TP-SW16GBT/AT/PSV-U

20 Port L3 Managed PoE Switch

Advanced Web Configuration Guide

V4.1 20240605

About This Document

This product includes three documents as the table below.

Documents	Description	How to get it
Quick Guide	Including product introductions and installation steps.	In the packing box
Web-based Configuration Guide	Including Web network management system configuration instructions.	tyconsystems.com
CLI-based Configuration Guide	Including CLI-based configuration instructions	tyconsystems.com

This document is **Web-based Configuration Guide**, including Web network management system (short for Web system) configuration instructions. It is intended for engineers or anyone who needs to configure the device by Web system.

The advanced configuration instructions here take industrial 16-Port Gigabit PoE + 4-Port 10G SFP+ L3 Managed Ethernet Switch as example. If there is inconsistency between the instruction (eg. port number, PoE function, etc.) and the actual product, please refer to the actual product.

Announcement

The information in this document is subject to change without notice.

The document is only used as operation guide, except for other promises. No warranties of any kind, either express or implied are made in relation to the description, information or suggestion or any other contents of the manual.

The images shown here are indicative only. If there is inconsistency between the image and the actual product, the actual product shall govern.

Symbol Conventions

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

Symbol	Description
DANGER	Indicates a hazard with a high level of risk, which if not avoided, will result in death or serious injury.
WARNING	Indicates a hazard with a medium or low level of risk, which if not avoided, could result in minor or moderate injury.
CAUTION	Indicates a potentially hazardous situation, which if not avoided, could result in equipment damage, data loss, performance degradation, or unexpected results.
NOTE	Provides additional information to emphasize or supplement important points in the main text.

Change History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

Version	State	Release Date	Descriptions
V1.0	Released	2018-12-04	Initial commercial release.
V2.0	Released	2020-04-27	Make the section of “3 Function Configuration Guide” a document to introduce the Web system configuration steps completely.
V3.0	Released	2020-08-05	Add new chapters of “12.4 ERPS Ring”, “12.5 ERPS Instance” and “13 Alarm Management” to introduce the new features of Web System.
V3.1	Released	2020-12-07	Correct the version of browser in “2.2 Software Requirements”.
V4.1	Released	2024-06-05	Add the version based on user requirement.

Content

1 Configuration Instructions 1
2 Requirements 2
2.1 Hardware Requirements 2
2.2 Software Requirements 2
3 Set Up Network Connection 3
3.1 Set Static IP for the Management Computer 3
3.2 Confirm the Network Connection by Ping Command 5
3.3 Cancel the Proxy Server 5
4 Login the Web system 7
4.1 Login and Start 7
4.2 Web System User Interface 7
4.3 Saving Configuration 8
4.4 Viewing Configuration 8
4.5 User Timeout 8
4.6 Logging-out Web System 8
5 System State 10
5.1 System Status 10
5.2 Traffic Statistics 10
5.3 MAC Address Table 10
5.4 SFP information 11
6 Energy Management 11
6.1 Solar System Configuration 11
6.2 Solar System Working Curve 13
6.3 History Data 14
7 Port Configuration 15
7.1 Port Setting 15
7.2 Rate Limit 16
7.3 Storm Control 18
7.4 Port Isolation 18
7.5 LLDP Configuration 19
7.6 LLDP Neighbors 20
7.7 MAC Limit 21
7.8 PoE Setting 22
7.9 PoE Schedule 24
8 Ethernet Switch 26
8.1 Link Aggregation 26
8.2 802.1Q VLAN 27
8.3 VLAN Description 28
8.4 Multicast Traffic Control 28
8.5 QinQ Setting 29
8.6 VLAN Mapping 30
8.7 MAC-based VLAN 31
8.8 Port-based VLAN 32
8.9 Private VLAN 32
8.10 802.1Q QoS 34

8.11 DSCP QoS 35
8.12 WRR Configuration 36
9 IP Service 37
9.1 Interface IP 37
9.2 DHCP Server 38
9.3 DHCP Snooping 40
9.4 DNS Client Configuration 40
10 IP Routing 42
10.1 RIP 42
10.2 OSPF 43
10.3 Routing Table 44
11 IP Multicast 46
11.1 IGMP Snooping 46
11.2 MLD Snooping 47
11.3 Multicast MAC Address Table 48
12 Security Configuration 49
12.1 802.1x Authentication 49
12.2 AAA Setting 50
12.3 Static Address Lock 51
12.4 MAC Flapping 52
12.5 MAC Dynamic Aging 52
12.6 ACL Configuration 53
12.7 Port ACL 54
12.8 Login Filter ACL 55
13 Reliability 57
13.1 Rapid Spanning Tree 57
13.2 MSTP Region Configuration 59
13.3 MSTP Instance Configuration 59
13.4 MSTP Port Configuration 60
13.5 MSTP Instance Information 61
13.6 Fast-Ring Protect 62
13.7 Loopback Protect 63
13.8 CCM 64
13.9 ERPS Ring 65
13.10 ERPS Instance 66
13.11 VRRP Setting 67
14 Network Diagnosis 69
14.1 ICMPv4 69
14.2 ICMPv6 69
14.3 Traceroute 70
15 RMON 72
15.1 Statistics Config 72
15.2 Statistics Status 72
15.3 History Control Table 72
15.4 Ether History Table 73
15.5 Alarm Table 73

15.6 Event Table 74
15.7 Log Table 75
16 DMS 76
16.1 Device List 76
16.2 Topology View 76
17 System Management 76
17.1 Port mirroring 76
17.2 SNMP 77
17.3 Login 79
17.4 Time 79
17.5 Syslog 81
17.6 Management 81
17.7 User Setting 83
17.8 Timing Restart 84

1 Configuration Instructions

To facilitate configuration and the maintenance of the device, the Web system is provided to users. You can log in to the Web system to configure and maintain devices through the graphic user interface (GUI).

The Advanced Web-based configuration guide describes the configuration and maintenance of the device through the Web system. It is intended for engineers or anyone who needs to configure the device through the Web system.

Web System Overview

The Web system provides the functions as below.

System State

Port Configuration

Ethernet Switch

IP Service

IP Routing

IP Multicast

Security Configuration

Reliability

Alarm Management

System Management

Please follow the instructions below to configure the Web system.

2 Requirements

2.1 Hardware Requirements

The management PC recommended as below.

Make sure the management PC has already been with Ethernet port.

Use a network cable to connect the Ethernet port of PC and the Ethernet port of the switch.

2.2 Software Requirements

The browser version recommend as below.

IE10 or higher

Firefox browser

Chrome

3 Set Up Network Connection

Before login the Web system to start configuration, users need to set up the network connection as follow steps.

Set the IP of the PC and the switch in the same network segment. The default IP address of the switch is 192.168.1.200, network gate is 255.255.255.0.

The port to connect management PC for Web setting must be management VLAN. By default, management VLAN is VLAN 1, and each port of the switch is VLAN1.

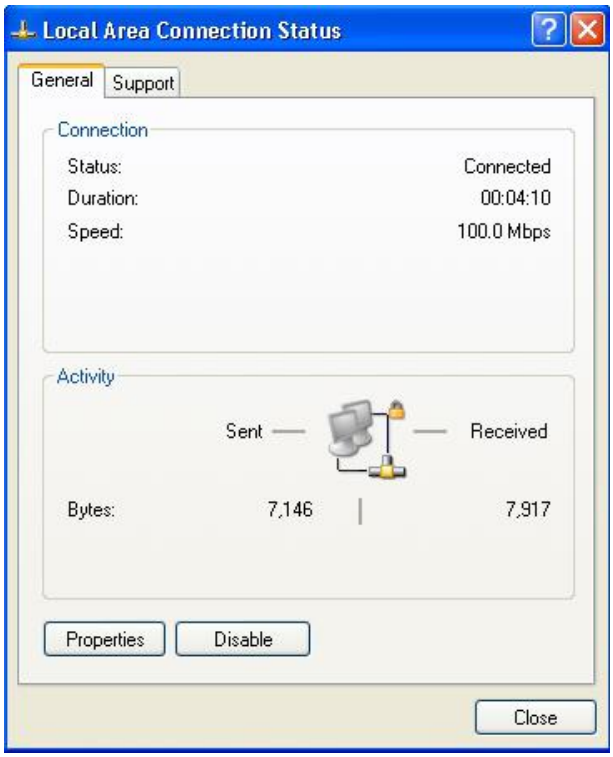
If you need to connect the remote network, please make sure the management PC and the router can do the jobs above.

This product can't assign the IP address for the management PC, please configure the management static IP manually before web configuration.

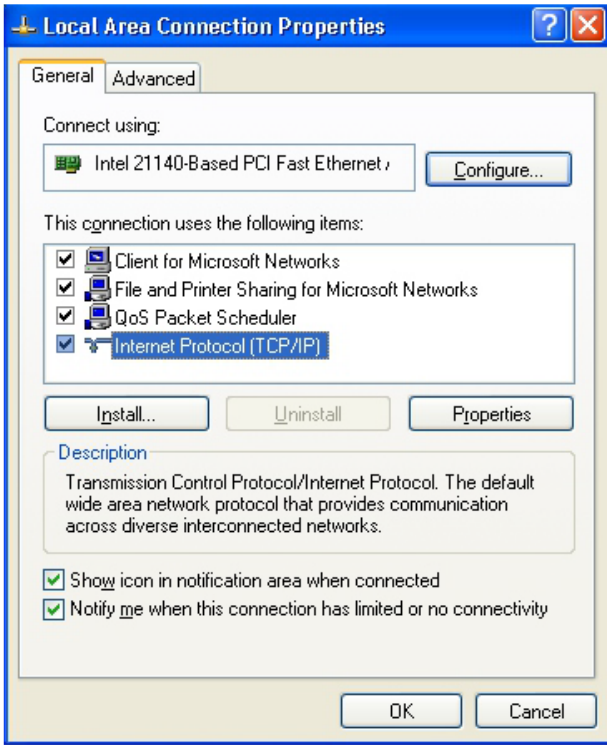
3.1 Set Static IP for the Management Computer

Operation steps (take Windows 10 as sample)：

Click <start> to enter the <start> menu, select “control panel”. Double click “network connection” icon, then double click the “local connection” icon, “local Area Connection Status” window pops out.

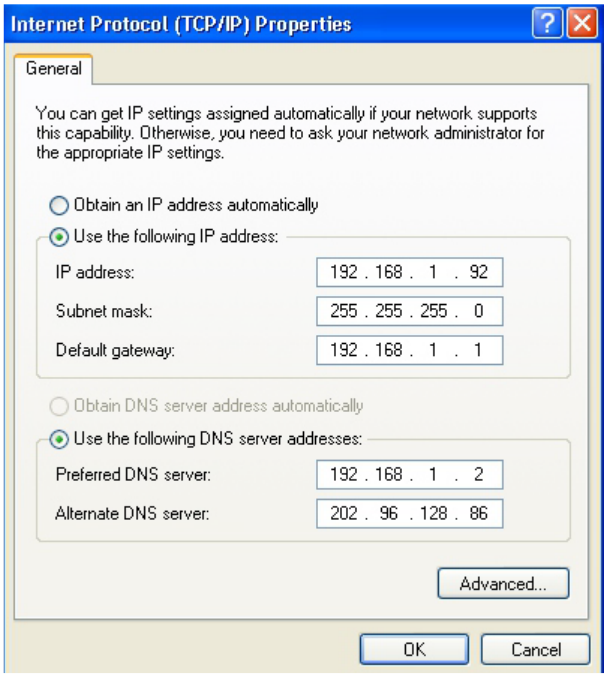


Click <property> button, enter "Local Area Connection Property" window.



Select "Internet protocol (TCP/IP), click <property> button, enter “Internet Protocol (TCP/IP) Properties” window. Select the option “Use the following IP address”, input IP address (use arbitrary value between 192.168.1.1~ 192.168.1.254, besides 192.168.1.200) and the subnet mask (255.255.255.0).

Click "OK" to finish the configuration.



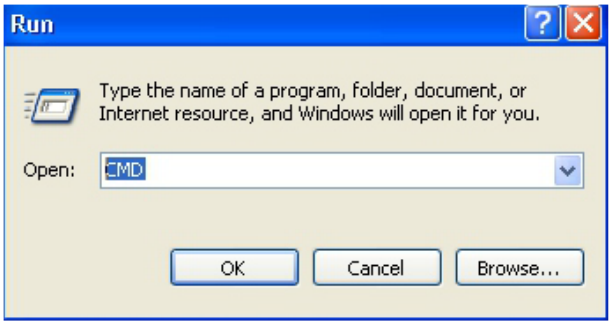
Note:

DNS server address can be empty or be filled in with the real server address.

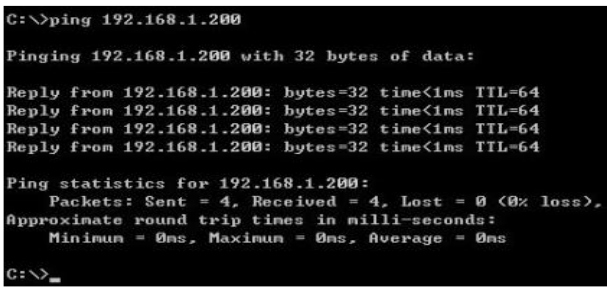
3.2 Confirm the Network Connection by Ping Command

Operation Steps as below:

Click <Start> button to enter <Start> menu, select <Run>, popping out the dialog.



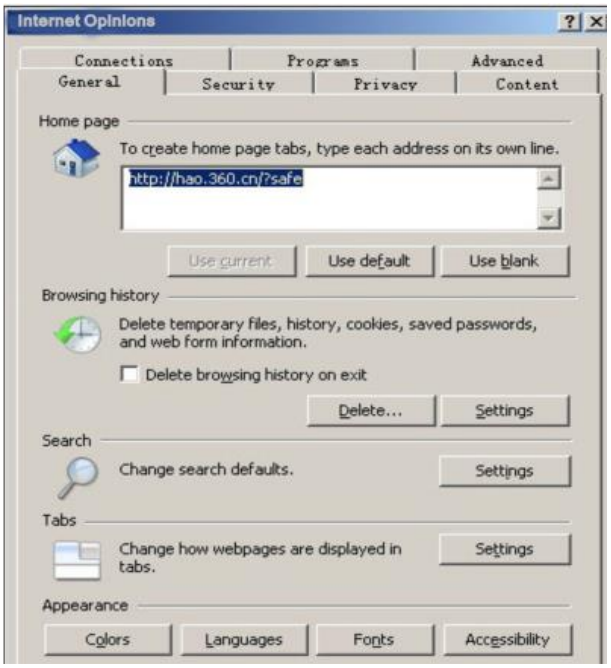
Input "ping 192.168.1.200", and press enter. If there is equipment response displaying in the pop out dialog, that means network connection succeed, otherwise please check if the network connection is correct.



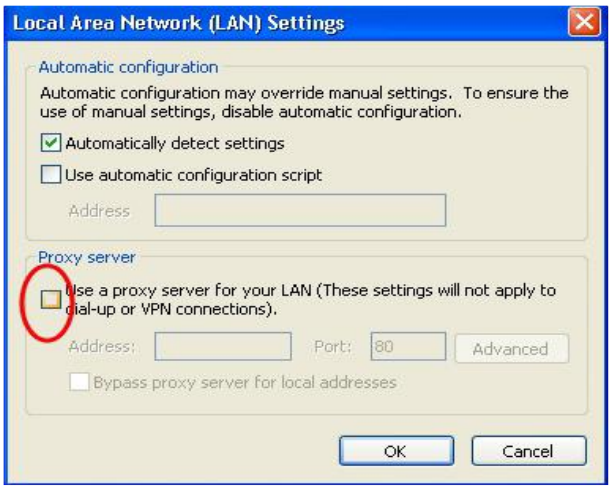
3.3 Cancel the Proxy Server

If this management PC uses proxy server to visit the internet, then the proxy service must be prohibited as follows:

In browser, select <Tool/Internet Option> to enter <Internet Options> window.



Select “Connections” tab in <Internet Options> window, and click <LAN Setting> button.



Check if the “Use a proxy server for your LAN” option is selected. If selected, please deselect the option. Then click <OK> button.

Note:

Please follow the steps to check if the switch is installed correctly:

Whether the physical connection of the equipment is correct?

Use network cable to connect the product’s Ethernet port (except the console port) with managed computer network card, and ensure the link LED of the port is on.

Whether the computer TCP/IP agreement setting is correct?

Management PC's IP address must be 192.168.1.x (x range is 1~254 and x can’t be 200, otherwise it will conflict with the product IP address 192.168.1.200), subnet mask: 255.255.255.0.

Whether the computer's port VLAN ID is 1?

By default, the management VLAN is VLAN 1, same as each port of switch.

Now the setting up tasks are finished.

Users can login the Web system and start configuration as following.

4 Login the Web system

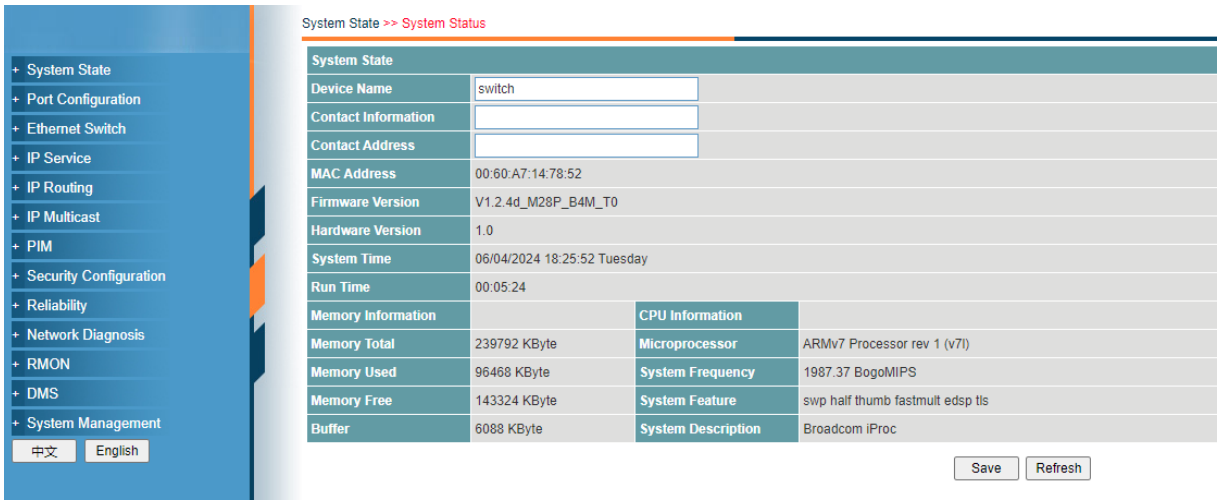
4.1 Login and Start

Open the browser, input the switch default address.

Press Enter, the user login page will show in front of you as follows.

Items	Default value
Switch default address	192.168.1.200
Subnet mask	255.255.255.0
Administrator's account	admin
Administrator's password	admin

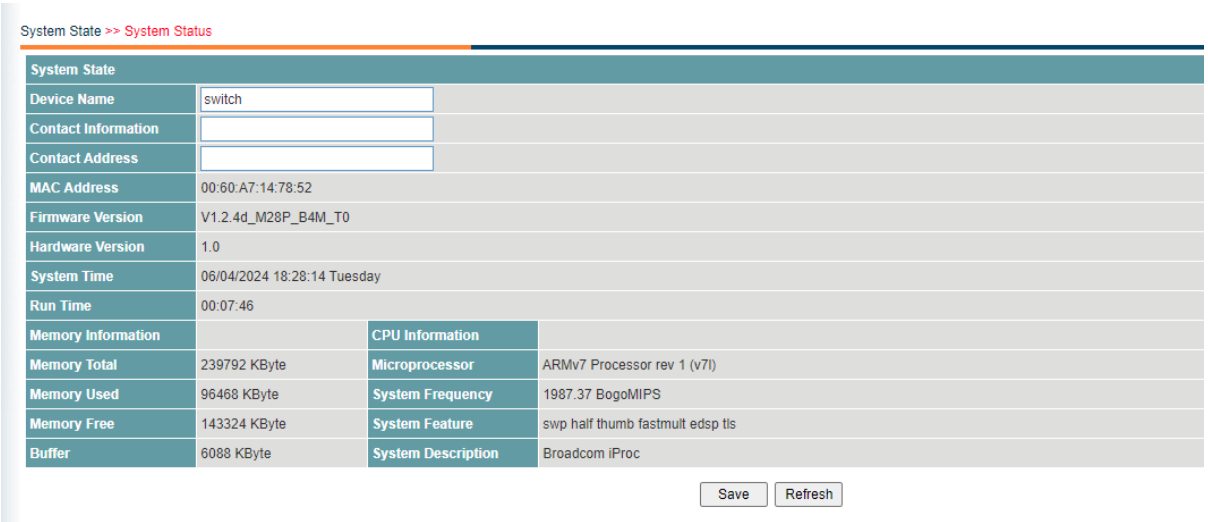
Input Administrator's account and password, press Enter, and click <Login in>, the Web system page will be shown as below:



4.2 Web System User Interface

Interface Layout

The layout and style of the Web system client GUI are described as follows.



Items	Descriptions
1	Navigation tree
2	Your Position
3	Configuration area

Operation Field and Buttons

The elements that users usually use on the Web system GUI are described as follows.

Items	Descriptions
	Input box. Please input the value as required.
Automatical ▼	Drop down list box. Please choose the value as required.
Enable Disable	Enable/ disable option. Please choose as required.
Modify	Modify button. Click to change the configured parameter.
Add	Add button. Click to add the parameter into the system.
Delete	Delete button. Click to delete the parameter from the system.
Edit	Edit button. The same as <Modify>, click to change the configured parameter.
Save	Save button. Click to the save the configurations.
Refresh	Refresh button. Click to reload the page.

4.3 Saving Configuration

After performing configuration, users need to save the configuration data. If you do not save the configuration data, the configuration that you made will be lost after reboot.

To save configurations, please click the <Save> button at the bottom of the page to save the configuration data to memory.

4.4 Viewing Configuration

Finished configuration, click <Refresh> button on the page, users can view the saved configuration.

4.5 User Timeout

If users do not perform any operations on the Web system GUI for a long time, your account will be logged out and the login page is displayed.

The auto-log out interval time is 5 minutes by default.

If you need to continue operations, please log in again.

4.6 Logging-out Web System

To protect security of user accounts and switches, please log out of the Web system immediately

after finishing the configurations.

Users can log out of the Web system in either of the following ways:

Click on the top right corner of the page to close the browser.

Click Exit on the top right corner of the page of Web system.

5 System State

5.1 System Status

Users can query the main information of the device, including device name, MAC address, firmware version, hardware version, system time, update time, memory information and CPU information.

System State			
Device Name	switch		
MAC Address	C4:08:80:01:5C:23		
Firmware Version	V1.1.3d_M28P_B4M_T12		
Hardware Version	1.0		
System Time	04/15/2020 17:55:00 Wednsday		
Update Time	07:54:23		
Memory Information		CPU Information	
Memory Total	239820 KByte	Microprocessor	ARMv7 Processor rev 1 (v7l)
Memory Used	95404 KByte	System Frequency	1987.37 BogoMIPS
Memory Free	144416 KByte	System Feature	swp half thumb fastmult edsp tls
Buffer	5572 KByte	System Description	Broadcom iProc

5.2 Traffic Statistics

Users can view traffic statistics on interfaces and update the statistics.

Port No	Sent Frame Statistics				Received Frame Statistics			
	Unicast	Muticast	Broadcast	Error	Unicast	Muticast	Broadcast	Error
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0

Procedure

Click <Refresh> button to reload the page.

5.3 MAC Address Table

Users can view the MAC table of the interfaces.

MAC Address Table

Sort Type: Automatical ▾ Refresh

No	MAC Address	VLAN ID	Port	Address Type
1	00:0B:82:C4:C3:22	1	11	dynamic
2	50:46:5D:A9:2D:29	1	11	dynamic
3	18:31:BF:0B:C4:12	1	11	dynamic
4	98:45:62:1A:F7:11	1	11	dynamic
5	50:46:5D:A9:2D:32	1	11	dynamic
6	00:22:A2:00:03:01	1	11	dynamic
7	54:AB:3A:2F:09:6E	1	11	dynamic
8	98:45:62:1A:F7:1F	1	11	dynamic
9	88:D7:F6:E0:A2:DB	1	11	dynamic
10	40:8D:5C:3F:4D:BA	1	11	dynamic
11	8C:89:A5:FD:DF:30	1	11	dynamic
12	FC:AA:14:8C:F9:BA	1	11	dynamic
13	00:00:00:00:04:29	1	11	dynamic
14	00:22:A2:00:0E:01	1	11	dynamic
15	00:E0:66:70:B7:0B	1	11	dynamic
16	00:0B:82:C0:07:A7	1	11	dynamic

Procedure

1) Click the drop down list to select the sort type, including

- Automatic
- By MAC Address
- By VLAN
- By port

2) Click <Refresh> button to reload the page.

5.4 SFP information

Enables users to access detailed data regarding Small Form-Factor Pluggable (SFP) modules installed in switch ports. This feature provides essential insights into the status, type, compatibility, and performance metrics of the SFP modules.

Users can view the SFP table as bellow.

Common Information

SFP Port	Transceiver Type	Connector Type	Wavelength (nm)	Transfer Distance(m)	DDM Support
G1					
G2					
G3					
G4					

Manufacture Information

SFP Port	Vendor Name	Vendor Part Number	Vendor Serial Number	Manufacturing Date	Vendor Rev
G1					
G2					
G3					
G4					

Diagnostic Information

SFP Port	Temperature(℃)	Voltage(V)	Bias (ma)	TX Power(dbm)	RX Power(dbm)
G1					
G2					
G3					
G4					

Procedure

In this page, including

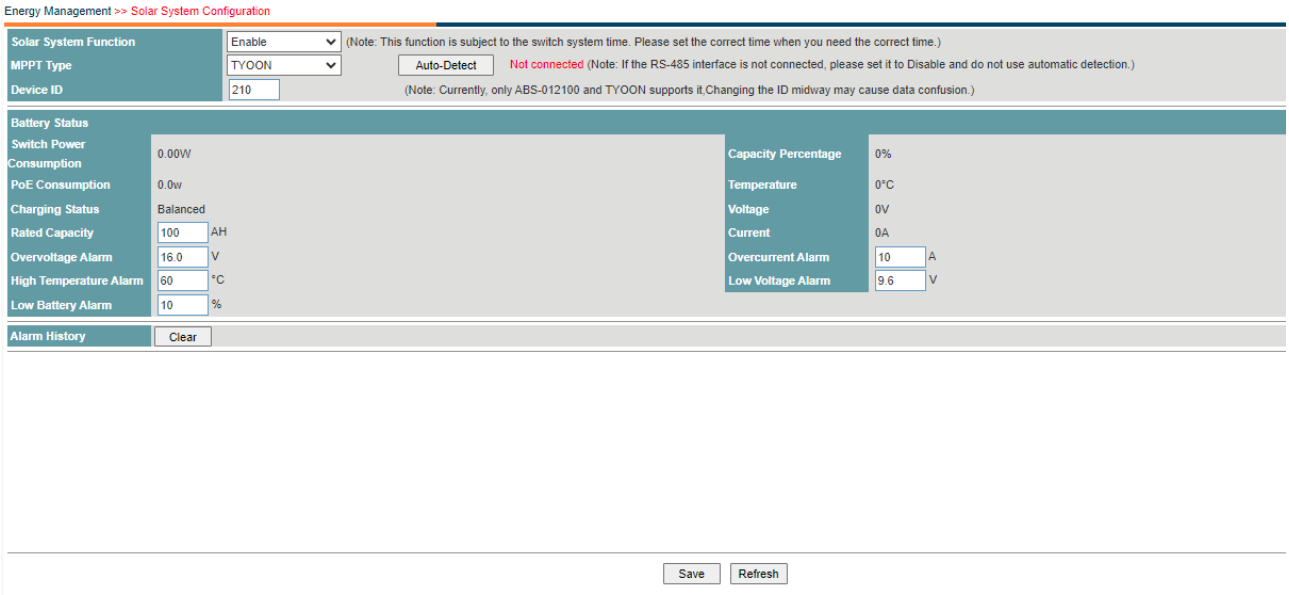
- Common Information
- Manufacture Information
- Diagnostic Information

This page does not support configuration.

6 Energy Management

6.1 Solar System Configuration

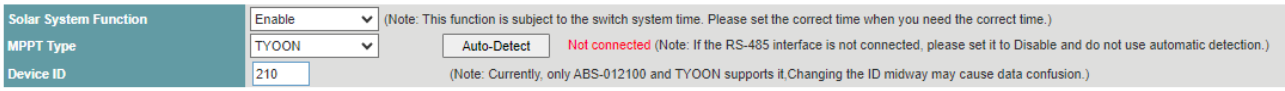
Users can query the main information of the solar system configuration and status via accessing MPPT connected to battery.



