

## Xiamen Four-Faith Communication Technology Co.,Ltd

# **FNS420-Series Industrial Switch**

# Web configuration manual

## Index

1.	Log i	n to the switch web	4
	1.1	System requirements for WEB access	4
	1.2	Log in to the WEB configuration interface	4
2.	Syste	em Information	5
	2.1	Global Information	5
	2.2	Statistics	6
	2.3	Log	7
3.	Port I	Management	8
	3.1	Port Config	8
	3.2	Port Isolate	9
	3.3	Port Mirror	9
	3.4	Port Limit	10
	3.5	Storm Control	11
	3.6	EEE(Enery-Efficient-Ethernet)	12
4.	Basic	c(Layer 2 Management)	13
	4.1	MAC Table	13
	4.2	VLAN	13
	4.3	GVRP	17
	4.4	Link aggregation	17
	4.5	MSTP Configration	21
	4.6	ERPS	24
	4.7	Loop Protect	26
	4.8	PTP	27
	4.9	DHCP-snooping	28
	4.10	802.1X 认证	29
5.	Layeı	r 3 Config	31
	5.1	Interface Config	31
	5.2	Route Config	32
	5.3	ARP	34
	5.4	ND Config	35
	5.5	DHCP Server	36
	5.6	DHCP Relay	39
	5.7	RIP	39
	5.8	OSPF	41
	5.9	RIPng	45
	5.10	OSPFv3	46
6.	Multio	cast Management	47
	6.1	IGMP Snooping	47
	6.2	MLD Snooping	49

	6.3	IP Multicast	50
	6.4	IGMP	51
7.	Adva	nce	52
	7.1	QOS	52
	7.2	ACL	53
	7.3	SNMP	56
	7.4	RMON	60
	7.5	LLDP	61
	7.6	NTP	62
	7.7	Secure	63
8.	Syste	em Management	64
	8.1	User Config	64
	8.2	Network	65
	8.3	Service Config	65
	8.4	Configration management	66
	8.5	Firmware Upgrade	66
	8.6	Diagnostic	67
	8.7	Restart	67

# 1. Log in to the switch web

# **1.1 System requirements for WEB access**

Using this series of switches, the system should meet the following conditions..

Hardware&Software	System Requirement
CPU	Pentium 586 ↑
RAM	128MB ↑
Resolution	1024x768 ↑
Browser	IE 8.0↑ /Firefox/Google Chrome/Opera, etc.
OS	Windows XP
	<ul> <li>Windows Vista</li> </ul>
	• Windows 7
	• Windows 8
	<ul> <li>Windows 10</li> </ul>
	• Linux
	• Unix

# 1.2 Log in to the WEB configuration interface

To log in to the WEB configuration interface of this series of switches, the user needs to confirm the following conditions:

- The switch has been configured with IP. By default, the interface IP address of VLAN1 of the switch is 192.168.10.12;
- The user ensures that the IP of the network card of his local PC (management host) is in the 192.168.10.\* network segment;
- The user ensures that the network cable of his local PC is connected to any RJ45 network port of the switch;
- A host with a web browser has been connected to the network, and the host can ping the switch.

The steps to log in to the WEB configuration interface are as follows:

Step 1 Run the computer browser;

Step 2 Enter the address of the switch "http://192.168.10.12" in the address bar of the browser, and press Enter;

Step 3 As shown in Figure 1-1, enter the user name and password in the login window (the default user name and password are both admin), and click "OK".

Figure 1-1 WEB interface login window

L User Name
Password

After successfully logging in, you can configure the relevant parameters and information of the WEB interface according to your needs.

# **2. System Information**

# 2.1 Global Information

[Function Description]

On the "System Information" page, you can view Product Model, Serial Number, MAC Address, Firmware Version, Uptime, System Time and other information.

[Operation path]

Information > Global

[Interface description]

Figure 2-1 System Information Interface

Ports Status	
	$\begin{array}{cccccccccccccccccccccccccccccccccccc$
Global	
Product Model	YH6824GST4-SFP
Serial Number	SN20210301
MAC Address	AC:90:00:40:3D:00
Firmware Version	V1.0.0.1-gd06e45122
Uptime	0 Day 18 Hours 10 Minutes
System Time	2021-05-13 09:32:52 Time Sync
System	

#### Table 2-1 Main elements of the system information interface

Interface elements	Description
Product Model	Display the product model of the switch.
Serial Number	Display the serial number of the switch.
MAC Address	Display the MAC address of the switch.
Firmware Version	Display the firmware version of the switch.
Uptime	Display the operating time of the switch (the time
	from startup to the present).
System Time	Display the current time of the system.

