IPS-M2SF60008
Industrial Ethernet switch
Web Operation Manual

CONTENTS

1 Overview

The IPS-M2SF60008 instruction manual is used to guide the device installer on how to properly configure the required functionality over the Web (HTTP).

This document will help the reader quickly understand the basic situation of the IPS-M2SF60008 industrial Ethernet switch (hereinafter referred to as IPS-M2SF60008) and facilitate smooth debugging.

The IPS-M2SF60008 industrial Ethernet switch provides Web management capabilities.

Default parameters are shown in the following table:

parameter	Default value
Default user name	admin (admin user)
Default password	admin (admin user)
Default IP Address	192.168.1.254

2 WEB

Enter "http://192.168.1.254" to enter the login interface. Enter the correct user name and password (admin/admin) to login successfully.

3 Product information

Click "Basic Setting → Product Information" in the navigation bar to view the product information interface.

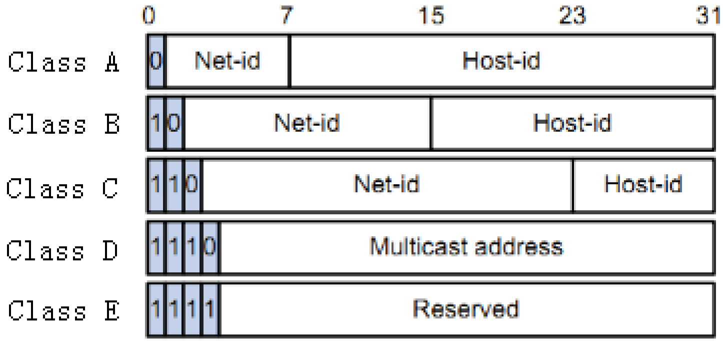
The explanation of each parameter in the Web is shown in the following table:

Name	Explain
Device type	The device model of the system.
Name of the device	Device description of the system.
Product number	Product factory number.
Software version	System software version.
Software generation time	Date and time of switch software.
Manufacturers	Switch manufacturer.
Hardware version	Device hardware version.
Firmware version	System firmware version.
Port number	The number of ports on the device.
Local MAC address	The MAC address of the system.
The elapsed time	The uptime of the system.
CPU utilization	The current CPU utilization of the system.
Memory utilization	The current memory usage of the system.
Working voltage	The current operating voltage of the system. It's in mV.

4 Manage IP Settings

4.1 IP Address Introduction

An IP address is a 32-bit length address assigned to a device connected to the Internet. The IP address consists of two fields: the network number field (Net-ID) and the host number field (Host-ID). To facilitate the management of IP addresses, IP addresses are divided into five categories. As shown in the figure below.

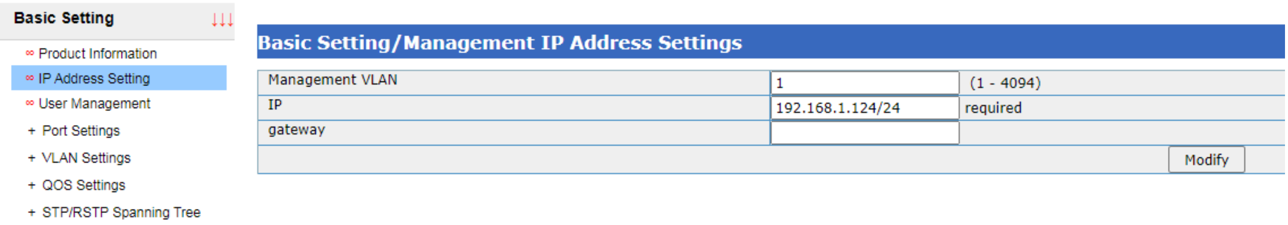


Class A, B and C addresses are unicast addresses; Class D addresses are multicast addresses. Class E addresses are reserved for future special use. At present, A large number of IP addresses in use belong to A, B and C addresses.

IP addresses are recorded in dot - decimal mode. Each IP address is represented as four decimal integers separated by a decimal point, each of which corresponds to one byte, such as 10.110.50.101.

4.2 Managing IP addresses

Click "Basic Setting → Manage IP Settings" in the navigation bar to enter the interface of IP Settings Management, as shown in the figure below: :



Basic Setting/Management IP Address Settings

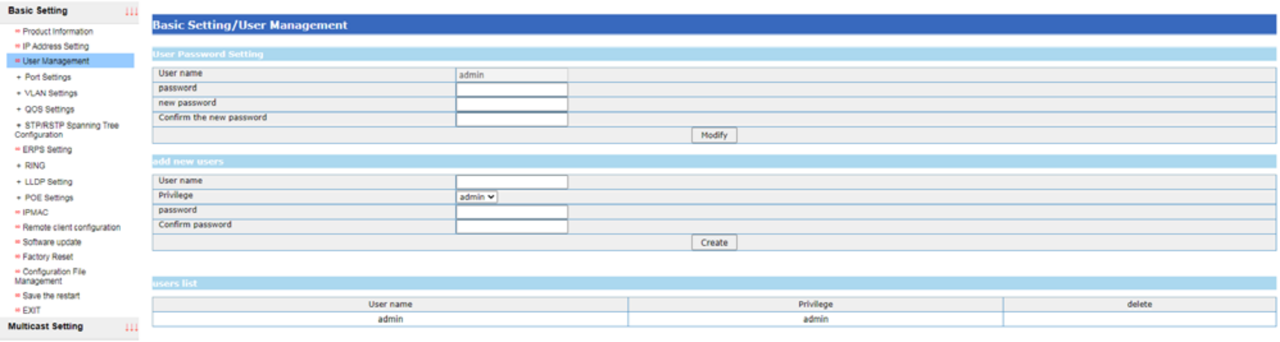
Management VLAN	1	(1 - 4094)
IP	192.168.1.124/24	required
gateway		

The various parameters in this Web are explained in the following table:

Name	Explain
Management VLAN	The administrative VLAN used to set up and display the system. Default is 1.
IP	Use to set and display IP addresses. Default is 192.168.1.254/24.
Gateway	The gateway address used to set and display the system.

5 User management

Click the navigation bar "Basic Settings → User Management" to enter the user management interface, as shown in the figure below:



Basic Setting/User Management

User Password Setting

User name	admin
password	
new password	
Confirm the new password	

add new users

User name	
Privilege	admin
password	
Confirm password	

users list

User name	Privilege	delete
admin	admin	

1、The User Parameter Configuration section is used to change the password of the current logged-in user. User Parameter Configuration The various parameters in the Web are explained in the following table:

Name	Explain
User name	The user name that is currently logged in.
password	The original password of the current logged-in user. Passwords consist of 0 to 16 bytes of NVT ASCII characters (32-126).
New password	The new password for the currently logged in user.
Confirm password	Enter the new password for the current logged-in user again. Enter the confirmation password and click < modify > button to change the password of the current login user. After successfully changing the password, you need to log in again.

2、The new part is used to add new users.

The explanation of each parameter in the new user Web is shown in the following table:

Name	Explain
User name	Enter the username for the new user. The user name consists of numbers, letters, and underscores, and the string length is from 1 to 16 bytes.
permissions	Select the permissions for the new user. There are two types of management authority: (1) Manage user permissions -- Admin: Manage the configuration of the system that users can view and edit. Guest: A normal user can only view the system configuration information.
password	Enter the password for the new user. Passwords consist of 0 to 16 bytes of NVT ASCII characters (32-126).
Confirm password	Enter the new user's password again.

3、The user list shows the user names and permissions of all registered users in the current system. Only administrative users can delete other users.

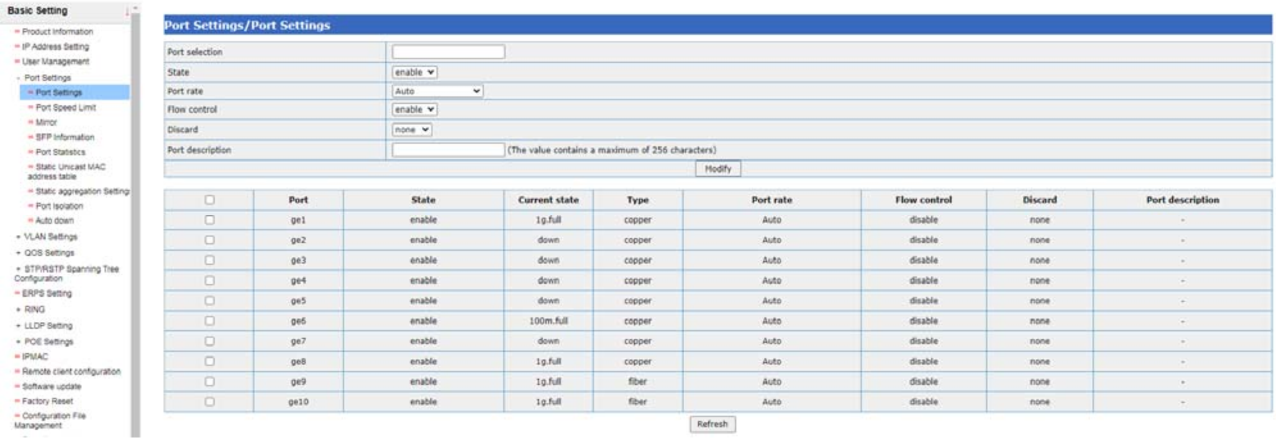
The explanation of each parameter in the user list Web is shown in the following table:

Name	Explain
User name	The user name of the registered user.
permissions	The permissions for the registered user.
Delete	Delete the registered user. Only administrative users can delete other users.

6 PORT

6.1 Port Settings

Click the navigation bar "Basic Settings → Port Settings → Port Settings" to enter the port management interface, as shown in the figure below:



Port Settings/Port Settings

Port selection	
State	enable
Port rate	Auto
Flow control	enable
Discard	none
Port description	(The value contains a maximum of 256 characters)

□	Port	State	Current state	Type	Port rate	Flow control	Discard	Port description
□	ge1	enable	1g.full	copper	Auto	disable	none	-
□	ge2	enable	down	copper	Auto	disable	none	-
□	ge3	enable	down	copper	Auto	disable	none	-
□	ge4	enable	down	copper	Auto	disable	none	-
□	ge5	enable	down	copper	Auto	disable	none	-
□	ge6	enable	100m.full	copper	Auto	disable	none	-
□	ge7	enable	down	copper	Auto	disable	none	-
□	ge8	enable	1g.full	copper	Auto	disable	none	-
□	ge9	enable	1g.full	fiber	Auto	disable	none	-
□	ge10	enable	1g.full	fiber	Auto	disable	none	-

（1）The explanation for modifying various parameters in the Port Management Web is shown in the following table:

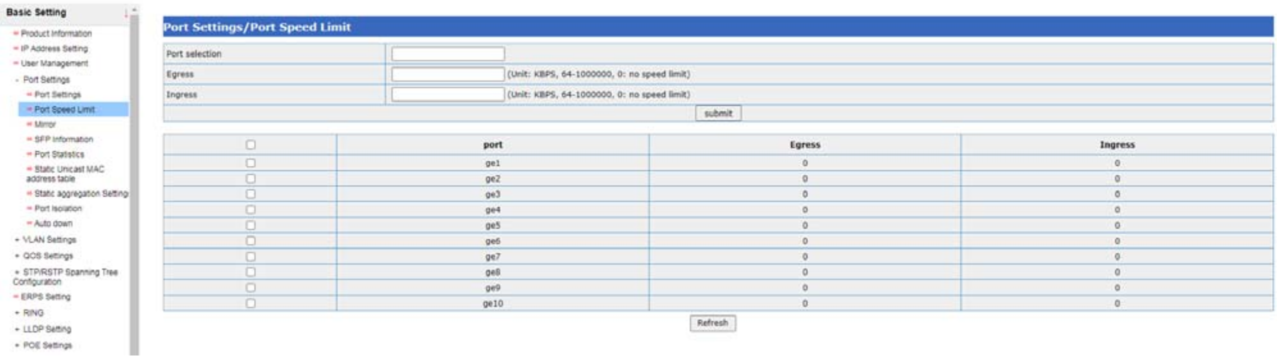
Name	Explain
Port selection	Select the port number you want to operate on. Check the check box in the list of ports.
Port is enabled	Sets the enabled/disabled state of the selected port. All ports are enabled by default.
Port rate	Sets the port rate for the selected port. Default is automatic negotiation.
Flow control	Sets flow control options for the selected port. Default is off.
packet	Sets the type of packet discarded for the selected port. Default is None.
Interface description	Sets the interface description for the selected port. No more than 256 characters.

（2）The various parameters for viewing ports in the Port Management Web are explained in the following table:

Name	Explain
port	List of port numbers.
Port is enabled	Displays the enabled/disabled status of the corresponding port.
Current state	Displays the UP/DOWN status of the corresponding port.
Type	Displays the type of corresponding port: optical port or electrical port.
Port rate	Displays the port rate for the corresponding port.
Flow control	Displays flow control Settings for corresponding ports. Includes flow control Settings in both TX and RX directions.
packet	Displays the type of packet dropped for the corresponding port.
Interface description	Displays the interface description of the corresponding port.

6.2 Port speed limit

Click "Basic Settings → Port Settings → Port Speed Limit" in the navigation bar to enter the port speed limit interface, as shown in the figure below:



Port Settings/Port Speed Limit

Port selection	
Egress	(Unit: KBPS, 64-1000000, 0: no speed limit)
Ingress	(Unit: KBPS, 64-1000000, 0: no speed limit)

□	port	Egress	Ingress
□	ge1	0	0
□	ge2	0	0
□	ge3	0	0
□	ge4	0	0
□	ge5	0	0
□	ge6	0	0
□	ge7	0	0
□	ge8	0	0
□	ge9	0	0
□	ge10	0	0

The various parameters in this Web are explained in the following table:

Name	Explain
Port selection	Select the port that you want to configure the port speed limit on. Check the check box in the list of ports.
Export the speed limit	The speed limit value of the exit speed limit required to fill the port. The range is 62.5-1000000kbps. Enter a "0" to close the exit limit.
Exports into the bucket	Buffer Settings for output ports. The unit is Kbps and the port range is 64-1000000Kbps.
Entrance to the speed limit	The speed limit value of the entry speed limit required to fill the port. Port range is 62.5-1000000Kbps. Enter a "0" to close the entrance speed limit.
Entry into the bucket	Buffer Settings for input ports. The unit is Kbps and the port range is 64-1000000Kbps.