Procedure

Choose <Energy Management> <Solar System Configuration> in the navigation tree to open the page.

1) Configure solar system.



- Set the parameters as required.

Items	Descriptions	Default value
Solar System Function	Choose <Enable> to enable the function.	Enable
MPPT Type	Specify the MPPT type as the following: · Disable · UPS100AH-01 · SRNE · EPEVER · ABS-012100 · TYOON	TYOON
Auto-Detect Button	When it is clicked, the MPPT type would be detected automatically via the adjacent line MPPT vendors	
Device ID	Specify the ID for the MPPT type. It is available only when MPPT type is ABS-012100 or TYOON	210

- Click <Save>.

2) Configure battery configuration.

· Set the parameters as required.

Items	Descriptions	Default value
Rated Capacity	Specify rated capacity value for the battery. The units is AH	100
Overvoltage Alarm	Specify overvoltage alarm threshold value for the battery. The units is V	16
Overcurrent Alarm	Specify overcurrent alarm threshold value for the battery. The units is A	10
High Temperature Alarm	Specify high temperature alarm threshold value for the battery. The units is ℃	60
Lowvoltage Alarm	Specify lowvoltage alarm threshold value for the battery. The units is V	9.6
Low Battery Alarm	Specify low battery alarm threshold value for the battery. The units is percentage	10
Alarm History	Click the clear and the history alarm would be cleared.	

· Click <Save>.

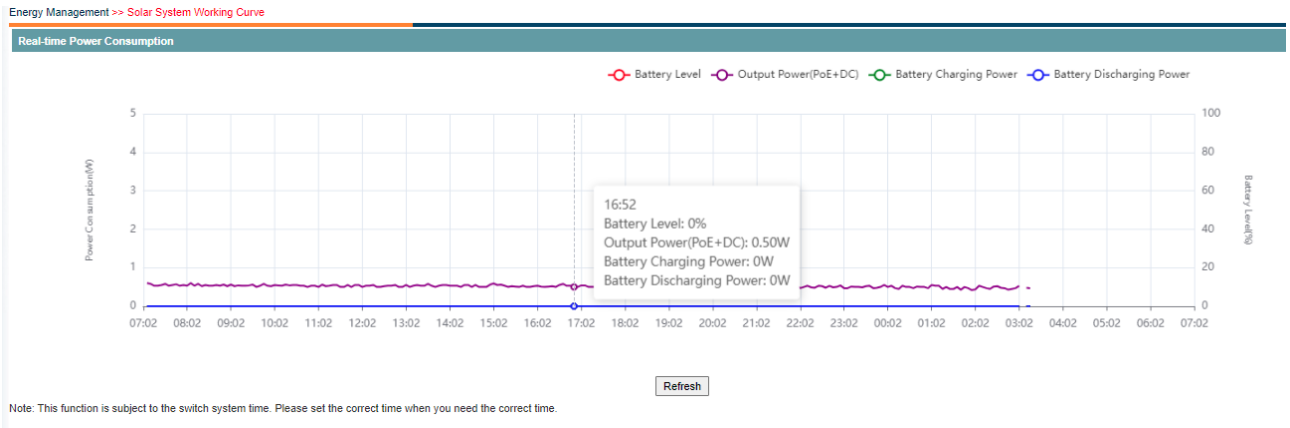
3) View the basic attributes.

· Click the <Refresh> button to reload the page.

· View the information.

6.2 Solar System Working Curve

Users can view the solar system working curve.



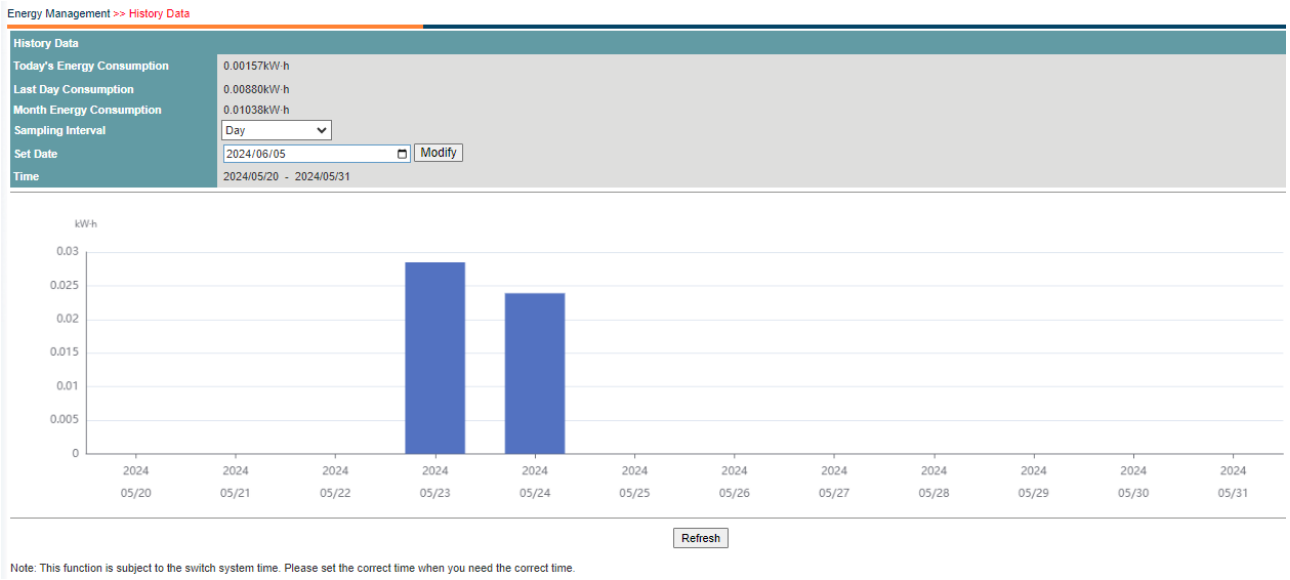
Procedure

Choose <Energy Management> <Solar System Working Curve> in the navigation tree to open the page.

1) Click <Refresh> button to reload the page.

6.3 History Data

User can get the power consuming information for 12 days or 12 months history data



Procedure

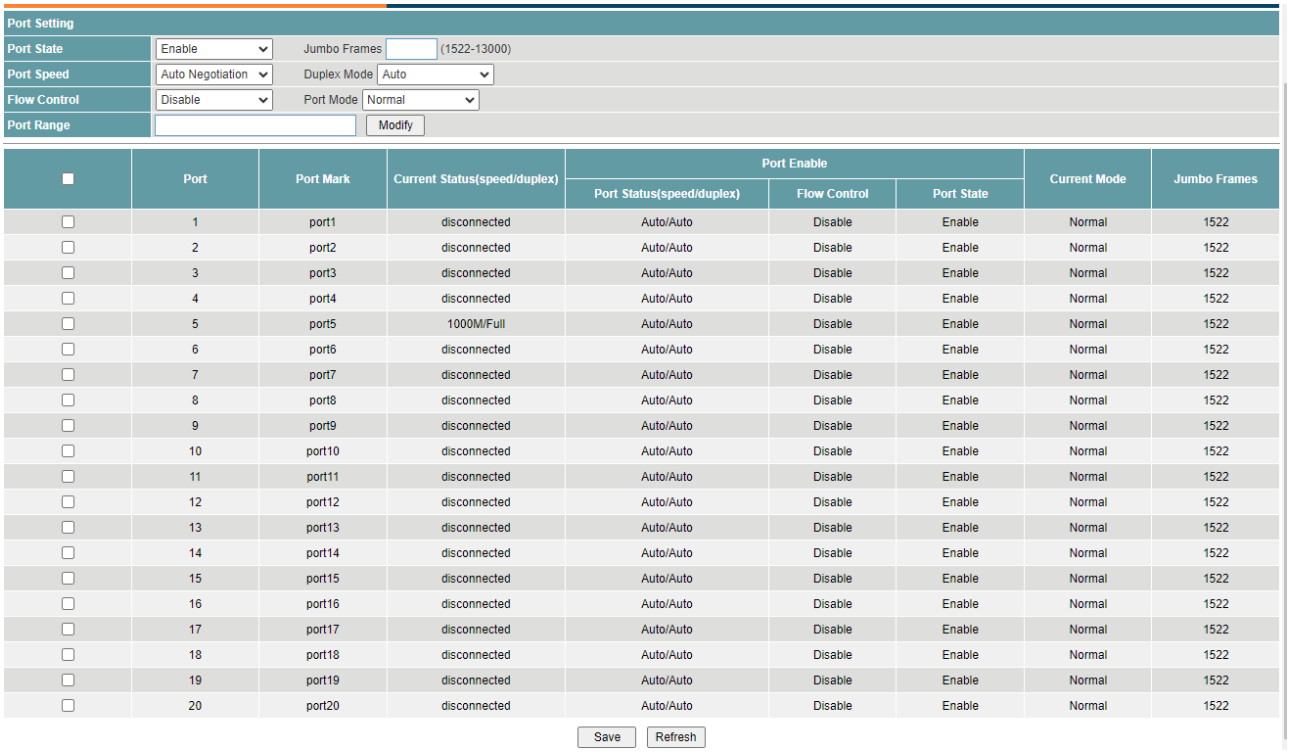
Choose <Energy Management> <History Data> in the navigation tree to open the page.

1) Click <Refresh> button to reload the page.

7 Port Configuration

7.1 Port Setting

Users can view the basic attributes of Ethernet interfaces, and configure the Ethernet interfaces as required.

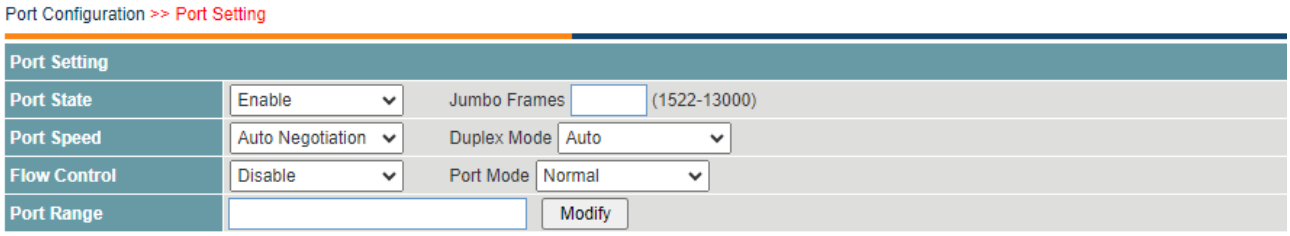


Port	Port Mark	Current Status(speed/duplex)	Port Status(speed/duplex)	Flow Control	Port State	Current Mode	Jumbo Frames
1	port1	disconnected	Auto/Auto	Disable	Enable	Normal	1522
2	port2	disconnected	Auto/Auto	Disable	Enable	Normal	1522
3	port3	disconnected	Auto/Auto	Disable	Enable	Normal	1522
4	port4	disconnected	Auto/Auto	Disable	Enable	Normal	1522
5	port5	1000M/Full	Auto/Auto	Disable	Enable	Normal	1522
6	port6	disconnected	Auto/Auto	Disable	Enable	Normal	1522
7	port7	disconnected	Auto/Auto	Disable	Enable	Normal	1522
8	port8	disconnected	Auto/Auto	Disable	Enable	Normal	1522
9	port9	disconnected	Auto/Auto	Disable	Enable	Normal	1522
10	port10	disconnected	Auto/Auto	Disable	Enable	Normal	1522
11	port11	disconnected	Auto/Auto	Disable	Enable	Normal	1522
12	port12	disconnected	Auto/Auto	Disable	Enable	Normal	1522
13	port13	disconnected	Auto/Auto	Disable	Enable	Normal	1522
14	port14	disconnected	Auto/Auto	Disable	Enable	Normal	1522
15	port15	disconnected	Auto/Auto	Disable	Enable	Normal	1522
16	port16	disconnected	Auto/Auto	Disable	Enable	Normal	1522
17	port17	disconnected	Auto/Auto	Disable	Enable	Normal	1522
18	port18	disconnected	Auto/Auto	Disable	Enable	Normal	1522
19	port19	disconnected	Auto/Auto	Disable	Enable	Normal	1522
20	port20	disconnected	Auto/Auto	Disable	Enable	Normal	1522

Procedure

Choose <Port Configuration> <Port Setting> in the navigation tree to open the page.

4) Configure the interfaces.



- Set the parameters as required.

Items	Descriptions	Default value
Port State	Choose <Enable> to enable the function.	Enable
Jumbo Frames	Specify the length for Jumbo Frames. It is from 1522B to 13000	Null
Port Speed	Indicates the interface speed, including · Auto Negotiation · 10 Mbits/s · 100 Mbits/s · 1000 Mbits/s · 10 Gbits/s	Auto Negotiation

	By default the SFP port is 10Gbits/s, it supports to be set to 1000Mbits/s.	
Duplex Mode	Indicates the duplex mode of the interface, including · Auto · Full duplex · Half duplex To enable an interface to send and receive packets at the same time, enable the full duplex mode on the interface. To disable an interface from sending and receiving packets at the same time, enable the half duplex mode on the interface.	Auto
Flow Control	Enable or disable the traffic flow control function.	Disable
Port Mode	Specify the port mode of the interface, including · Normal · Loopback	Normal
Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. The value ranges from 1~28. Format as “2” or “1-5” or “3, 1-5”.	Null

· Click <Modify> to change the configuration.

· Click <Save>.

5) View the basic attributes.

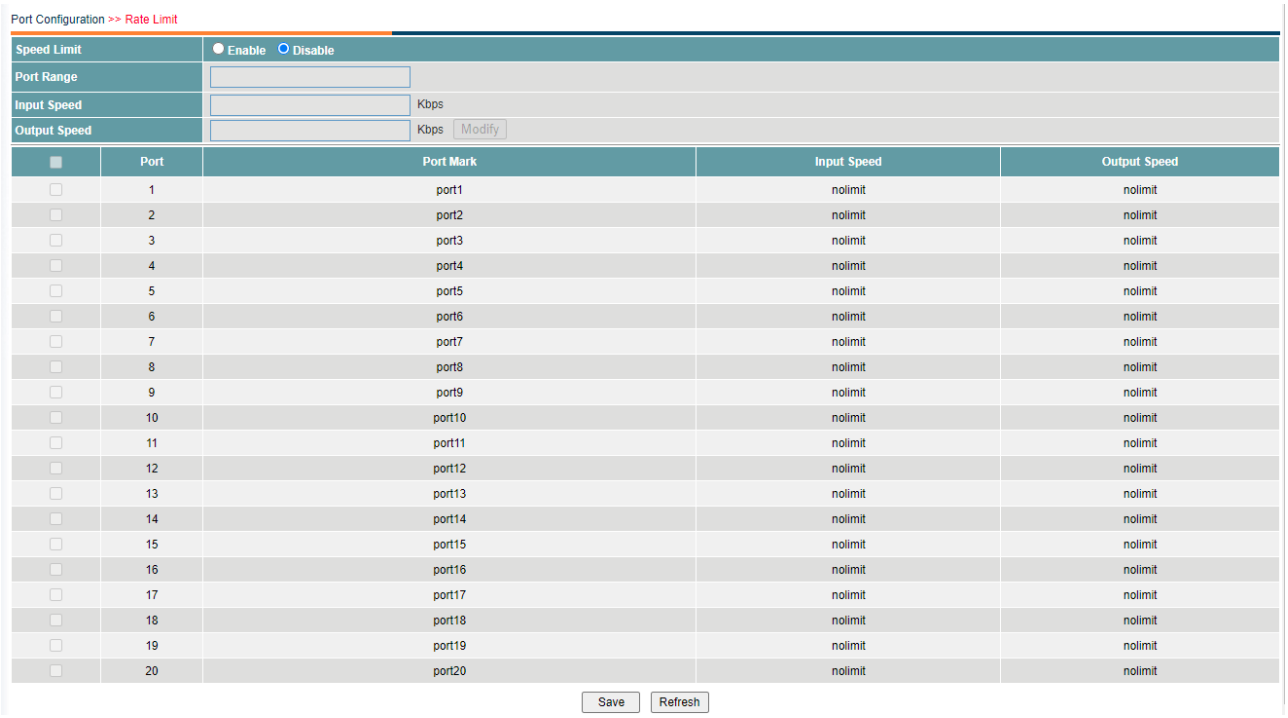
· Click the <Refresh> button to reload the page.

· View the information.

7.2 Rate Limit

This function is used to limit the rate of outgoing traffic or incoming traffic on a physical interface.

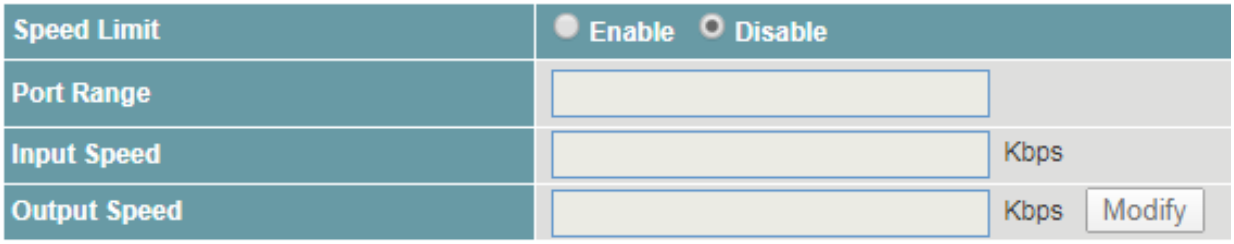
Users can view detailed information about interface-based rate limiting. Before sending traffic from an interface, users can configure rate limit on the interface in the outbound direction to control all outgoing packets, and configure rate limit on the interface inbound direction to control all incoming packets.



Procedure

Choose <Port Configuration> <Rate Limit> in the navigation tree to open the page.

1) Configure the interfaces.



· Set the parameters as required.

Items	Descriptions	Default value
Speed Limit	Choose <Enable> to enable the function.	Disable
Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. The value ranges from 1~28. Format as “2” or “1-5” or “3, 1-5”.	Null
Input Speed	Input the speed limit in the inbound direction. The value ranges 64 Kbps ~1000000 Kbps.	Null
Output Speed	Input the speed limit in the outbound direction. The value ranges 64 Kbps ~1000000 Kbps.	Null

· Click <Modify> to change the configuration.

· Click <Save>.

2) View the input and output speed.

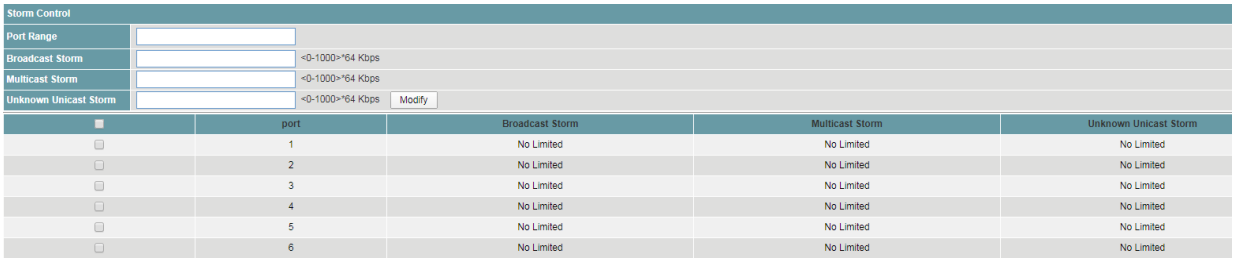
· Click the <Refresh> button to reload the page.

· View the information.

7.3 Storm Control

Storm control prevents broadcast storms and ensures device forwarding performance.

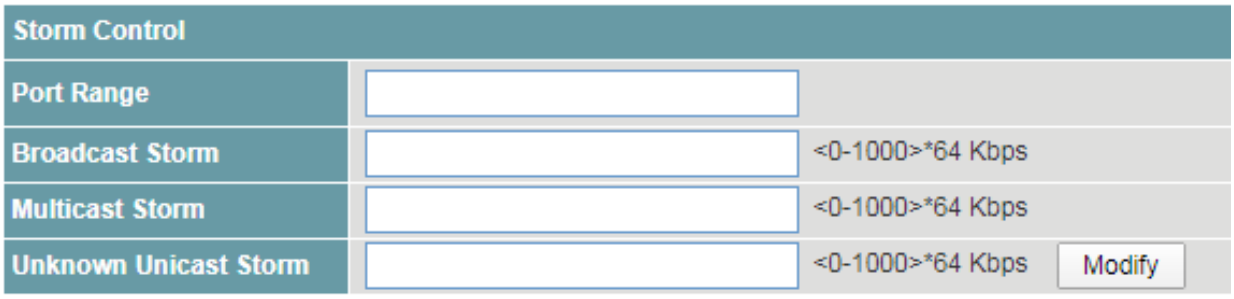
To limit the rate of incoming broadcast packets, multicast packets, and unknown unicast packets and prevent heavy traffic on a device, users can configure storm control on an interface.



Procedure

Choose <Port Configuration> <Storm Control> in the navigation tree to open the page.

1) Configure the interfaces.



- Set the parameters as required.

Items	Descriptions	Default value
Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. The value ranges from 1~28. Format as “2” or “1-5” or “3, 1-5”.	Null
Broadcast Storm	Configure the broadcast storm control. The value ranges from 1~1000.	Null
Multicast Storm	Configure the multicast storm control. The value ranges from 1~1000.	Null
Unicast Storm	Configure the unicast storm control. The value ranges from 1~1000.	Null

- Click <Modify> to change the configuration.
- Click <Save>.

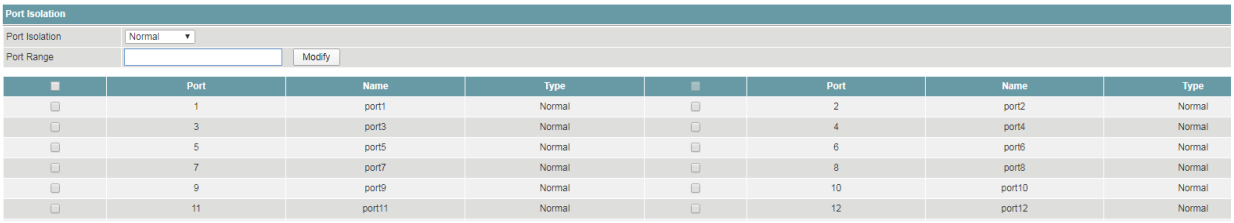
2) View the storm control state of the interfaces.

- Click the <Refresh> button to reload the page.
- View the information.

7.4 Port Isolation

Interfaces in a port isolation group are isolated from each other, but interfaces in different port isolation groups can communicate.

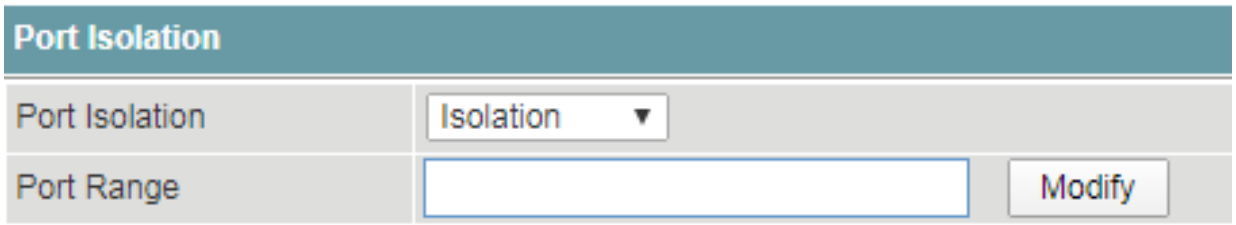
The switch supports one isolation group. Users can add or delete the ports from the group as required, and view the isolation mode of the ports.



Procedure

Choose <Port Configuration> <Port Isolation> in the navigation tree to open the page.

1) Configure the isolation modes of the ports.



· Select the ports that need to be set in <Port Range>.

Items	Descriptions	Default value
Port isolation	Choose <Isolation> to enable the function. Choose <Normal> to disable the function.	Isolation
Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. The value ranges from 1~28. Format as “2” or “1-5” or “3, 1-5”.	Null

The ports can communicate at both Layer 2 and Layer 3 by default, after the isolation mode is selected, all is the isolation at both Layer 2 and Layer 3.

· Click <Modify> to change the configuration.

· Click <Save>.

2) View the isolation modes of the ports.

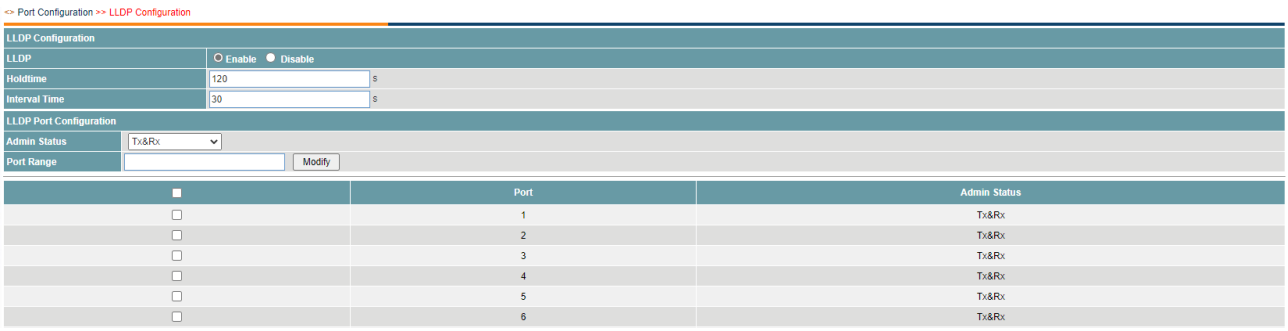
· Click the <Refresh> button to reload the page.

· View the information.

7.5 LLDP Configuration

The switch supports the Link Layer Discovery Protocol (LLDP) that conforms to IEEE 802.1ab. LLDP is a link layer protocol used for interconnected devices to obtain the connection information of each other.

Based on Layer 2 information obtained using LLDP, the web management system can quickly detect configuration conflicts between devices and locate network faults. Users can use the web management system to monitor link status of LLDP-enabled devices and quickly locate faults on the network.



Procedure

Choose <Port Configuration><LLDP Configuration> in the navigation tree to open the page.

1）LLDP configuration.

· Global LLDP configuration.

Items	Descriptions	Default value
LLDP	Choose <Enable> to enable the function.	Enable
Holdtime	Hold time multiplier of device information on neighbors The hold time multiplier is used to calculate the Time to Live, which determines how long information about a device can be saved on the neighbors. After receiving an LLDP packet, a neighbor updates the aging time of the device information from the sender based on the hold time.	120s
Interval Time	Interval between sending LLDP packets When the LLDP status of the device keeps unchanged or the device does not discover new neighbors, the device sends LLDP packets to the neighbors at a certain interval.	30s

· Port LDP configuration.

Items	Descriptions	Default value
Admin Status	Choose <Enable> to enable the function.	Enable
Holdtime	There are 4 options for the port sending and receiving LLDP packet modes: · Tx only: transport only · Rx only: receive only · Tx & Rx: Both transport and receive · Disabled: Neither send nor receive	Tx & Rx
Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. Format as “2” or “1-5” or “3, 1-5”.	Null

· Click <Modify> to change the configuration.

· Click <Save>.

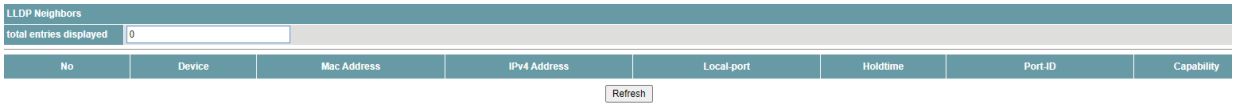
2）View the isolation modes of the ports.

· Click the <Refresh> button to reload the page.

· View the information.

7.6 LLDP Neighbors

Displays the discovered neighbor devices.