## 2.2 Statistics

[Function Description]

On the "Statistics" page, you can view port summary statistics and detailed port statistics related information.

[Operation path]

Information > Statistics

[Interface description]

Figure 2-2 Port data

#### statistics

Basic Packet Statistics Detailed packet Statistics		MAC Frame Lei	ngth Statistics	MAC Frame Error	Statistics			
/iew Switching:	Statistics	s from last clear-up 🗸						
Port	Rx Bytes	Rx Packets	Rx Dropped	Rx Errors	Tx Bytes	Tx Packets	Tx Dropped	Tx Errors
G1	0	0	0	0	0	0	0	0
G2	284716	2371	0	0	3492824	3187	0	0
G3	0	0	0	0	0	0	0	0
G4	0	0	0	0	0	0	0	0
G5	0	0	0	0	0	0	0	0
G6	340300	1938	37	0	1276222	2232	0	0
G7	0	0	0	0	0	0	0	0
G8	678904	3849	0	0	15710 <mark>1</mark> 9	3948	0	0
G9	O	0	0	0	0	O	0	0
G10	2224	29	11	0	338627	2654	0	0

# 2.3 Log

[Function Description]

On the "Log" page, you can view and download the system log.

[Operation path]

Information > Log

Log List

[Interface description]

Figure 2-3-1 Log interface

							C	2.	Clear Log
Index	System Time	Log Level	Туре	Module	Param	Log Content			
1	2021-05-13 09:35:15	event	Login	System	User	User admin login form ip [192.168.10.18]			
2	2021-05-13 09:34:29	alert	Link	PORT	G6	Interface [G6] state change to up.			
3	2021-05-13 09:32:44	alert	Link	PORT	G8	Interface [G8] state change to up.			
4	2021-05- <mark>1</mark> 3 09:32:42	alert	Link	PORT	G2	Interface [G2] state change to down.			
5	2021-05-13 09:32:42	alert	Link	PORT	G10	Interface [G10] state change to up.			
6	2021-05-13 09:32:38	alert	Link	PORT	G10	Interface [G10] state change to down.			
7	2021-05-13 09:31:57	event	Login	System	User	User admin login form ip [192.168.10.88]			
8	2021-05-13 09:31:00	event	Login	System	User	User admin login form ip [192.168.10.88]			
9	2021-05- <mark>1</mark> 3 09:30:53	alert	Link	PORT	G2	Interface [G2] state change to up.			
10	2021-05-12 15:23:19	alert	Link	PORT	G10	Interface [G10] state change to up.			

Showing 1 to 20 of 25 rows 20 rows per page

· 1 2 ·

# 3. Port Management

# 3.1 Port Config

[Function Description]

On the "Port Config" page, you can enable or disable ports, set port speed and flow control, or view basic information about all ports.

[Operation path]

Port > Port Config

[Interface description]

#### Figure 3-1 Port configuration

#### interface

Name	State	Medium	Speed	Duplex	Flowctl State	Speed Config	Max Frame	Flowctl	Enable
Select All						Auto 👻	1518	0	
G1	*	COMBO	1000M	Half	*	Auto 🗸	1518	0	
G2	*	COMBO	1000M	Half	*	Auto 👻	1518	0	
G3	*	СОМВО	1000M	Half	*	Auto 🗸	1518	0	
G4	*	СОМВО	1000M	Half	*	Auto 👻	1518	0	
G5	*	COMBO	1000M	Half	*	Auto 🗸	1518	0	
G6	*	COMBO	1000M	Full	*	Auto 🗸	1518	0	
G7	*	COMBO	1000M	Half	*	Auto 🗸	1518	0	
G8	*	СОМВО	1000M	Full	*	Auto 🗸	1518	0	
G9	*	COPPER	1000M	Half	*	Auto 🗸	1518	0	
G10		COPPER	1000M	Full	*	Auto 🗸	1518	0	

#### Table 3-1 Main elements of the port configuration interface

Interface elements	Description
Name	Display the port name.
State	Display port status.
Medium	Displays the type of media that the port can use.
Speed	Display port speed.
Duplex	Displays the port duplex mode.
Speed Config	Configure the port speed and duplex mode.