6.3 Mirror configuration

6.3.1 Introduction to the

A switch copies identical data frames received or sent on one port to another. The copied port is called the mirror source port, and the copied port is called the mirror destination port. The mirrored destination port will be connected to the data detection device, and the user will use the data detection device to analyze the messages received by the mirrored port for network monitoring and troubleshooting. The mirror is shown in Figure 6.1:

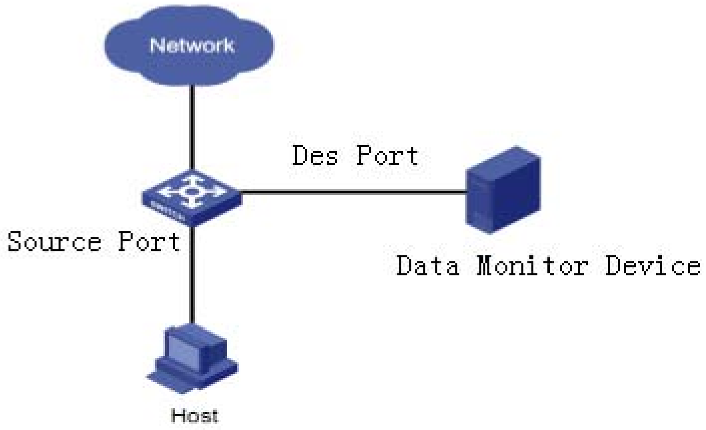
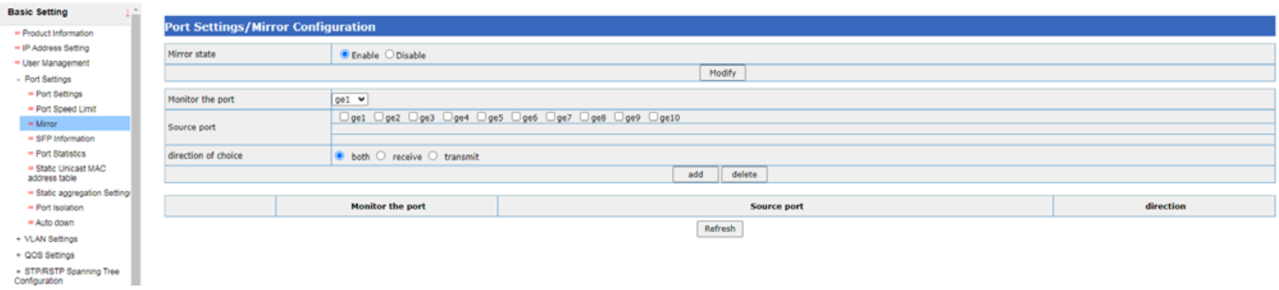


Fig. 6.1 mirroring diagram

6.3.2 Port mirror

Click "Basic Settings → Port Settings → Mirror Configuration" in the navigation bar to enter the port mirror interface, as shown in the figure below:



Port Settings/Mirror Configuration

Mirror state: ● Enable ○ Disable

Monitor the port: ge1

Source port: □ge1 □ge2 □ge3 □ge4 □ge5 □ge6 □ge7 □ge8 □ge9 □ge10

direction of choice: ● both ○ receive ○ transmit

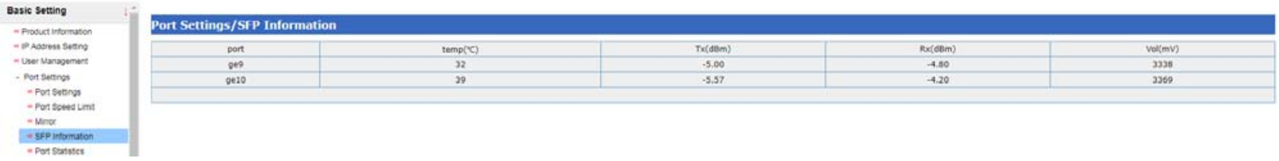
	Monitor the port	Source port	direction

The various parameters in this Web are explained in the following table:

Name	Explain
Mirror can make	Turn on or off mirroring.
Mirror port	Select the mirror port, which is the port being monitored.
Monitor the port	Select the monitor port, that is, the port used for monitoring, to which the mirrored port data will be copied.
Direction of	Select the direction of monitoring, including bi-directional, in-direction and out-direction.

6.4 Optical Module Information

Click "Basic Settings → Port Settings → Optical Module Information" in the navigation bar to enter the optical module information interface, as shown in the figure below:



Port Settings/SFP Information

port	temp(℃)	Tx(dBm)	Rx(dBm)	Vol(mV)
ge9	32	-5.00	-4.80	3338
ge10	39	-5.57	-4.20	3369

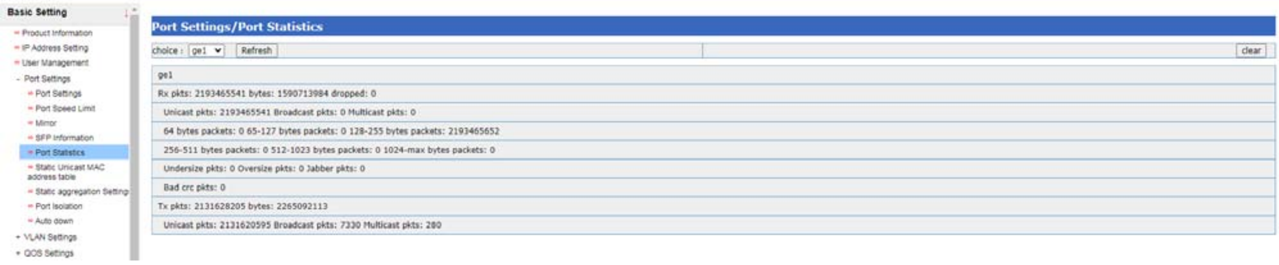
The various parameters in this Web are explained in the following table:

Name	Explain

Port	The port number used to display the optical port of the device.
Temperature	Used to display the temperature of the corresponding light port.
Transmitted optical power	Used to display the transmitting power of the corresponding light port.
Received optical power	Used to display the received light power of the corresponding light port.
voltage	Used to display the voltage of the corresponding light port.

6.5 port statistical

Click "Basic Settings →+ Port Settings → Port Statistics" in the navigation bar to enter the interface of port statistics, as shown in the figure below:



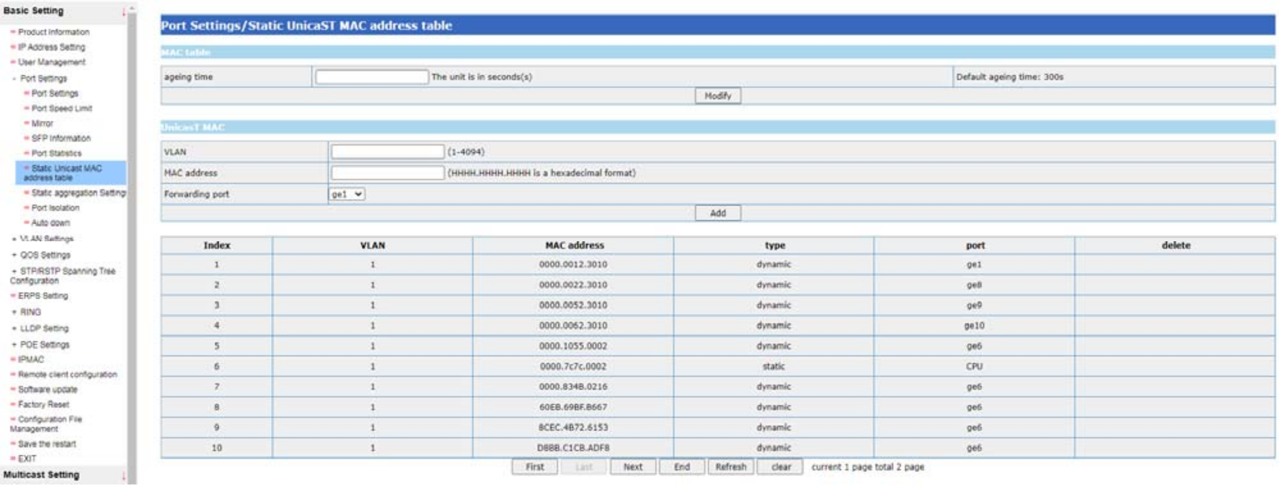
```
ge1
Rx pkts: 2193465541 bytes: 1590713984 dropped: 0
  Unicast pkts: 2193465541 Broadcast pkts: 0 Multicast pkts: 0
  64 bytes packets: 0 65-127 bytes packets: 0 128-255 bytes packets: 2193465652
  256-511 bytes packets: 0 512-1023 bytes packets: 0 1024-max bytes packets: 0
  Undersize pkts: 0 Oversize pkts: 0 Jabber pkts: 0
  Bad crc pkts: 0
Tx pkts: 2131628205 bytes: 2265092113
  Unicast pkts: 2131620595 Broadcast pkts: 7330 Multicast pkts: 280
```

The various parameters in this Web are explained in the following table:

Name	Explain
Input packets	Displays the number of input packets for the corresponding port
Input bytes	Displays the number of input byte packets for the corresponding port
Input dropped	Displays the number of incoming dropped packets for the corresponding port
Unicast packets	Displays the number of input unicast packets for the corresponding port
Broadcast packets	Displays the number of input broadcast packets for the corresponding port
Multicast packets	Displays the number of input multicast packets for the corresponding port
Undersize packets	Displays the number of incoming UNDERSIZE packets for the corresponding port
Oversize packets	Displays the number of input oversize packets for the corresponding port
Jabber packets	Displays the number of input Jabber packets for the corresponding port
Bad crc packets	Displays the number of CRC error packets input for the corresponding port
Output packets	Displays the number of output packets for the corresponding port
Output bytes	Displays the number of output byte packets for the corresponding port
Unicast packets	Displays the number of output unicast packets for the corresponding port
Broadcast packets	Displays the number of output broadcast packets for the corresponding port
Multicast packets	Displays the number of output multicast packets for the corresponding port

6.6 Static unicast MAC address table

Click "Basic Settings → Port Configuration → Static unicast MAC Address Table" in the navigation bar to enter the unicast MAC address setting interface, as shown in the figure below:



Port Settings/Static UnicaST MAC address table

MAC table

ageing time: The unit is in seconds(s) Default ageing time: 300s

UnicasT MAC

VLAN: (1-4094)

MAC address: (HHHH.HHHH.HHHH is a hexadecimal format)

Forwarding port: ge1

Index	VLAN	MAC address	type	port	delete
1	1	0000.0012.3010	dynamic	ge1	
2	1	0000.0022.3010	dynamic	ge8	
3	1	0000.0052.3010	dynamic	ge9	
4	1	0000.0062.3010	dynamic	ge10	
5	1	0000.1055.0002	dynamic	ge6	
6	1	0000.7c7c.0002	static	CPU	
7	1	0000.834B.0216	dynamic	ge6	
8	1	60EB.69BF.B667	dynamic	ge6	
9	1	8CEC.4B72.6153	dynamic	ge6	
10	1	D8BB.C1CB.ADF8	dynamic	ge6	

current 1 page total 2 page

The various parameters in this Web are explained in the following table：

Name	Explain
Aging time	Dynamic MAC address entries in the MAC address table aging time, the default is 300s. The range is 0,10-1000000s.
VLAN	VLAN used to add static MAC addresses.
MAC address	The MAC address used to add static MAC addresses. The format is hexadecimal: hhh.hhh.hhhh.
Forwarding port	The port number used to add static MAC addresses.
Type	MAC address types, divided into dynamic and static categories.
MAC address table	Displays the MAC address table.

6.7 Static aggregation Settings

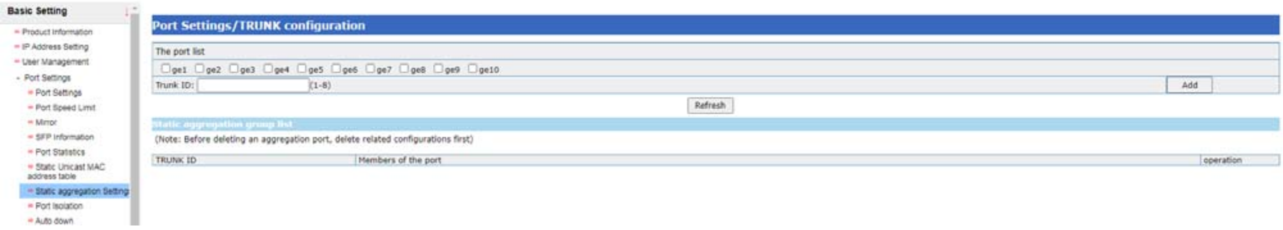
6.7.1Introduction to Port Convergence

Port aggregation is to gather multiple ports together to form a sink group, so as to realize the sharing of outbound/inbound load among member ports in the sink group, and at the same time to provide higher connection reliability. The Basic Setting of ports in the same sink group must be consistent, which mainly includes STP, VLAN, port properties and other relevant configurations.

- The STP configuration includes: the STP enabling/closing of the port, the link attributes associated with the port (such as point-to-point or non-point-to-point), the STP priority STP overhead, the STP standard message format, whether it is an edge port, etc.
- The VLAN configuration includes: the VLAN allowed on the port, the port default VLAN ID.
- The port properties configuration includes: for static sink groups, only the link types of the ports (i.e., Trunk, Hybrid, and Access types) are required to be consistent.

6.7.2 Aggregation set

Click "Basic Settings → Port Settings → Static Aggregation Settings" in the navigation bar to enter the interface of aggregation configuration, as shown in the figure below:



Port Settings/TRUNK configuration

The port list

□ge1 □ge2 □ge3 □ge4 □ge5 □ge6 □ge7 □ge8 □ge9 □ge10

Trunk ID: (1-8)

Static aggregation group list

(Note: Before deleting an aggregation port, delete related configurations first)

TRUNK ID	Members of the port	operation

The various parameters in this Web are explained in the following table:

Name	Explain
Port list	Used to create a static sink group. Check the box to select the port number for the new aggregation group member. Up to 8 ports can be selected to join the same sink group.
Gather the group ID	Enter the sink group ID for the new sink group. It ranges from 1 to 8.
Static sink group list	Displays the ID and port members of all static sink groups.

7 VLAN configuration

7.1 Summary of VLAN

VLAN (Virtual Local Area Network, Virtual Local Area Network), VLAN can be divided into a number of broadcast domain, so as to effectively control the occurrence of broadcast storm, and make the Network topology becomes very flexible advantages, but also can be used to control the Network of different departments, different sites between each other access.

VLAN is a protocol proposed to solve the problem of Ethernet broadcast and security. It adds VLAN header on the basis of Ethernet frame, divides users into smaller working groups with VLAN ID, and restricts the user visits between different working groups. Each working group is a virtual LAN. The benefits of a virtual LAN are the ability to limit the broadcast range and to form virtual workgroups to dynamically manage the network.

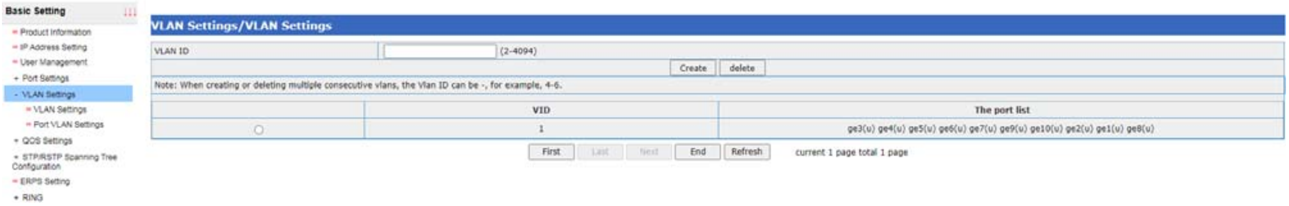
According to the different partition, can be divided into different types of VLAN, the commonly used several partition methods are as follows: VLAN based on port, VLAN based on MAC address, VLAN based on IP subnet, VLAN based on protocol

Port-based VLAN

Port-based VLANs are the simplest and most efficient way to partition a virtual LAN, which is essentially a collection of switched ports that a network administrator only needs to manage and configure regardless of what device the switched ports are connected to.

7.2 Membership configuration of the VLAN

Click "Basic Settings →VLAN Configuration →VLAN Configuration" in the navigation bar to enter the VLAN member setting interface, as shown in the figure below:



VLAN Settings/VLAN Settings

VLAN ID (2-4094)

Note: When creating or deleting multiple consecutive vlans, the Vlan ID can be -, for example, 4-6.

	VID	The port list
○	1	ge3(u) ge4(u) ge5(u) ge6(u) ge7(u) ge9(u) ge10(u) ge2(u) ge1(u) ge8(u)

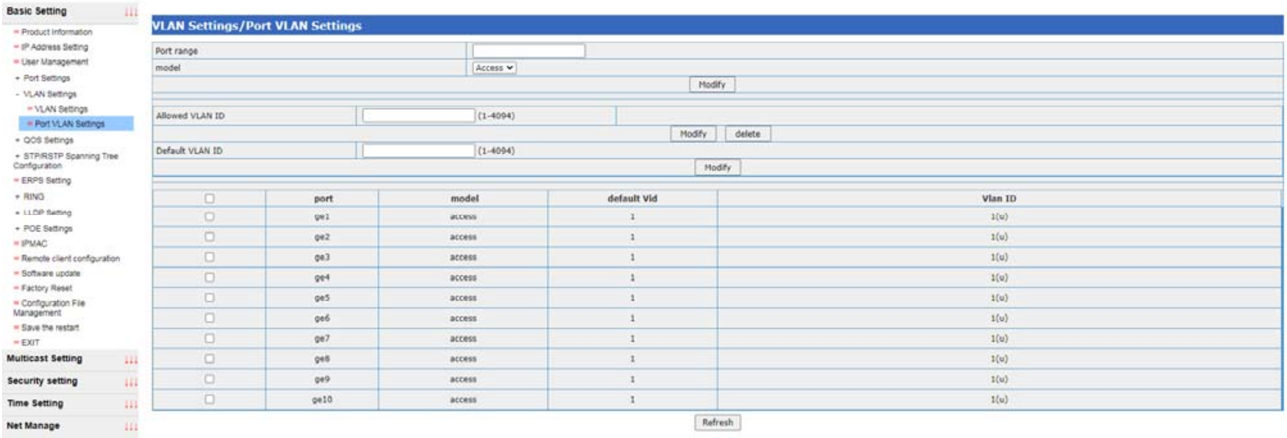
current 1 page total 1 page

The various parameters in this Web are explained in the following table:

Name	Explain
VLAN ID	Use to create or delete a VLAN. The VLAN can be created or deleted by filling in the VLAN ID that needs to be operated. The range is 2-4094. VLAN 1 has been added by default and cannot be removed. Click < add > button to create the corresponding VLAN, and click < delete > button to delete the corresponding VLAN.
Port range	Displays the member ports corresponding to the VLAN.
(u)	Indicates that the port is a member of the VLAN and that it is the UNTAG port of the VLAN.
(t)	Indicates that the port is a member of the VLAN and that it is the Tag port of the VLAN.
VLAN list	Displays a list of VLANs that the system has created and a list of ports that the VLAN allows.