Procedure

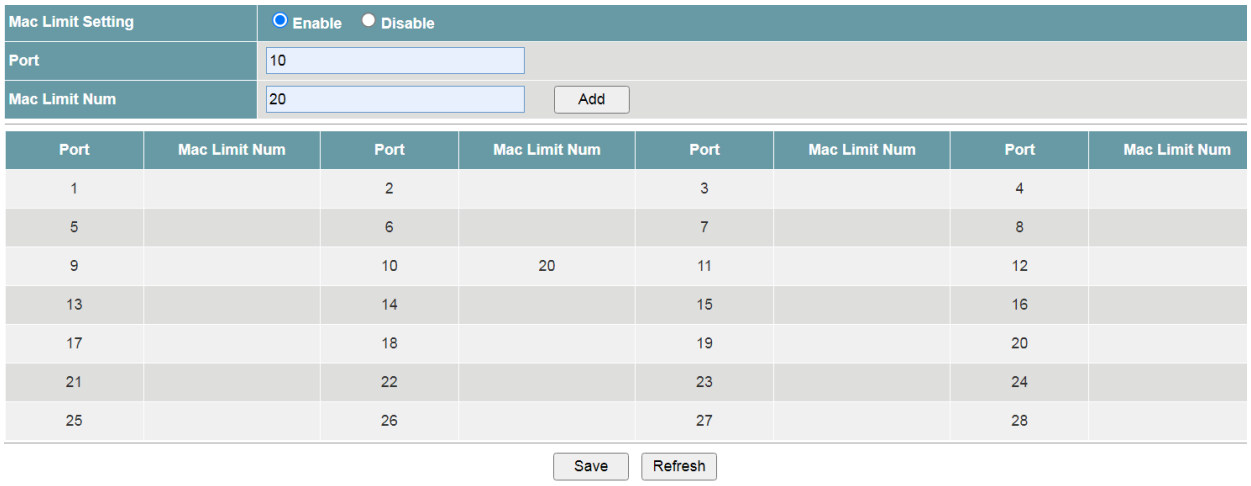
Choose <Port Configuration><LLDP Neighbors> in the navigation tree to open the page.

This page does not support configuration.

7.7 MAC Limit

Setting restrictions on the number of MAC addresses that can be learned or allowed on a specific s witch port. This feature helps in controlling network access, preventing MAC flooding attacks, and o ptimizing network performance.

Users can configure the Mac Limit Setting as bellow.



Procedure

Choose <Port Configuration>< MAC Limit > in the navigation tree to open the page.

1) Enable Mac Limit Setting firstly.

2) Input port ID and Mac Limit Num.

· Set the parameters as required.

Items	Descriptions	Default value
Mac Limit Setting	Set the Mac Limit Setting enabled/disabled	3Enable
Port	put the ports numbers that need to be set. Multiple interfaces can be selected. The value ranges from 1~28. Format as “2” or “1-5” or “3, 1-5”.	5Null
Mac Limit Num	Input the limited Mac Number value. The number is from 0 to 9000	Null

· Click <Edit> to change the configuration.

· Click <Save>.

3) View the Mac Limit Num of the ports.

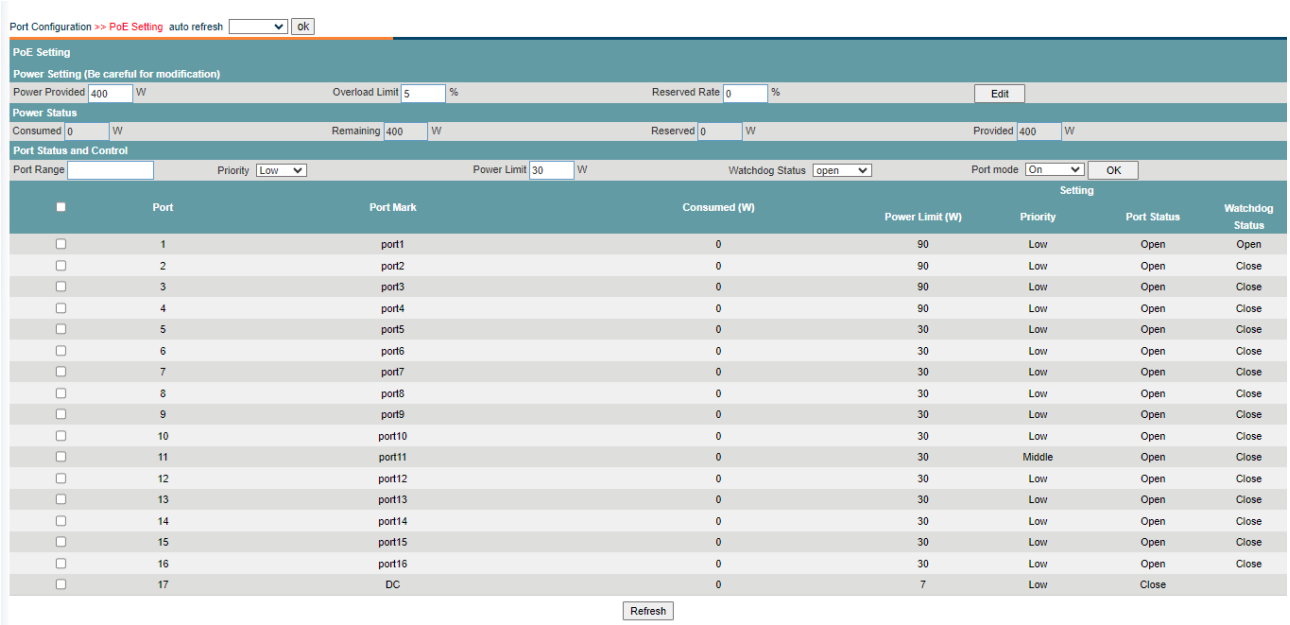
· Click the <Refresh> button to reload the page.

· View the information.

7.8 PoE Setting

Currently, the network devices are deployed flexibly; therefore, the cabling of power supply is complicated. To simplify cabling, users can configure the PoE function on the switch.

Users can set global PoE parameters and the PoE parameters on an interface, and view the PoE status of the device and ports.

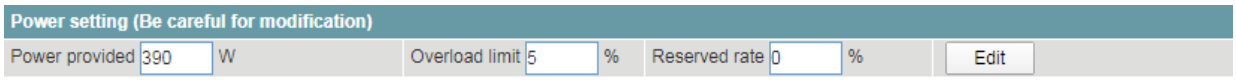


Port	Port Mark	Consumed (W)	Setting			
			Power Limit (W)	Priority	Port Status	Watchdog Status
1	port1	0	90	Low	Open	Open
2	port2	0	90	Low	Open	Close
3	port3	0	90	Low	Open	Close
4	port4	0	90	Low	Open	Close
5	port5	0	30	Low	Open	Close
6	port6	0	30	Low	Open	Close
7	port7	0	30	Low	Open	Close
8	port8	0	30	Low	Open	Close
9	port9	0	30	Low	Open	Close
10	port10	0	30	Low	Open	Close
11	port11	0	30	Middle	Open	Close
12	port12	0	30	Low	Open	Close
13	port13	0	30	Low	Open	Close
14	port14	0	30	Low	Open	Close
15	port15	0	30	Low	Open	Close
16	port16	0	30	Low	Open	Close
17	DC	0	7	Low	Close	

Procedure

Choose <Port Configuration> <PoE Setting> in the navigation tree to open the page.

1) Set global PoE parameters.



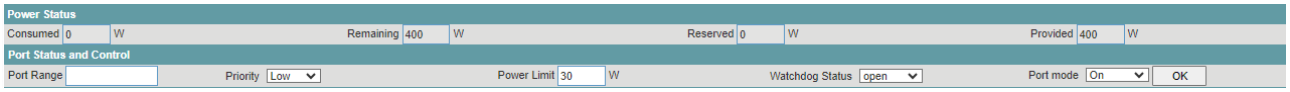
· Set the parameters as required.

Items	Descriptions	Default value
Power Provided	Input the maximum provided power of the device. The value is less than 400W.	390W
Overload Limit	The limit percentage that allows over the preset <Power Provided> value. The value is less than 10%. This parameter is optional.	5%
Reserved Rate	Input the reserved rate from the preset <Power Provided> value. The value ranges from 0 to 100%. The device supports reserved power function for reliability. The actual value of input power the device divides to the interfaces (named as V) is equal to the value of <Power Provided> minus the value of <Power Provided> multiplies <Reserved Rate>. If the required input power of the devices over the value of	0%

	real input power, the reserved power will be divided to each port as further demand. This parameter is optional.	

- Click <Edit> to change the configuration.
- Click <Save>.

2) Set the PoE parameters on an interface



- The current power status will be displayed in the items of <Power status> as below.

Items	Descriptions
Power Status	
Consumed	The total actual output power of all the interfaces.
Remaining	The actual remained input power of the device, not including the reserved power.
Reserved	The actual reserved power of the device. The value is equal to the value of <Power Provided> minus <Remaining>minus<Consumed>.
Provided	The preset input power. The value is equal to <Power Provided>.

- Set the parameters as required.

Items	Descriptions	Default value
Port Status and Control		
Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. The value ranges from 1~28. Format as “2” or “1-5” or “3, 1-5”.	Null
Priority	Indicates the power priority of an interface, including · Low · Middle · High In the same priority, the interfaces with larger port number will be shut off first when the power is not enough.	Low
Power Limit	Input the maximum output power of the interfaces. The value ranges from 0 to 90W.	Null
Watchdog Status	Set the watchdog status of an interface, including · Open · Close	Open
Port mode	Set the watchdog status of an interface, including · Off · On · 24V · 54V	On
ON	Click to enable the PoE function of the interfaces.	Enable

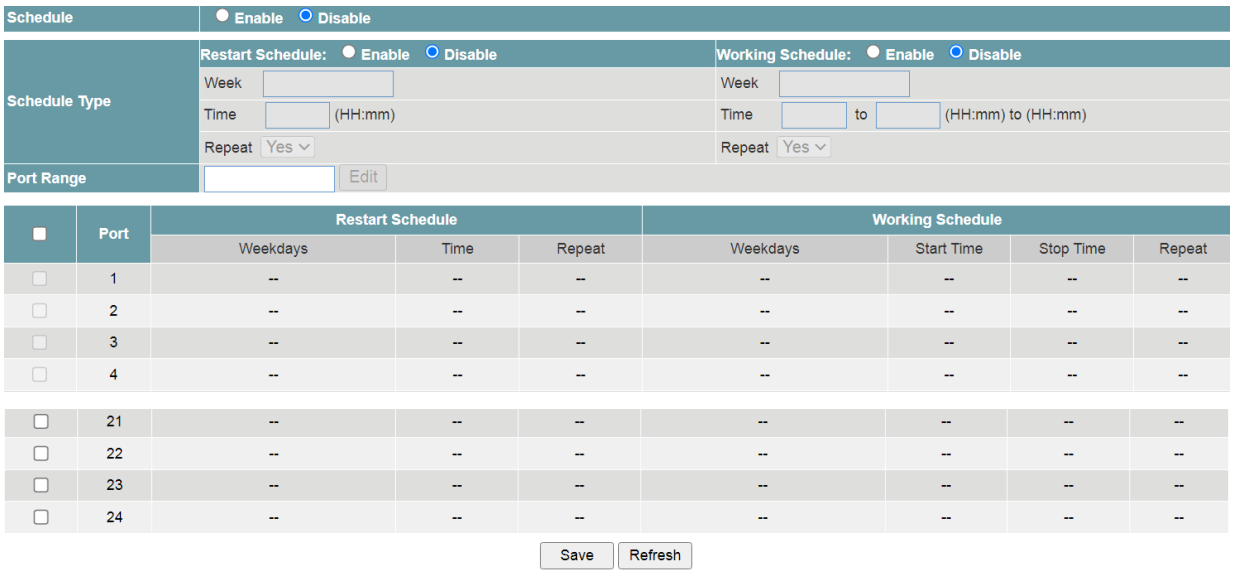
OFF	Click to disable the PoE function of the interfaces.	

- Click <Edit> to change the configuration.
- Click <Save>.

7.9 PoE Schedule

PoE schedule functionality allows administrators to control and schedule the power delivery to PoE-enabled devices connected to switch ports. This feature provides flexibility and efficiency in managi ng power allocation, especially for devices with specific power requirements or operating schedules .

- Users can view the PoE Schedule Setting as bellow.



Procedure

Choose <Port Configuration>< PoE Schedule > in the navigation tree to open the page.

1) Enable PoE Schedule firstly.

- Set the parameters as required.

Items	Descriptions	Default value
Schedule	Input whether PoE Schedule Enable/Disable	3Disable

2) To set PoE Restart Schedule, need Enable firstly.

- Set the parameters as required.

Items	Descriptions	Default value
Restart Schedule	Input whether PoE Schedule Enable/Disable	Disable
Week	Input the day for the week. It is from Monday to Sunday	
Time	Input the time for the day. It is from 00:00 to 23:59	
Repeat	Input whether the schedule is repeated or not	Yes

3) To set PoE working Schedule, need Enable firstly

- Set the parameters as required.

Items	Descriptions	Default value

Working Schedule	Input whether PoE working Schedule Enable/Disable	Disable
Week	Input the day for the week. It is from Monday to Sunday	
Time	Input the time for the day. It is from 00:00 to 23:59	
Repeat	Input whether the schedule is repeated or not	Yes

4) To set Port range

· Set the parameters as required.

Items	Descriptions	Default value
Port Range	Input Port range. It can be 1 or 1, 2 or 1-N for continuous port. The range is from 1 to 24	3

5) Save configurations and reload.

· Click <Save>.

· Click the <Refresh> button to reload the page.

· View the information.

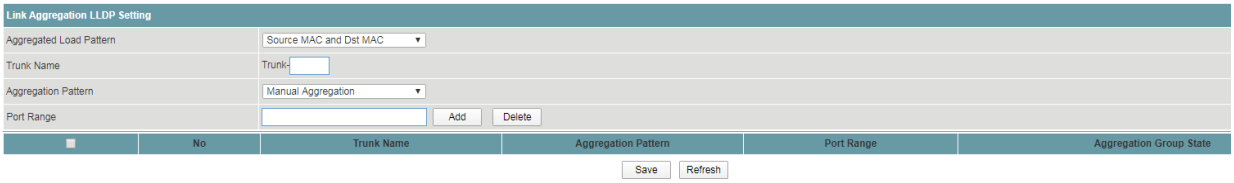
8 Ethernet Switch

8.1 Link Aggregation

Link aggregation is a technology that bundles multiple Ethernet links into a logical link to increase bandwidth, improve reliability, and load balance traffic.

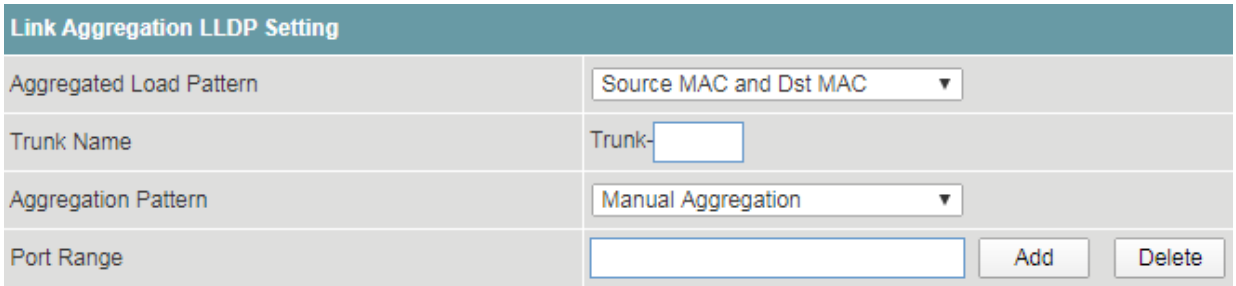
The Switch supports the manual load balancing mode and Link Aggregation Control Protocol (LACP) mode. The Switch also supports inter-device link aggregation.

Users can create link aggregation group, configure load pattern mode, working mode and members of link aggregation group, and delete the group.



Procedure

Choose <Ethernet Switch> <Link Aggregation> in the navigation tree to open the page.



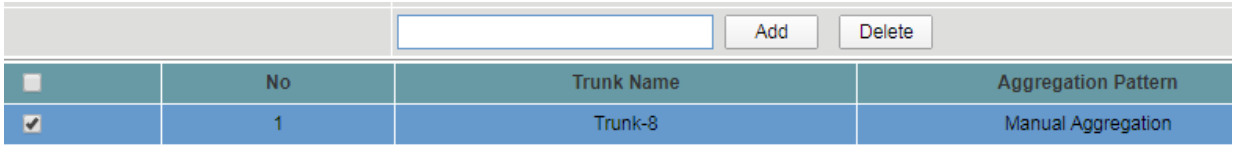
1) Create link aggregation group and configuration.

· Set the parameters as required.

Items	Descriptions	Default value
Aggregated Load Pattern	Choose the aggregation load pattern, including · Source MAC · Destination MAC · Source MAC and Dst MAC · Destination IP Address · Source IP and Dst IP Address	Source MAC and Dst MAC
Trunk Name	Indicates the trunk number. The value ranges from 1 to 8.	Null
Aggregation Pattern	Choose the aggregation pattern, including · Manual Aggregation: not under LACP protocol, by setting register to make aggregation. · Static LACP Aggregation: under LACP protocol, manually configured by the user, and the system is not allowed to automatically add or delete ports in the aggregation group.	Manual Aggregation
Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. The value ranges from 1~28. Format as “2” or “1-5” or “3, 1-5”.	Null

- Click <Add>.
- Click <Save>.

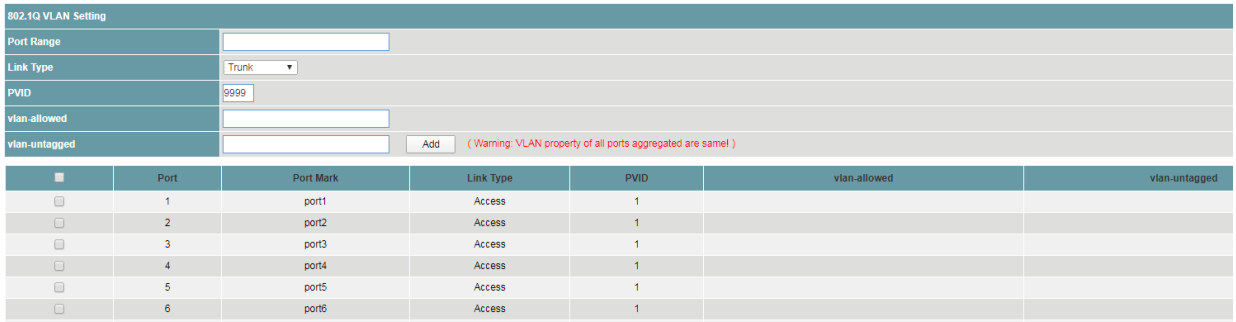
2) Delete trunk.



- Choose the trunk that need to be deleted.
- Click <Delete>.
- Click <Save>.

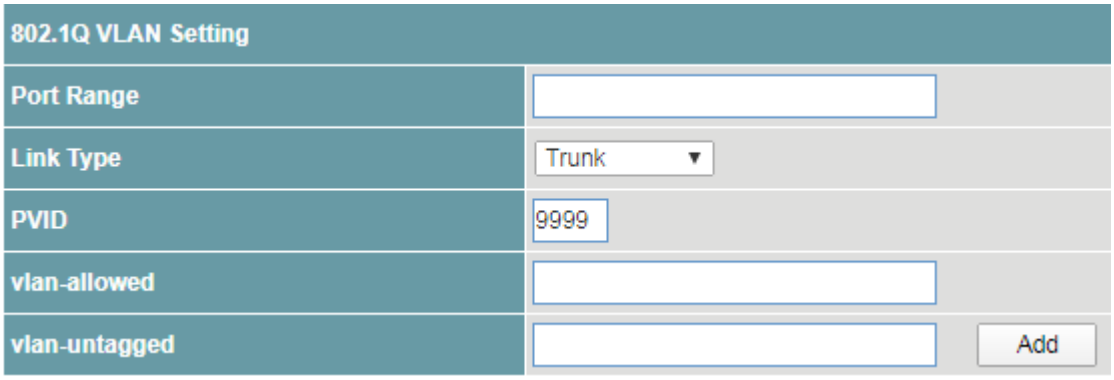
8.2 802.1Q VLAN

User can configure the link-type of the interfaces and view the configuration.



Procedure

Choose <Ethernet Switch> <802.1Q VLAN> in the navigation tree to open the page.



1) Configure the link-type of interfaces.

- Set the parameters as required.

Items	Descriptions	Default value
Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. The value ranges from 1~28. Format as “2” or “1-5” or “3, 1-5”.	Null
Link Type	Link type of the interfaces, including · Access · Trunk	Access

PVID	Input the VLAN ID of the interface. The value ranges from 1 to 4094.	Null
VLAN-allowed	Input ID of VLAN that allowed to access in Trunk. The value ranges from 1 to 4094.	Null
VLAN-untagged	Input ID of untagged VLAN in Trunk. The value ranges from 1 to 4094.	Null

- Click <Add>.
- Click <Save>.

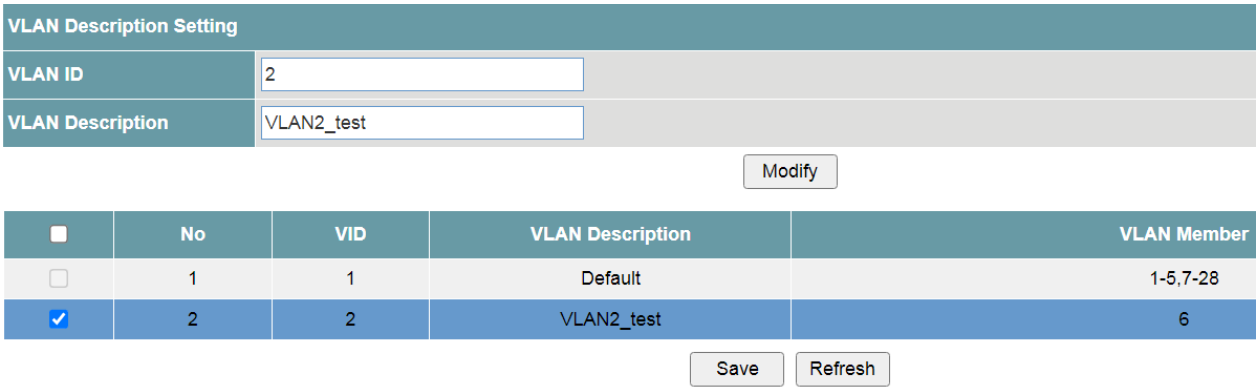
2) View the link-type of the interfaces.

- Click the <Refresh> button to reload the page.
- View the information.

8.3 VLAN Description

User can specify the meaning for each VLAN so that it is obviously shown via WEB.

Users can view and modify VLAN Description Setting as bellow.



Procedure

Choose < Ethernet Switch >< VLAN Description > in the navigation tree to open the page.

1) Configure the VLAN Description Setting.

- Set the parameters as required.

Items	Descriptions	Default value
VLAN ID	Input the VLAN Range from 1 to 4094	Null
VLAN Description	Input the string of VLAN Description and the length is up to 256 characters. The description of VID 1 is set as 'Default' and it cannot be edited/deleted.	Null

- Click <Modify>.
- Click <Save>.

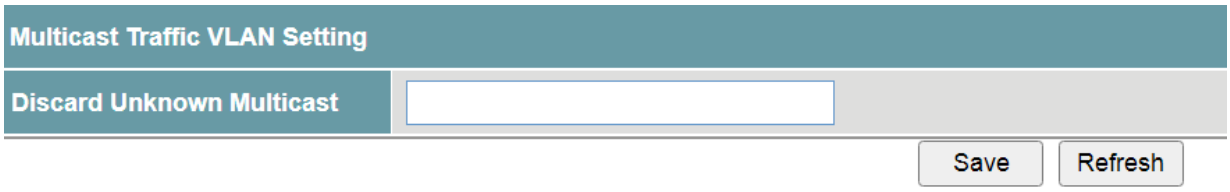
2) Save configurations and reload.

- Click the <Refresh> button to reload the page.
- View the information.

8.4 Multicast Traffic Control

User specify the VID lists to discard unknown multicast packets.

Users can view and modify Multicast Traffic Control Setting as bellow.



Procedure

Choose < Ethernet Switch >< Multicast Traffic Control > in the navigation tree to open the page.

1) Configure the Multicast Traffic VLAN Setting.

· Set the parameters as required.

Items	Descriptions	Default value
Discard Unknown Multicast	Input the VLAN Range from 1 to 4094	Null

· Click <Save>.

2) Save configurations and reload.

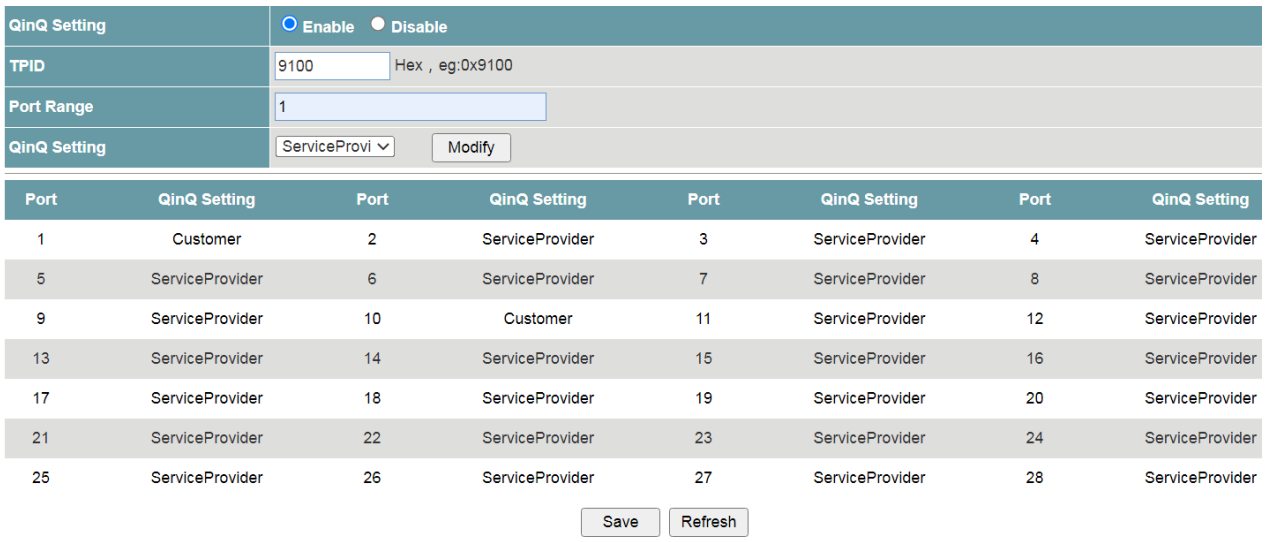
· Click the <Refresh> button to reload the page.

· View the information.

8.5 QinQ Setting

QinQ, also known as VLAN stacking or VLAN-in-VLAN, is a feature on switches that allows Multiple VLAN tags to be encapsulated within another VLAN tag. This facilitates the creation of hierarchical VLAN structures, enhancing network scalability and isolation.

Users can view and modify QinQ Setting as bellow.



Procedure

Choose < Ethernet Switch >< QinQ Setting > in the navigation tree to open the page.

1) Turn on this function need enable QinQ Setting firstly.

· Set the parameters as required.

Items	Descriptions	Default value
QinQ Setting	Set the feature Enable/Disable	Disable

3) Configure QinQ Setting.

· Set the parameters as required.

Items	Descriptions	Default value
TPID	Input the TPID Range from 0000 to FFFF (HEX)	Null
Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. Format as “2” or “1-5” or “3, 1-5” .	Null
QinQ Setting	Set the value as customer or Service Provide	Service Provide

· Click <Modify>.

· Click <Save>.

4) Save configurations and reload.

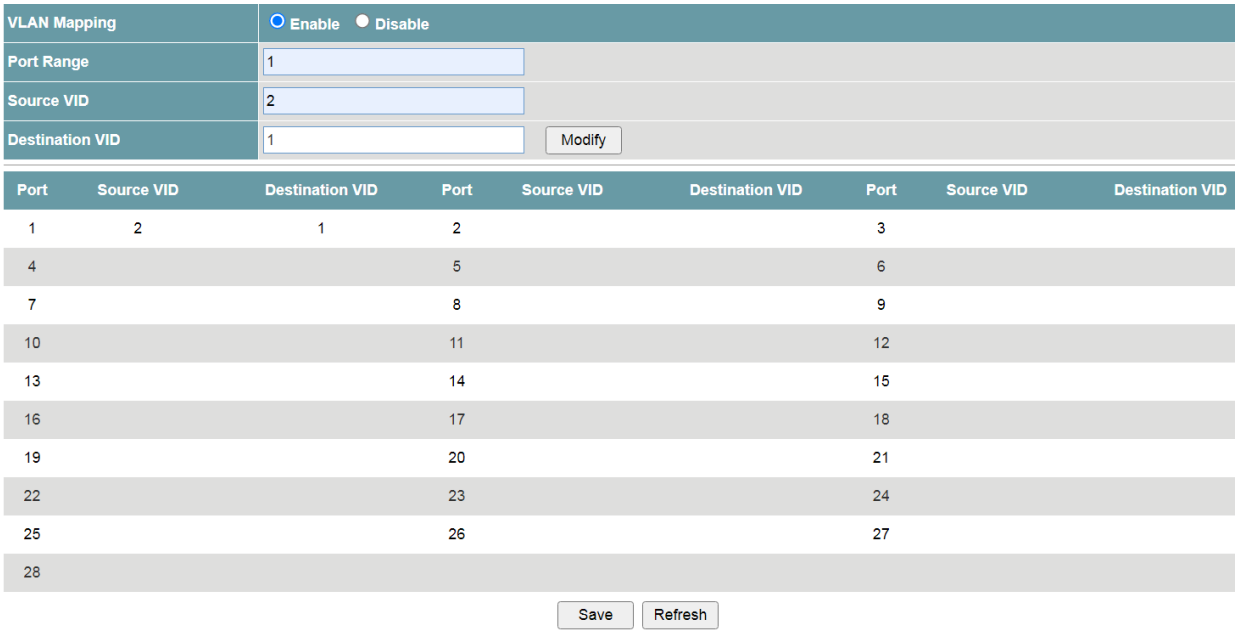
· Click the <Refresh> button to reload the page.