Max Frame	Set the maximum frame.
Flowcrtl	Select the "Flow Control " check box to enable the port
	flow control function.
Enable	Select the "Enable" check box to enable the
	corresponding port. Enabled by default.

## 3.2 Port Isolate

[Function Description]

On the "Port Isolation" page, you can configure the port isolation.

[Operation path]

Port > Port Isolate

[Interface description]

Figure 3-2 Port Isolate interface

Select All	All Not Isolatio 🐱		
Name	Port Isolate	Name	Port Isolate
G1	0	G2	0
G3	0	G4	0
G5	0	G6	0
G7	0	G8	0
G9	0	G10	0
G11	0	G12	0
G13	0	G14	0
G15	0	G16	0
G17	0	G18	0
G19	0	G20	0
G21	0	G22	0
G23	0	G24	0
X1	0	X2	0
X3	0	×4	0
p: Unable to communicate between isolated points of the second points and communicate with other de	rts	Apply	

Communication between isolated ports is not possible, and isolated ports can communicate with other non-isolated ports.

# 3.3 Port Mirror

## [Function Description]

Port mirroring is also called port monitoring. Port monitoring is a data packet acquisition technology. By configuring the switch, you can copy data packets of one/several ports (mirroring source port) to a specific port (mirroring destination

port), and install one on the mirroring destination port. The host of the data packet analysis software analyzes the collected data packets, so as to achieve the purpose of network monitoring and troubleshooting.

[Operation path]

Port > Port Mirror

[Interface description]

Figure 3-3 Port mirror interface

Example: Mirror the message data sent from port 4 to port 1.

Mirror Destination Port	G1 🗸	Port Config	None Mirror 🗸
Port	Mirror Direction	Port	Mirror Direction
G1	None Mirror 🗸	G2	None Mirror 🗸
G3	None Mirror 🗸	G4	Both Mirror 🗸
G5	None Mirror 🗸	G6	None Mirror 🗸
G7	None Mirror 🗸	G8	None Mirror 🗸
G9	None Mirror 🗸	G10	None Mirror 🗸
G11	None Mirror 🗸	G12	None Mirror 🗸
G13	None Mirror 🗸	G14	None Mirror 🗸
G15	None Mirror 🗸	G16	None Mirror 🗸
G17	None Mirror 🗸	G18	None Mirror 🗸
G19	None Mirror 🗸	G20	None Mirror 🗸
G21	None Mirror 🗸	G22	None Mirror 🗸
G23	None Mirror 🗸	G24	None Mirror 🗸
X1	None Mirror 🗸	X2	None Mirror 🗸
X3	None Mirror 🗸	X4	None Mirror 🗸
		Apply	

# 3.4 Port Limit

[Function Description]

On the "Port Limit" page, you can configure the access rate of all ports.

[Operation path]

Port > Port Limit

[Interface description]

Figure 3-4 Port rate limit

interface

Port	Ingress Rate(kbps)	Ingress Burst Size ( Kbits )	Egress Rate(kbps)	Egress Burst Size (Kbits
*	Global Config	Global Config	Global Config	Global Config
G1	0	2048	0	2048
G2	0	2048	0	2048
G3	0	2048	0	2048
G4	0	2048	0	2048
G5	0	2048	0	2048
G6	0	2048	0	2048
G7	0	2048	0	2048
G8	0	2048	0	2048
G9	0	2048	0	2048
G10	0	2048	0	2048

#### Table 3-4 Main elements of the port rate limit interface

Interface elements	Description
Port	Display the port name.
Ingress rate	Configure the corresponding port ingress rate.
Ingress burst size	Configure burst packet size.
Engress rate	Configure the corresponding port export rate
Engress burst size	Configure burst packet size.

# 3.5 Storm Control

[Function Description]

On the "Storm Control" page, you can configure the rate of broadcast packets, multicast packets, and unknown unicast packets for each port to achieve port suppression.