7.3 VLAN port configuration

Click "Device Control →+VLAN Settings → Port VLAN Settings" in the navigation bar to enter the interface of VLAN port setting, as shown in the figure below:



VLAN Settings/Port VLAN Settings

Port range

model: Access

Allowed VLAN ID (1-4094)

Default VLAN ID (1-4094)

□	port	model	default Vid	Vlan ID
□	ge1	access	1	1(u)
□	ge2	access	1	1(u)
□	ge3	access	1	1(u)
□	ge4	access	1	1(u)
□	ge5	access	1	1(u)
□	ge6	access	1	1(u)
□	ge7	access	1	1(u)
□	ge8	access	1	1(u)
□	ge9	access	1	1(u)
□	ge10	access	1	1(u)

The various parameters in this Web are explained in the following table:

Name	Explain
Port range	Link type used to modify the port. Select the check box in the port list to modify the link type operation on the selected port.
Model	Link types for editing ports, including Access, Trunk, and Hybrid.
Allowed VLAN ID	Use to edit the list of VLAN IDs that are allowed through the port. The < add > button indicates that the port is allowed to correspond to the VLAN, and the <

	delete > button indicates that the port is not allowed to correspond to the VLAN.
Default VLAN ID	PVIDs for editing ports. The range is 1-4094.
VLAN port configuration	Use to display the port VLAN configuration, including the mode, the default VID, and the list of allowed VLANs VLAN IDs.

8 QoS

8.1 Description of QoS

QoS is known as "Quality of Service" in English and "Quality of Service" in Chinese. QoS is a security mechanism of network, which is used to solve the problems of network delay and blocking. For network services, QoS includes transmission bandwidth, transmission delay, data packet loss rate and so on. In the network, the quality of service can be improved by ensuring the bandwidth of transmission, reducing the delay of transmission, reducing the packet loss rate of data and the delay jitter. Network resources are always limited, as long as there is a looting of network resources, there will be quality of service requirements. The quality of service is relative to the network business, while ensuring the quality of service of a certain type of business, it may be damaging the quality of service of other businesses. For example, if the total network bandwidth is fixed, the more bandwidth occupied by a certain type of service, the less bandwidth other services can use, which may affect the use of other services. Therefore, network managers need to reasonably plan and allocate network resources according to the characteristics of various services, so as to make efficient use of network resources.

8.2 Introduction to common priorities

8.2.1 802.1 p priority

The 802.1p priority is located in the Tier 2 header and is suitable for applications where QoS is guaranteed in the Tier 2 environment rather than the analysis of the Tier 3 header. Packets with 802.1q Tag have 802.1p priority, as shown in Figure 8.1 below, the 4-bit 802.1q Tag header contains 2-bit TPID (Tag Protocol Identifier, Tag Protocol Identifier, Value 0x8100) and 2 bits of TCI (Tag Control Information)

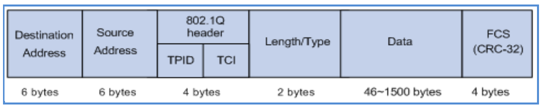


Figure 8. 1 Ethernet frame with 802.1q tag header

Figure 8.2 shows the details of the 802.1q tag header. The Priority field in TCI is the 802.1p Priority, also known as COS Priority. It consists of three bits with values ranging from 0 to 7.

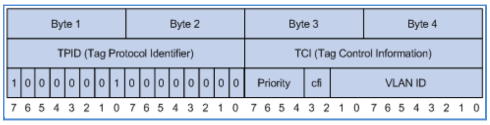


Figure 8. 2 802.1Q tag header

8.2.2 IP priority, TOS priority and DSCP priority

The IP packet header has DSCP priority, and the TOS field of the IP header has 8 bits, where:

- The first three bits represent IP priorities, with values ranging from 0 to 7
- The 4 bits from 3rd to 6th represent TOS priority, and their value range is 0 to 15
- RFC2474 redefines the TOS domain of the header of IP packets, which is called DS domain, in which the priority of DSCP (Connected Services Code Point) is expressed by the first 6 bits (0 ~ 5 bits) of the field, and the value range is 0 ~ 63. The last two bits (6 and 7 bits) are reserved bits.

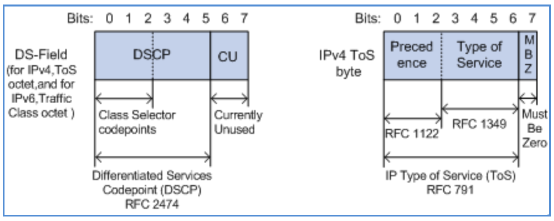

Bits: 0 1 2 3 4 5 6 7
DS-Field (for IPv4,ToS octet,and for IPv6,Traffic Class octet)
DSCP
CU
Class Selector codepoints
Currently Unused
Differentiated Services Codepoint (DSCP) RFC 2474
Bits: 0 1 2 3 4 5 6 7
IPv4 ToS byte
Precedence
Type of Service
MBZ
RFC 1122
RFC 1349
Must Be Zero
IP Type of Service (ToS) RFC 791

Figure 8. 3 DS fields and TOS bytes

8.3 Introduction to Queue Scheduling

8.3.1 Strict priority queue (SPQ)

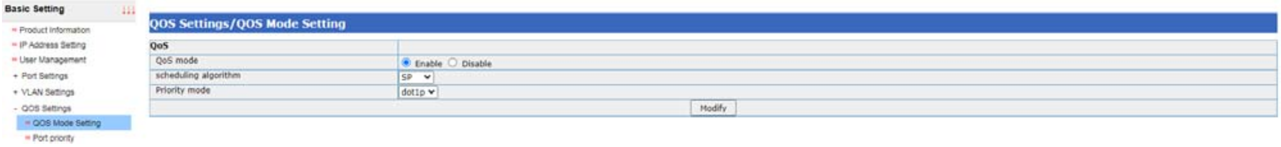
This is the simplest form of queuing, which first serves the highest-priority queue until it becomes empty, then serves the next next-highest priority queue, and so on. The advantage of this approach is that high-priority businesses are always processed before low-priority businesses. However, it is possible for a low-priority business to be completely blocked by a high-priority business.

8.3.2 Weighted Cycle (WRR)

This approach serves all business queues and allocates priority to higher-priority queues. In most cases, relatively low priority, WRR will process high priority first, but when there are many high priority businesses, the lower priority businesses are not completely blocked.

8.4 QoS mode setting interface

Click "Basic Settings →QoS Settings →QoS Mode Settings" in the navigation bar to enter the QoS mode setting interface, as shown in the figure below:



QOS Settings/QOS Mode Setting

QoS

QoS mode ● Enable ○ Disable

scheduling algorithm SP

Priority mode dot1p

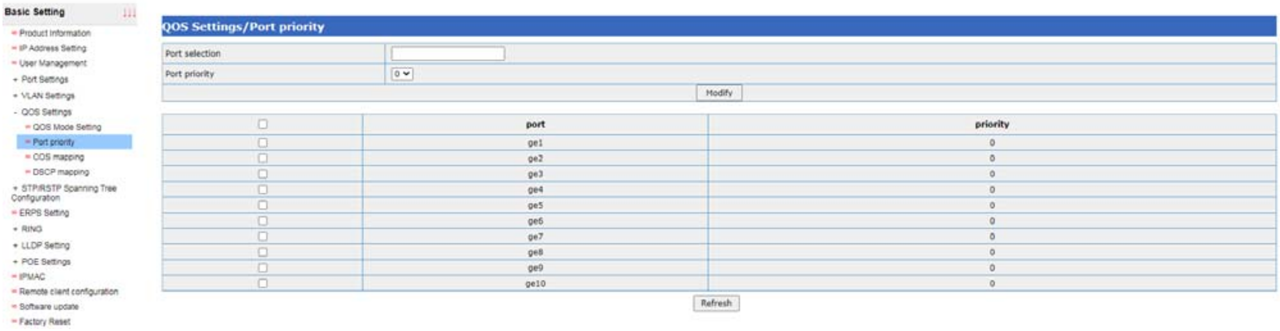
The various parameters in this Web are explained in the following table:

Name	Explain
QoS model	Use to enable/disable QoS functionality of the system. QoS is enabled by default.
Scheduling algorithm	Used to configure the scheduling algorithm currently selected by the system. Including WRR and SP two modes. SP mode is enabled by default.
Priority pattern	The default dot1p (COS) also supports port priority and DSCP.

When the scheduling algorithm is selected as WRR, this Web can configure and display the weight of the queue, as shown in the figure below:

8.5 Port priority

Click "Basic Settings →QoS Settings → Port Priority" in the navigation bar to enter the port priority interface, as shown in the figure below:



QOS Settings/Port priority

Port selection	
Port priority	0

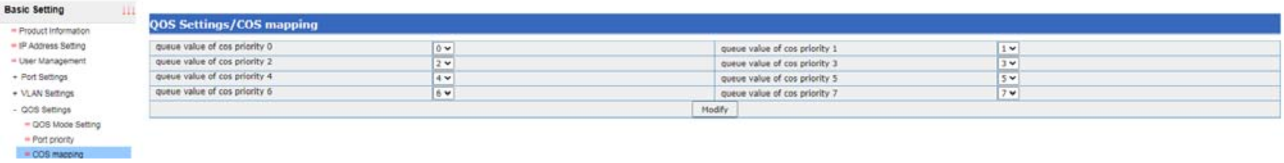
□	port	priority
□	ge1	0
□	ge2	0
□	ge3	0
□	ge4	0
□	ge5	0
□	ge6	0
□	ge7	0
□	ge8	0
□	ge9	0
□	ge10	0

The various parameters in this Web are explained in the following table:

Name	Explain
Port range	Check the port in the list that you want to change the priority of the port.
Priority	Use to configure the priority of the ports, ranging from 0 to 7.
Port priority list	Displays the priority of the port.

8.6 COS mapping interface

Click "Basic Settings →QoS Settings → COS Mapping" in the navigation bar to enter the COS mapping interface, as shown below:



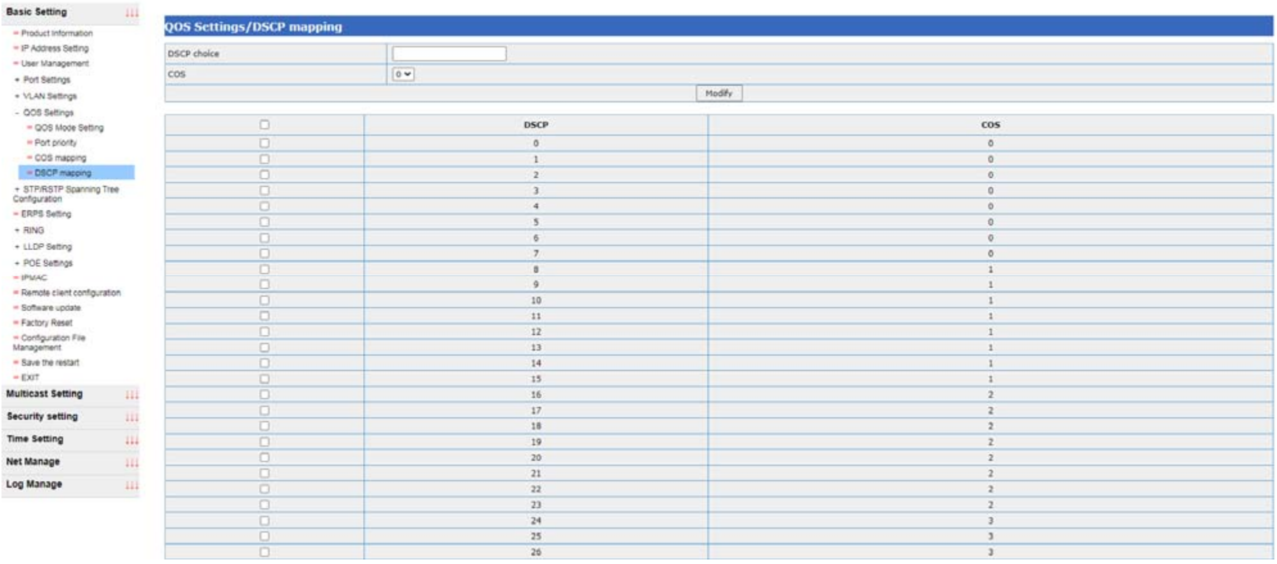
QOS Settings/COS mapping

queue value of cos priority 0	0	queue value of cos priority 1	1
queue value of cos priority 2	2	queue value of cos priority 3	3
queue value of cos priority 4	4	queue value of cos priority 5	5
queue value of cos priority 6	6	queue value of cos priority 7	7

Name	Explain
802.1p Queue value for priority X	The queue value used to configure 802.1p priority X in the range of 0-7.

8.7 DSCP mapping interface

Click "Device Control →QoS→ DSCP Mapping" in the navigation bar to enter the DSCP mapping interface, as shown in the figure below:



QOS Settings/DSCP mapping

DSCP choice

COS 0

□	DSCP	COS
□	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

Name	Explain
DSCP choice	The DSCP value to be mapped.
Mapping the cosine value	The cosine value mapped to this DSCP value.

9 STP

9.1 Introduction to Spanning Tree

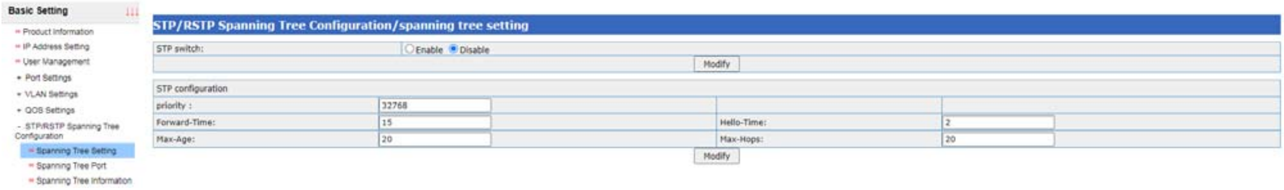
STP (Spanning Tree Protocol) is an acronym for a Spanning Tree Protocol. This protocol can be used to build a tree topology in the network and eliminate the loops in the network, and the path redundancy can be realized in a certain way, but not necessarily. The spanning tree protocol is suitable for all the network equipment of the manufacturer, which varies in configuration and strength of embodied function, but is consistent in principle and application effect.

The basic principle of STP is to determine the topology of the network by passing a special Protocol packet, the Bridge Protocol Data Unit (BPDU), between switches. There are two types of BPDU, Configuration BPDU and TCN BPDU. The former is used to calculate the acyclic spanning tree, and the latter is used to generate the refresh time of CAM entries (shortened from the default 300s to 15s) when the layer 2 network topology changes.

Spanning Tree Protocol(STP) is defined in the eeee802.1d document. The principle of the protocol is to construct the network topology according to the tree structure, eliminate the loop in the network, and avoid the broadcast storm caused by the existence of the loop。

9.2 Spanning tree set

Spanning tree setting interface can be accessed by clicking "Basic Setting →STP/RSTP→spanning tree setting" in the navigation bar, as shown below:



STP/RSTP Spanning Tree Configuration/spanning tree setting

STP switch: ○ Enable ● Disable

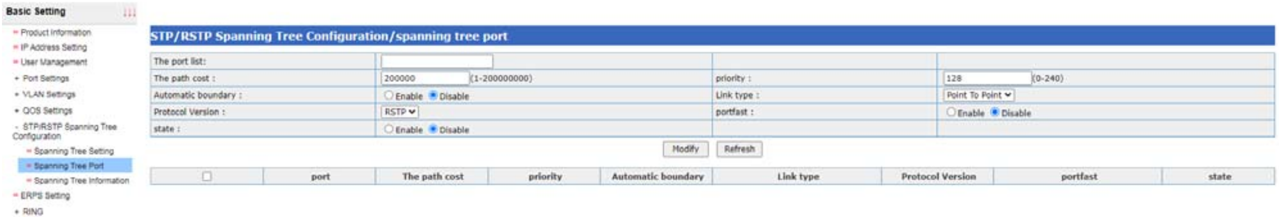
STP configuration

priority :	32768		
Forward-Time:	15	Hello-Time:	2
Max-Age:	20	Max-Hops:	20

Name	Explain
STP switch	Used to enable/disable STP. STP is turned off by default.
Priority	Use to set the priority of the system. The default priority is 32768.
Forwarding delay	Sets spanning tree configuration message forwarding delay. Default is 15s.
Hello delay	Sets the spanning tree configuration message Hello delay. Default is 2s.
Maximum aging time	Sets the maximum lifetime of spanning tree configuration messages. Default is 20s.
Largest hop	Sets the spanning tree configuration message maximum number of hops. Default is 20 hops.