· View the information.

8.6 VLAN Mapping

VLAN mapping is a feature on switches that allows the mapping of VLAN IDs between different VLAN domains or between VLANs and other network protocols. It enables efficient management and translation of VLAN configurations within the network.

Users can view and modify VLAN Mapping Setting as bellow.



Users can view and modify ---- Setting as bellow.

Procedure

Choose < Ethernet Switch >< VLAN Mapping > in the navigation tree to open the page.

1) Enable VLAN Mapping firstly.

· Set the parameters as required.

Items	Descriptions	Default value
VLAN Mapping	Set the feature Enable/Disable	Disable

2) Configure VLAN Mapping.

· Set the parameters as required.

Items	Descriptions	Default value
Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. Format as "2" or "1-5" or "3, 1-5".	Null
Source VID	Input the VLAN from 1 to 4094	Null
Destination VID	Input the VLAN from 1 to 4094	Null

· Click <Modify>.

· Click <Save>.

3) Save configurations and reload.

· Click <Save>.

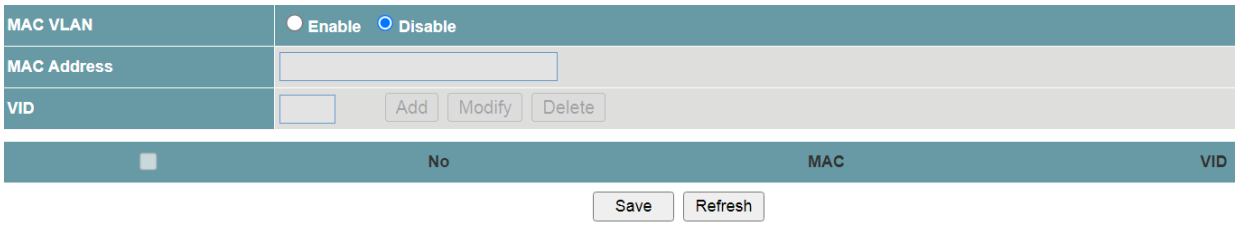
· Click the <Refresh> button to reload the page.

· View the information.

8.7 MAC-based VLAN

MAC-based VLAN, also known as MAC VLAN, is a feature that allows the assignment of VLAN memberships based on MAC addresses. It provides granular control over network access by associating specific MAC addresses with designated VLANs.

Users can view and modify MAC-based VLAN Setting as bellow.



Procedure

Choose < Ethernet Switch >< MAC-based VLAN > in the navigation tree to open the page.

1) Enable MAC VLAN firstly.

· Set the parameters as required.

Items	Descriptions	Default value
MAC VLAN	Set the feature Enable/Disable	Disable

2) Configure MAC Based VLAN.

· Set the parameters as required.

Items	Descriptions	Default value
MAC Address	Input the valid MAC Address like xx:xx:xx:xx:xx:xx	Null
VID	Input the VLAN from 1 to 4094	Null

- Click <Add> or <Modify> or <Delete>.
- Click <Save>.

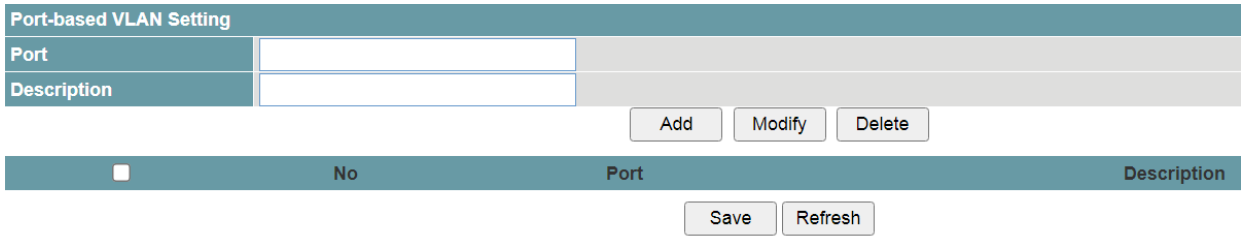
3) Save configurations and reload.

- Click <Save>.
- Click the <Refresh> button to reload the page.
- View the information.

8.8 Port-based VLAN

Port-based VLAN is a feature on switches that enables the assignment of VLAN memberships based on physical switch ports. Each port is associated with a specific VLAN, allowing for network segmentation and traffic isolation.

Users can view and modify Port-based VLAN Setting as bellow.



Procedure

Choose < Ethernet Switch >< Port-based VLAN > in the navigation tree to open the page.

1) Configure Port Based VLAN.

- Set the parameters as required.

Items	Descriptions	Default value
Port	Input the ports numbers that need to be set. Multiple interfaces can be selected. Format as “2” or “1-5” or “3, 1-5” .	Null
Description	Input the string and the length is up to 256 character	Null

- Click <Add> or <Modify> or <Delete>.
- Click <Save>.

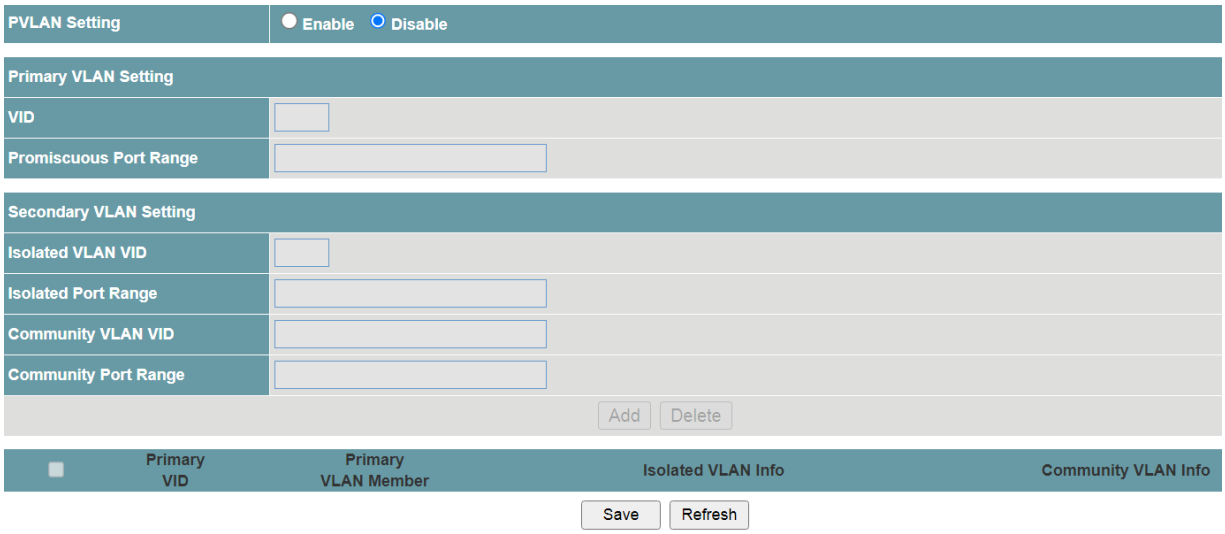
2) Save configurations and reload.

- Click <Save>.
- Click the <Refresh> button to reload the page.
- View the information.

8.9 Private VLAN

Private VLAN (PVLAN) is a feature that enhances network segmentation by subdividing VLANs into smaller isolated communities. It provides granular control over network traffic within the same VLAN, ensuring privacy and security for devices connected to the switch.

Users can view and modify Private VLAN Setting as bellow.



Procedure

Choose < Ethernet Switch >< Private VLAN > in the navigation tree to open the page.

1) Enable Private VLAN firstly.

· Set the parameters as required.

Items	Descriptions	Default value
PVLAN Setting	Set the feature Enable/Disable	Disable

2) Configure Primary VLAN.

· Set the parameters as required.

Items	Descriptions	Default value
VID	Input the VLAN from 1 to 4094	Null
Promiscuous Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. Format as “2” or “1-5” or “3, 1-5” .	Null

3) Configure Secondary VLAN.

· Set the parameters as required.

Items	Descriptions	Default value
Isolated VLAN VID	Input the VLAN from 1 to 4094	Null
Isolated Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. Format as “2” or “1-5” or “3, 1-5” .	Null
Community VLAN VID	Input the VLAN from 1 to 4094	Null
Community Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. Format as “2” or “1-5” or “3, 1-5” . Promiscuous Port Range, Isolated Port Range and Community Port Range can’t be overlap.	Null

· Click <Add> or <Modify> or <Delete>.

- Click <Save>.

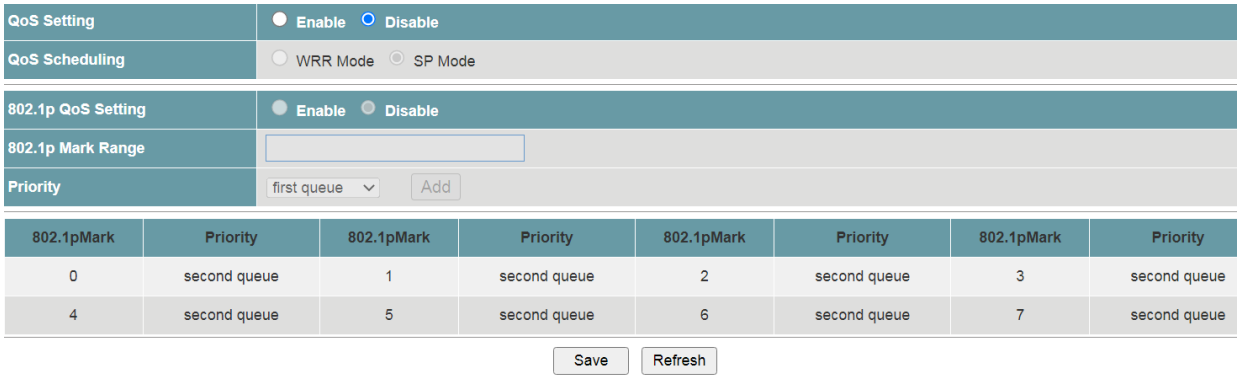
4) Save configurations and reload.

- Click <Save>.
- Click the <Refresh> button to reload the page.
- View the information.

8.10 802.1Q QoS

802.1Q is a standard for VLAN tagging in Ethernet networks, and it also incorporates Quality of Service (QoS) features to prioritize and manage network traffic effectively. This functionality on switches allows administrators to implement QoS policies based on VLAN tags, ensuring optimal performance for critical applications and services.

Users can view and modify 802.1Q QoS setting as bellow.



Procedure

Choose < Ethernet Switch >< 802.1Q QoS > in the navigation tree to open the page.

1) Enable QoS firstly.

- Set the parameters as required.

Items	Descriptions	Default value
QoS Setting	Set the feature Enable/Disable	Disable

2) Configure QoS VLAN.

- Set the parameters as required.

Items	Descriptions	Default value
802.1p QoS Setting	let the feature Enable/Disable	Disable
QoS Scheduling	Select the QoS schedule as WRR mode or SP mode	SP Mode
802.1P Mark Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. Format as “2” or “1-5” or “3, 1-5”.	Null
Priority	Select the proper Queue for the priority · First Queue · Second Queue · Third Queue	First Queue

	· Fourth Queue · Fifth Queue · Sixth Queue · Seventh Queue · Fastest Queue	

· Click <Add>.

· Click <Save>.

3) Save configurations and reload.

· Click <Save>.

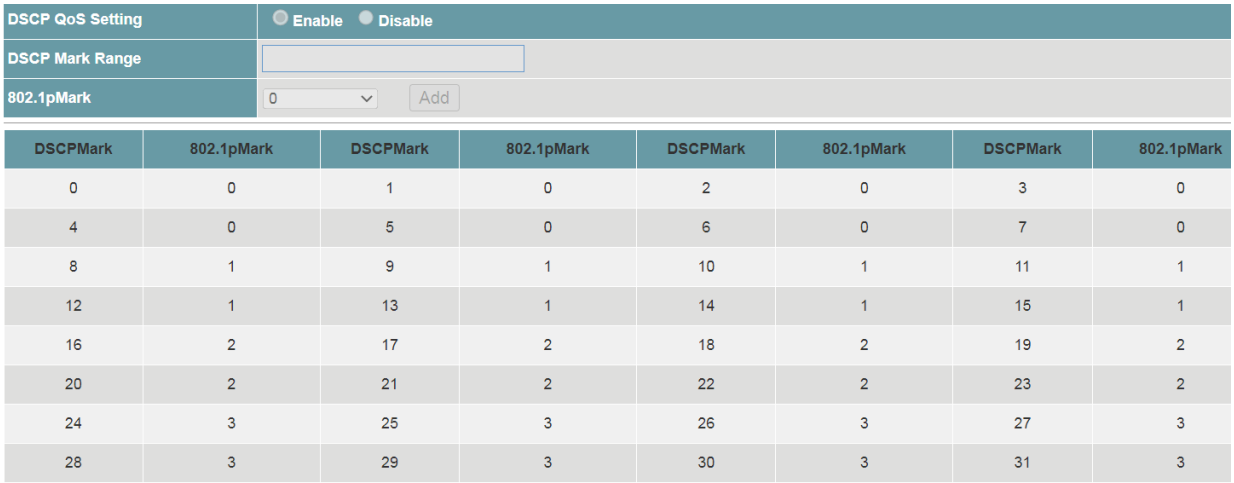
· Click the <Refresh> button to reload the page.

· View the information.

8.11 DSCP QoS

Differentiated Services Code Point (DSCP) is a QoS mechanism that allows switches to prioritize and manage network traffic based on the DSCP value in IP packet headers. This feature enables administrators to implement granular QoS policies for efficient traffic handling.

Users can view and modify DSCP QoS Setting as bellow.



DSCP QoS Setting	Enable Disable
DSCP Mark Range	
802.1pMark	0 Add

DSCPMark	802.1pMark	DSCPMark	802.1pMark	DSCPMark	802.1pMark	DSCPMark	802.1pMark
0	0	1	0	2	0	3	0
4	0	5	0	6	0	7	0
8	1	9	1	10	1	11	1
12	1	13	1	14	1	15	1
16	2	17	2	18	2	19	2
20	2	21	2	22	2	23	2
24	3	25	3	26	3	27	3
28	3	29	3	30	3	31	3

Procedure

Choose < Ethernet Switch >< DSCP QoS > in the navigation tree to open the page.

1) Enable DSCP QoS firstly.

· Set the parameters as required.

Items	Descriptions	Default value
DSCP QoS Setting	Set the feature Enable/Disable	Disable

2) Configure DSCP QoS .

· Set the parameters as required.

Items	Descriptions	Default value
DSCP Mark Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. Format as “2” or “1-5” or “3, 1-5” .	Null

802.1pMark	Select the proper Queue for the priority from 0 to 7	0

- Click <Add>.
- Click <Save>.

3) Save configurations and reload.

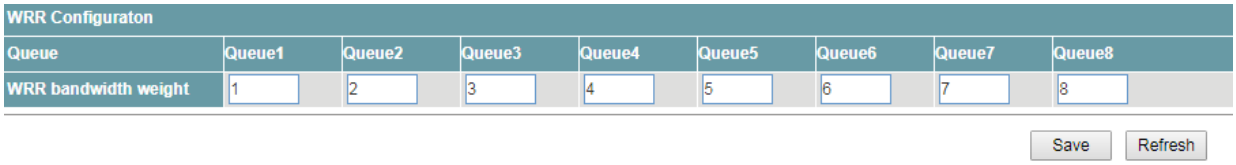
- Click <Save>.
- Click the <Refresh> button to reload the page.
- View the information.

8.12 WRR Configuration

Weighted round robin (WRR) scheduling ensures that packets in all the queues are scheduled in turn.

By default, eight queues are configured on the switch. Each queue is set with a weight value, namely, Queue 1, Queue 2, Queue 3, Queue 4, Queue 5, Queue 6, Queue 7, and Queue 8. The weight represents the percentage of obtaining resources.

For example, assuming that the weights of queues on the 1000M interface are 1, 2, 3, 4, 5, 6, 7, and 8. Therefore, the queue with the lowest priority can obtain at least 27.8 Mbit/s bandwidth (1/36 multiplied by 1000 Mbit/s).



Procedure

Choose <Ethernet Switch><WRR> in the navigation tree to open the page.

1) Configure WRR.

- Set the parameters as required.

Items	Descriptions	Default value
Queue	Queue number	Disable
WRR bandwidth weight	Bandwidth weight value of the queue. The value ranges from 1~255.	1~8

- Click <Save>.

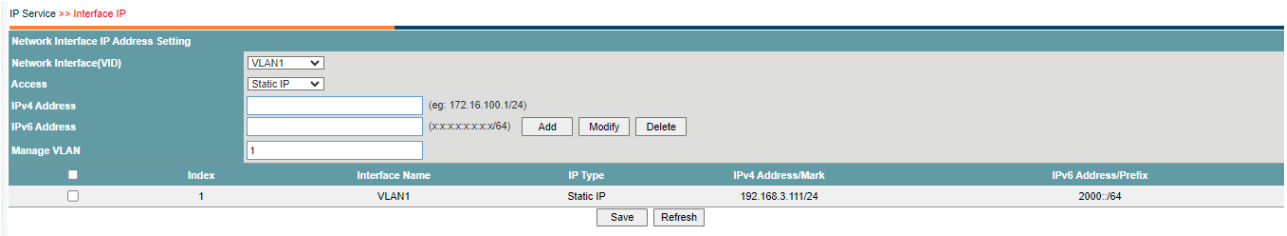
2) View the configuration.

- Click <Refresh> to reload the page.
- View the information.

9 IP Service

9.1 Interface IP

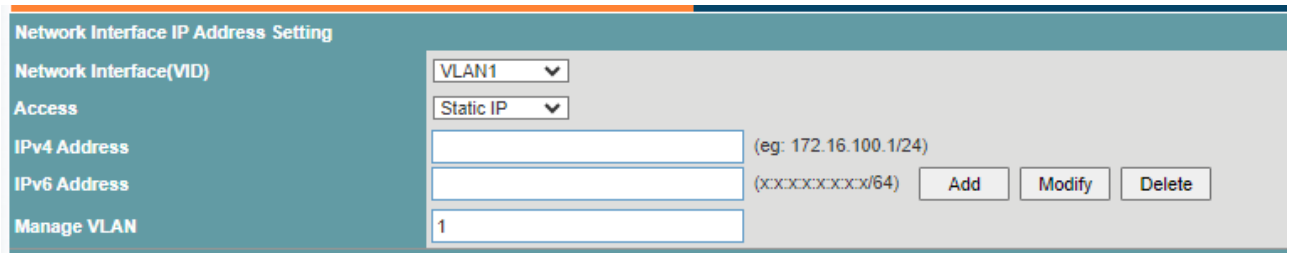
Users can add, modify delete the IP address of the VLANs, including IPv4 and IPv6, and view the IP address of VLAN for the device.



Procedure

Choose <IP Service> <Interface IP> in the navigation tree to open the page.

1) Add the IP address



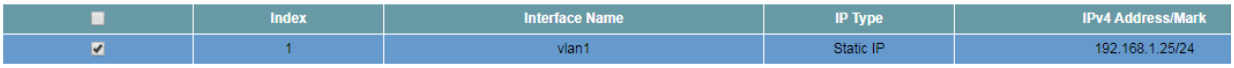
- Set the parameters as required.

Items	Descriptions	Default value
Network Interface (VID)	VLAN ID of the interface. This parameter is not able to be set.	VLAN 1
Access	The access mode of the IP. This parameter is not able to be set.	Static IP
IPv4 Address	The IPv4 Address of the IP address of the Ethernet interface and the subnet mask of the IP address.	Null
IPv6 Address	The IPv6 Address of the IP address of the Ethernet interface and the subnet mask of the IP address.	Null
Manage VLAN	The manage VLAN for the IP packet of the Ethernet interface.	1

- Click <Add> to add the IP address.
- Click <Save>.

2) Modify the IP address

- Select the IP Address that need to be modified.



- Set the parameters as required.
- Click <Modify>.
- Click <Save>.

3) Delete the IP address

· Select the IP Address that need to be deleted.

	Index	Interface Name	IP Type	IPv4 Address/Mark
☑	1	vlan1	Static IP	192.168.1.25/24

· Click <Delete>.

· Click <Save>.

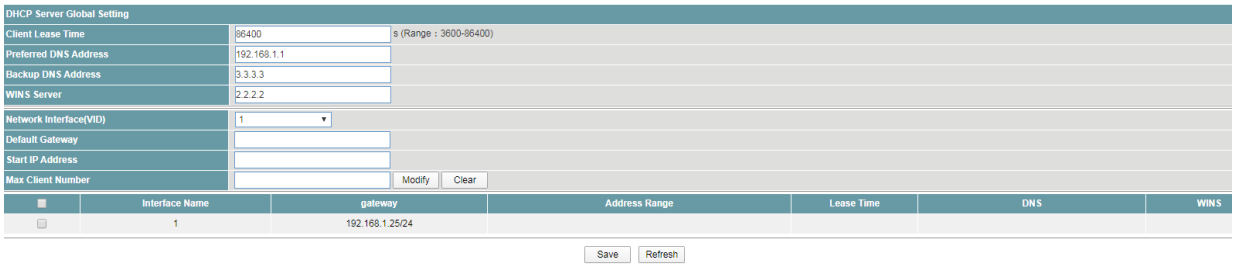
9.2 DHCP Server

DHCP is a technology used to dynamically manage and configure clients in a concentrated manner.

The client applies to the server for configurations such as the IP address, subnet mask, and default gateway, and the server replies with corresponding configurations according to policies.

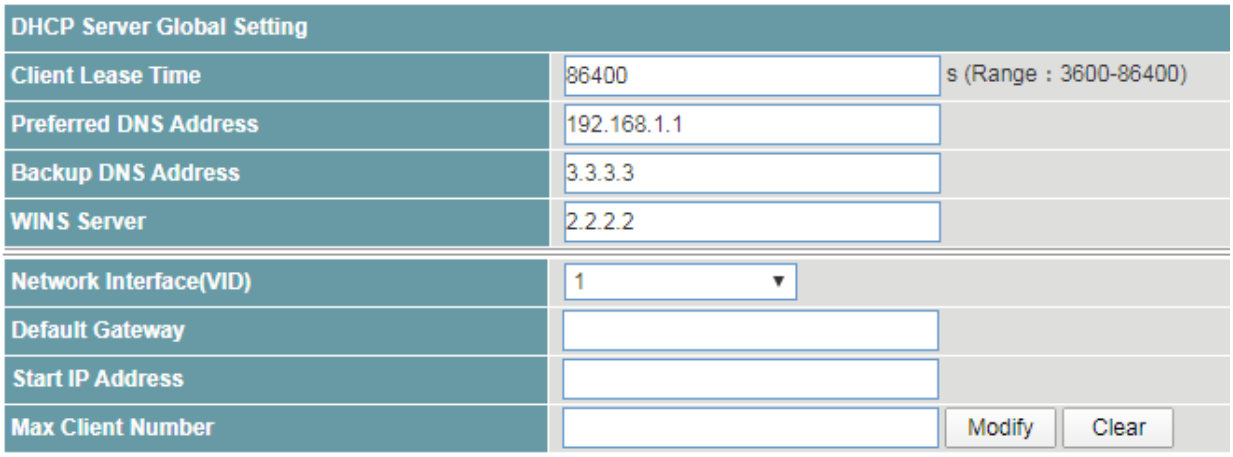
Users need to configure a DHCP server based on the global address pool to enable computers to obtain IP addresses from the global address pool dynamically.

Users can configure an address pool on a VLAN when a device supports switched Ethernet interfaces. IP addresses cannot be configured on switched Ethernet interfaces directly; therefore, you need to create a VLAN and configure a DHCP address pool on the VLAN.



Procedure

Choose <IP Service> <DHCP Server> in the navigation tree to open the page.



1) Set the global the DHCP server parameter.

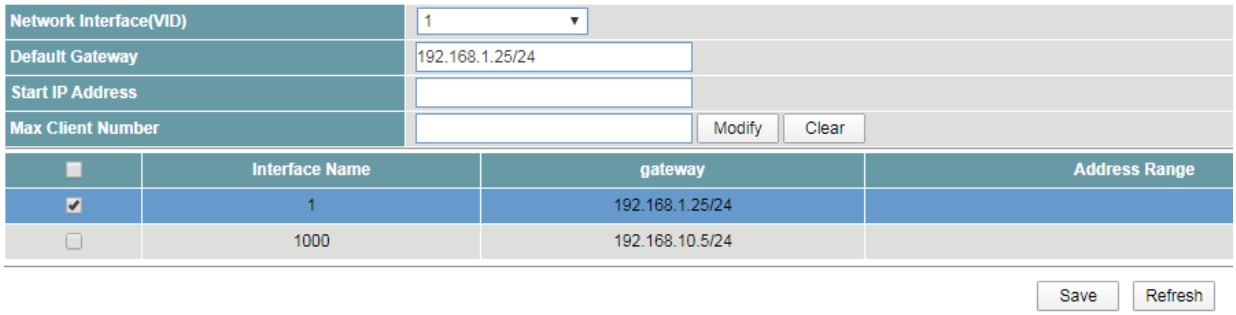
· Set the parameters as required.

Items	Descriptions	Default value
Client Lease Time	Indicates the lease of dynamic IP addresses. The default lease is one day (86400s). The value ranges from 3600 to 86400 s.	86400

Preferred DNS Address	Indicates the main IP address of a DNS server.	192.168.1.1
Backup DNS Address	Indicates the backup IP address of a DNS server.	Null
WINS Server	Indicates the IP address of a WINS server.	Null

- Click <Modify>.
- Click <Save>.

2) Set an address pool on a VLAN.



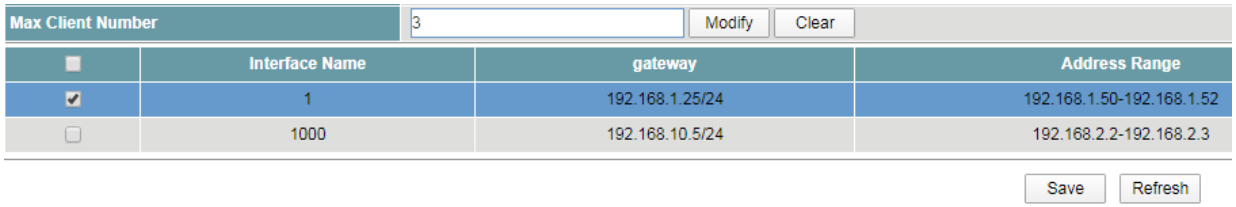
- Set the parameters as required.

Items	Descriptions	Default value
Network Interface (VID)	Select a record in the table to indicate the name of a VLNAIF interface. The VLANs in the table are created in the <Ethernet Switch> <802.1Q VLAN> and <IP Service> <Interface IP> modules.	1
Default Gateway	Indicates the default IP address and subnet mask of the selected VLAN. The value is displayed automatically after you select the <Network Interface (VID)>.	Null
Start IP Address	Indicate the start IP address of the interface.	Null
Max Client Number	Input the max client number. The value ranges from 2 to 255.	50

- Click <Modify>.
- Click <Save>.

3) Clear the record

User can clear the DHCP configuration of the selected VLAN.

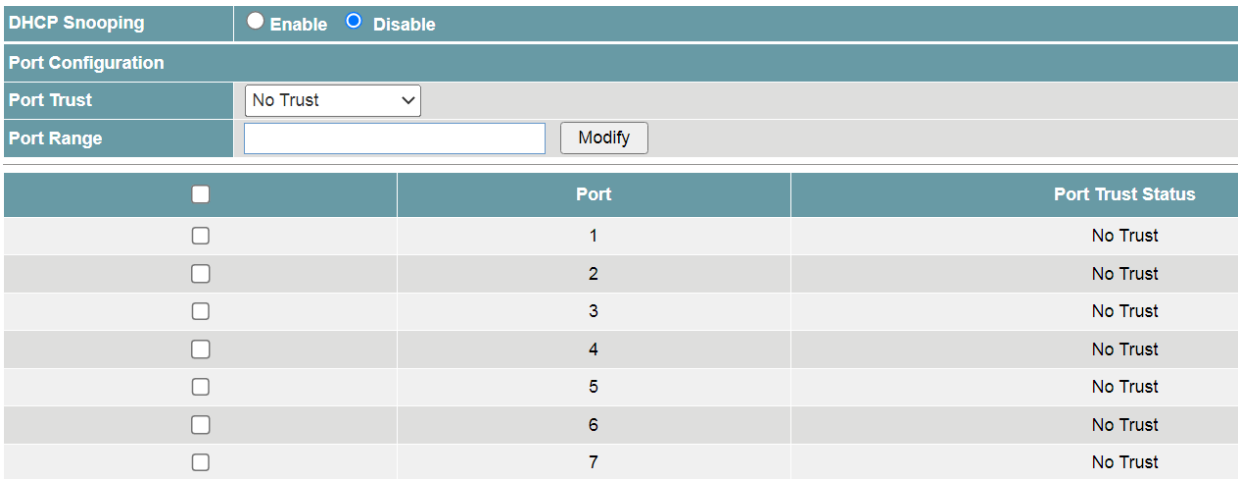


- Choose the record that need to be cleared, multiple records can be selected.
- Click <Clear>.
- Click <Save>.