[Operation path]

Port> Storm Control

[Interface description]

Figure 3-5 Storm control interface

Port	Broadcast(pps)	Multicast(pps)	Unknown Unicast(pps)
*	Global Config	Global Config	Global Config
G1	0	0	0
G2	0	0	0
G3	0	0	0
G4	0	0	0
G5	0	0	0
G6	0	0	0
G7	0	0	0
G8	0	0	0
G9	0	0	0
G10	0	0	0

### Table 3-5 Main elements of storm Control interface

Interface elements	Description
Port	Display the port name.
Broadcast	Configure the broadcast suppression rate of the corresponding port. Unit: pps
Multicast	Configure the multicast suppression rate of the corresponding port. Unit: pps
Unknown Unicast	Configure the unknown unicast suppression rate of the corresponding port. Unit: pps

# 3.6 EEE(Enery-Efficient-Ethernet)

[Function Description]

On the "EEE" page, you can configure EEE for each Ethernet port

[Operation path]

Port> EEE

[Interface description]

Figure 3-6 EEE

Interface

Select All	0		
Name	EEE	Name	EEE
G1	0	G2	0
G3	0	G4	0
G5	0	G6	0
G7	0	G8	0
G9	0	G10	0
G11	0	G12	0
G13	0	G14	0
G15	0	G16	0
G17	0	G18	0
G19	0	G20	0
G21	0	G22	0
G23	0	G24	0
		Annly	
		- 4193 	

# 4. Basic(Layer 2 Management)

## 4.1 MAC Table

[Function Description]

On the "MAC Table" page, you can configure the aging time of the MAC address and view the MAC address information of the port.

[Operation path]

Basic > mac

[Interface description]

#### Figure 4-1 MAC Table

#### interface

Add	Del			Expired Time(s):	300	Set
	Index	MAC Address	VLAN	Port	Туре	
	1	00-00-00-61-35	1	G6 dyn	amic Bind	
	2	4c-cc-6a-70-b4-60	1	G6 dyn	amic Bind	
	3	00-26-9e-f6-93-f5	1	G8 dyn	amic Bind	

Total 3 records Total 1 pages Current 1 page First < Previous Next > Last



### [Function Description]

On the "VLAN" page, you can view VLAN status, set port VLAN, voice VLAN, and configure MAC-based VLAN and IP-based VLAN.

[Operation path]

Basic > VLAN

[Interface description]

The following figure shows the view of the VLAN status of the switch,

Vlan S	itate	N	/lan C	onfig		Voice	VLA	V Con	fig	MAG		V Confi	g	IP VLA	AN Con	fig												
Man															Port													
Vlan	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	<b>X</b> 1	X2	ХЗ	<b>X4</b>
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

The following figure shows the configuration of port

VLAN,

/lan State VI	an Config Voice VLAN Config	MAC VLAN Config IP VLAN Con	fig	
Port	Vlan Mode	PVID	vlan untag	vlan tag
Select All	hybrid 🗸			
G1	access 🗸	1	1	
G2	access 🗸	1	1	
G3	access 🗸	1	1	
G4	access 🗸	1	1	
G5	access 🗸	1	1	
G6	access 🗸	1	1	
G7	access 🗸	1	1	
G8	access 🗸	1	1	
G9	access 🗸	1	1	
G10	access 🗸	1	1	

Port properties that can be set:

#### Access:

The access port is usually used to connect to the terminal. The access port has the following characteristics:

- There is only one VLAN, port VLAN (also known as access VLAN), which is a member of 1 by default,
- Accept unmarked frames and C-marked frames,
- Discard all frames in the unclassified access VLAN,
- All frames on the egress are sent untagged.

#### Trunk:

Trunk ports can carry multiple VLAN traffic at the same time, and are usually used to connect to other switches. Trunk port has the following characteristics:

- By default, trunk ports are members of all existing VLANs. This can be limited by using allowed VLANs,
- Unless VLAN trunking is enabled on the port and divided into different VLANs, the frames of whether the port is a member or not will be discarded,
- By default, all frames but are classified into the port VLAN (also known as the native VLAN) frame tag gets on the egress. Frames that fall into the port VLAN do not get C-tagged egress,
- The exit marking can change all the marked frames, in this case, only the entrance of the marked frame is accepted,
  - VLAN trunking may be enabled.