9.3 Spanning tree port

Click on the navigation bar "Basic Setting →STP/RSTP→spanning tree port", then the STP port setting interface can be accessed, as shown below:



STP/RSTP Spanning Tree Configuration/spanning tree port

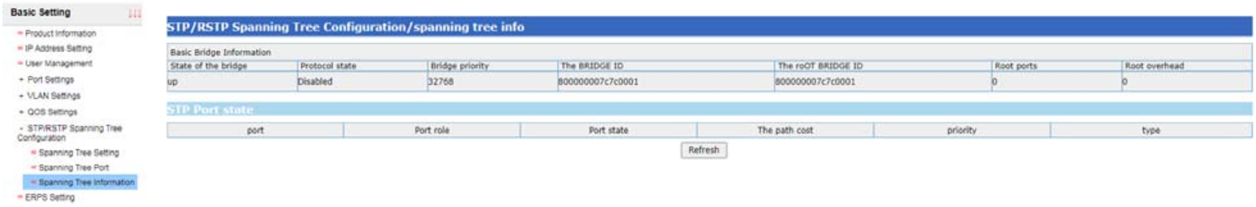
The port list:			
The path cost :	200000 (1-200000000)	priority :	128 (0-240)
Automatic boundary :	○ Enable ● Disable	Link type :	Point To Point
Protocol Version :	RSTP	portfast :	○ Enable ● Disable
state :	○ Enable ● Disable		

□	port	The path cost	priority	Automatic boundary	Link type	Protocol Version	portfast	state

Name	Explain
Port list	The port number used to select the port that needs to be modified.
Path cost	Use to set the path overhead for the selected port.
Priority	Use to set the priority of the selected port. The range is 0-240.
Automatic boundary	Enable/disable to set the automatic boundaries of the selected port.
Link type	The link type used to set the selected port. There are two link types: Point To Point and Shared.
Protocol version	Used to set the protocol version of the selected port. Includes RSTP and STP versions.
portfast	The portFast switch used to set the selected port, defaults to Disable. Terminal ports are recommended to open portfast to speed up convergence.

9.4 Spanning tree information

Click the navigation bar "Basic Setting →STP/RSTP→ Spann Tree Information" to enter the spanning tree information interface of STP, as shown in the figure below:



STP/RSTP Spanning Tree Configuration/spanning tree info

Basic Bridge Information

State of the bridge	Protocol state	Bridge priority	The BRIDGE ID	The roOT BRIDGE ID	Root ports	Root overhead
up	Disabled	32768	800000007c7c0001	800000007c7c0001	0	0

STP Port state

port	Port role	Port state	The path cost	priority	type

Name	Explain
State of the bridge	Displays the UP/DOWN status of the current bridge.
Protocol state	Displays the current spanning tree enable/disable state.
Bridge priority	Displays the current spanning tree enable/disable state.
Bridge ID	Displays the bridge ID.
Root bridge ID	Displays the root bridge ID. The root bridge ID consists of the root bridge priority and the root bridge MAC address and is displayed in hexadecimal.
Root ports	Displays the port number of the root port.
Root overhead	Shows the path overhead to the root bridge.
Port	The port number of the device.
Port role	Displays the port role for the corresponding port.
Port state	Displays the port status of the corresponding port.
Path cost	Displays the path overhead of the corresponding port.
Priority	Displays the port priority of the corresponding port.
Type	Displays the type of the corresponding port.

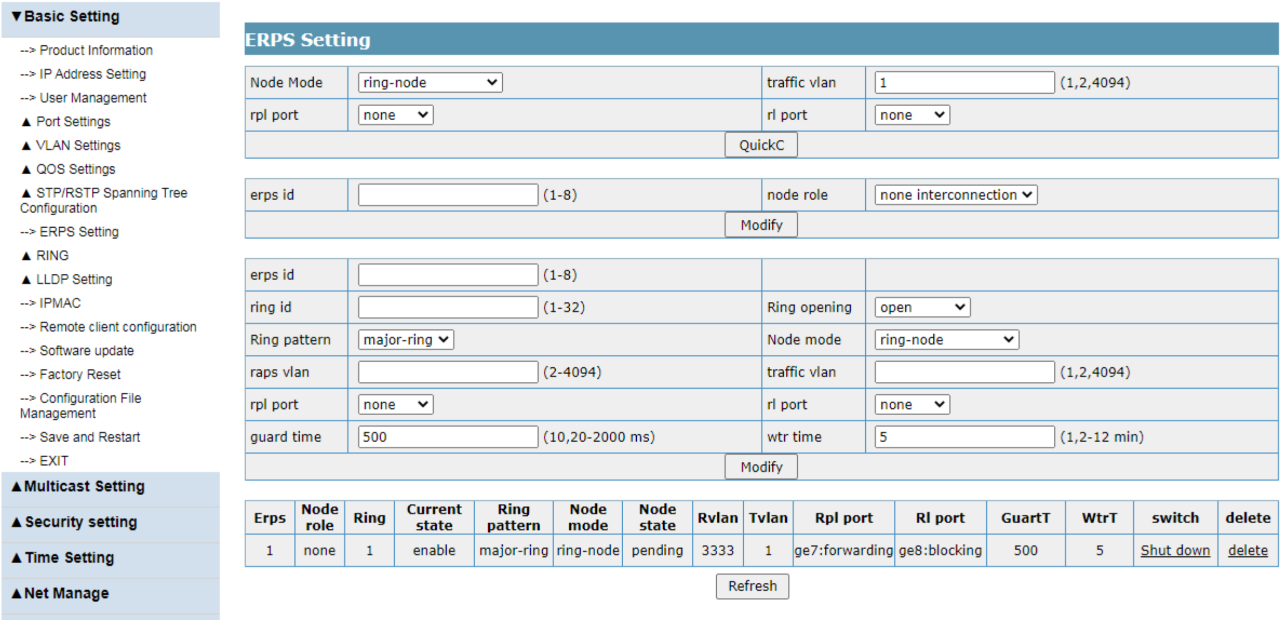
10 ERPS

10.1 Description of ERPS

ERPS (Ethernet Ring Protection Switching, Ethernet Ring network Protection Switching protocol) is a kind of Ring network Protection protocol developed by ITU, also calls the g. 8032. It is a special link layer protocol used in Ethernet ring network. It can prevent data in Ethernet ring network complete loop of broadcast storm, and when the Ethernet ring online a link disconnected can quickly restore the ring online communication between each node. ERPS agreement provides a fast Ethernet ring network protection mechanism, can be in the ring network fault occurs, quickly restore network transmission, so as to safeguard switch in the ring network topology under the condition of high availability, high reliability.

10.2 ERPS Setting

lick the navigation bar "Basic Setting →ERPS Setting" to enter the ERPS Setting information interface , as shown in the figure below:



ERPS Setting

Node Mode	ring-node	traffic vlan	1 (1,2,4094)
rpl port	none	rl port	none

erps id	(1-8)	node role	none interconnection

erps id	(1-8)		
ring id	(1-32)	Ring opening	open
Ring pattern	major-ring	Node mode	ring-node
raps vlan	(2-4094)	traffic vlan	(1,2,4094)
rpl port	none	rl port	none
guard time	500 (10,20-2000 ms)	wtr time	5 (1,2-12 min)

Erps	Node role	Ring	Current state	Ring pattern	Node mode	Node state	Rvlan	Tvlan	Rpl port	Rl port	GuartT	WtrT	switch	delete
1	none	1	enable	major-ring	ring-node	pending	3333	1	ge7:forwarding	ge8:blocking	500	5	Shut down	delete

Name	Explain
erps id	ERPS domain ID identification, add the loop to protect group, the article first ERPS group ID is 1, the second for 2, and so on.
node role	Node is configured in ERPS ring, the role of interconnected or not interconnected nodes (note: the configuration polycyclic, must first sets whether this node to interconnected nodes).
ring id	Create a ring of ERPS.
Ring opening	Created ERPS ring configuration is enabled or directly after shut down.
Ring pattern	Configuration ERPS ring mode, the main ring or a child.
Node model	Configuration ERPS link point pattern, RPL owner node, RPL neighbor nodes or ordinary link points.
raps vlan	VLAN configuration ERPS ring agreement.
traffic vlan	VLAN configuration ERPS ring data.
rpl port	RPL port.
rl port	Ordinary ring port.
guard time	Configuration ERPS ring guard time.
wtr time	Configuration ERPS ring WTR) (wait to restore time.

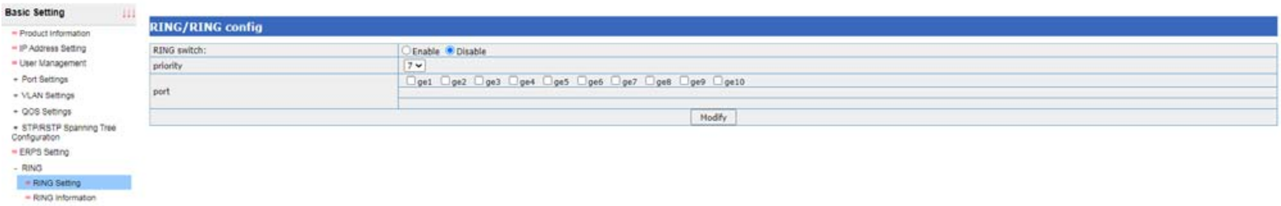
11 RING

11.1 Summary of RING

RING is a private RING protocol. This protocol can be used to build a tree topology in the network and eliminate the loops in the network, and the path redundancy can be realized in a certain way, but not necessarily. The RING protocol is only suitable for Utol's network equipment.

11.2 RING set

Click "Basic Setting → Ring Settings" in the navigation bar to enter the Ring Settings interface, as shown in the figure below:



RING/RING config

RING switch: ○ Enable ● Disable

priority 7

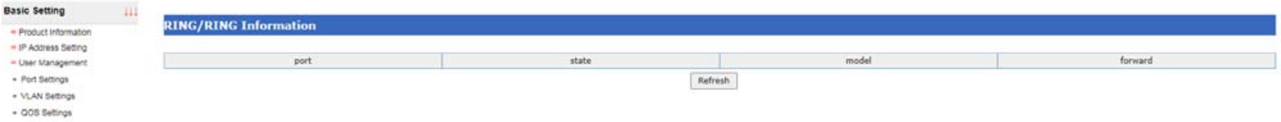
port □ge1 □ge2 □ge3 □ge4 □ge5 □ge6 □ge7 □ge8 □ge9 □ge10

Modify

Name	Explain
RING switch	Used to enable/disable RING. Ring is off by default.
Priority	Displays the port priority of the corresponding port.

11.3 RING information

Click "Basic Setting → Ring Settings" in the navigation bar to enter the Ring Settings interface, as shown in the figure below:



RING/RING Information

port	state	model	forward

Refresh

12 LLDP

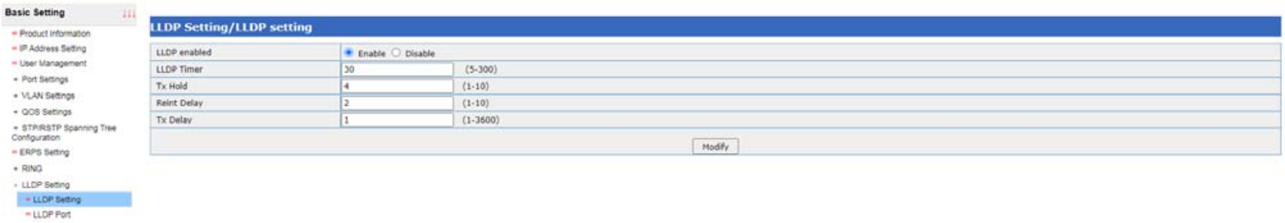
12.1 LLDP profile

LLDP (Link Layer Discovery Protocol) provides a standard way of Link Layer Discovery, which can organize the main capability, management address, device identification, interface identification and other information of the terminal device into different TLV (Type/Length/Value). Type/length/value), and encapsulated in LLDPDU (Link Layer Discovery Protocol Data Unit) for publishing to its directly connected neighbors. After receiving the Information, the neighbor will store it in the form of standard MIB (Management Information Base) for the network Management system to inquire and judge the communication status of the link.

LLDP defines a standard method for Ethernet network devices, such as switches, routers, and WLAN access points, to announce their presence to other nodes in the network and to preserve discovery information for individual neighboring devices. Detailed information such as device configuration and device identification can be published using this protocol.

12.2 LLDP set

Click the navigation bar "Basic Setting →LLDP→LLDP Settings" to enter the LLDP Settings interface, as shown in the figure below:



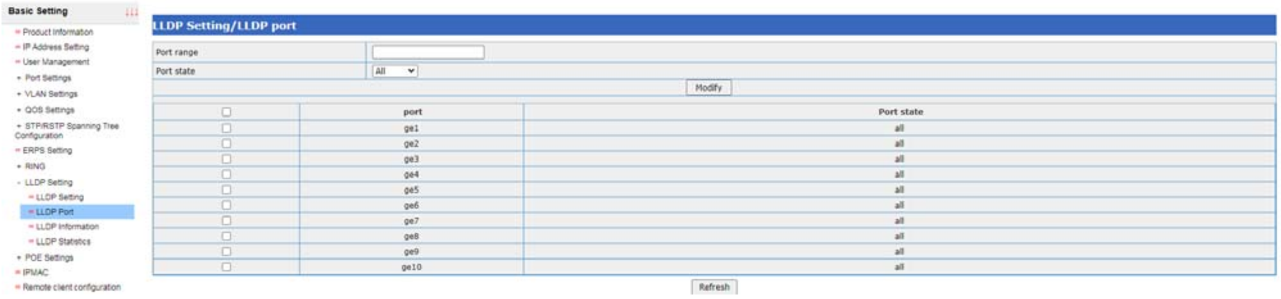
LLDP Setting/LLDP setting

LLDP enabled	● Enable ○ Disable	
LLDP Timer	30	(5-300)
Tx Hold	4	(1-10)
Reint Delay	2	(1-10)
Tx Delay	1	(1-3600)

Name	Explain
LLDP switch	Used to enable/disable LLDP.
LLDP Timer	Configure the packet sending interval of LLDP, the default value is 30s, and the value range is 5-300s.
Tx Hold	Configure the LLDP packet sending parameter multiplier. Default value is 4 and ranges from 1 to 10.
Reint Delay	Configure the LLDP packet reinitialization delay time, the default value is 2s, and the value range is 1-10s.
Tx Delay	Configure LLDP message fast sending time interval, default: 1s, and the value range is 1-3600s.