9.3 DHCP Snooping

DHCP (Dynamic Host Configuration Protocol) snooping is a security feature that enhances network integrity by preventing rogue DHCP server attacks and unauthorized IP address assignments. It monitors DHCP messages and ensures only authorized DHCP servers are allowed to assign IP addresses.

Users can view and modify DHCP Snooping Setting as bellow.



Procedure

Choose < IP Service >< DHCP Snooping > in the navigation tree to open the page.

1) Enable DHCP Snooping firstly.

· Set the parameters as required.

Items	Descriptions	Default value
DHCP Snooping	Set the feature Enable/Disable	Disable

2) Configure Port Configuration.

· Set the parameters as required.

Items	Descriptions	Default value
Port Trust	Set the mode as No Trust or Trust	No Trust
Aging time	When mode is set as auto, aging time attribute is available. The value is 0, 5-43200.1440 by default.0 means no aging. The unit is minute	1440
Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. Format as "2" or "1-5" or "3, 1-5".	Null

· Click <Save>.

3) Save configurations and reload.

· Click <Save>.

· Click the <Refresh> button to reload the page.

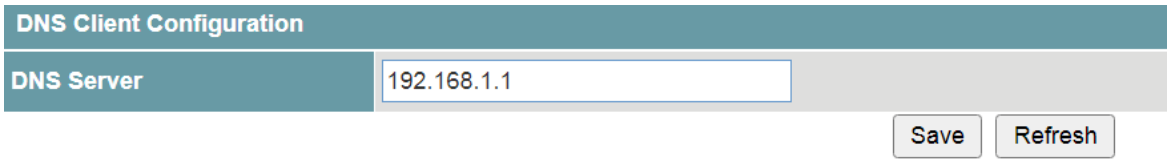
· View the information.

9.4 DNS Client Configuration

The DNS (Domain Name System) client feature on switches allows them to perform DNS queries

and resolve domain names to IP addresses. This functionality is crucial for network devices to access resources using domain names instead of IP addresses.

Users can view and modify DNS Client Configuration Setting as bellow.



Procedure

Choose < IP Service >< DNS Client Configuration > in the navigation tree to open the page.

1) Configure DNS Server Configuration.

· Set the parameters as required.

Items	Descriptions	Default value
DNS Server	Set the IPv4 Address for IPv4 Subnet VLAN. The format is A:B:C:D	192.168.1.1

2) Save configurations and reload.

· Click <Save>.

· Click the <Refresh> button to reload the page.

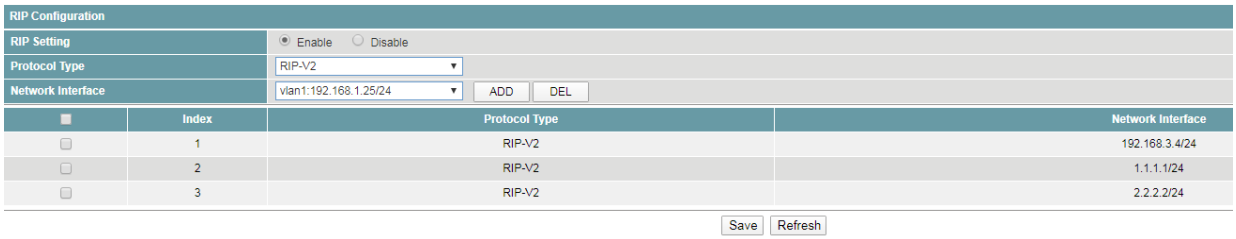
· View the information.

10 IP Routing

10.1 RIP

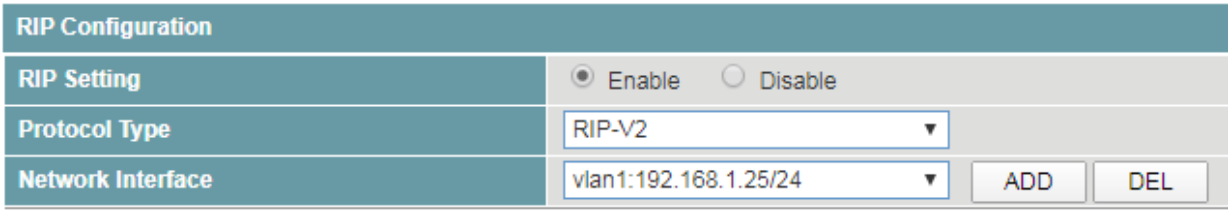
RIP is a simple Interior Gateway Protocol (IGP) used in small-scale networks, such as campus networks and regional networks with simple structure.

Users can configure RIP, delete the network segment as required and view the configuration.



Procedure

Choose <IP Routing> <RIP> in the navigation tree to open the page.



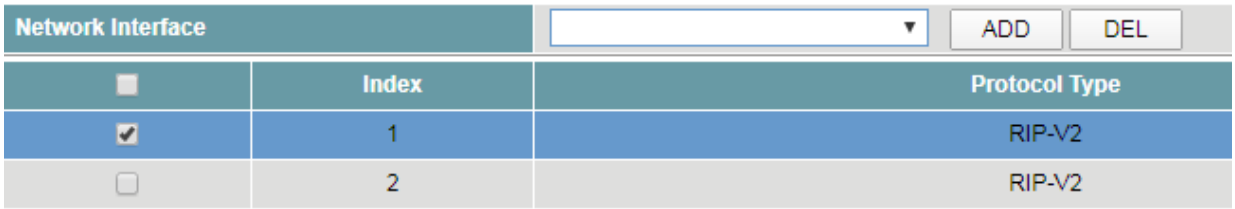
1) Create the RIP routing

- Set the parameters as required.

Items	Descriptions	Default value
RIP Setting	Choose <Enable> to enable the function.	Disable
Protocol Type	Choose the protocol type of RIP routing, including · RIP-V2 · RIP-V1	RIP-V2
Network Interface	Choose the network segment in the drop down list box. The value is created in the <Ethernet Switch> <802.1Q VLAN> and <IP Service> <Interface IP> modules.	VLAN1:192.168.1.200/8

- Click <Add>.
- Click <Save>.

2) Delete the network segment



- Choose the record that need to be cleared.
- Click <DEL>.

- Click <Save>.
- Click <Refresh>.

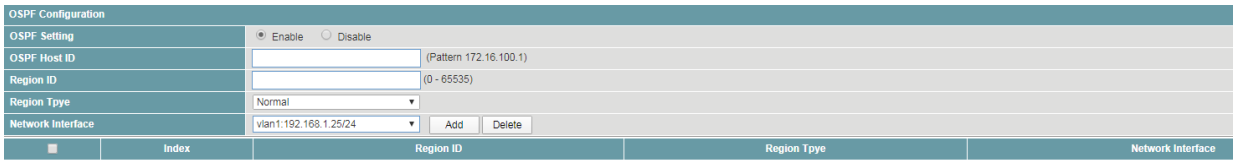
3) View the RIP configuration.

- Click <Refresh>.
- View the configuration.

10.2 OSPF

By building OSPF networks, users can enable OSPF to discover and calculate routes in Autonomous Systems. OSPF is applicable to a large-scale network that consists of hundreds of devices.

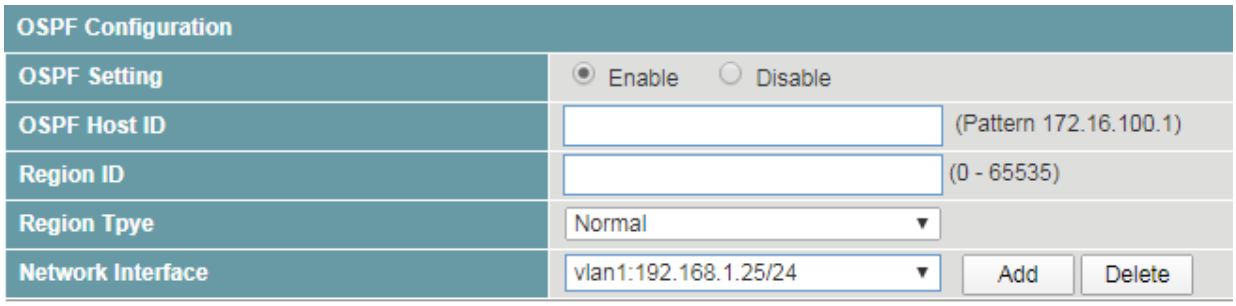
Users can configure the OSPF network, delete the network segment as required and view the configuration.



Procedure

Choose <IP Routing> <OSPF> in the navigation tree to open the page.

1) Configure OSPF network.

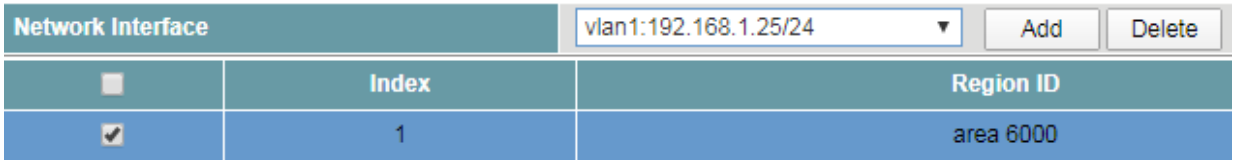


- Set the parameters as required.

Items	Descriptions	Default value
OSPF Setting	Choose <Enable> to enable the function.	Disable
OSPF Host ID	Input IP address of OSPF host.	Null
Region ID	Input the range of OSPF network. The value ranges from 0 to 65535.	Null
Region Type	Choose the region type, including · Normal · Stub · NSSA	Normal
Network Interface	Choose the network segment in the drop down list box. The value is created in the <Ethernet Switch> <802.1Q VLAN> and <IP Service> <Interface IP> modules.	VLAN1:192.168.1.200/8

- Click <Add>.
- Click <Save>.

2) Delete the network segment.



- Choose the record that need to be deleted.
- Click <Delete>.
- Click <Save>.
- Click <Refresh>.

10.3 Routing Table

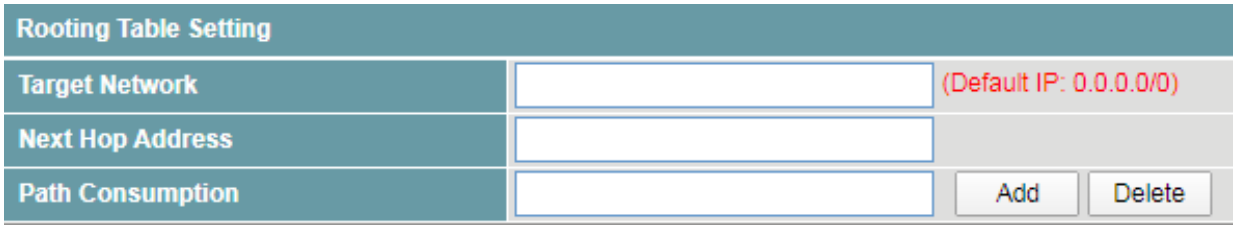
A router forwards packets by using a routing table. Each router saves a routing table. Each entry in the routing table contains a physical interface of the router, and the router sends packets to the physical interfaces.

Users can configure the static routing tables and view the information of the routing table.

Procedure

Choose <IP Routing> <Routing Table> in the navigation tree to open the page.

1) Create an IPv4 routing table.

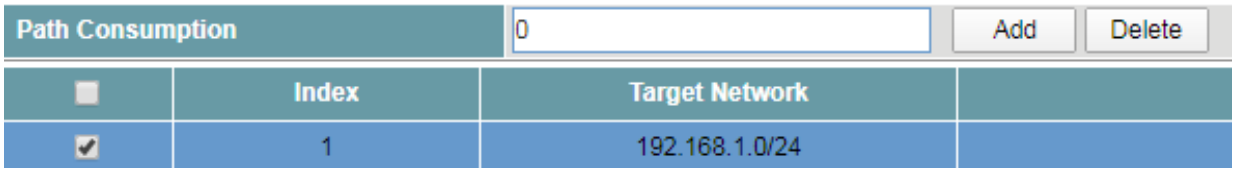


- Set the parameters as required.

Items	Descriptions	Default value
Target Network	Indicates the destination IP address and subnet mask of an IP packet.	Null
Next Hop Address	Indicates the next-hop router address that IP packets pass through.	Null
Path Consumption	Indicate the length of static route path. The value ranges from 1 to 255.	Null

- Click <Add>.
- Click <Save>.

2) Delete an IPv4 routing table.



- Choose the record that need to be deleted.
- Click <Delete>.
- Click <Save>.

3) View the routing table.

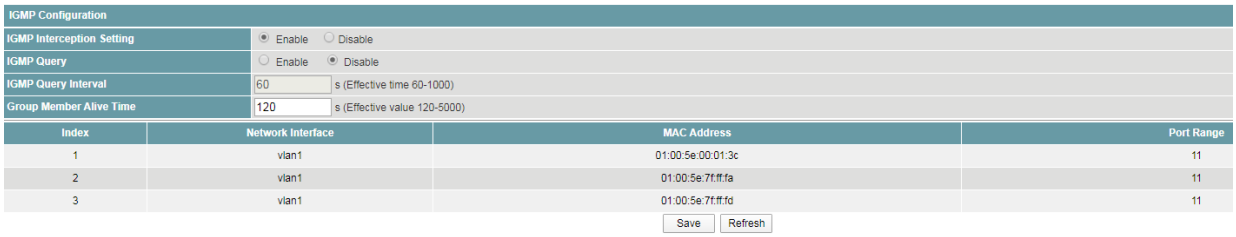
- Click <Refresh>.
- View the configuration.

11 IP Multicast

11.1 IGMP Snooping

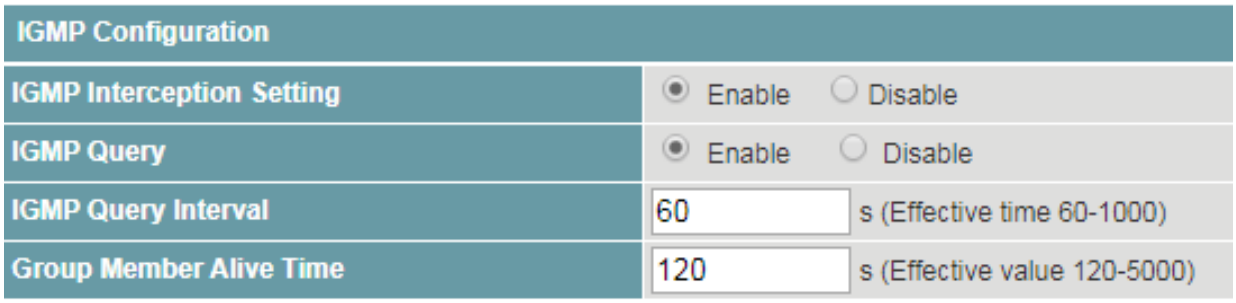
Internet Group Management Protocol Snooping (IGMP-Snooping) is a Layer 2 IPv4 multicast protocol. The IGMP-Snooping protocol maintains information about the outgoing interfaces of multicast packets by snooping multicast protocol packets exchanged between the Layer 3 multicast device and user hosts. The IGMP-Snooping protocol manages and controls the forwarding of multicast packets at the data link layer.

Users could turn on/off the IGMP-Snooping function and configure the IGMP-Snooping Timer.



Procedure

Choose <IP Multicast> <IGMP Snooping> in the navigation tree to open the page.



1) Configure the IGMP-Snooping function.

· Set the parameters as required.

Items	Descriptions	Default value
IGMP Interception Setting	Choose <Enable> to enable the IGMP-Snooping function.	Disable
IGMP Query	Choose <Enable> to enable the IGMP-Snooping query function.	Disable
Fast Leave	Set the feature as Enable or Disable	Disable
IGMP Query Interval	Indicate the query interval time. The value ranges from 60~1000 s.	660s
Group Member Alive Time	Indicate the group members survival time. The value ranges from 120~5000 s.	1120s
Route Port	Input the ports numbers that need to be set. Multiple interfaces can be selected. Format as “2” or “1-5” or “3, 1-5”.	Null

2) Configure the Static Multicast Table Configuration function.

· Set the parameters as required.

Items	Descriptions	Default value
Static Multicast MAC Address	Set the MAC address and the format is A:B:C:D:E:F	Null
VLAN ID	Input the VLAN from 1 to 4094	Null
Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. Format as “2” or “1-5” or “3, 1-5” .	Null

- Click <Add> or <Delete>.
- Click <Save>

3) View the IGMP Snooping configuration.

- Click <Refresh> to reload the page.
- View the information.

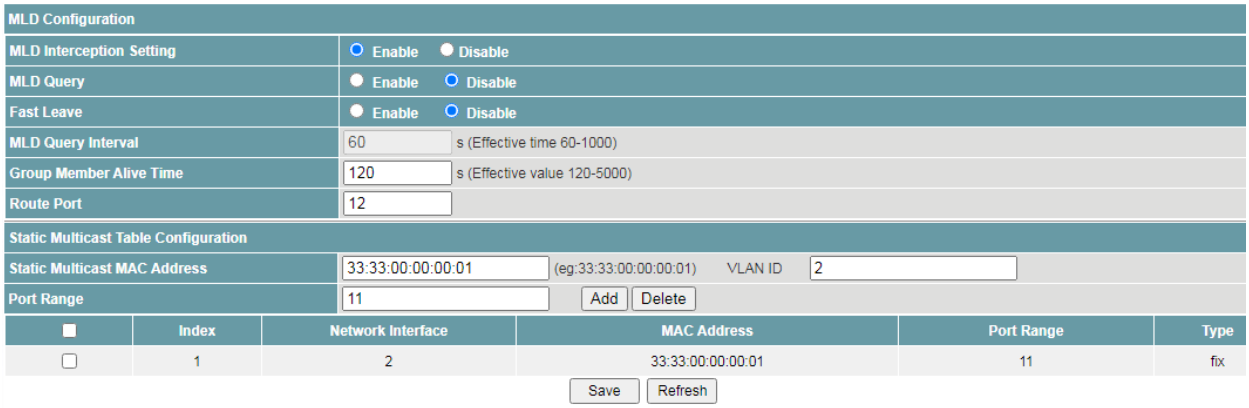
11.2 MLD Snooping

MLD (Multicast Listener Discovery) snooping is a feature that enhances multicast traffic efficiency by intelligently managing multicast group memberships within a network. It operates similarly to IGMP (Internet Group Management Protocol) snooping but is specific to IPv6 multicast traffic.

Key Features:

- IPv6 Multicast Management: MLD snooping manages IPv6 multicast group memberships dynamically.
- Snooping Database: It maintains a snooping database to track multicast group memberships per VLAN.
- Optimized Traffic Forwarding: MLD snooping forwards multicast traffic only to ports with interested receivers, reducing unnecessary network flooding.

Users can view and modify MLD Snooping Setting as bellow.



1) Configure the MLD-Snooping function.

- Set the parameters as required.

Items	Descriptions	Default value
MLD Interception Setting	Choose <Enable> to enable the MLD-Snooping function.	Disable
MLD Query	Choose <Enable> to enable the MLD-Snooping query function.	Disable
Fast Leave	Set the feature as Enable or Disable	Disable

MLD Query Interval	Indicate the query interval time. The value ranges from 60~1000 s.	660
Group Member Alive Time	Indicate the group members survival time. The value ranges from 120~5000 s.	1120
Route Port	Input the ports numbers that need to be set. Multiple interfaces can be selected. Format as “2” or “1-5” or “3, 1-5”.	Null

2) Configure the Static Multicast Table Configuration function.

· Set the parameters as required.

Items	Descriptions	Default value
Static Multicast MAC Address	Set the MAC address and the format is A:B:C:D:E:F	Null
VLAN ID	Input the VLAN from 1 to 4094	Null
Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. Format as “2” or “1-5” or “3, 1-5”.	Null

· Click <Add> or <Delete>.

· Click <Save>

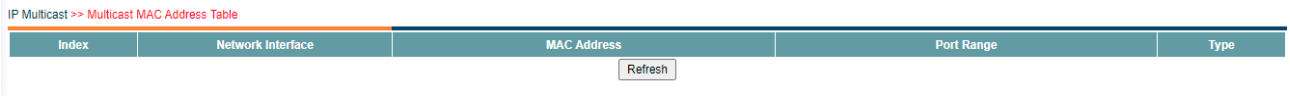
3) View the IGMP Snooping configuration.

· Click <Refresh> to reload the page.

· View the information.

11.3 Multicast MAC Address Table

Users can view the Multicast MAC table of the interfaces.



Procedure

1) Click <Refresh> button to reload the page.

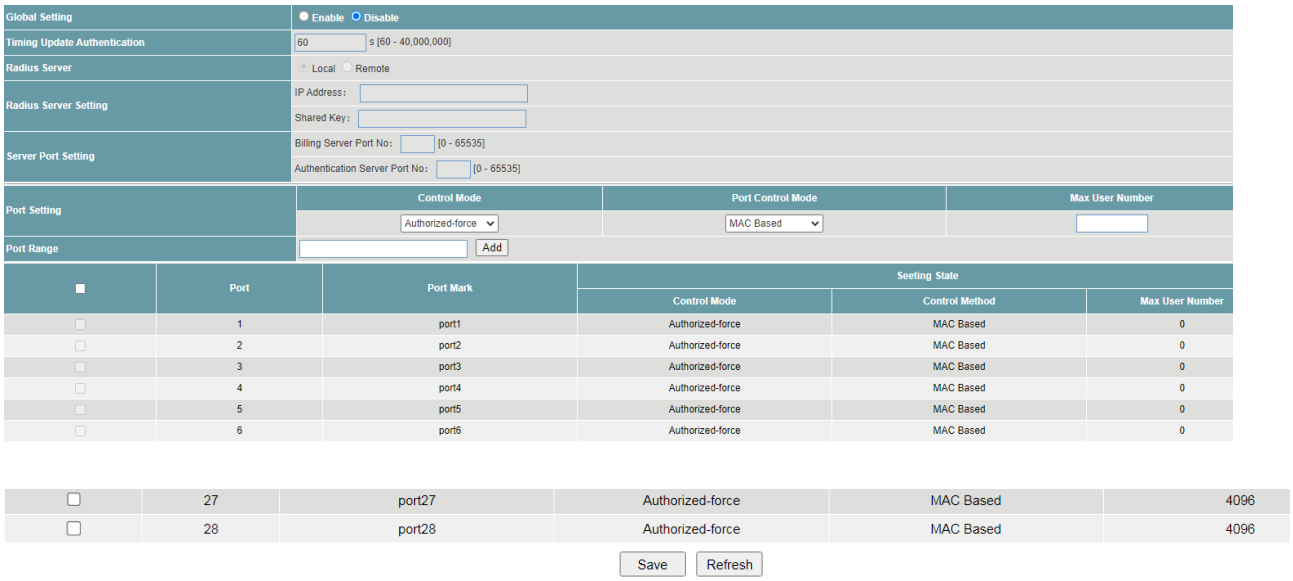
12 Security Configuration

12.1 802.1x Authentication

In the network planning deployment of the access layer, users need to deploy access-side security, only legitimate users can access the network after authentication. 802.1x can be well deployed on the access switch ports to achieve access-side security control.

802.1x authentication is available as a local-based authentication method or as a radius-based remote authentication method. We go through case examples to explain 802.1x local and remote radius authentication in detail.

The function is disable by default.



Procedure

Choose <Security Configuration><802.1xAuthentication> in the navigation tree to open the page.

1) Enable the function.

2) Configure the global parameters.

Items	Descriptions	Default value
Timing Update Authentication	Input the authentication timer, the value ranges from 60~40,000,000s.	Null
Radius Server	Choose the radius server, including two types: · Local: local radius server. · Remote: remote radius server.	Remote

3) Configure local authentication.

Items		Descriptions	Default value
Radius Server		Choose <Local>.	Local
Port Setting	Control Mode	Set to <Auto>.	Null
	Port Control Mode	Support <Mac Based> only.	Mac Based

· Go to <Local RADIUS> page to add new account and password.

- Click <Edit>.
- Click <Save>.

4) Configure remote authentication.

Items		Descriptions	Default value
Radius Server		Choose <Remote>.	Local
Port Setting	Control Mode	Set to <Auto>.	Null
	Port Control Mode	Support <Mac Based> only.	Mac Based
Radius Server Setting	IP Address	Input the IP address of Radius server.	Null
	Secret Shared Key	Indicate the secret shared key of the IP address.	Null
Server Port Setting	Billing Server Port	Indicate the accounting port. The value ranges from 0 to 65535.	1813
	Certification Server Port	Indicate the authentication port. The value ranges from 0 to 65535.	1812
Port Setting	Control Mode	Set to <Auto>.	Null
	Port Control Mode	Support <Mac Based> only.	Mac Based
	Maximum User Number	Input the maximum user quantity, the value ranges from 1 to 4096.	Null
Port Range		Select the interfaces or input the ports numbers that need to be set.	Null

- Click <Edit>.
- Click <Save>.

12.2 AAA Setting

Authentication, Authorization, and Accounting (AAA) is a security technology. The AAA-capable device checks validity of users and assigns rights to authorized users to ensure network security.

The switch supports two authentication mode:

Local: After local authentication and authorization are configured, the device authenticates and authorizes access users based on the local user information.

Radius: Use the Radius protocol to achieve AAA authentication. After selecting this mode, go to <802.1x authentication> page to configure Radius server. For details, see "802.1X Authentication".

After setting, click <Save> button.

The switch supports to add or delete user name and password for local 802.1x authentication.

Procedure

Choose <Security Configuration>< Local Radius Setting> in the navigation tree to open the page.

1) Create user account function.

Items	Descriptions	Default value

User Login	Specify the name of user login and the value is string	Null
User Password	Specify the password of the user name, the value support 5~16 bits string.	Null

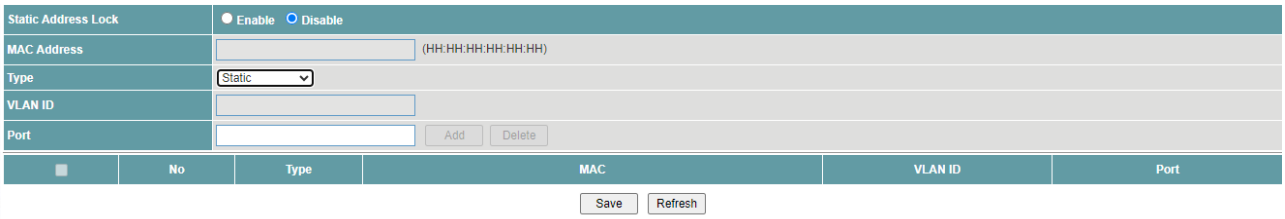
- Click <Add>.
- Click <Save>.

2) Delete an account.

- Select the account that need to be deleted.
- Click <Delete>.
- Click <Save>.

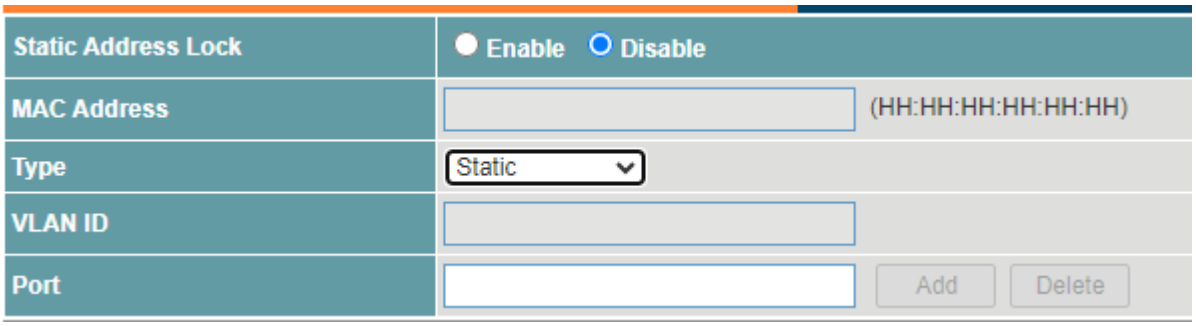
12.3 Static Address Lock

User can create, delete the static MAC table and view the configuration information.