#### Hybrid:

Hybrid ports are similar to Trunk ports in many ways, but with additional port configuration capabilities. In addition to the features described for trunk ports, Hybrid ports have these capabilities:

• Can be configured as VLAN tag or unknown, C-tag all, S tag all, or

S-custom tag all,

- Inlet filtering can be controlled,
- Enter the acceptance frame, the exit label and configuration can be

configured independently.

#### Port VLAN:

The VLAN ID of the port (also called PVID). The allowed VLAN range is 1 to 4095, and the default is 1..

The following page is the voice VLAN config interface;

VLAN		
Enable voice vlan	0	
Vlan id	1 range: 1-4094	
cos	5 range: 0-7	
dscp	46 range: 0-63	
	Set	
Voice vlan MAC		
MAC	For Example: 00-01-02-03-04-05	

When the voice VLAN feature is enabled, the Access port can carry IP voice traffic from IP phones. When the switch is connected to a Cisco IP phone (such as a Cisco 7960 IP phone), the voice traffic sent by the IP phone has three layers of IP priority. And the CoS value of the second layer, both of these two values are set to 5 by default. For IEEE 802.1Q or IEEE 802.1p tagged traffic, the default COS value is untrusted.

Configure MAC address-based VLAN,

an State	Vlan Config	Voice VLAN Config	MAC VLAN Config	IP VLAN Config	J	
Vlan id					range: 1-4094	
MAC						For Example: 00-01-02-03-04-05
				Add		

#### No matching records found

#### Configure IP-based VLAN,

Vlan State	Vlan Config	Voice VLAN Config	MAC VLAN Config	IP VLAN Config	
Vlan id				range: 1-4094	
IP				Fo	or Example: 10.1.1.0/24
				Add	
No		VID		IP	
			No m	atching records found	

# 4.3 **GVRP**

[Function Description]

On the "GVRP" page, you can configure GVRP related functions.

[Operation path]

Basic > GVRP

[Interface description]

Enable or disable GVRP function;

Global Config	Port Config	GVRP Statistics	
Enable GVR	P		0
Create Dyna	mic VLAN		0
			Apply

Apply the enabled GVRP function to the designated port and configure its timer;

obal Config	Port Config GV	RP Statistics				
Port	Enable GVRP	Registration Mode	Applicant State	Join Timer(cs)	Leave Timer(cs)	LeaveAll Timer(cs
Select All	0	normal 🗸	normal 🗸			
G1	0	normal 🗸	normal 🗸	20	60	1000
G2	0	normal 🗸	normal 🗸	20	60	1000
G3	0	normal 🗸	normal 🗸	20	60	1000
G4	0	normal 🗸	normal 🗸	20	60	1000
G5	0	normal 🗸	normal 🗸	20	60	1000
G6	0	normal 🗸	normal 🗸	20	60	1000
G7	0	normal 🗸	normal 🗸	20	60	1000
G8	0	normal 🗸	normal 🗸	20	60	1000
G9	0	normal 🗸	normal 🗸	20	60	1000
G10	0	normal 🗸	normal 🗸	20	60	1000

View the operating information of

GVRP;

 Global Config
 Port Config
 GVRP Statistics

 Port
 JoinEmpty Rx
 JoinIn Rx
 LeaveEmpty Rx
 LeaveIn Rx
 Empty Rx
 JoinEmpty Tx
 JoinIn Tx
 LeaveIn Tx
 Empty Tx

 No matching records found
 Figure 1
 Graduate 1
 Figure 2
 Figure 2
 Figure 2
 Figure 2

# 4.4 Link aggregation

[Function Description]

Link aggregation is the formation of a logical port from multiple physical ports of the switch, and multiple links belonging to the same aggregation group can be regarded as a logical link with a larger bandwidth.

Link aggregation can realize the sharing of communication traffic among the member ports in the aggregation group to increase bandwidth. At the same time, each member port of the same aggregation group dynamically backs up each other, which improves the reliability of the link.

Member ports belonging to the same aggregation group must have consistent configurations. These configurations mainly include STP, QoS, VLAN, port attributes, MAC address learning, ERPS configuration, loop Protect configuration, mirroring, 802.1x, IP filtering, Mac filtering, Port isolation, etc.

**Tip**: It is not recommended to configure the ports and advanced functions for the ports used for link aggregation.

Link aggregation is divided into static aggregation and dynamic aggregation (LACP). The peer devices of link aggregation with switches are generally switches and NICs.