12.3 LLDP port

Click "Basic Setting →LLDP→LLDP Port" in the navigation bar to enter the interface of setting LLDP port, as shown in the figure below:



LLDP Setting/LLDP port

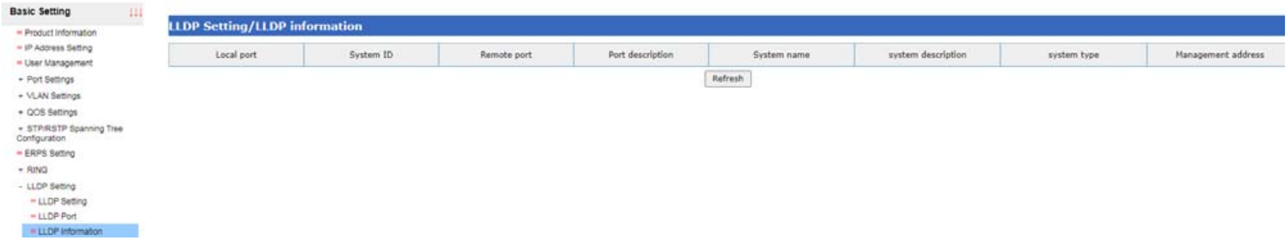
Port range	
Port state	All

□	port	Port state
□	ge1	all
□	ge2	all
□	ge3	all
□	ge4	all
□	ge5	all
□	ge6	all
□	ge7	all
□	ge8	all
□	ge9	all
□	ge10	all

Name	Explain
Port range	The port number used to modify the state of the LLDP port. Check the check box in the list of ports.
Port state	LLDP port state, including ALL, RX, TX and Disable

12.4 LLDP information

Click "Basic Setting →LLDP→LLDP Information" in the navigation bar to enter the LLDP information interface, as shown below:



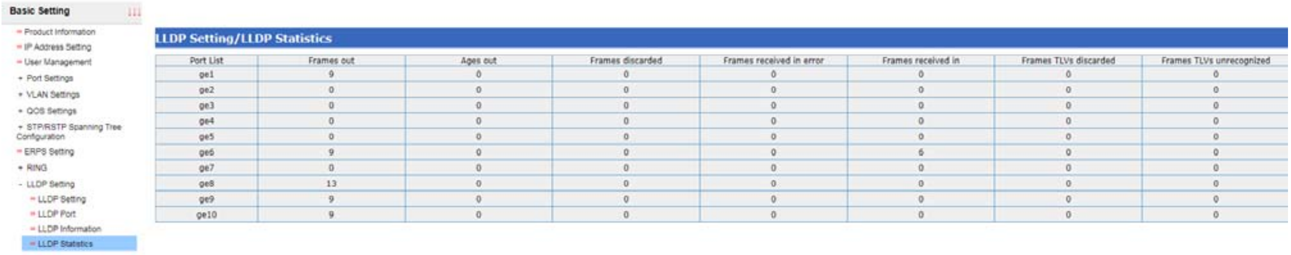
LLDP Setting/LLDP information

Local port	System ID	Remote port	Port description	System name	system description	system type	Management address

Name	Explain
Local port	Displays the port number for the local port
System ID	Displays the system ID of the remote device
Remote port	Displays the remote port of the remote device
Port description	Displays the port description of the remote device
System name	Displays the system name of the remote device
System description	Displays the system description of the remote device
System type	Displays the system type of the remote device
Management address	Displays the administrative address of the remote device

12.5 LLDP statistics

Click "Basic Setting →LLDP→LLDP Statistics" in the navigation bar to enter the LLDP statistics interface, as shown in the figure below:



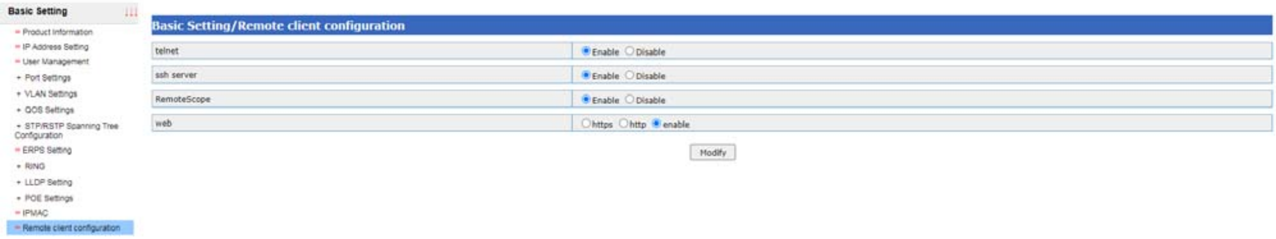
LLDP Setting/LLDP Statistics

Port List	Frames out	Ages out	Frames discarded	Frames received in error	Frames received in	Frames TLVs discarded	Frames TLVs unrecognized
ge1	9	0	0	0	0	0	0
ge2	0	0	0	0	0	0	0
ge3	0	0	0	0	0	0	0
ge4	0	0	0	0	0	0	0
ge5	0	0	0	0	0	0	0
ge6	9	0	0	0	6	0	0
ge7	0	0	0	0	0	0	0
ge8	13	0	0	0	0	0	0
ge9	9	0	0	0	0	0	0
ge10	9	0	0	0	0	0	0

Name	Explain
Frames out	Number of LLDP packet Frames out
Ages out	LLDP packet Ages out number
Frames discarded	LLDP package Frames discarded
Frames received in error	LLDP packet Frames received in error number
Frames received in	LLDP packet Frames received in number
Frames TLVs discarded	LLDP packet Frames TLVs discarded number
Frames TLVs unrecognized	LLDP packet Frames TLVS unrecognized

13 Remote client configuration

Click "Basic Setting → Remote Client Configuration" in the navigation bar, as shown in the figure below:



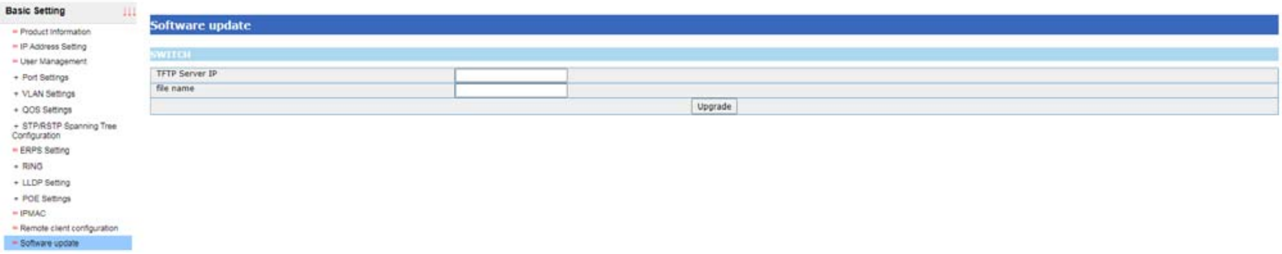
Basic Setting/Remote client configuration

telnet	● Enable ○ Disable
ssh server	● Enable ○ Disable
RemoteScope	● Enable ○ Disable
web	○ https ○ http ● enable

Name	**Explain**
telnet	Enable or disable Telnet functionality
ssh server	Enable or disable SSH Server functionality
Network management software	Enable or disable network management software functions

14 Software upgrade

Click "Basic Setting → Software Upgrade" in the navigation bar to enter the software upgrade interface, as shown in the figure below:



Software update

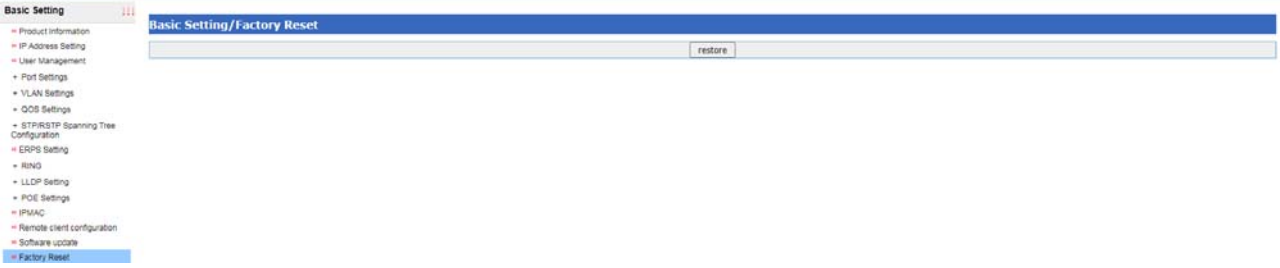
SWITCH

TFTP Server IP	
file name	

Name	**Explain**
TFTP Server IP	The IP address of the TFTP server
File name	The file name of the software, usually program.zip

15 Factory data reset

Click "Basic Setting → Restore Factory Settings" in the navigation bar to enter the interface for restoring factory Settings, as shown in the figure below:

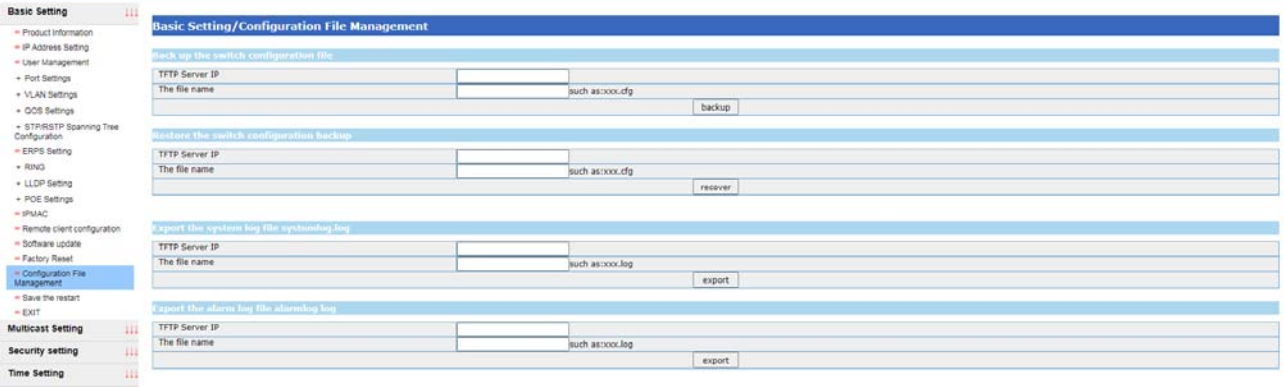


Basic Setting/Factory Reset

Click the < restore > button to restore factory Settings.

16 Profile management

Click "Basic Setting → Configuration File Management" in the navigation bar to enter the configuration file management interface, as shown below:



Basic Setting/Configuration File Management

Back up the switch configuration file

TFTP Server IP

The file name such as:xxx.cfg

backup

Restore the switch configuration backup

TFTP Server IP

The file name such as:xxx.cfg

recover

Export the system log file systemlog.log

TFTP Server IP

The file name such as:xxx.log

export

Export the alarm log file alarmlog.log

TFTP Server IP

The file name such as:xxx.log

export

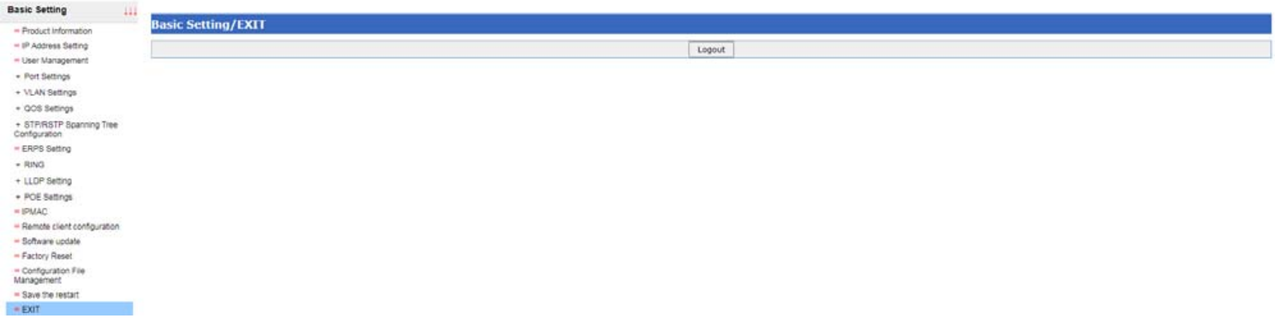
Configuration management needs the support of TFTP Server. Configuration backup is to upload the configuration files stored in Flash to TFTP Server. Configuration recovery is to download configuration files from TFTP Server into Flash.

Name	Explain
TFTP server IP	The IP address of the TFTP Server. It should be noted that the TFTP Server and the switch can communicate normally.
File name	The name of the file, in the format of the specific file.

Note: When backing up configuration files, you need to save the configuration first. After the configuration is restored, the switch needs to be restarted for the restored configuration to take effect.

17 Exit

Click the navigation bar "Basic Setting → Exit" to exit the Web. Quickly exit from the top right corner of the navigation bar.

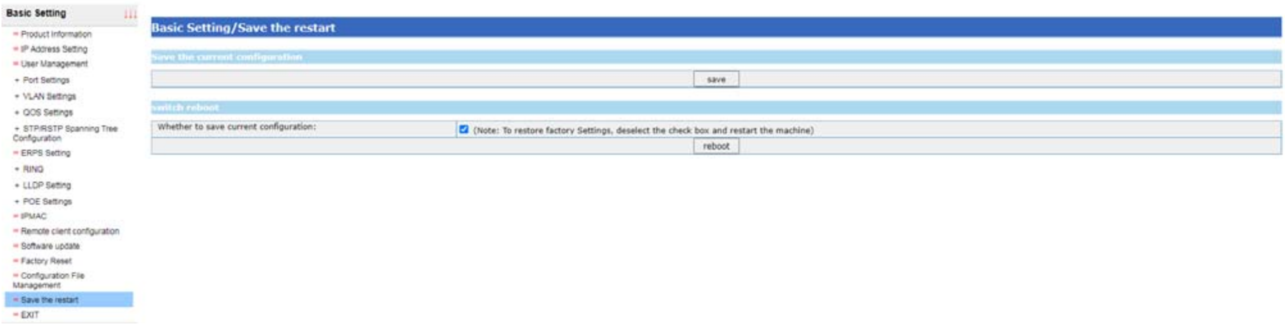


Basic Setting/EXIT

Logout

18 Save the restart

Click "Basic Setting → Save and Restart" in the navigation bar to save and restart the configuration operation. The configuration can also be saved in the upper right corner of the navigation bar.



Basic Setting/Save the restart

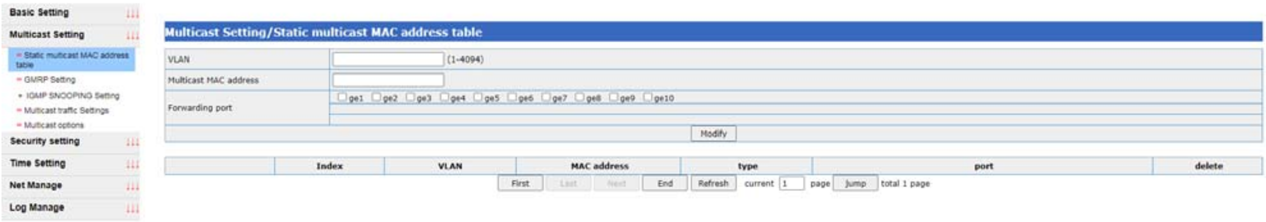
Save the current configuration

switch reboot

Whether to save current configuration: ☑ (Note: To restore factory Settings, deselect the check box and restart the machine)

19 Static multicast MAC address

Click "Multicast Settings → Static Multicast MAC Address Table" in the navigation bar to enter the multicast MAC address interface, as shown in the figure below:



Multicast Setting/Static multicast MAC address table

VLAN (1-4094)

Multicast MAC address

Forwarding port □ge1 □ge2 □ge3 □ge4 □ge5 □ge6 □ge7 □ge8 □ge9 □ge10

	Index	VLAN	MAC address	type	port	delete

current 1 page total 1 page

Name	Explain
VLAN	VLAN used to add static multicast MAC addresses.
Multicast MAC address	A multicast MAC address used to add static multicast MAC addresses.
Forwarding port	The port used to add the static multicast MAC address.
Type	MAC address types, GMRP, IGMP, and static types.
Static multicast address table	Displays a list of static multicast addresses.

20 GMRP feature configuration

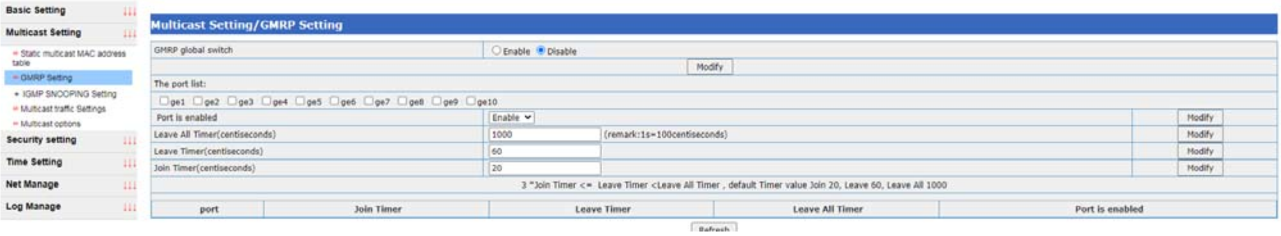
20.1 GMRP definition

GMRP is a garp-based multicast registration protocol, which supports the transmission and registration of multicast groups between network devices. In the application of smart power grid, since messages such as GOOSE and sample value are pure two-layer ether messages with only destination multicast MAC address without IP address, and IP multicast protocols such as IGMP cannot be used, only GMRP can be applied to establish two-layer multicast group and carry out effective multicast replication and forwarding of messages such as GOOSE. It can be said that GRMP is a necessary protocol for industrial Ethernet switches in smart grid.