Procedure

Choose <Security Configuration> <Static Address Lock> in the navigation tree to open the page.



1) Configure the static MAC table.

- Set the parameters as required.

Items	Descriptions	Default value
Static Address Lock	Choose <Enable> to enable the function.	Disable
MAC Address	Input the 48 bit mac address.	Null
Type	Set the value as Static or Blackhole	Static
VLAN ID	Input the VLAN ID. The value ranges from 1~4094.	Null
Port	Input the ports numbers that need to be set. Multiple interfaces can be selected. The value ranges from 1~28. Format as “2” or “1-5” or “3, 1-5”.	Null

- Click <Add>.

- Click <Save>.

2) Delete the static MAC table.

- Choose the record that need to be deleted.
- Click <Delete>.
- Click <Save>.

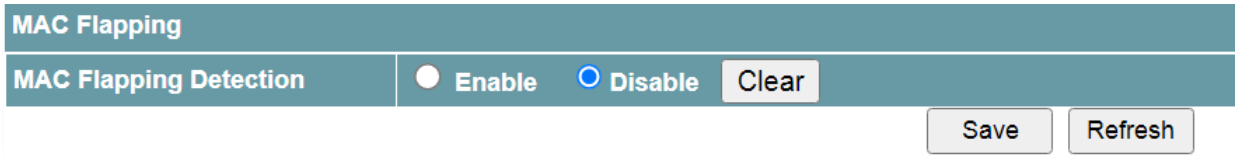
3) View the static MAC table.

- Click <Refresh> to reload the page.
- View the information.

12.4 MAC Flapping

MAC flapping is a phenomenon where a MAC address repeatedly alternates between different switch ports. This can disrupt network operations, cause broadcast storms, and lead to performance issues. Understanding MAC flapping is crucial for network administrators to identify and resolve spanning tree or physical connectivity problems. Monitoring MAC address tables and analyzing switch logs can help diagnose and mitigate flapping incidents, ensuring a stable and efficient network environment.

Users can view and modify MAC Flapping Setting as bellow.



Procedure

Choose < Security Configuration >< MAC Flapping > in the navigation tree to open the page.

3) Enable MAC Flapping function.

Items	Descriptions	Default value
MAC Flapping Detection	Set the feature as Enable/Disable	Disable

4) Save configurations and reload.

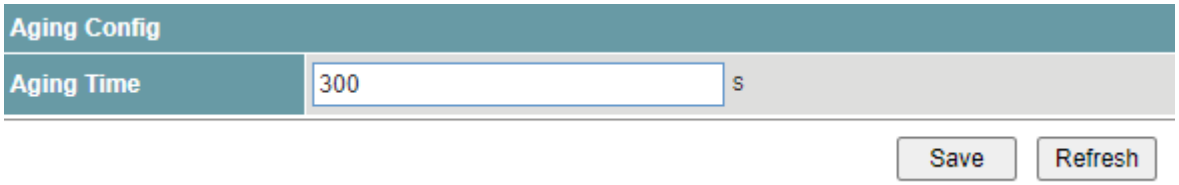
- Click <Save>.
- Click the <Refresh> button to reload the page.
- View the information.

12.5 MAC Dynamic Aging

After the aging time of dynamic MAC address entries is set, the device can delete unneeded MAC address entries to prevent sharp increase of MAC address entries. A shorter aging time is applicable to networks where network topology changes frequently, and a longer aging time is applicable to stable networks.

Procedure

Choose <Security Configuration><MAC Dynamic Aging> in the navigation tree to open the page.



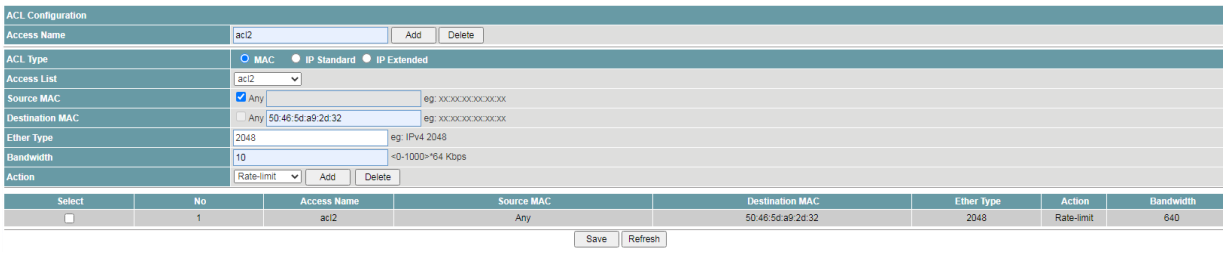
· Set aging time of dynamic MAC address:

Items	Descriptions	Default value
Aging Time	The aging time of dynamic MAC address. The value ranges from 10~1,000,000s.	300s

12.6 ACL Configuration

ACL (Access Control List) configuration enables users to define rules that filter and control network traffic based on criteria like source/destination IP addresses, ports, and protocols. ACLs help enforce security policies by permitting or denying specific types of traffic, such as allowing access to certain services while blocking unauthorized traffic. By configuring ACLs, users can enhance network security, manage bandwidth usage, and control access to resources. It is essential to understand ACL syntax and guidelines to effectively implement and maintain a secure and efficient network environment.

Users can view and modify ACL Configuration Setting as bellow.



Procedure

Choose < Security Configuration >< ACL Configuration > in the navigation tree to open the page.

1) Configure ACL Configuration firstly.

· Set the parameters as required.

Items	Descriptions	Default value
Access Name	Set the ACL Access name and the maximum character number is 5	Null

2) Configure ACL Configuration.

· Set the parameters as required.

Items	Descriptions	Default value
ACL Type	Set the ACL type as MAC/IP Standard/IP Extended	MAC
Access List	Set the ACL Access Name	autobind
When ACL Type = MAC		
Source MAC	Set the MAC as Any or specific MAC address by user	Null
Destination MAC	Set the MAC as Any or specific MAC address by user	Null
Ether Type	Set the value for Ether type	2048
Bandwidth	Set the value for the bandwidth when Action is set as Rate-limit. The value is from 0 to 1000. The unit is 64Kbps	Null
Action	Set the value as Permit/Deny/Rate-limit.	Deny
When ACL Type = IP Standard		
Source IP	Set the Source IP as Any or specific IP address by user	Null

Source Mask	Set the mask as specific IP mask address by user	Null
Bandwidth	Set the value for the bandwidth when Action is set as Rate-limit. The value is from 0 to 1000. The unit is 64Kbps	Null
Action	Set the value as Permit/Deny/Rate-limit.	Deny
When ACL Type = IP Extended		
IP Protocol Number	Set the IP protocol number and the value is from 0 to 255	Null
Source IP	Set the IP as Any or specific IP address by user	Null
Source Mask	Set the mask as specific IP mask address by user	Null
Source Port	Set the source port and the value from 0 to 65535	Null
Destination IP	Set the IP as Any or specific IP address by user	Null
Destination Mask	Set the mask as specific IP mask address by user	Null
Destination Port	Set the source port and the value from 0 to 65535	Null
Tos	Set the value as 2-Minimize-monet/4-Maximize-reliability/ 8-Maximize-Throuughput/16-Minimize-delay	Null
VLAN	Input the VLAN Range from 1 to 4094	Null
Precedence	Set the precedence and the value is from 1 to 7	
Bandwidth	Set the value for the bandwidth when Action is set as Rate-limit. The value is from 0 to 1000. The unit is 64Kbps	Null
Action	Set the value as Permit/Deny/Rate-limit.	Deny

- Click <Add> or <Delete>.

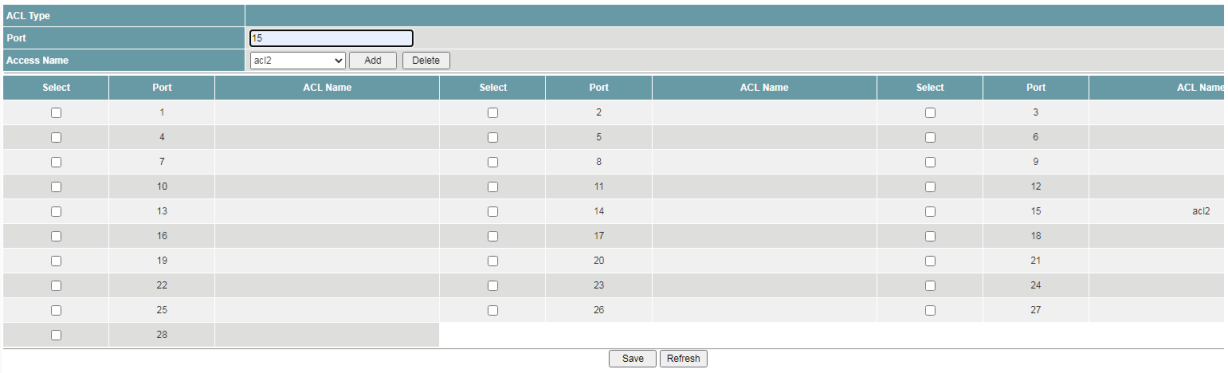
3) Save configurations and reload.

- Click <Save>.
- Click the <Refresh> button to reload the page.
- View the information.

12.7 Port ACL

Port ACL (Access Control List) functionality allows users to apply access control rules directly to switch ports. These rules filter incoming traffic based on criteria like source/destination IP addresses, ports, and protocols. Port ACLs provide granular control over network access at the port level, helping enforce security policies and mitigate potential threats. By configuring port ACLs, users can restrict unauthorized access, manage bandwidth usage, and enhance overall network security. It’s important to understand ACL syntax and guidelines to effectively implement and maintain a secure network environment using port ACLs.

Users can view and modify Port ACL Setting as bellow.



Procedure

Choose < Security Configuration >< Port ACL > in the navigation tree to open the page.

1) Set Access Name firstly.

Items	Descriptions	Default value
Access Name	Select the Access Name set in ACL Configuration	Null

2) Set the ACL configuration applied in the port

Items	Descriptions	Default value
Port	Input the ports numbers that need to be set. Multiple interfaces can be selected. Format as “2” or “1-5” or “3, 1-5” .	Null

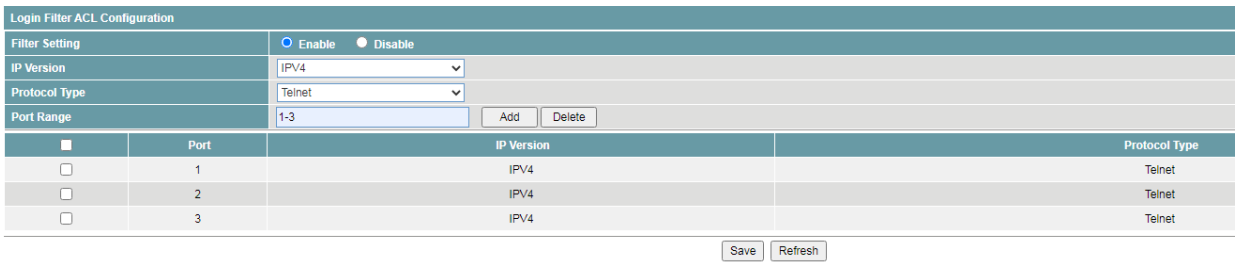
3) Save configurations and reload.

- Click <Save>.
- Click the <Refresh> button to reload the page.
- View the information.

12.8 Login Filter ACL

Login filter ACL (Access Control List) functionality allows users to define access rules for login attempts based on criteria like source IP type or protocol type. This feature enhances network security by filtering incoming login requests, allowing only authorized devices or users to access the switch for management purposes. By configuring login filter ACLs, administrators can prevent unauthorized access attempts, protect sensitive network configurations, and ensure a secure management environment. It’s crucial to understand ACL syntax and guidelines to effectively implement login filter ACLs and maintain a robust network security posture.

Users can view and modify Login Filter ACL Setting as bellow.



Procedure

Choose < Security Configuration >< Login Filter ACL > in the navigation tree to open the page.

1) Enable Login Filter function firstly.

Items	Descriptions	Default value
Filter Setting	Set the filter as Enable/Disable	Enable

2) Set Login Filter ACL Configuration.

Items	Descriptions	Default value
IP Version	Set the value as IPv4/IPv6	IPv4
Protocol Type	Set the value as telnet/ssh	telnet
Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. Format as “2” or “1-5” or “3, 1-5”.	Null

· Click <Add> or <Delete>.

3) Save configurations and reload.

· Click <Save>.

· Click the <Refresh> button to reload the page.

· View the information.

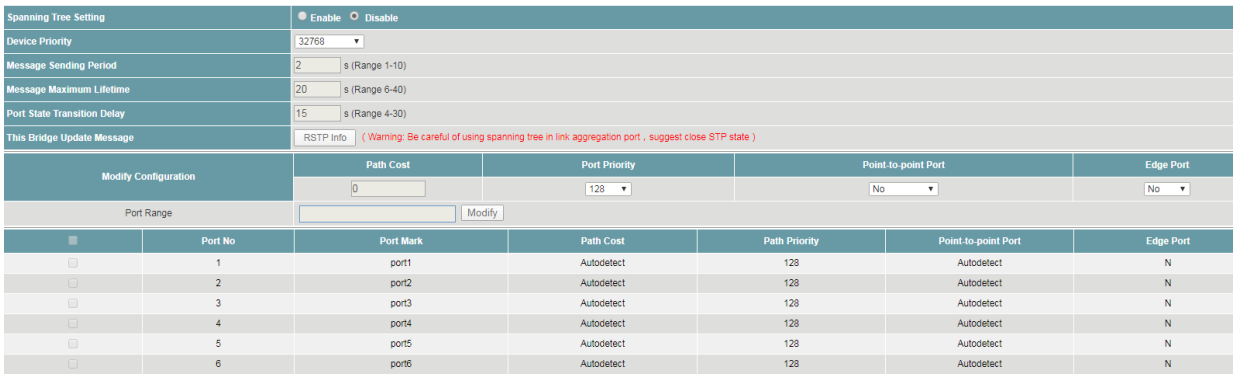
13 Reliability

13.1 Rapid Spanning Tree

RSTP is the abbreviation of Rapid Spanning Tree Protocol.

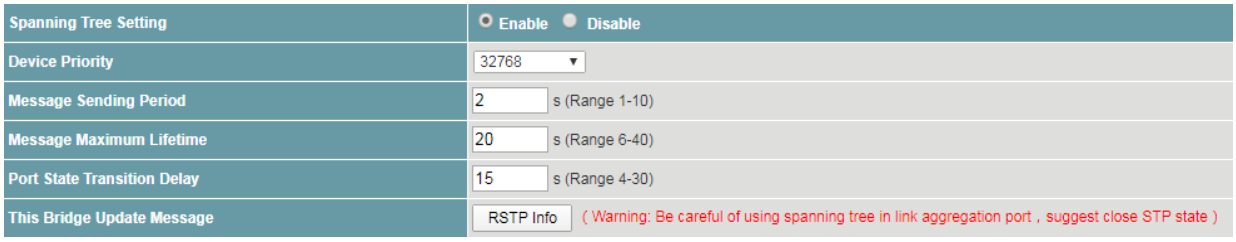
This protocol provides the same function as STP, and is completely backward compatible with 802.1D STP. Relative to the STP, the most important feature is "fast", if a LAN within the bridge are supported RSTP protocol, and the administrator configured properly, once the network topology changes, and to regenerate the topology tree only need not more than 1 second time (traditional STP takes about 50 seconds).

Users can configure global parameter and ports parameters of Rapid Spanning Tree.



Procedure

Choose <Reliability> <Rapid Spanning Tree> in the navigation tree to open the page.



1) Configure global parameters.

· Set the parameters as required.

Items	Descriptions	Default value
Spanning Tree Setting	Choose <Enable> to enable the function.	Disable
Device Priority	Choose the priority of the device. The lager number takes lower priority. Step length: 4096.	32768
Message Sending Period	Input the interval time to send message. The value ranges from 1 to 10.	2s
Message Maximum Lifetime	Input the maximum lifetime of the message. The value ranges from 6 to 40.	20s
Port State Transition Delay	Input the interval time of state transition delay for the ports. The value ranges from 4 to 30.	15s

- Click <RSTP Info>, view the current RSTP information for the bridge. Click <Close> to exit.

Spanning Tree>>RSTP Information

RSTP Information	Root Bridge Information
Device ID	
Root Bridge ID	
Root Port No	
Root Port Path Cost	

Port Information							
Port No	Priority	Path Cost	P2P	Edge	Neighbor Bridge	Port Role	Port State

Close

- Click <Modify>.
- Click <Save>.

2) Configure ports parameters.

Modify Configuration	Path Cost	Port Priority	Point-to-point Port	Edge Port
	0	128	No	No
Port Range		Modify		

- Set the parameters as required.

Items	Descriptions	Default value
Path Cost	Indicates the path cost of local port and target port. The value ranges from 0 to 200,000,000. 0 means auto detect. On an STP/RSTP network, the accumulated cost of path from a port to the root bridge consists of all path costs of ports on the passed bridges. This cost is called root path cost, which determines root port selection.	0
Port Priority	Choose the priority of the port. The lager number takes lower priority. Step length: 16.	128
Point-to-point Port	Choose the state of point-to-point, including · No. · Yes. · Auto Detect	No
Edge Port	Choose <Yes> to enable the edge port. Choose <No> to disable the edge port.	No
Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. The value ranges from 1~28. Format as “2” or “1-5” or “3, 1-5”.	Null

- Click <Modify>.
- Click <Save>.

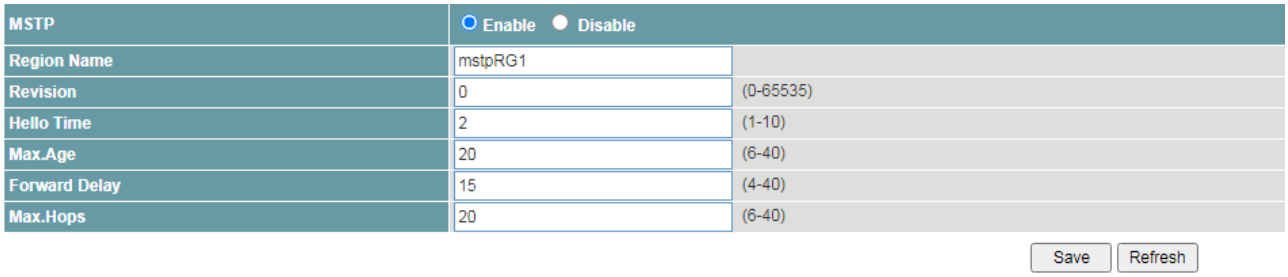
3) View the configuration.

- Click <Refresh> to reload the page.
- View the information.

13.2 MSTP Region Configuration

MSTP (Multiple Spanning Tree Protocol) region configuration on a switch allows users to group VL ANs into regions, optimizing network efficiency by reducing spanning tree instances and enhancing network stability and performance."

Users can view and modify MSTP Region Configuration as bellow.



Procedure

Choose < Reliability >< MSTP Region Configuration > in the navigation tree to open the page.

1) Enable MSTP firstly.

- Set the parameters as required.

Items	Descriptions	Default value
MSTP	Set the feature Enable/Disable	Disable

2) Configure MSTP Configuration.

- Set the parameters as required.

Items	Descriptions	Default value
Region Name	Set the region name for MSTP	
Revision	Set revision for MSTP. The value is from 0 to 65535	0
Hello Time	Set the time for hello message and the value is from 1 to 10	2
Max.Age	Set the maximum age timeout and the value is from 6 to 40.	20
Forward Delay	Set the forward delay time and the value is from 4 to 40	15
Max.Hops	Set the maximum hops and the value is from 6 to 40	20

- Click <Save>.

3) Save configurations and reload.

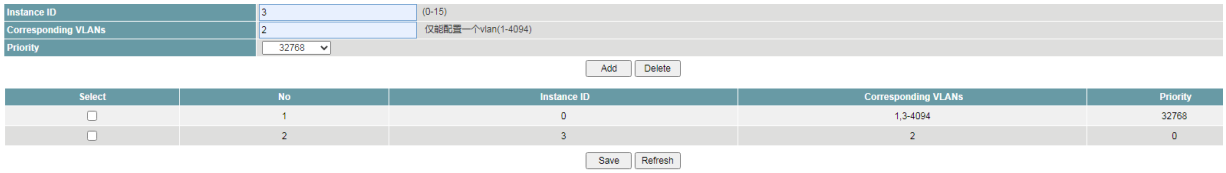
- Click <Save>.
- Click the <Refresh> button to reload the page.
- View the information.

13.3 MSTP Instance Configuration

MSTP (Multiple Spanning Tree Protocol) instance configuration on a switch enables users to create

multiple spanning tree instances within a network, providing segmentation and efficient management of traffic across VLANs, optimizing network performance, and ensuring redundancy and fault tolerance.

Users can view and modify MSTP Instance Configuration as bellow.



Procedure

Choose < Reliability >< MSTP Instance Configuration > in the navigation tree to open the page.

1) Configure MSTP Instance Configuration.

· Set the parameters as required.

Items	Descriptions	Default value
Instance ID	Set the instance ID and the value is from 0 to 15	Null
Corresponding VLANs	Set the related VLAN for the instance and the value is from 1 to 4094	Null
Priority	Set the priority for the instance and the value is listed from 0 to 61440	32768

· Click <Add> or <Delete>.

2) Save configurations and reload.

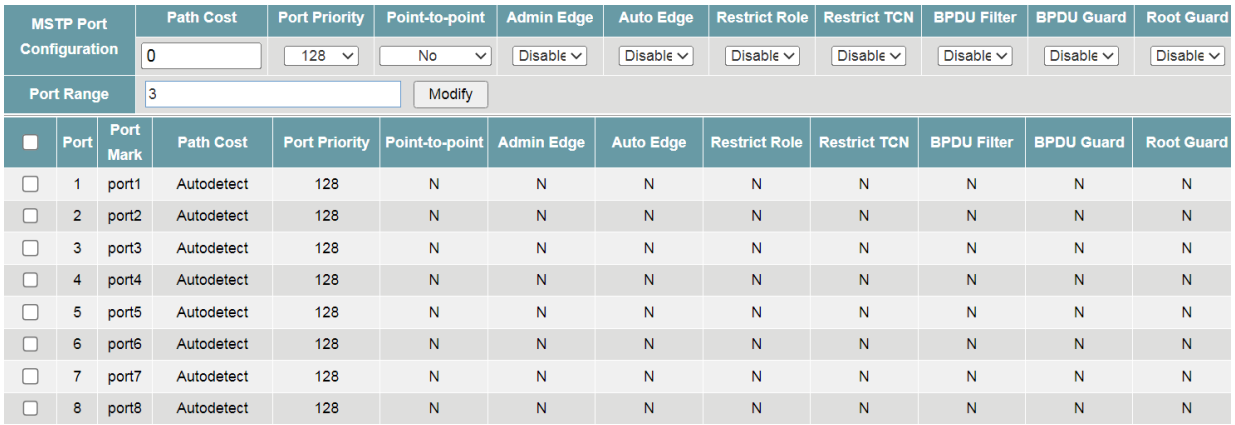
· Click <Save>.

· Click the <Refresh> button to reload the page.

13.4 MSTP Port Configuration

MSTP (Multiple Spanning Tree Protocol) port configuration on a switch allows users to designate ports as either edge or network ports, controlling how spanning tree operates and ensuring optimal traffic flow, loop prevention, and network stability within the spanning tree topology.

Users can view and modify MSTP Port Configuration as bellow.



☐	27	port27	Autodetect	128	N	N	N	N	N	N	N	N
☐	28	port28	Autodetect	128	N	N	N	N	N	N	N	N

Save Refresh

Procedure

Choose < Reliability >< MSTP Port Configuration > in the navigation tree to open the page.

1) Configure MSTP Port Configuration.

· Set the parameters as required.

Items	Descriptions	Default value
Path Cost	Set the path cost for MSTP port and the value is from 0 to 65535, Null. When the value is Null, it means auto detect.	0
Port Priority	Set the MSTP port priority and the value is from 0 to 240	128
Point-to-point	Set the point-to-point type of port as No/Yes/Auto Detect	No
Admin Edge	Set the admin edge of MSTP port as Disable/Enable	Disable
Auto Edge	Set the auto edge of MSTP port as Disable/Enable	Disable
Restrict Role	Set the restrict role of MSTP port as Disable/Enable	Disable
Restrict TCN	Set the restrict TCN of MSTP port as Disable/Enable	Disable
BPDU Filter	Set the BPDU filter of MSTP port as Disable/Enable	Disable
BPDU Guard	Set the BPDU guard of MSTP port as Disable/Enable	Disable
Root Guard	Set the root guard of MSTP port as Disable/Enable	Disable
Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. Format as “2” or “1-5” or “3, 1-5”.	Null

· Click <Add> or <Delete>.

2) Save configurations and reload.

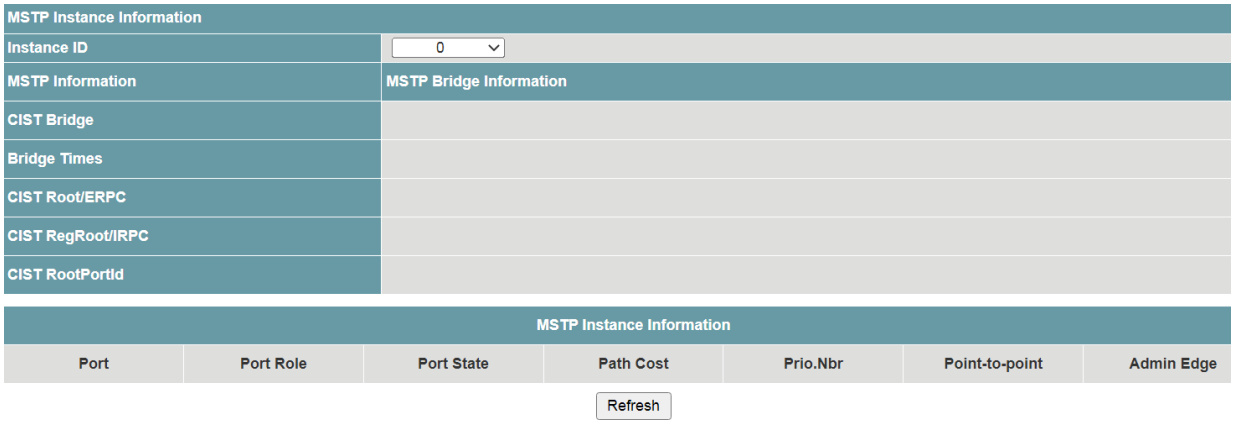
· Click <Save>.

· Click the <Refresh> button to reload the page.

13.5 MSTP Instance Information

The function to query MSTP (Multiple Spanning Tree Protocol) instance information on a switch allows users to retrieve details such as instance ID, VLAN mapping, port status, and priority settings etc. This information aids in monitoring network topology, troubleshooting spanning tree issues, and ensuring optimal configuration for efficient and stable network operation.

Users can view MSTP Instance Information Setting as bellow.



MSTP Instance Information	
Instance ID	0
MSTP Information	MSTP Bridge Information
CIST Bridge	
Bridge Times	
CIST Root/ERPC	
CIST RegRoot/IRPC	
CIST RootPortId	

MSTP Instance Information						
Port	Port Role	Port State	Path Cost	Prio.Nbr	Point-to-point	Admin Edge

Refresh

Procedure

Choose < Reliability >< MSTP Instance Information > in the navigation tree to open the page.

1) Configure MSTP Instance Information.

· Set the parameters as required.

Items	Descriptions	Default value
Instance ID	Set the instance ID and the value is from 0 to 15.	0

2) Check information.

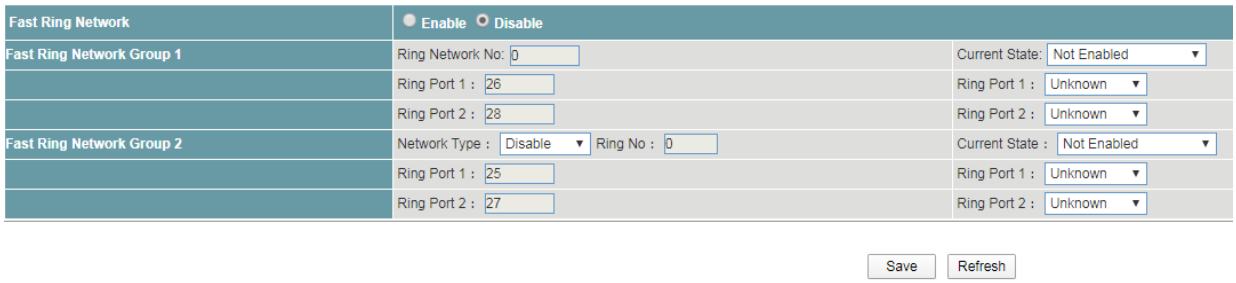
· Click the <Refresh> button to reload the page.