## 4.4.1 Static aggregarion config

### [Function Description]

Static aggregation requires manual configuration by the user and does not allow the system to automatically add or delete ports in the aggregation group. The static aggregation configuration logic is simple and easy to understand and use.

[Operation path]

Basic >Link Aggr

[Interface description]

Figure 4-4-1 Static aggregation

interface

Stat	ic aggree	gation	confi	9	Dyn	amic	aggre	gation	n confi	g	Link	Aggreg	ation In	format	ion													
Est	ablish	Del																	Loa	d balaı	ncing r	nodel:	SRC	&DST	MAC			•]
_	-															Port												
U	Trunk	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	X1	X2	X
	NOt Trunk	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	•
													N	lo mate	hing re	ecords f	ound											

Table 4-4-1 Main elements of static aggregation interface

Interface elements	Description
Load balancing mode	Select the load balancing mode of the data stream. There
	are 6 types:
	1.SRC MAC
	2.DST MAC
	3.SRC&DST MAC
	4.SRC IP
	5.DST IP
	6.SRC&DST IP
Port member	Select the ports that need to be aggregated into a
	group. The switch has created all aggregation groups by
	default, and the port members are empty. To configure
	member ports for the aggregation group, click the port to
	the corresponding aggregation group, and the port can be
	added to the aggregation group.

Special Note:

(1) The static aggregation of the same port cannot be configured at the same time as the dynamic LACP aggregation;

(2) Please keep the configuration consistency of the member ports of the aggregation group;

(3) The number of member ports in the aggregation group is 2-8.

[Example]

Select SMAC&DMAC for load balancing mode, and add ports 15, 16, 17, 18 to

aggregation group 1, as shown in the figure below:

Sta	tic aggree	gation	confi	9	Dyn	amic	aggre	gation	confi	g	Link	Aggreg	ation In	nformat	ion													
Es	tablish	De	1																Loa	d balaı	ncin <mark>g</mark> r	nodel:	SRC	&DST	MAC		,	•
_	-															Port												
U	Irunk	G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20	G21	G22	G23	G24	<b>X1</b>	X2	X3
	NOt Trunk	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	1	0	0	0	0	0	0	$\bigcirc$	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	С
	-													Appl	v													

# 4.4.2 Dynamic aggregation config

### [Function Description]

LACP (Link Aggregation Control Protocol, Link Aggregation Control Protocol) is a protocol based on the IEEE 802.3ad standard to realize dynamic link aggregation and disassembly. The two parties of the aggregation device exchange aggregation information through LACPDU messages, and aggregate the matching links together to send and receive data. The addition and deletion of ports in the aggregation group are automatically completed by the protocol, which has high flexibility and provides load balancing capabilities.

The configuration parameters of the LACP protocol mainly include: port LACP function enable, key value, port role (active/passive mode), port priority.

Only the ports with the LACP protocol enabled will carry out LACP negotiation, which may form an aggregation link. The key is the basis of negotiation, and only ports with the same key can negotiate to form an aggregation link. The negotiation mode is "active/passive". When "active" is selected, the device will actively initiate convergence negotiation; when "passive" is selected, the device passively accepts the convergence negotiation initiated by other devices. When two devices are interconnected, at least one or both ends need to be set to "active" mode to successfully negotiate.

### 【Operation path】

Basic > Link Aggr > Dynamic aggregarion config

[Interface description]

Figure 4-4-2 LACP configuration interface

Static aggre	egation config	Dynami	c aggregation con	fig Link Ag	gregation Inform	ation		
System ID:	AC-90-00-40-	3D-00	System Price	rity: 3276	8 Set			
Nar	me	Activit	y Mode	Send I	Mode	Port Priority	Key Value	Enabled
Selec	ct All		~		~	1-65535	0-65535	0
G	1		~		~	32768	0	0
G	2		~		~	32768	0	0
G	3		~		~	32768	0	0
G	4		~		~	32768	0	0
G	5		~		~	32768	0	0
G	6		~		~	32768	0	0
G	7		~		~	32768	0	0
G	8		~		~	32768	0	0
G	9		~		~	32768	0	0
G1	10		~		~	32768	0	0

Link aggregation information: view switch aggregation port information;

This switch supports dynamic aggregation of ports. After the dynamic protocol is

enabled on the ports, the devices of the two parties in the aggregation exchange information through the protocol. According to the parameters and status of the two parties, the matching links are automatically aggregated to send and receive data. After the convergence is formed, the switching equipment maintains the status of the convergence link, and automatically adjusts or disbands the convergence link when the configuration of both parties changes.