There is another important reason to need a layer 2 multicast protocol. Like the IGMP protocol, if we set up a multicast group on our own LAN, our LAN may contain many switches. If these switches do not implement the Layer 2 Multicast protocol, then when a group member sends a packet to another group member, the switch will broadcast the packet to all ports. Since the switch does not know on which port someone has joined the multicast group, the only solution is for the administrator to configure the switch to limit the transmission of such broadcast forwarding packets. Multicast itself is dynamic, so it is not practical to rely on the configuration of the administrator to achieve multicast. Therefore, a two-layer multicast protocol is needed to dynamically manage team members.

20.2 GMRP

Click "Multicast Settings → GRMP Function Configuration" in the navigation bar to enter the GRMP interface, as shown below:



Multicast Setting/GMRP Setting

GMRP global switch ○ Enable ● Disable

The port list: □ge1 □ge2 □ge3 □ge4 □ge5 □ge6 □ge7 □ge8 □ge9 □ge10

Port is enabled: Enable

Leave All Timer(centiseconds): 1000 (remark:1s=100centiseconds)

Leave Timer(centiseconds): 60

Join Timer(centiseconds): 20

3 *Join Timer <= Leave Timer <Leave All Timer , default Timer value Join 20, Leave 60, Leave All 1000

port	Join Timer	Leave Timer	Leave All Timer	Port is enabled

Name	Explain
GMRP global switch	The enabled/disabled state of the GRMP.
Port is enabled	The enabled/disabled GRMP configuration used to set the corresponding port.
Leave All Timer	GRMP's Leave All timer. The default value is 100000ms.
Leave Timer	The GRMP Leave timer. The default value is 60000ms.
Join Timer	Join timer for GRMP. The default value is 200ms.
GMRP list	Display configuration information for All GRMP enabled ports, including the port number, the value of Leave All Timer, the value of Leave Timer, and the value of Join Timer.

21 IGMP snooping set

21.1 IGMP principle

IGMP Snooping (Internet Group Management Protocol Snooping) is a multicast constraint mechanism running on a Layer 2 Ethernet switch to manage and control multicast groups.

The second layer equipment running IGMP Snooping analyzes the received IGMP messages, establishes a mapping relationship between the port and MAC multicast address, and forwards the multicast packets according to the mapping relationship. When Layer 2 devices do not run IGMP Snooping, multicast packets are broadcast at Layer 2. When the Tier 2 device has run IGMP Snooping, the known multicast packets will not be broadcast on Tier 2, but will be multicast to the designated receiver on Tier 2, but the unknown multicast packets will still be broadcast on Tier 2.

Before and after the IGMP function is enabled is shown in Figure 20.1:

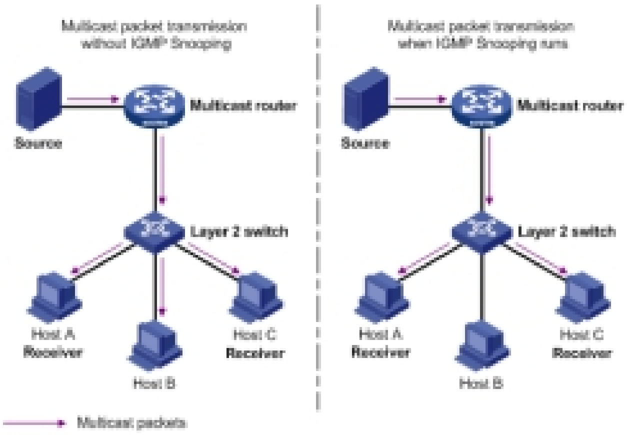
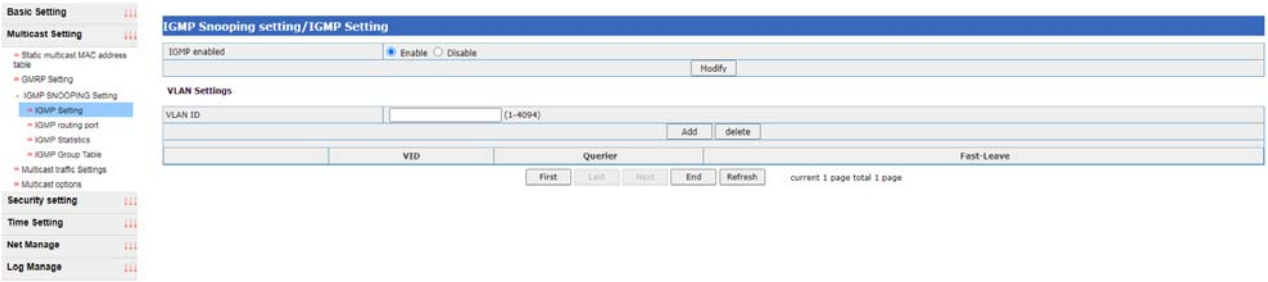


图 20. 1 IGMP 对比图

21.2 IGMP set

Click the navigation bar "Multicast Settings →IGMP snooping→IGMP Settings" to enter the IGMP configuration interface, as shown in the figure below:



IGMP Snooping setting/IGMP Setting

IGMP enabled ● Enable ○ Disable

VLAN Settings

VLAN ID (1-4094)

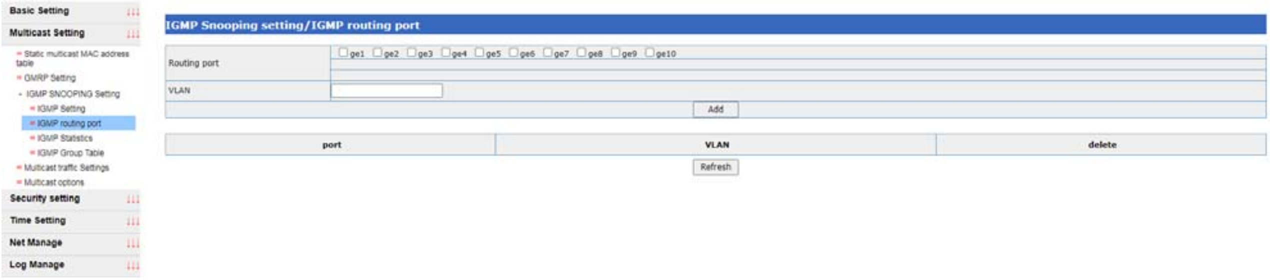
	VID	Querier	Fast-Leave

current 1 page total 1 page

Name	Explain
IGMP switch	Used to enable/disable IGMP.
VLAN ID	Create the ID of the VLAN in IGMP Snooping.

21.3 IGMP routing port

Click "Multicast Settings →IGMP snooping→ IGMP Routing Port" in the navigation bar to enter the interface of IGMP routing port, as shown in the figure below:



IGMP Snooping setting/IGMP routing port

Routing port □ge1 □ge2 □ge3 □ge4 □ge5 □ge6 □ge7 □ge8 □ge9 □ge10

VLAN

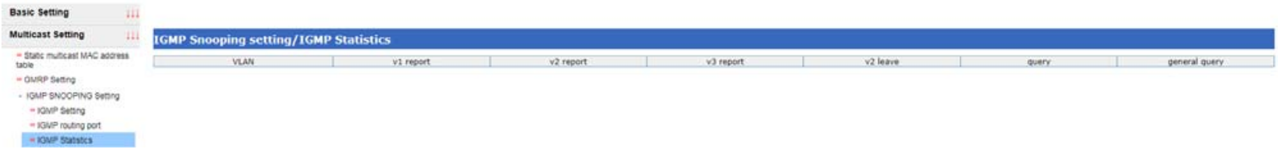
port	VLAN	delete

Name	Explain
Routing port	The port number used to add the routing port.
VLAN	The VLAN ID used to add the routing port.

Routing Port List	Displays all added routing port configuration information.

21.4 IGMP statistics

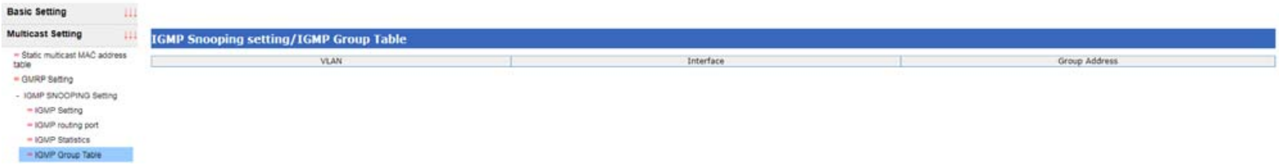
Click "Multicast Settings →IGMP snooping→IGMP Statistics" in the navigation bar to enter the IGMP Statistics interface, as shown in the figure below



Name	Explain
VLAN	The VLAN ID enabled for IGMP Snooping
v1 report	The number of IGMP Snooping v1 messages received
v2 report	Number of IGMP Snooping V2 messages received
v3 report	The number of IGMP Snooping V3 messages received
v2 leave	Number of IGMP Snooping v2 outgoing messages received
query	Number of IGMP Snooping query messages received
general query	The number of IGMP Snooping messages received

21.5 IGMP group

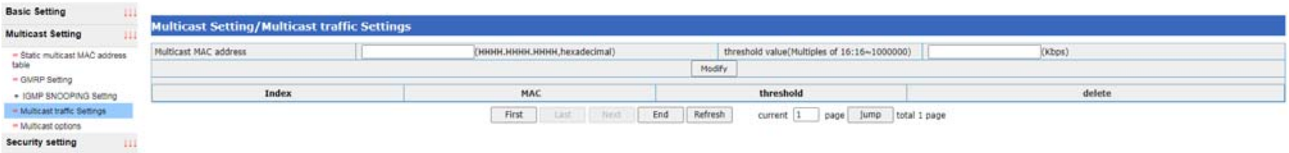
Click the navigation bar "Multicast Settings →IGMP snooping→IGMP Group" to enter the IGMP group for viewing, as shown in the figure below:



Name	Explain
VLAN	The VLAN ID of the VLAN on which the IGMPSNOoping group resides.
Interface	Receive interface for the IGMP Snooping group.
Group Address	The IP address of the IGMP Snooping group.

22 Multicast traffic speed limit

Click "Multicast Settings → Multicast Traffic Settings" in the navigation bar to enter the interface of multicast traffic setting, as shown in the figure below:

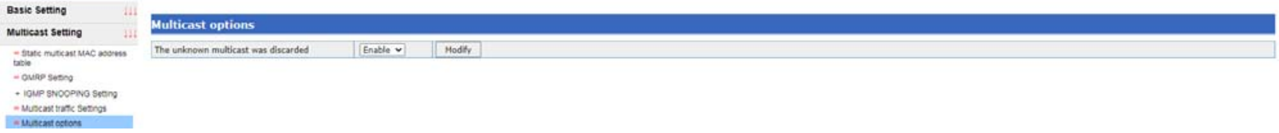


Name	Explain

Multicast MAC address	A multicast MAC address that requires speed limits. The format is hexadecimal: hhh.hhh.hhhh.
Threshold value	The speed limit value of the multicast traffic limit. The range is 64 to 1000000Kpbs and is a multiple of 64.
Port	The port on which multicast MAC address speed limits are required.
List of multicast speed limits	Display multicast address list information for all speed limits, including MAC address, threshold, port number.
Delete	Click < delete > button to delete this multicast speed limit item.

23 Multicast options

Click "Multicast Settings → Multicast Options" in the navigation bar to enter the interface of multicast options and enable the function of filtering unknown multicast. As shown in the figure below



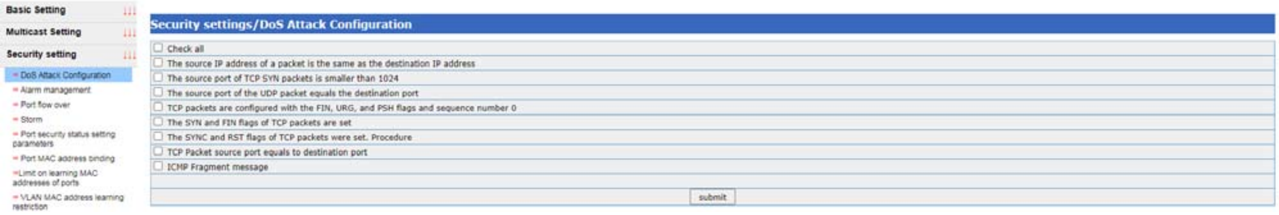
Multicast options

The unknown multicast was discarded: Enable

This page is disabled by default, unfiltered for unknown multicast; When GMRP or IGMPSNOoping is enabled, it will be enabled automatically.

24 DoS attack defense

Click the navigation bar "Security Settings → DoS Attack Configuration" to enter the DoS attack defense interface, as shown in the figure below:



Security settings/DoS Attack Configuration

- □ Check all
- □ The source IP address of a packet is the same as the destination IP address
- □ The source port of TCP SYN packets is smaller than 1024
- □ The source port of the UDP packet equals the destination port
- □ TCP packets are configured with the FIN, URG, and PSH flags and sequence number 0
- □ The SYN and FIN flags of TCP packets are set
- □ The SYNC and RST flags of TCP packets were set. Procedure
- □ TCP Packet source port equals to destination port
- □ ICMP Fragment message

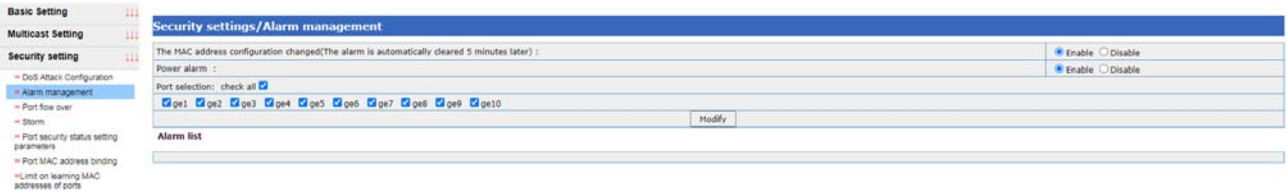
25 Alarm management

25.1 Introduction to the

The main implementation of the power supply (power failure to switch), port (port from up to down state).

25.2 Alarm management

Click "Security Settings → Alarm Management" in the navigation bar to enter the interface of alarm management, as shown in the figure below:



Security settings/Alarm management

The MAC address configuration changed(The alarm is automatically cleared 5 minutes later) : ● Enable ○ Disable

Power alarm : ● Enable ○ Disable

Port selection: check all ☑

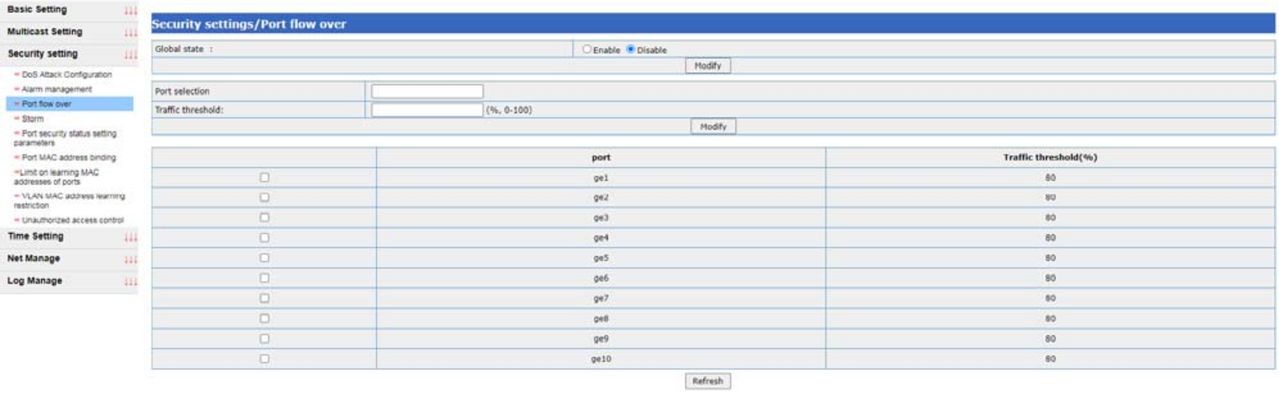
☑ge1 ☑ge2 ☑ge3 ☑ge4 ☑ge5 ☑ge6 ☑ge7 ☑ge8 ☑ge9 ☑ge10

Alarm list

Name	Explain
MAC address configuration change alert	Global switch. An alert message is generated when a MAC address binding is added or removed. The alarm lasts for 5 minutes.
Port alarm	For enabling/disabling global port alerts; Used in conjunction with Port Selection
Port selection	Use to enable/disable specified port alarms. An alert is raised when the selected port changes from the UP state to the DOWN state.