· View the information.

13.6 Fast-Ring Protect

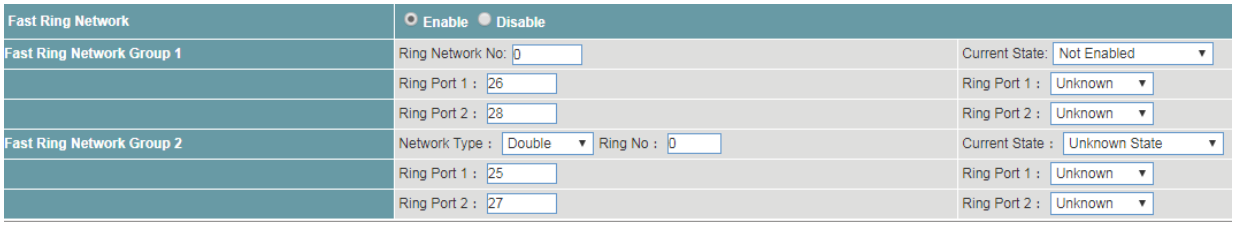
Users can configure the Fast-Ring protect function of the device. Fast Ring is a private protocol applied on Ethernet loop protection to provide fast recovery switching for Ethernet traffic in ring topology.

Fast Ring provides a faster redundant recovery than spanning tree topology. The action is similar to STP or RSTP, but the algorithms between them are not the same. In the ring topology, every switch should support fast ring and be enabled with Fast Ring and two ports should be assigned as the member ports in the fast ring group. When the failure of network connection occurs, the traffic will go through via the backup link.



Procedure

Choose <Reliability> <Fast-Ring Protect> in the navigation tree to open the page.



1) Configure the Fast-Ring protect.

· Set the parameters as required.

Items	Descriptions	Default value
Fast-Ring Network	Choose <Enable> to enable the function.	Disable
Fast-Ring Network Group 1		
Ring Network No:	Indicates the number of main ring network the device accesses.	0

	The value ranges from 0 to 255.	
Ring Port 1：	Indicates the port number that access the ring network. The value ranges from 1 to 28.	26
Ring Port 2：	Indicates the port number that access the ring network. The port number can't be the same if it is used in other ring network. The value ranges from 1 to 28.	28
Current State:	Actual status of the ring network group 1. This parameter is not able to be set.	Not Enabled
Ring Port 1：	Actual port number that being accessing the network. This parameter is not able to be set.	Unknown
Ring Port 2：	Actual port number that being accessing the network. This parameter is not able to be set.	Unknown
Fast-Ring Network Group 2		
Network Type：	Choose the network type of the sub ring network, including · Double · Coupling Click <Disable>, the function of sub ring network is disabled.	Disable
Ring No：	Indicates the number of sub ring network the device accesses. The value ranges from 0 to 255.	0
Ring Port 1：	Indicates the port number that access the ring network. The value ranges from 1 to 28.	25
Ring Port 2：	Indicates the port number that access the ring network. The port number can't be the same if it is used in other ring network. The value ranges from 1 to 28.	27
Current State：	Actual status of the ring network group 2. This parameter is not able to be set.	Not Enabled
Ring Port 1：	Actual port number that being accessing the network. This parameter is not able to be set.	Unknown
Ring Port 2：	Actual port number that being accessing the network. This parameter is not able to be set.	Unknown

· Click <Save>.

2) View the current status of Fast-Ring protection.

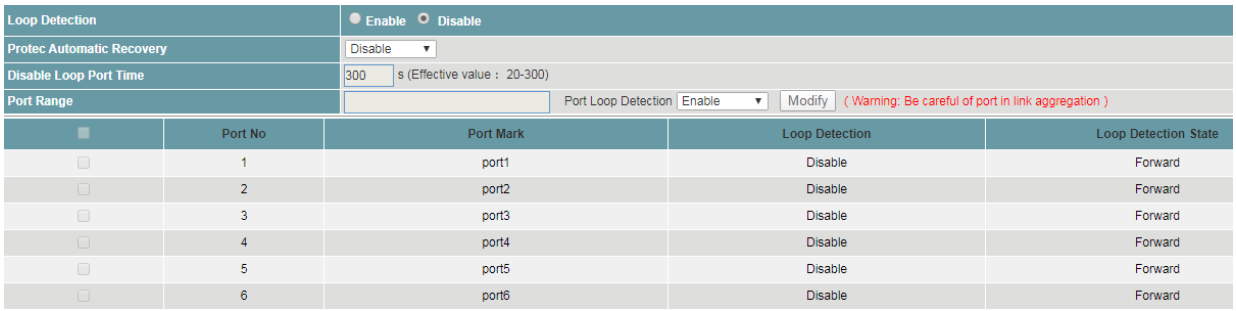
· Click <Refresh> to reload the page.

· View the current state information.

13.7 Loopback Protect

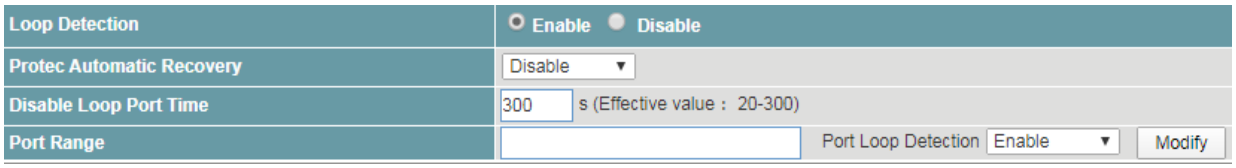
The device supports loopback protection function.

While the function is turned on, users can check if there is a Loopback for the device under this port. If there is Loopback, the port will be shutdown.



Procedure

Choose <Reliability> <Loopback Protect> in the navigation tree to open the page.



1) Configure the loopback function.

· Set the parameters as required.

Items	Descriptions	Default value
Loop Direction	Choose <Enable> to enable the loopback detection function for the device.	Enable
Protect Automatic Recovery	Choose <Enable> to enable the protection automatic recovery function. The ports will be recovered automatically.	Disable
Disable Loop Port Time	Indicate the disable loop protect time. The port will be recovered automatically, if the port detection no loopback packet after the time range, when <Protect Automatic Recovery> is enable. The port will keep shutdown, if the port detection no loopback packet after the time range, when <Protect Automatic Recovery> is disable. The value ranges from 20 to 300s.	20s
Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. The value ranges from 1~28. Format as “2” or “1-5” or “3, 1-5”.	Null
Port Loop Detection	The device supports to enable or disable the loopback function of each port. Choose <Enable> to enable the function of the ports needed to be set.	Enable

· Click <Modify>.

· Click <Save>.

2) View the loopback protect information.

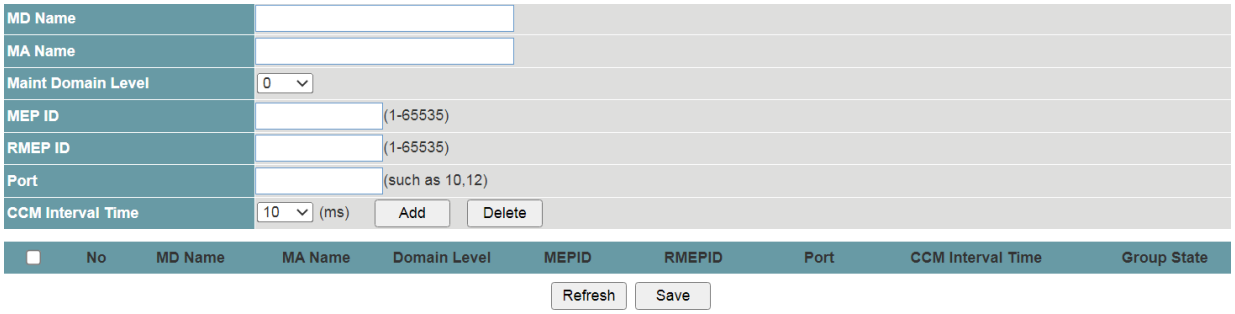
· Click <Refresh> to reload the page.

· View the information.

13.8 CCM

CCM (Continuous Connectivity Monitoring) is a vital feature that ensures seamless network operation. It constantly monitors the connectivity status between network devices, such as switches, and endpoints, detecting failures or disruptions in real-time. CCM actively verifies link integrity, preventing network loops and downtime by promptly isolating faulty connections. This proactive approach enhances network reliability, reduces downtime, and maintains uninterrupted data transmission, critical for efficient network management.

Users can view and modify CCM Setting as bellow.



Procedure

Choose < Reliability >< CCM > in the navigation tree to open the page.

1) Configure CCM function

· Set the parameters as required.

Items	Descriptions	Default value
MD Name	Set the name for MD and the value is string	Null
MA Name	Set the name for MA and the value is string	Null
Maintenance Domain Level	Set the MD level and the value is from 0 to 7	00
MEP ID	Set the MEP ID and the value is from 1 to 65535	Null
RMEP ID	Set the remote MEP ID and the value is from 1 to 65535	Null
Port Range	Input the ports numbers that need to be set. Multiple interfaces can be selected. The value ranges from 1~28. Format as “2” or “1-5” or “3, 1-5”.	Null
CCM Interval Time	Specify the CCM interval time and the value is 10ms/100ms/1000ms/10000ms	10

· Click <Add> or <Delete>.

2) View the VRRP configuration.

· Click <Save> to save the page

· Click <Refresh> to reload the page.

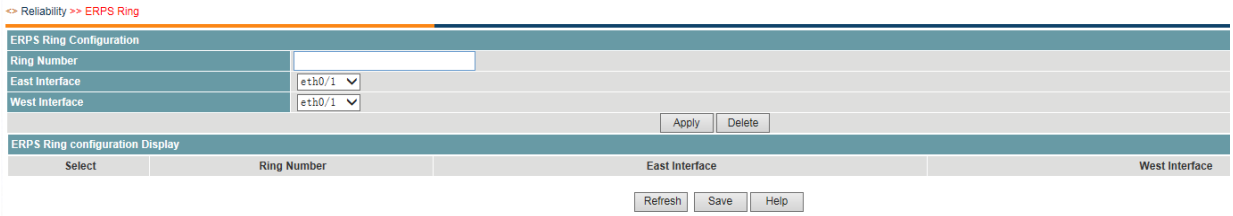
· View the information.

13.9 ERPS Ring

Ethernet Ring Protection Switching (ERPS) is defined in ITU-T G.8032 Recommendation. It prevents logical loops on a ring network by blocking redundant links.

ERPSv1 supports only the single-ring topology. When there is no faulty link on a ring network, ERPS can eliminate loops on the network. When a link fails on the ring network, ERPS can immediately restore the communication between the nodes on the network. Compared with other ring network protocols, ERPS has the following advantages:

- The network converges fast.
- ERPS is a standard protocol published by the ITU-T; therefore devices from different vendors can communicate with each other when they run ERPS.
- ERPS works for ERPS rings. An ERPS ring consists of interconnected Layer 2 switching devices configured with the same control VLAN and data VLAN. Logically, an ERPS ring is a necessity before you configure other related functions.



Procedure

Choose <Reliability> <ERPS Ring> in the navigation tree to open the page.

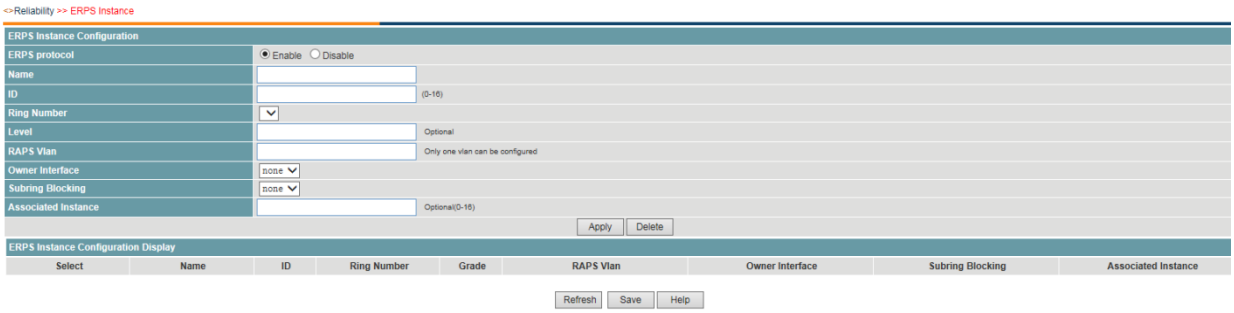
- Create an ERPS Ring.

Items	Descriptions	Default value
Ring Number	Input the number of ERPS Ring. The value ranges from 1 to 16.	Null
East Interface	Select the interface that in the ERPS Ring.	Null
West Interface	Select the interface that in the ERPS Ring.	Null

- Click <Save>.

13.10 ERPS Instance

The VLAN in which ERPS PDUs and data packets are transmitted must be mapped to a protected instance so that ERPS forwards or blocks the packets based on rules. If the mapping is not performed, the preceding packets may cause broadcast storms on the ring network, leading to the network failure.



Procedure

Choose <Reliability> <ERPS Instance> in the navigation tree to open the page.

- Configure the ERPS instance as required.

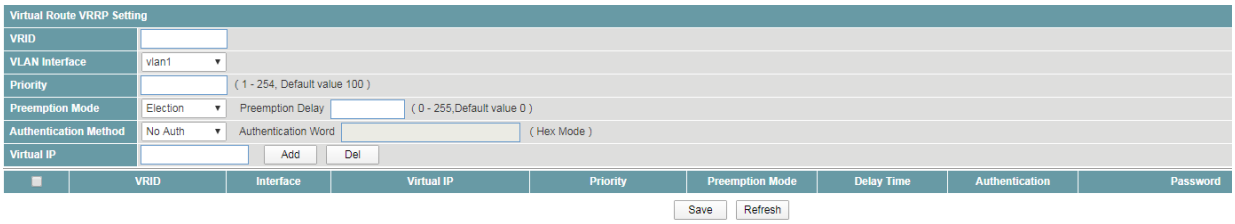
Items	Descriptions	Default value
ERPS Protocol	Choose <Enable> to enable the loopback detection function for the device.	Null

Name	Name the ERPS instance.	Null
ID	Input the ID of the ERPS instance.	Null
Ring Number	Choose the number of the ERPS Ring that the instance linking with.	Null
Level	Define the ERPS Ring level. This parameter is optional.	Null
RAPS VLAN	Configure the control VLAN of the ERPS Ring. The RAPS VLAN specified here must be a VLAN that has not been created or used.	Null
Owner Interface	Choose the owner interface of the ERPS Ring. The link where the RPL Owner port resides is a ring protection link. An ERPS ring has only one RPL Owner interface. Blocking the RPL Owner interface prevents loops in the ERPS ring.	None
Subring Blocking	Select the subring of the ERPS Ring. The protecting instance of the subring is 0 in default.	None
Associating Instance	Define the associating ERPS interface of subring. This parameter is optional.	Null

· Click <Save>.

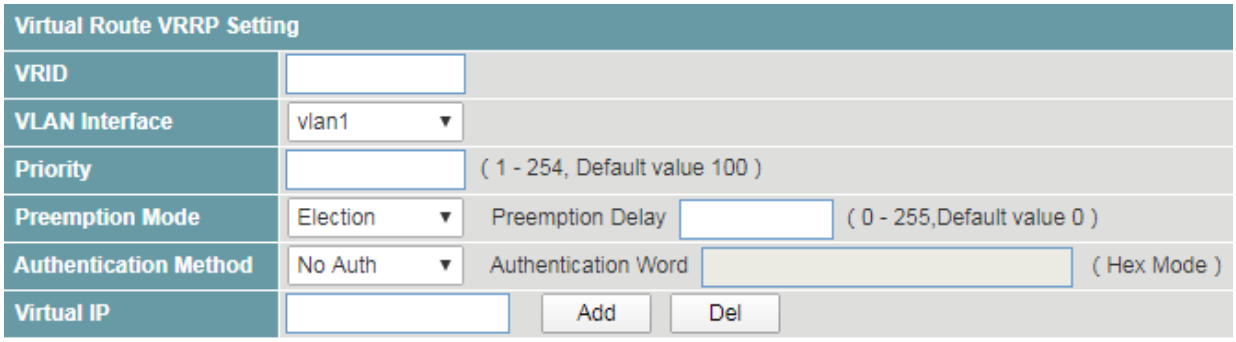
13.11 VRRP Setting

The Virtual Router Redundancy Protocol (VRRP) groups multiple routing devices into a virtual router. One device functions as the master, and the others as the backup devices. When the next hop device of the master device fails, VRRP switches services to a backup device. This implementation ensures nonstop service transmission and reliability.



Procedure

Choose <Reliability> <VRRP Setting> in the navigation tree to open the page.



1) Configure VRRP

· Set the parameters as required.

Items	Descriptions	Default value
VRID	Input the virtual router ID. The value ranges from 1 to 255.	Null
VLAN Interface	Choose the primary IP address. It is selected from one of actual IP addresses of interfaces. Usually, it is the first configured IP address. The primary IP address is often used as the source IP address for VRRP broadcast packets.	VLAN1
Priority	Input the priority of a VRRP router. The virtual router selects the master and backup devices based on the priority. The value ranges from 1 to 254.	100
Preemption Mode	Choose the preemption mode, including · Election · No Election	Election
Preemption Delay	Input the time of preemption delay.	0
Authentication Method	Choose the type of authentication method, including · Plaintext Key · MD5 Key Choose <No Auth> to disable the authentication function.	No Auth
Authentication Word	Input the authentication key.	Null
Virtual IP	Input the IP address of virtual router. A virtual router can be assigned one or more virtual IP addresses. Virtual IP addresses are configurable.	Null

· Click <Save>.

2) View the VRRP configuration.

· Click <Refresh> to reload the page.

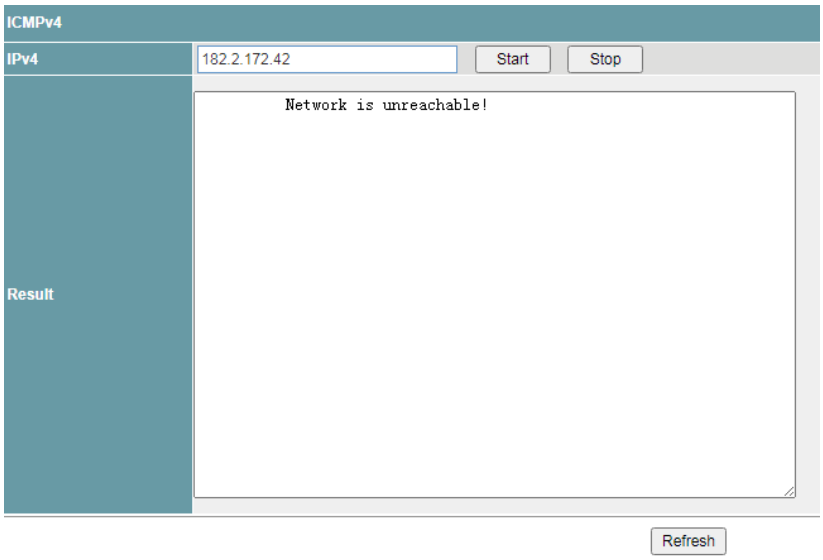
· View the information.

14 Network Diagnosis

14.1 ICMPv4

ICMPv4 (Internet Control Message Protocol version 4) enables network diagnostics by sending echo requests and receiving echo replies. It verifies device connectivity, troubleshoots network issues, and assesses packet delivery, aiding in network monitoring and management.

Users can start a V4 ping operation as bellow.



Procedure

Choose < Network Diagnosis >< ICMPv4 > in the navigation tree to open the page.

1) Configure ICMPv4 function

· Set the parameters as required.

Items	Descriptions	Default value
IPv4	Set the IPv4 Address. The format is A:B:C:D	Null

· Click <Start> and <Stop>.

2) Check result and reload.

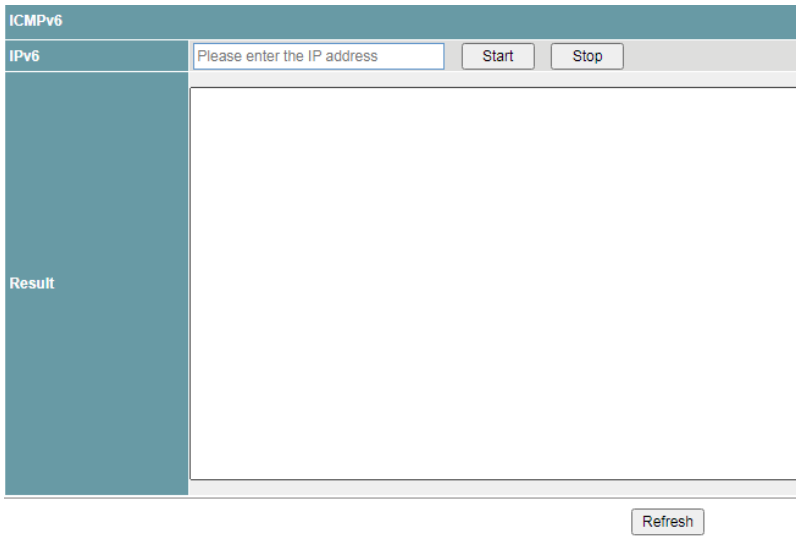
· Click the <Refresh> button to reload the page.

· View the information.

14.2 ICMPv6

ICMPv6 (Internet Control Message Protocol version 6) facilitates network diagnostics and management by sending ICMPv6 messages. It verifies device connectivity, assesses packet delivery, and troubleshoots network issues like IPv6 address configuration and reachability, aiding in efficient network monitoring and maintenance.

Users can start a V6 ping operation as bellow.



Procedure

Choose < Network Diagnosis >< ICMPv6 > in the navigation tree to open the page.

1) Configure ICMPv6 function

· Set the parameters as required.

Items	Descriptions	Default value
IPv6	Set the IPv6 Address. The format is x:x:x:x:x:x:x:x	Null

· Click <Start> and <Stop>.

2) Check result and reload.

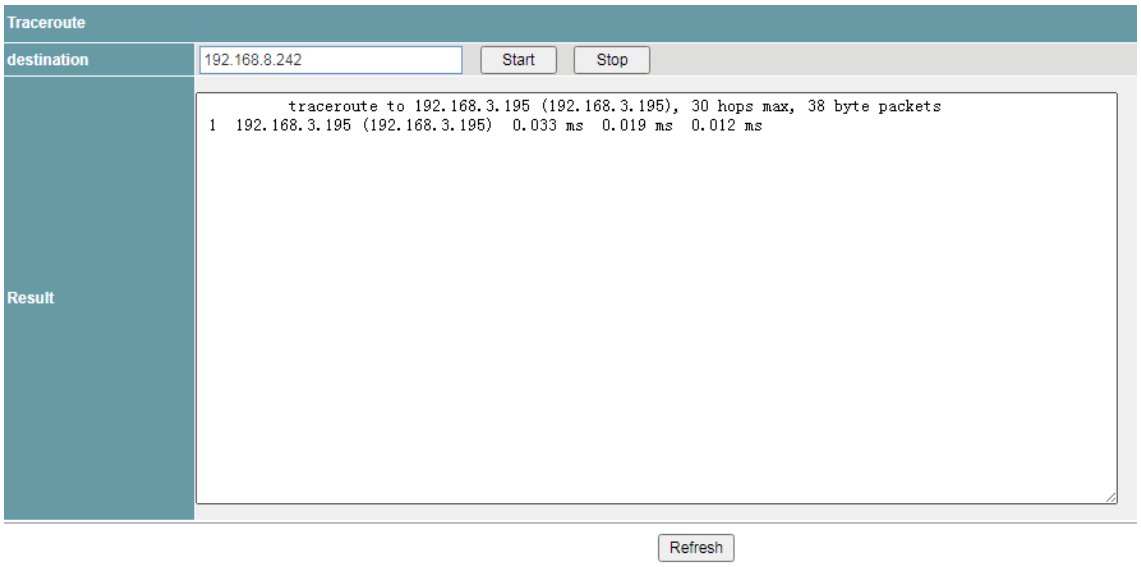
· Click the <Refresh> button to reload the page.

· View the information.

14.3 Traceroute

Traceroute is a diagnostic tool that traces the path packets take through a network. It identifies network hops, measures latency, and identifies connectivity issues, helping troubleshoot and optimize network performance. Traceroute aids in understanding network topology and locating bottlenecks for efficient troubleshooting.

Users can view and modify Traceroute Setting as bellow.



Procedure

Choose < Network Diagnosis >< Traceroute > in the navigation tree to open the page.

1) Configure Traceroute function

· Set the parameters as required.

Items	Descriptions	Default value
Destination	Set the IPv6 Address. The format is x:x:x:x:x:x:x:x or Set the IPv4 Address. The format is A:B:C:D	Null

· Click <Start> and <Stop>.

2) Check result and reload.

· Click the <Refresh> button to reload the page.

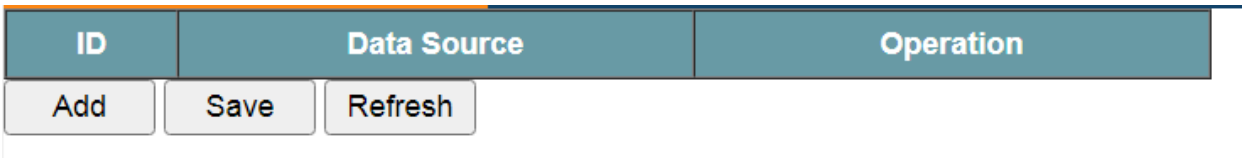
· View the information.

15 RMON

User can specify statistics, history counter, alarm, events and logs configuration for MIB object via OID and get those data/information on specific OID.

15.1 Statistics Config

Users can view and modify Statistics Config Setting as bellow.



Procedure

Choose < RMON >< Statistics Config > in the navigation tree to open the page.

1) Configure Statistics Config Configuration.

· Click <Add>.

· Set the parameters as required.

Items	Descriptions	Default value
ID	Input the ports numbers that need to be set. Multiple interfaces can be selected. Format as “2” or “1-5” or “3, 1-5” .	Null
Data Source	Set the OID of MIB object.	0

2) Save configurations and reload.

· Click <Save>.

· Click the <Refresh> button to reload the page.

· View the information.

15.2 Statistics Status

Users can view Statistics Status as bellow.

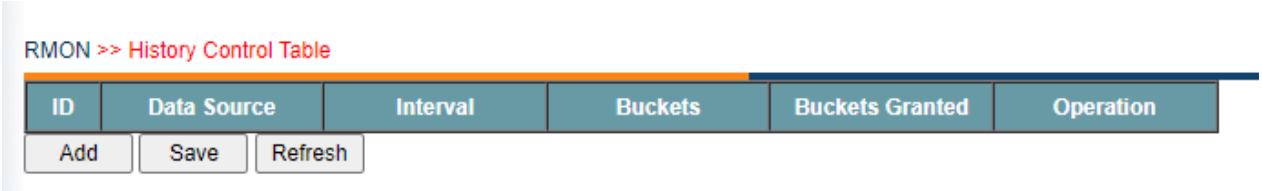
Procedure

Choose < RMON >< Statistics Status > in the navigation tree to open the page.

Only provide review function.

15.3 History Control Table

Users can view and modify History Control Table Setting as bellow.



Procedure

Choose < RMON >< History Control Table > in the navigation tree to open the page.

1) Configure History Control Table Configuration.

· Click <Add>.

· Set the parameters as required.

Items	Descriptions	Default value
ID	Input the ports numbers that need to be set. Multiple interfaces can be selected. Format as "2" or "1-5" or "3, 1-5".	Null
Data Source	Set the OID of MIB object. The value is from 1 to 28	0
Interval	Set the interval time and the value is from 1 to 3600	1800
Buckets	Set the buckets and the value is from 1 to 65535	50

· Click <Enter>.

2) Save configurations and reload.

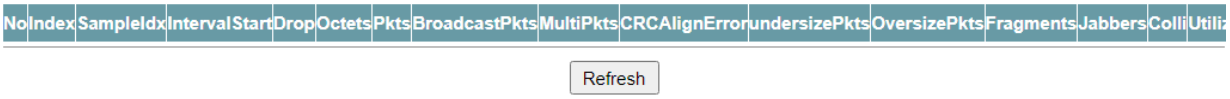
· Click <Save>.

· Click the <Refresh> button to reload the page.

· View the information.

15.4 Ether History Table

Users can view Ether History Table Setting as bellow.



Procedure

Choose < RMON >< Ether History Table > in the navigation tree to open the page.

Only provide review function.

15.5 Alarm Table

Users can view and modify Alarm Table Setting as bellow.

Procedure

Choose < RMON >< Alarm Table > in the navigation tree to open the page.

1) Configure Alarm Table Configuration.

- Click <Add>.
- Set the parameters as required.

