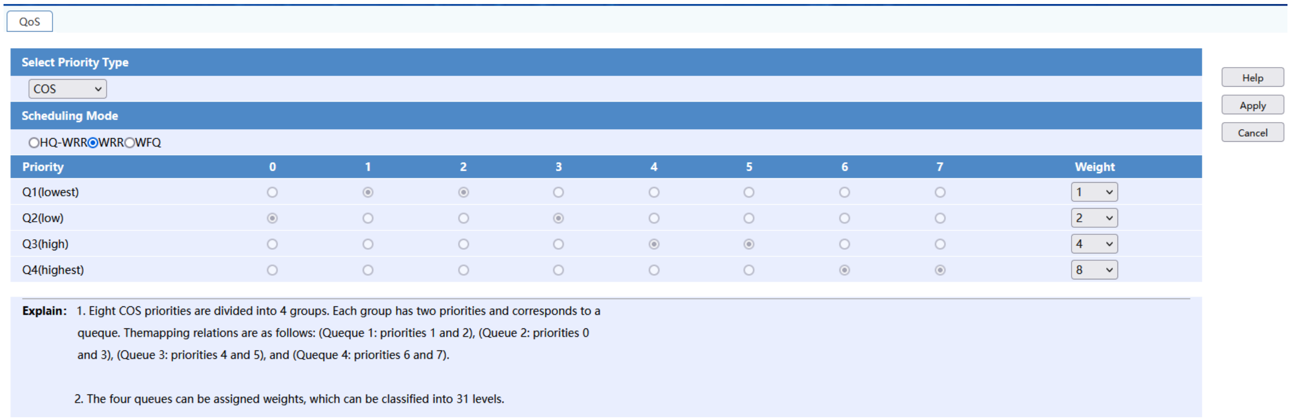
2. Actual Rate: A rate that the system automatically adjusts according to your specified rate.

3. The actual Rate conversion method: The specified rate is less than 64 Kbps, the actual rate is adjusted to 64 Kpbs. The specified rate is larger than 64 Kpbs, the actual rate is adjusted to a value (multiple of 64 Kbps) nearest to the specified rate.

Inbound port speed limit performs a drop action for packets that exceed the speed limit. This behavior will affect the transmission efficiency of most applications based on the TCP protocol. The reaction is that the actual transmission speed is much slower than the speed limit value. It is recommended that users do not enable the inbound Port speed limit function, there is no application limit for the output port speed limit.

2.5.6 QoS > QoS

Page Wizard: QoS → QoS. This page can configure priority trust mode and queue scheduling mode.



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

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.

The meaning of the key items on the page is shown in the table below.

Operation	Explanation
Priority type selection	Choose the priority mode you want to trust: - COS: Put the packet into the port output queue of the corresponding priority according to the 802.1p priority. - DSCP: Put the packet into the port output queue of the corresponding priority according to the DSCP priority. By default, 48G-4GF puts packets into the port output queue of the corresponding priority according to the 802.1p priority.
Scheduling mode	Select queue scheduling mode By default, 48G-4GF uses WRR scheduling algorithm. Example: If the weight ratio of queue 1, queue 2, queue 3, and queue 4 is 1:2:4:8, and the queue scheduling mode is WRR. Then, when the data packets of queues 1, 2, 3, and 4 are congested on a certain port, the port will send packets according to the flow ratio of 1:2:4:8; if the scheduling mode is selected as HQ-WRR 48G-4GF will first ensure that the

	packets of queue 4 are sent out first, and then implement WRR scheduling for the remaining 3 queues.
Weights	Configure the priority weight of each queue.

3. Appendix

1. Why can't the bandwidth be increased after trunking is configured?

A: Please check if the information of trunking set port is as same, including rate, duplex mode, and VLAN etc.

2. How to deal with the problem of partial ports of switch?

A: When some ports are blocked on the switch, it may be the network cable's fault, the network card failure, or the switch port failure. Users can test by following steps:

a. If the connection of the computer and switch ports remains unchanged, try replacing other

network cables.

b. Try different switch ports to see if the issue is persistent. This will help narrow down if the specific port is an issue or not.

d. If confirmed that is caused by the switch port failure, please contact the supplier for maintenance

3. What is the order of the port self-adaptive status detection?

A: Port of state testing was conducted in the following order: 1000Mbps full-duplex, 100Mbps full-duplex, 100Mbps half-duplex, 10Mbps full-duplex, 10 Mbps half-duplex.

4. Forgot the Password?

A: You can restore the switch to factory settings by pressing the reset button on the front panel of the switch for 10 seconds. This will reset the username to **admin**, and the password to **system**.

4. Maintenance

Clean this unit with a soft, dry cloth. Never use alcohol, paint thinner, or benzine to clean.

5. Warranty

If your product does not work properly because of a defect in materials of workmanship, our company (referred to as "the warrantor") will, for the length of the period indicated as below, "Parts and Labor

(5) Years", which starts with the date of original purchase ("Limited Warranty period"), at its option either (a) repair your product with new or refurbished parts, or (b) replace it with a new or a refurbished product. The decision to repair or replace will be made by the warrantor.

During the "Labor" limited warranty period, there will be no charge for labor. During the "Parts" warranty period, there will be no charge for parts. You must mail-in your product during the warranty period. This Limited Warranty is extended only to the original purchaser and only covers products purchased as new. A purchase receipt or other proof of original purchase date is required for Limited Warranty service.

6. Mail-In Service

When shipping the unit, carefully pack and send it prepaid, adequately insured, and preferably in the original carton. Include a letter detailing the complaint and provide a day time phone and/or email address where you can be reached.

7. Limited Warranty Limits and Exclusions

This Limited Warranty ONLY COVERS failures due to defects in material or workmanship, and DOES NOT COVER normal wear and tear or cosmetic damage. The Limited Warranty ALSO DOES NOT COVER damages which occurred in shipment, or failures which are caused by products not supplied by warrantor, or failures which result from accidents, misuse, abuse, neglect, mishandling, misapplication, alteration, faulty installation, set-up adjustments, mis-adjustment of consumer controls, improper maintenance, power line surge, lightning damage, modification, or service by anyone other than a Factory Service center or other Authorized Servicer, or damage that is attributed to acts of God.

THERE ARE NO EXPRESS WARRANTIES EXCEPT AS LISTED UNDER "LIMITED WARRANTY COVERAGE". THE WARRANTOR IS NOT LIABLE FOR INCIDENTAL OR CONSEQUENTAIL DAMAGES RESULTING FROM THE USE OF THIS PRODUCT, OR ARISING OUT OF ANY BREACH OF THIS WARRANTY. (As examples, this excludes damages for lost time, cost of having someone remove or re-install an installed unit if applicable, travel to and from the service, loss of or damage to media or images, data or other recorded content. The items listed are not exclusive, but are for illustration only.) PARTS AND SERVICE, WHICH ARE NOT COVERED BY THIS LIMITED WARRANTY, ARE YOUR RESPONSIBILITY.

WWW.ZENTY.COM
9807 EMILY LANE
STAFFORD, TX 77477

(844) 200-1945
SALES@ZENTY.COM