26 Port traffic is out of limit

Click "Security Settings → Out-limit Port Flow" in the navigation bar to enter the interface of out-of-limit port flow, as shown in the figure below:



Security settings/Port flow over

Global state : ○ Enable ● Disable

Port selection

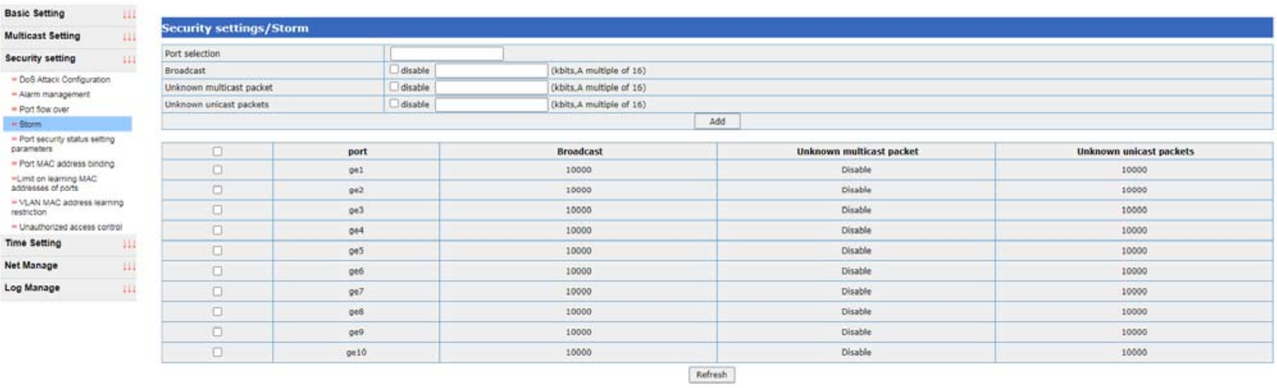
Traffic threshold: (%, 0-100)

	port	Traffic threshold(%)
□	ge1	80
□	ge2	80
□	ge3	80
□	ge4	80
□	ge5	80
□	ge6	80
□	ge7	80
□	ge8	80
□	ge9	80
□	ge10	80

Name	Explain
Port traffic is out of limit	Open or close port traffic over limit.
Port selection	Select the port you want to set.
Traffic threshold	Set the threshold value of out-of-limit port flow with a range of 0-100%. If the port flow exceeds the set value, information trap and alarm log information will appear.

27 Storm suppression

Click "Security Settings → Storm Suppression" in the navigation bar to enter the storm suppression interface of the port, as shown in the figure below:



Security settings/Storm

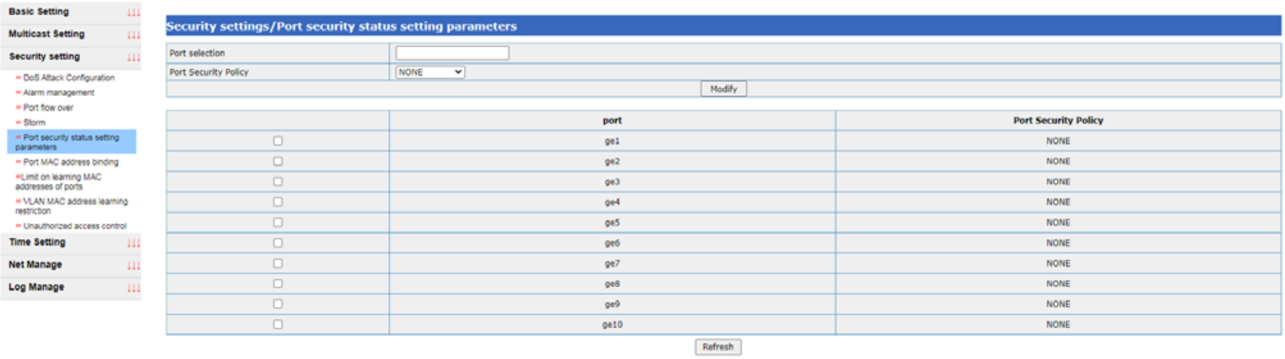
Port selection		
Broadcast	□ disable	(kbits,A multiple of 16)
Unknown multicast packet	□ disable	(kbits,A multiple of 16)
Unknown unicast packets	□ disable	(kbits,A multiple of 16)

□	port	Broadcast	Unknown multicast packet	Unknown unicast packets
□	ge1	10000	Disable	10000
□	ge2	10000	Disable	10000
□	ge3	10000	Disable	10000
□	ge4	10000	Disable	10000
□	ge5	10000	Disable	10000
□	ge6	10000	Disable	10000
□	ge7	10000	Disable	10000
□	ge8	10000	Disable	10000
□	ge9	10000	Disable	10000
□	ge10	10000	Disable	10000

Name	Explain
Port range	Select the port you want to modify.
Broadcast packet	Sets the number of broadcast packet limits for the selected port. The range is 0-1000000kbps. If checked, no restriction. Default is 10000Kbps.
Unknown multicast package	Sets the number of multicast packet limits for the selected port. The range is 0-1000000kbps. If checked, no restriction. Default to Disable.
Unknown unicast package	Sets the number of unknown unicast packet limits for the selected port. The range is 0-1000000kbps. If checked, no restriction. Default is 10000Kbps.

28 Port security state setting parameters

Click "Security Settings → Port Security State Settings Parameter" in the navigation bar to enter the interface for setting port security state parameters, as shown in the figure below:



Security settings/Port security status setting parameters

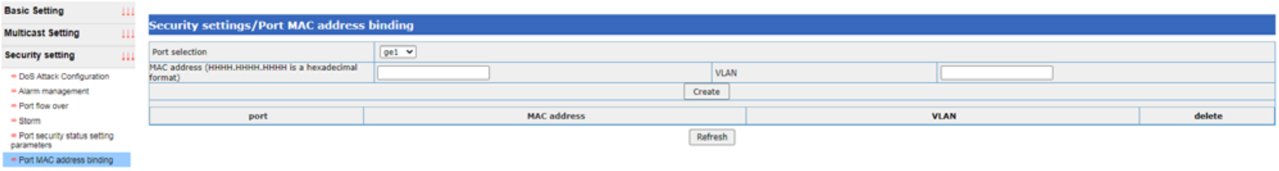
Port selection	
Port Security Policy	NONE

	port	Port Security Policy
□	ge1	NONE
□	ge2	NONE
□	ge3	NONE
□	ge4	NONE
□	ge5	NONE
□	ge6	NONE
□	ge7	NONE
□	ge8	NONE
□	ge9	NONE
□	ge10	NONE

Name	Explain
Port selection	The port number on which the port security status is to be set.
Port security policy	Port security policies, including NONE and STATIC_MAC. If static MAC mode is selected, dynamic MAC messages are not forwarded.

29 Port MAC address binding

Click "Security Settings → Port MAC address binding" in the navigation bar to enter the interface of MAC address binding, as shown in the figure below:



Security settings/Port MAC address binding

Port selection: ge1

MAC address (HHHH.HHHH.HHHH is a hexadecimal format)

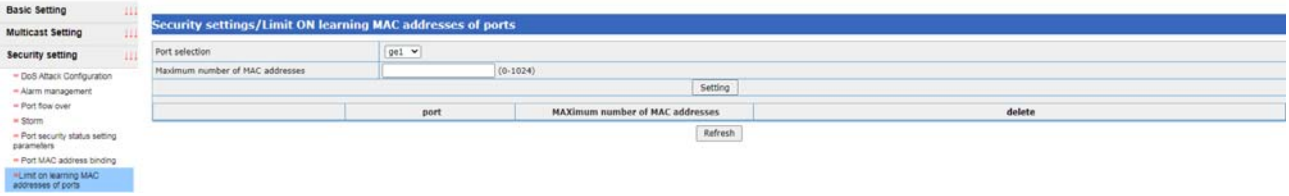
VLAN

port	MAC address	VLAN	delete

Name	Explain
Port	The port number required for MAC address binding.
MAC address	The MAC address required for MAC address binding, in the format HHHH.HHH.HHH.
VLAN	The VLAN that needs to be MAC address bound. The range is 1-4094.

30 Port MAC address learning restrictions

Click "Security Settings →MAC Address Learning Restriction" in the navigation bar to enter the MAC address learning restriction interface, as shown in the figure below:



Security settings/Limit ON learning MAC addresses of ports

Port selection: ge1

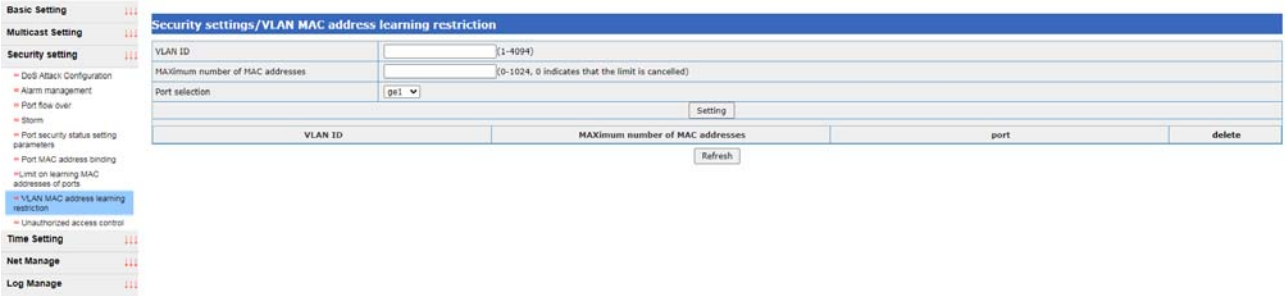
Maximum number of MAC addresses (0-1024)

	port	MAXimum number of MAC addresses	delete

Name	Explain
Port	The port number on which the number of MAC address learning limits are required.
MAC address limit maximum	Number of MAC address learning limits required. The range is 0-1024.

31 VLAN MAC address learning restrictions

Click "Security Settings →VLAN MAC address learning restriction" in the navigation bar to enter the VLAN MAC address learning restriction interface, as shown in the figure below:



Security settings/VLAN MAC address learning restriction

VLAN ID (1-4094)

MAXimum number of MAC addresses (0-1024, 0 indicates that the limit is cancelled)

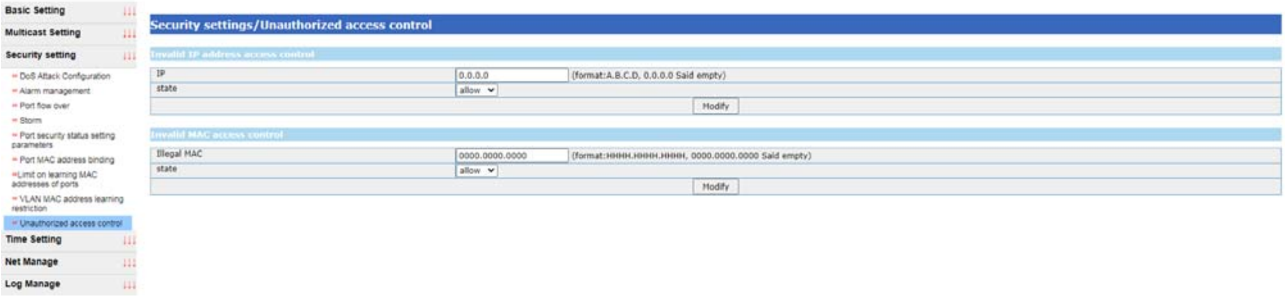
Port selection: ge1

VLAN ID	MAXimum number of MAC addresses	port	delete

Name	Explain
VLAN ID	VLANs that need to be limited to the number of Macs.
MAC address limit maximum	The number to be limited. The range is 0-32767.
Port selection	Corresponding port.

32 Illegal access control

Click the navigation bar "Security Settings → Illegal Access Control" to enter the Illegal Access Control Web, as shown in the figure below:



Security settings/Unauthorized access control

Invalid IP address access control

IP: 0.0.0.0 (format:A.B.C.D, 0.0.0.0 Said empty)
state: allow

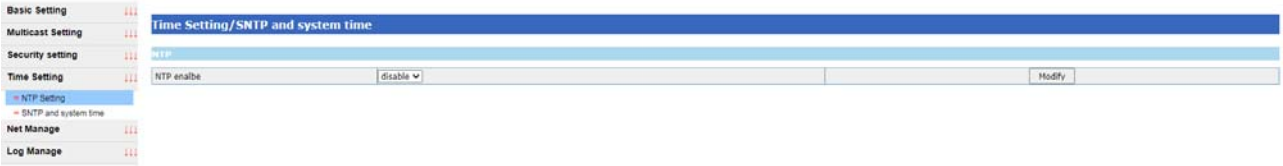
Invalid MAC access control

Illegal MAC: 0000.0000.0000 (format:HHHH.HHHH.HHHH, 0000.0000.0000 Said empty)
state: allow

Name	Explain
IP	The IP address to which access control is required.
state	The access control state corresponding to the IP address includes the following two access control states: (1) allow: allow devices using this IP address to access the switch; (2) REFUSE: Devices using that IP address are prohibited from accessing the switch.
Illegal MAC	The MAC address to which access control is required.
state	The access control state corresponding to the MAC address includes the following two access control states: (1) allow: allow devices using this MAC address to access the switch; (2) REFUSE: Devices with MAC addresses are prohibited from accessing the switch.

33 NTP set

Click the navigation bar "Time Management →NTP Settings" to enter the NTP interface, as shown in the figure below:



Time Setting/SNTP and system time

NTP

NTP enalbe: disable

Name	Explain
NTP	Configure to turn on or off NTP functionality.

34 SNTP and system time

34.1 SNTP profile

Network Time Protocol (NTP) is widely used to synchronize Network Time on the Internet. Another Protocol is a simplified version of NTP, known as SNTP (Simple Network Time Protocol).

The NTP protocol can span a variety of platforms and operating systems, with very sophisticated algorithms, which are almost immune to network latency and jitter, and can provide 1-50 ms accuracy. NTP also provides an authentication mechanism with a high level of security. However, NTP algorithm is complex and has high requirements on the system.

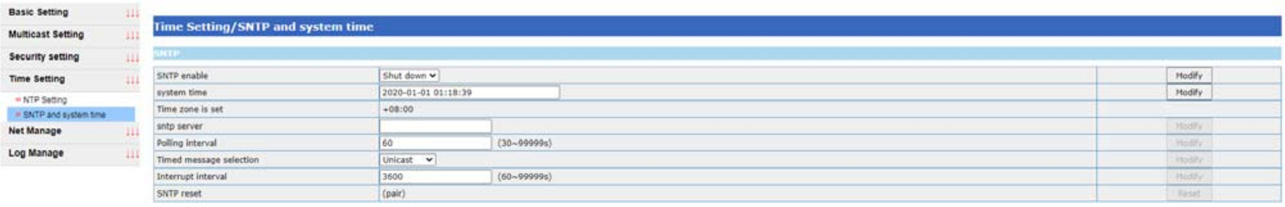
SNTP (Simple Network Time Protocol) is a simplified version of NTP, in the implementation, the calculation time using a simple algorithm, high performance. The accuracy can generally reach about 1 second, basically meet the needs of the vast majority of occasions.

The SNTP Client implemented by this device is fully compatible with NTP Server because the SNTP message is completely consistent with the NTP message.

SNTP protocol adopts the client/server working mode. The server receives GPS signals or its own atomic clock as the time benchmark of the system, and the client obtains accurate time information by regularly accessing the time service provided by the server, and adjusts its own system clock to achieve the purpose of network time synchronization.

34.2 SNTP and system time

Click the navigation bar "Time Management →SNTP and System Time" to enter the SNTP interface, as shown in the figure below:



Time Setting/SNTP and system time

SNTP

SNTP enable	Shut down	Modify
system time	2020-01-01 01:18:39	Modify
Time zone is set	+08:00	
sntp server		Modify
Polling interval	60 (30~99999s)	Modify
Timed message selection	Unicast	Modify
Interrupt interval	3600 (60~99999s)	Modify
SNTP reset	(pair)	Reset

Name	Explain
SNTP	Used to configure and display the enabled status of SNTP.
System time	The date and time used to configure and display the system.
Time zone is set	The time zone used to configure and display the system. Default is +8:00.
sntp master server	The master server used to configure and display SNTP.
sntp second server	The slave server used to configure and display SNTP.
Polling interval	The polling interval used to configure and display SNTP. The range is 30 to 99999s, and the default is 60s.
Time packet selection	Configure and display SNTP time-to-time packet selection, either Unicast or Broadcast.