Items	Descriptions	Default value
ID	Input the ID from 1 to 100	Null
Interval	Set the interval time and the value is from 1 to 3600	Null
Port	Input the ports numbers that need to be set. Multiple interfaces can be selected. Format as “2” or “1-5” or “3, 1-5”.	Null
Object	Set the object to support RMON	RMONDropEvents
Sample Type	Set Sample type as Absolute/Delta	Absolute
Value	Indicate the value for the object.	0
Rising Threshold	Set the rising threshold for the object	Null
Rising Index	Set the rising index and the value is from 1 to 100	Null
Falling Threshold	Set the falling threshold for the object	Null
Falling Index	Set the falling index and the value is from 1 to 100	Null

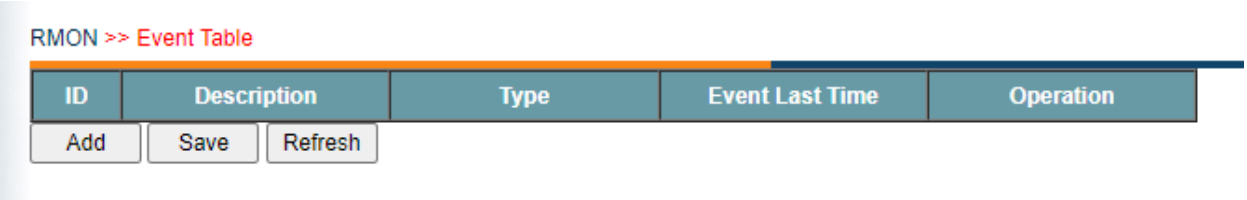
- Click <Enter>.

2) Save configurations and reload.

- Click <Save>.
- Click the <Refresh> button to reload the page.
- View the information.

15.6 Event Table

Users can view and modify Event Table Setting as bellow.



Procedure

Choose < RMON >< Event Table > in the navigation tree to open the page.

1) Configure Event Table Configuration.

- Click <Add>.
- Set the parameters as required.

Items	Descriptions	Default value
ID	Input the ID from 1 to 100	Null
Description	Set the description for the event	Null
Type	Set type for the event and the value can be none/log/snmp trap/logandtrap	None

Event Last Time	Indicate the even happening time	Null

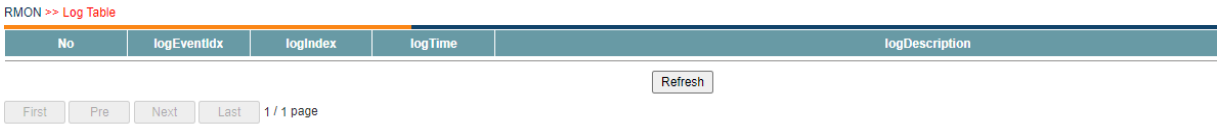
- Click <Enter>.

2) Save configurations and reload.

- Click <Save>.
- Click the <Refresh> button to reload the page.
- View the information.

15.7 Log Table

Users can view Log Table Setting as bellow.



Procedure

Choose < RMON >< Log Table > in the navigation tree to open the page.

Only provide review function for Log descriptions.

16 DMS

16.1 Device List

The Device list in DMS (Dashboard Management System) function automatically discovers the devices on the network and show in the list.

Procedure

Choose <DMS>< Device List> in the navigation tree to open the page.

1) Choose <Enable> to enable the function.
2) Click<ALL><Switch ><IPC><Others> to filtrate the device type which show in the list.
3) Click <Save>.
4) View the device topography.

- Click <Refresh> to reload the page.
- View the information.

16.2 Topology View

The Topology View function automatically discovers the devices on the network and forms the topography view.

17 System Management

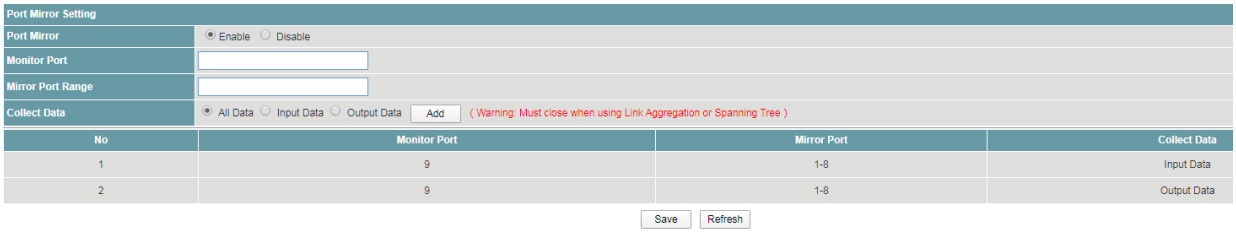
17.1 Port mirroring

Packet mirroring copies the packets on a mirrored port (source port) to an observing port (destination port).

During network maintenance, maintenance personnel need to capture and analyze packets (for example, when there are suspicious attack packets). However, these operations always affect packet forwarding.

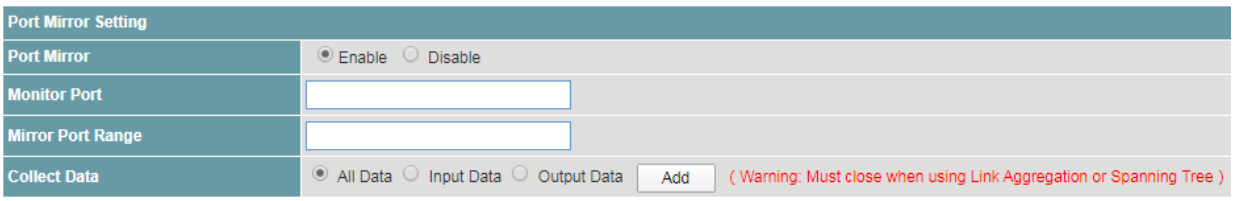
Packet mirroring copies packets on a mirrored port to an observing port so that users can analyze packets copied to the destination port by a monitoring device to monitor the network and rectify faults.

Users can configure the source interface and target interface of mirror. The function supports 1 to 1 and many to 1 modes.



Procedure

Choose <System Management> <Port mirroring> in the navigation tree to open the page.



1) Configure the port mirroring function.

· Set the parameters as required.

Items	Descriptions	Default value
Port mirror	Choose <Enable> to enable the function.	Disable
Monitor Port	Indicate the monitor port number. The value ranges from 1 to 28.	Null
Mirror Port Range	The port number range of mirror ports, Multiple ports can be selected. The value ranges from 1~28. Format as “2” or “1-5” or “3, 1-5”.	Null
Collect Data	The packets that the need to be copied and monitored on the mirrored ports, including · All data · Input data · Output data	All data

· Click <Modify>.

· Click <Save>.

2) View the port mirroring configuration.

· Click <Refresh> to reload the page.

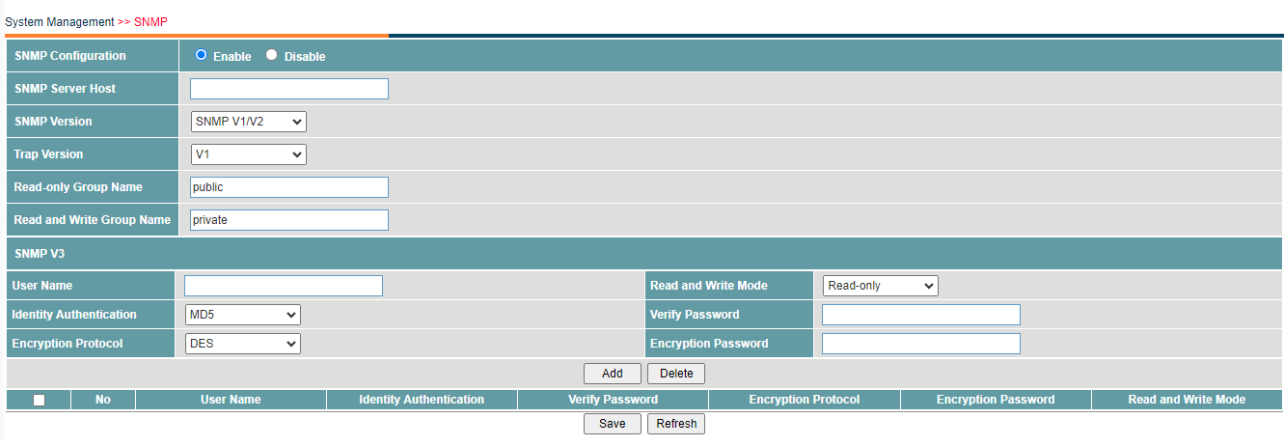
· View the information.

17.2 SNMP

As a network management standard protocol used on TCP/IP networks, SNMP uses a central computer (NMS) that runs network management software to manage network elements.

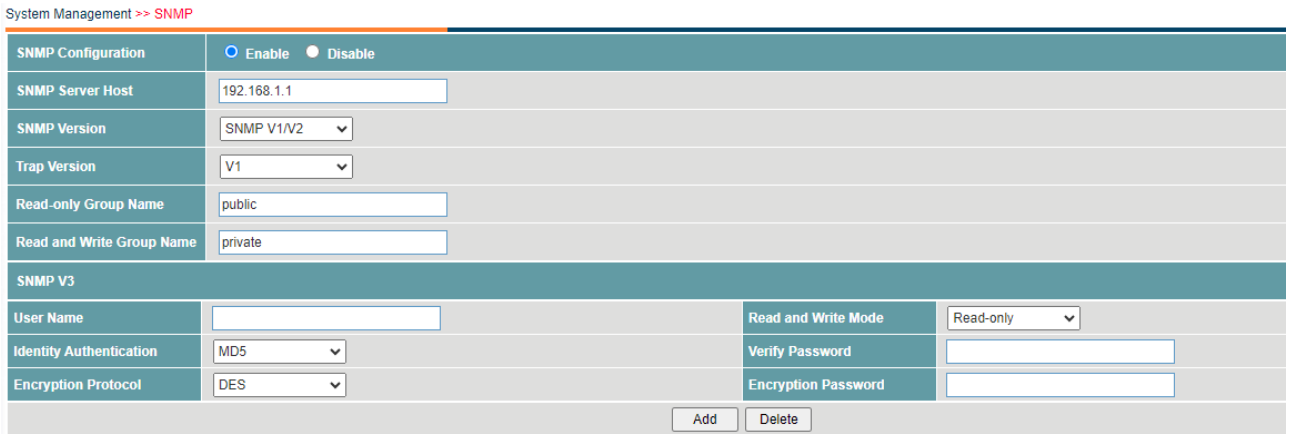
In a large network, it is very difficult for network administrator to detect, locate and rectify the fault as the devices does not report the fault. This affects maintenance efficiency and increases maintenance workload. To solve this problem, equipment vendors have provided network management functions in some products. The NMS then can query the status of remote devices, and devices can send traps to the NMS in the case of particular events.

Users can configure the function of the SNMP community permission and SNMP V3.



Procedure

Choose <System Management> <SNMP> in the navigation tree to open the page.



1) Configure SNMP community permission.

· Set the parameters as required.

Items	Descriptions	Default value
SNMP Configuration	Choose <Enable> to enable the function.	Disable
SNMP Gateway	Input the IP address of the server.	Null
SNMP Version	Choose the SNMP version, including · SNMP V1 · SNMP V2	SNMP V2
Read-only Group Name	Indicate the name of SNMP community for read-only permission. The value supports strings.	public
Read and Write Group Name	Indicate the name of SNMP community for read and write permission. The value supports strings.	private

· Click <Save>.

2) Configure SNMP V3

· Set the parameters as required.

Items	Descriptions	Default value
User name	Indicates the user name. The value supports 31 stings	Null
Read and Write Mode	Choose the read and write mode, including · Read-only · Read and Write	Read-only
Identity Authenticatio n	Choose the identity authentication, including · MD5 · SHA	MD5
Verify Password	Indicates the Authentication password, supporting 8-32 digits strings.	Null

Encryption Protocol	Choose the Encryption Protocol, including · DES · AES · 3DES	DES
Encryption Password	Indicates the Encryption password, supporting 8-32 digits strings.	Null

· Click <Save>.

3) View SNMP configuration.

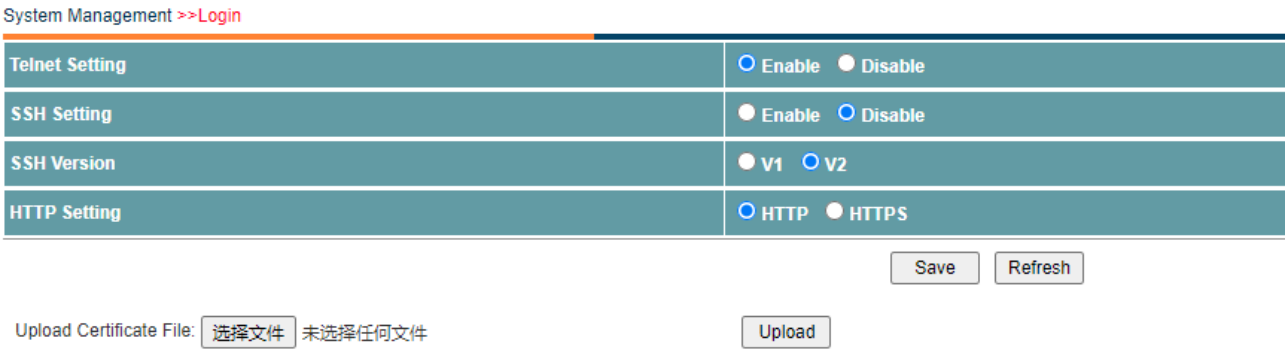
· Click <Refresh> to reload the page.

· View the information.

17.3 Login

User authentication enables configuration access via Telnet, SSH, and HTTP. These protocols provide secure remote management, ensuring authorized users can configure and manage network settings efficiently.

Users can modify Login Setting as bellow.



Procedure

Choose < System Management >< Login > in the navigation tree to open the page.

1) Configure Login.

· Set the parameters as required.

Items	Descriptions	Default value
Telnet Setting	Set the feature as Enable/Disable	Enable
SSH Setting	Set the feature as Enable/Disable	Disable
SSH Version	Set the version as v1/v2	V2
Https Setting	Set the HTTP or HTTPs	HTTP

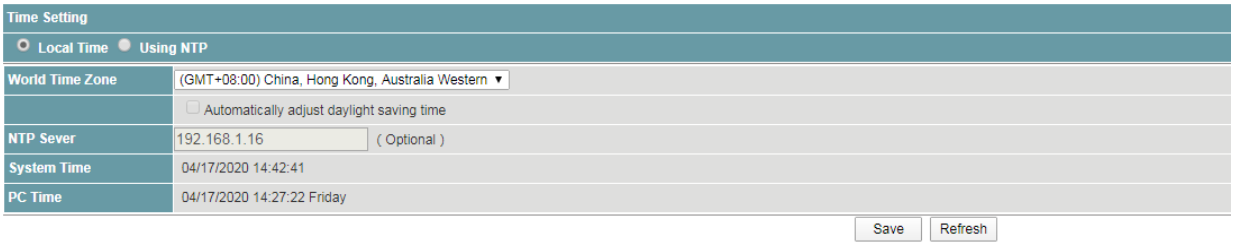
· Click <Save>.

2) For SSH Enabled or HTTPs, Select certificate file and upload.

17.4 Time

Users can set time of the device by choosing local time or NTP server.

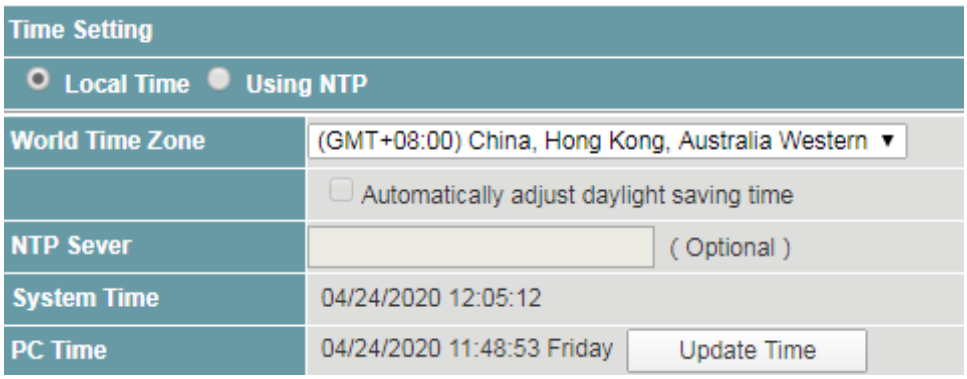
By default the device supports local time setting.



Procedure

Choose <System Management> <Time> in the navigation tree to open the page.

1) Local time.

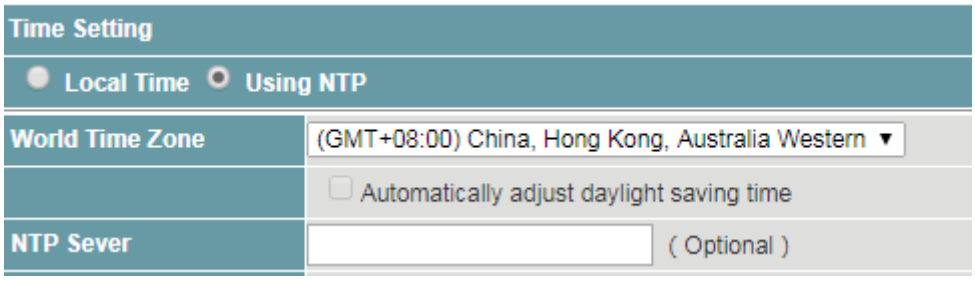


· Set the parameters as required.

Items	Descriptions	Default value
World Time Zone	Choose time zone in drop down list.	
System Time	Display the current time of the system.	-
PC Time	Display the current time of management PC.	-
Update Time	Click to update the <System Time> to synchronize with the <PC Time>.	-

· Click <Save>.

2) Using NTP.



· Choose <Using NTP>.

· Set the parameters as required.

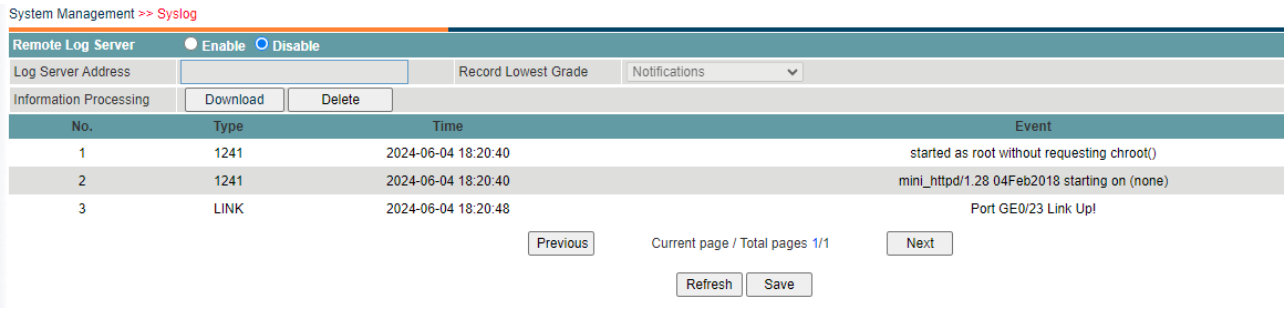
Items	Descriptions	Default value
NTP Server	Input the IP address of NTP server.	Null

· Click <Save>.

17.5 Syslog

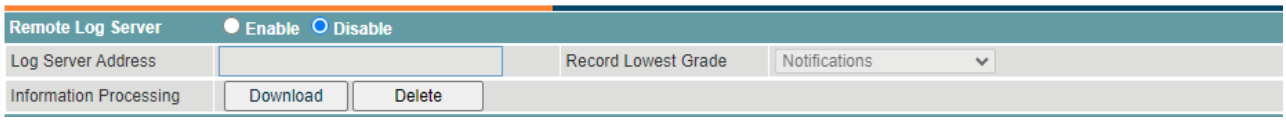
Users can view, download and clear the system log, including

- Operation information
- Network link
- Warning information



Procedure

Choose <System Management> <Syslog> in the navigation tree to open the page.



1) Configure system log function.

- Set the parameters as required.

Items	Descriptions	Default value
Remote Log Server	Choose <Enable> to enable the function.	Disable
Log Server Address	Set the IP address as Log Server Address	Null
Show type	Choose the contents of the system log, including · Errors · Informational · Alerts · Critical · Emergencies · Notifications · Debugging · Warnings	Notifications

- Click <Refresh>.

2) Clear the system log records.

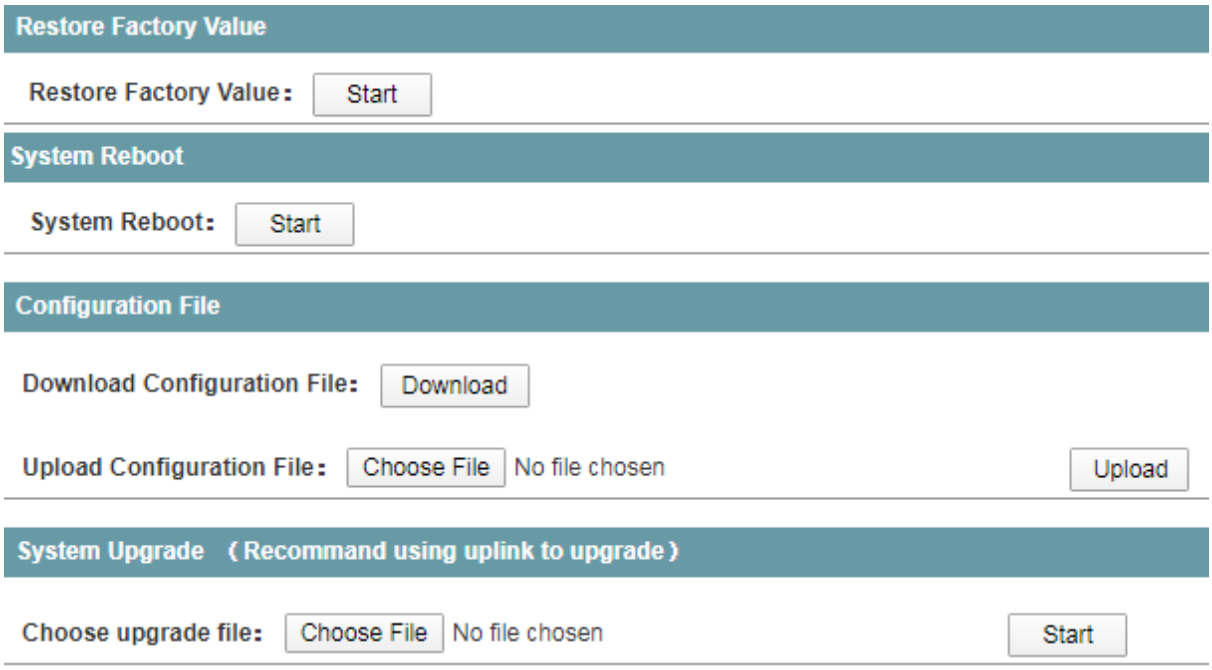
- Click <Delete> to delete the displayed log.
- Click <Refresh>.

3) Download the system log records.

- Click <Download > to download the displayed log.

17.6 Management

Users can restore the factory value, reboot the system, download the actual configuration file, upload configuration file, and upgrade the software version.

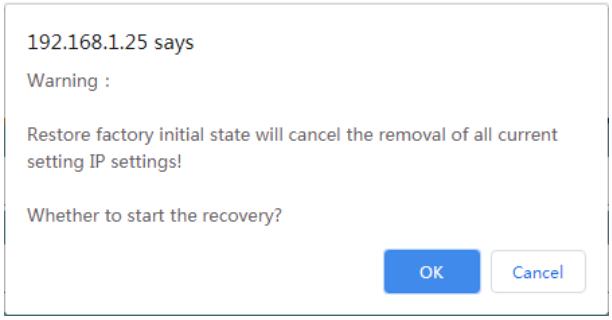


Procedure

Choose <System Management> <Management> in the navigation tree to open the page.

1) Restore factory value.

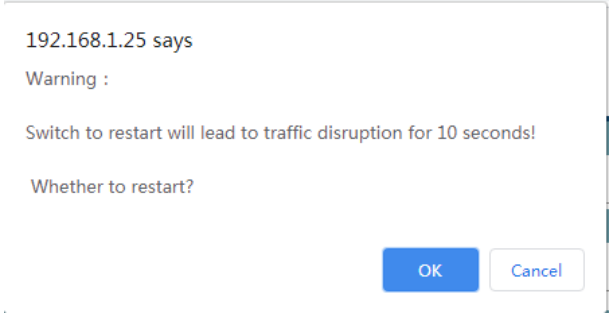
· Click <Start> under <Restore Factory Value>.



· Click <OK>.

2) Reboot the system.

· Click <Start> under <System Reboot>.



· Click <OK>.

3) Manage the configuration file.

- Click <Download> under <Configuration File>.
- The configuration file will be downloaded.

4) Upload configuration file.

- Click <Choose File> under <Configuration File>.
- Click <Upload>.

Note:

The actual configuration will be covered after uploading configuration file operation. Please download your configuration file before uploading, or the latest configuration can't be recovered.

5) Upgrade the software version.

- Click <Choose File> under <System Upgrade>.
- Click <Start>.

Note:

To upgrade the software version, please contact the seller for the software package.

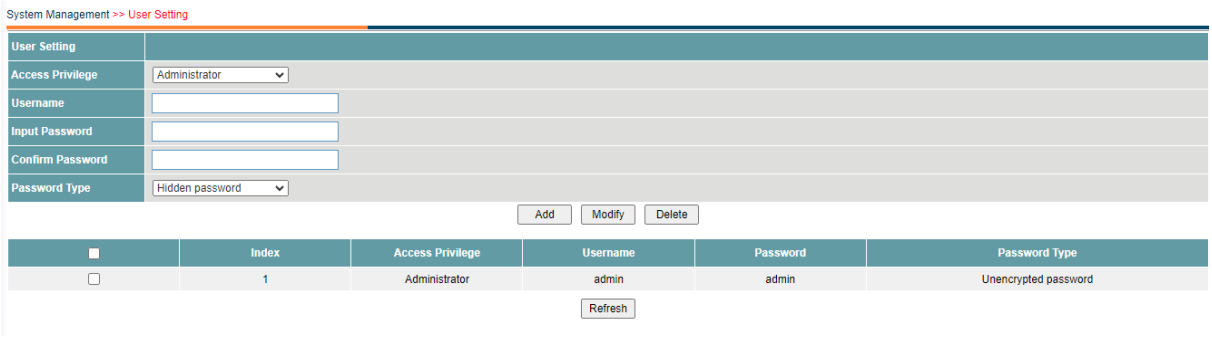
After software upgrade, please press the <Init> key on the front panel for 5s, to make sure the new version software will work normally.

17.7 User Setting

The Web system manages users at levels.

User levels are marked by numbers from 1 to 15, in ascending order.

The access privilege of user is determined by the level of this user.



Procedure

Choose <System Management> <User Setting> in the navigation tree to open the page.

1) Create username.

System Management >> User Setting

User Setting	
Access Privilege	Administrator
Username	
Input Password	
Confirm Password	
Password Type	Hidden password

- Set the parameters as required.

Items	Descriptions	Default value
Access Privilege	Choose the user level as the following: · User · Administrator	Administrator
User name	Input the username, supporting 32 digits of letters or numbers.	Null
Input password	Input the password, support 16 digits of letters or numbers.	Null
Confirm password	Confirm the password. The value must be the same as <Input password>.	Null
Password Type	Choose the password type as the following: · Hidden password · Unencrypted password	Hidden password

- Click <Add>.
- Click <Save>.

2) Delete username.

- Choose the username that need to be deleted.
- Click <Del>.
- Click <Save>.

3) View the usernames.

- Click <Refresh>.
- View the information.

17.8 Timing Restart

The switch supports to set the restart time of the system. After setting, the switch will restart regularly at setting time.

System Timing Restart			
Every day	Disable		(HH:mm)
Every week	Disable		(HH:mm)
Every month	Disable		(HH:mm)

Refresh Save Help

Procedure

Choose <System Management><Timing Restart> in the navigation tree to open the page.

3) Configure restart time of the switch.

· Set the parameters as required.

Items	Descriptions	Default value
Every day	Enable the function, the switch will restart at setting time every day. Set the restarting time, format as “HH:MM”.For example, set “15:00”, the switch will restart at “15:00:59”	Null
Every week	Enable the function. Choose the restarting day and time. The switch will restart at setting time on setting day every week. The restarting time is format as “HH:MM”.For example, set “15:00”, the switch will restart at “15:00:59”.	Null
Every month	Enable the function. Choose the restarting date and time. The switch will restart at setting time on setting day every month. The restarting time is format as “HH:MM”.For example, set “15:00”, the switch will restart at “15:00:59”.	Null

· Click <Save>.