35 SNMP Settings

35.1 Introduction of SNMP

SNMP (Simple Network Management Protocol) is used to ensure that Management information is transmitted between any two points in the Network, so that Network administrators can retrieve information, modify information, locate faults, complete fault diagnosis, carry out capacity planning and generate reports in any node on the Network.

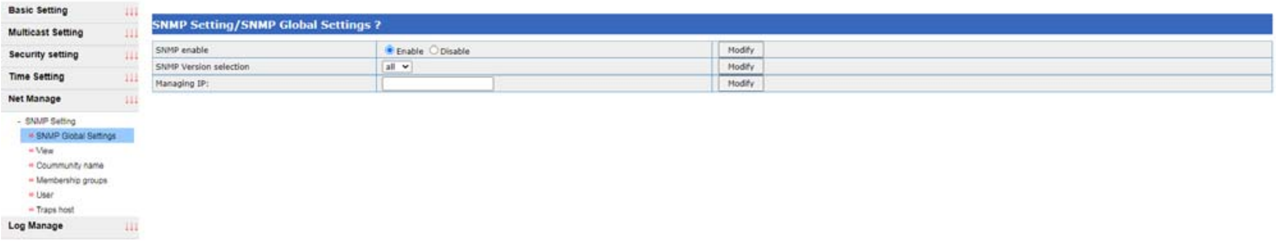
SNMP is the most commonly used environmental management protocol. SNMP is designed to be protocol independent, so it can be used over IP, IPX, AppleTalk, OSI, and other transport protocols that are used. SNMP is a family of protocols and specifications that provide a way to collect network management information from devices on a network. SNMP also provides a way for devices to report problems and errors to a network management workstation.

At present, almost all network equipment manufacturers have realized the support for SNMP. Leading the trend is SNMP, a common communication protocol that collects management information from devices on the network. The device manager collects this information and records it in the Management Information Base (MIB). This information reports on device characteristics, data throughput, communication overload, errors, and so on. MIB has a common format, so SNMP administration tools from multiple vendors can collect MIB information and present it to system administrators on the administrative console.

SNMP provides a unified, cross-platform approach to device management.

35.2 SNMP global Settings

Click the navigation bar "Network Management Settings →SNMP Global Settings" to enter the SNMP Global Settings interface, as shown in the figure below:



SNMP Setting/SNMP Global Settings ?

SNMP enable	● Enable ○ Disable	Modify
SNMP Version selection	all	Modify
Managing IP:		Modify

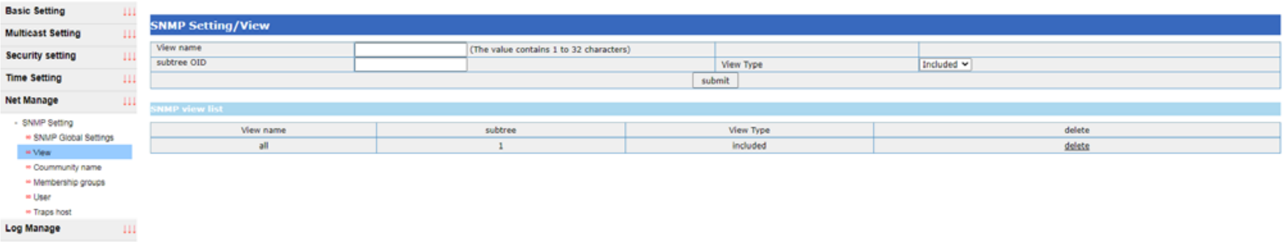
Name	Explain
SNMP	Configure to turn SNMP functionality on or off.

SNMP version selection	Configure the versions supported by SNMP, including ALL, V1, V2C, and V3.
	Option v1: Only the SNMP v1 version is supported;
	Option V2C: Only SNMP V2C version is supported;
	Option v3: Only SNMP v3 version is supported;
	Option All: All three versions are enabled simultaneously

Managing IP	The IP address of the NMS management station. All are allowed by default.

35.3 SNMP view

Click "Network Management Settings →SNMP→ View" in the navigation bar to enter the SNMP view interface, as shown below:



SNMP Setting/View

View name		(The value contains 1 to 32 characters)	
subtree OID		View Type	Included

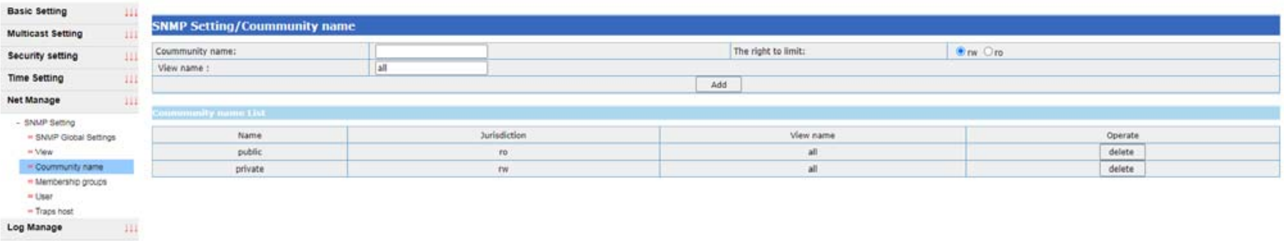
SNMP view list

View name	subtree	View Type	delete
all	1	included	delete

Name	Explain
View name	The name used to configure the SNMP view.
Subtree OID	The subtree OID used to configure SNMP views, such as "1.3.6.1".
View type	The view type (include and exclude) used to configure SNMP views.
SNMP visual chart	Use to display the name, subtree, and view type of the configured SNMP view.

35.4 SNMP community name

Click the navigation bar "Network Management Settings →SNMP→ Group Name" to enter the SNMP group interface, as shown in the figure below:



SNMP Setting/Coummunity name

Coummunity name:		The right to limit:	● rw ○ ro
View name :	all		

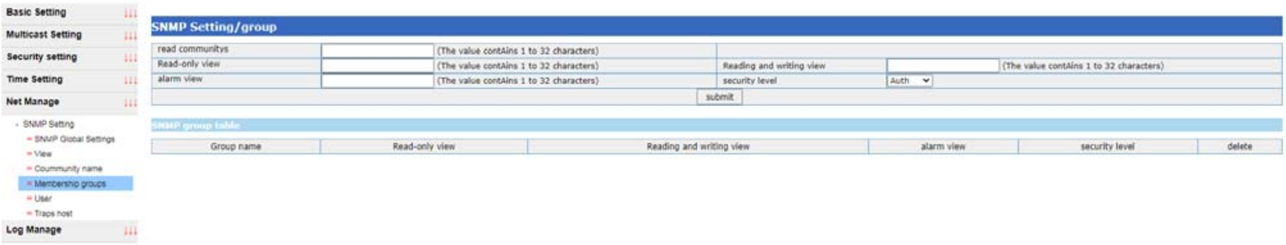
Coummunity name List

Name	Jurisdiction	View name	Operate
public	ro	all	delete
private	rw	all	delete

Name	Explain
Group name	Used to configure the SNMP community name.
permissions	Permissions used to configure the SNMP community, including RW (read-writable) and RO (writ-only).
View name	The view name used to configure the SNMP community.
Group List	Use to display the name, permissions, and view name of the configured SNMP community.

35.5 SNMP group

Click "Network Management Settings →SNMP→ Member Group" in the navigation bar to enter the interface of SNMP group, as shown in the figure below:



SNMP Setting/group

read communitys	(The value contAins 1 to 32 characters)			
Read-only view	(The value contAins 1 to 32 characters)	Reading and writing view		(The value contAins 1 to 32 characters)
alarm view	(The value contAins 1 to 32 characters)	security level	Auth	

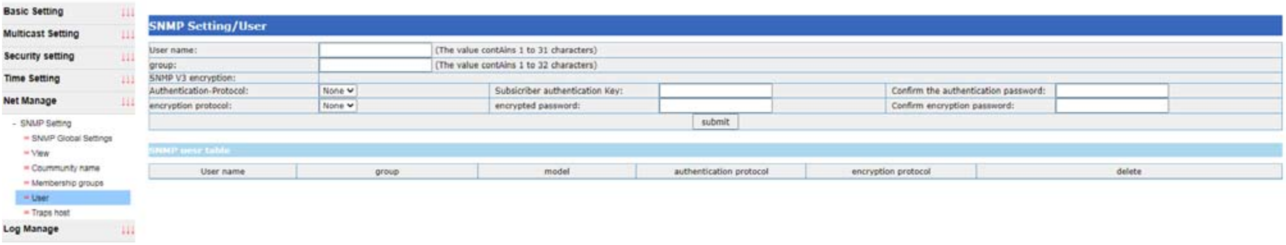
SNMP group table

Group name	Read-only view	Reading and writing view	alarm view	security level	delete

Name	Explain
Group name	The name of the group used to configure SNMP.
Read-only view	Configure the read-only view for the corresponding group.
Reading and writing view	Configure the read and write view for the corresponding group.
Alarm view	Use to configure the alerts view for the corresponding group.
Security level	It is used to configure the security level of the corresponding group and supports three security levels: AUTH, NOAUTH and PRIV.
SNMP group table	Use to display the name of the configured SNMP group, read-only view, read-write view, alert view, and security level.

35.6 SNMP users

Click the navigation bar "Network Management Settings →SNMP→ User" to enter the SNMP user interface, as shown in the figure below:



SNMP Setting/User

User name: (The value contAins 1 to 31 characters)

group: (The value contAins 1 to 32 characters)

SNMP V3 encryption:

Authentication-Protocol:	None	Subsicriber authentication Key:		Confirm the authentication password:	
encryption protocol:	None	encrypted password:		Confirm encryption password:	

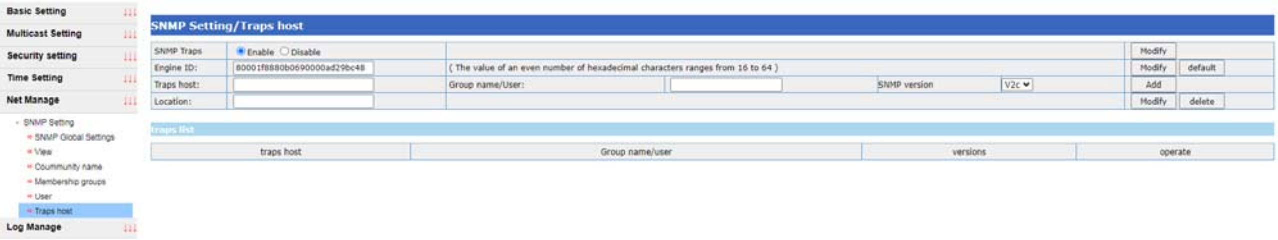
SNMP uesr table

User name	group	model	authentication protocol	encryption protocol	delete

Name	Explain
User name	Used to configure the SNMP user name.
Group	The group name used to configure the group corresponding to the SNMP user.
Authentication protocol	Authentication protocol for configuring SNMP users to support MD5 and SHA.
Authentication protocol password	The password used to configure the authentication protocol for SNMP users needs to be greater than 8.
Cryptographic protocol	The encryption protocol used to configure SNMP users. Optionally NONE, AES, and DES.
Authentication protocol password	The password used to configure the authentication protocol for the SNMP user.

35.7 SNMP host

Click "Network Management Settings →SNMP→SNMP Host" in the navigation bar to enter the SNMP host interface, as shown in the figure below:



SNMP Setting/Traps host

SNMP Traps ● Enable ○ Disable

Engine ID: 80001f8880b0690000ad29bc48 (The value of an even number of hexadecimal characters ranges from 16 to 64)

Traps host: Group name/User: SNMP version V2c

Location:

traps list

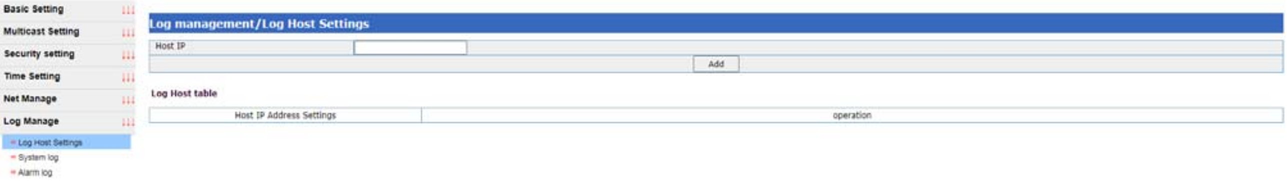
traps host	Group name/user	versions	operate

Name	Explain
SNMP Traps	Enable/Disable SNMP Traps。
Traps host	IP address for configuring the Traps host.
Group name/user name	The community name or user name used to configure the corresponding Traps host.
SNMP version	SNMP versions (SNMP v1, SNMP v2c, or SNMP v3) for configuring the corresponding Traps host
Equipment location	Used to configure the location of the device.
Traps list	Use to display the user name/user and SNMP version of the configured Traps host.

36 Log management

36.1 Log Host Settings

Login with the management user and click "Log Management → Log Host Settings" in the navigation bar to enter the Log Host interface, as shown in the figure below:



Log management/Log Host Settings

Host IP

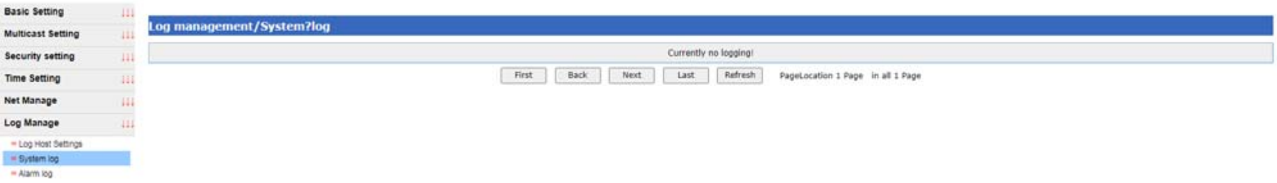
Log Host table

Host IP Address Settings	operation

Name	Explain
IP	The IP address of the system log host needs to be set.
System log host table	List of all system log hosts

36.2 System log

Click "Log Management → System Log" in the navigation bar to enter the system log interface:



Log management/System?log

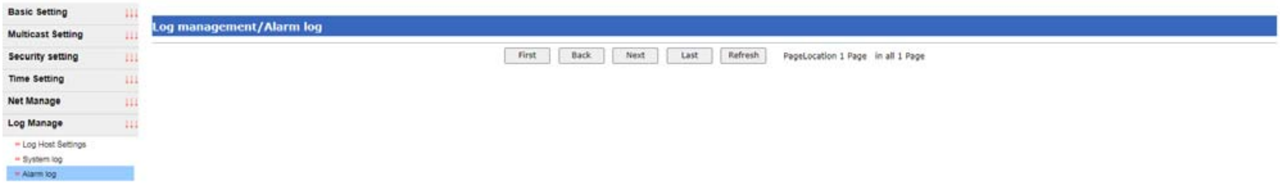
Currently no logging!

PageLocation 1 Page in all 1 Page

Name	Explain
System log	The system log records the operation information such as configuration management, including login success, logout, login failure, password modification, user operation information, etc
Log format	Log format for: < % > log level < | > time < | > equipment models < | > content description.
Level of logging	The logging levels are ERROR, WARNNING, and NOTICE. Notice: Critical operational information for the proper operation of the equipment.
Equipment model	Device model name.
Content description	Content description details the contents of the log.

35.3 Alarm log

Click "Log Management → Alarm Log" in the navigation bar to enter the interface of alarm log:



Name	explain
Alarm log	Alarm log records restart, power alarm, MAC change, port abnormal alarm, traffic out of limit alarm and other events.
Log format	Log format for: < % > log level < | > time < | > equipment models < | > content description.
Level of logging	The logging levels are ERROR, WARNNING, and NOTICE. Error: An erroneous operation or abnormal flow of equipment that requires attention and cause analysis. Warnning: An abnormal point in the operation of a device, a process that could cause a business failure, needs attention.
Equipment model	Device model name.
Content description	Content description details the contents of the log.