The configuration parameters of the dynamic protocol include the protocol switch state, negotiated key, and active and passive mode selection. Only the ports with dynamic protocol enabled will carry out dynamic negotiation, thus it is possible to form an aggregation link. The key is the basis of negotiation, and only ports with the same key can negotiate to form an aggregation link. The negotiation mode is "active passive". When "active" is selected, the device will actively initiate convergence negotiation; when "passive" is selected, the device passively accepts the convergence negotiation initiated by other devices. If some ports have already undergone static port aggregation, LACP dynamic aggregation may not be achieved.

**Note:** Dynamic LACP aggregation on the same port cannot be configured at the same time as static aggregation

tatic aggre	gation config	Dynamic aggregation	on config	Link Agg	regatio	n Information						
Trunk	Mode		Numbe	er Ports			Port List			Loa	d Balancing	
			Local						Peer	E		
	Manua Ctata	The Port Number	Priority F	Kev Value	Sign	Connection	The Port Number	Priority	Key Value	Sign	System ID	System Priorit

# 4.5 MSTP Configration

#### [Function Description]

The Spanning Tree Protocol is established in accordance with the IEEE 802.1D standard and is used to eliminate physical loops at the data link layer in a local area network. Devices running this protocol discover loops in the network by exchanging information with each other, and selectively block certain ports, and finally trim the loop network structure into a loop-free tree network structure, thereby preventing packets from being looped. The continuous growth and

infinite loop in the road network avoids the problem of reduced message processing capacity caused by the repeated reception of the same message.

The configuration of the spanning tree function of this device is simple. After the spanning tree function is enabled, it can be used by selecting the relevant protocol (STP or RSTP). The MSTP of multiple spanning tree can be used only after enabling the configuration example. **[**Operation path **]** 

Basic > mstp

[Interface description]

Figure 4-5-1 Global configuration interface

Enable Spanning-Tree	0	
Protocol Version	⊖ stp⊖rstp●mst	p
Max Age	20	range : 6-40
Hello Time	2	range : 1-10
Forward Delay	15	range : 4-60
Max Hops	20	range : 1-40
Revision Level	0	range : 0-65535
Configuration Name	AC9000403D00	Less than 32 Byte

Instance configuration: configure MSTP instance,

Set the mapping Vlan for multiple spanning trees

Configuration name: Identifies the name of the VLAN to MSTI mapping, the bridge must share the name and revision (see below), and the VLAN-to-MSTI mapping configuration in order to share the MSTI spanning tree. (In the area) The name can be up to 32 characters.

Configuration version: The revision of the above MSTI configuration. This must be an integer between 0 and 65535.

Mapping VLANs: A list of VLANs mapped to MSTI. VLANs must be separated by commas and/or spaces. VLAN can only be mapped to one MSTI. An unused MSTI should remain empty. (That is, there is no vlan mapped to it).

Glob	al Config	Instance Co	nfig Interface Ins	tance Config Interface					
м	ISTI ID				1 •				
P	riority					For exa	mple: 0-61440, the c	lefault 32768, st	ep 4096
v	lan Mapped	ľ			7.0.40.45	Separat	ed by a space, with	'-' said range. Si	ich as: 2 4-
					Add				
Desig	nated Root	8.000.AC:90	0:00:40:3D:00 Root	Port none F	Root Path Cost	0	]		
No	MSTI	Priority	Vian Mapped	Bridge ID	Regional Root	Internal	Time Since	Topo- change	
	ID			-		Path Cost	Topo-change	Count	

Interface instance configuration: configure the enablement of the instance on the

#### port.

Global Config	Instance Confi	g Interface Instar	ice Config	terface				
ISTI ID: 0	~							
Interface	Ports List	Enable Status	MSTI ID	Priority	Admin Cost	Oper Cost	Role	State
Select All								
G1	G1	*	0	128	0	20000	Disabled	forwarding
G2	G2	*	0	128	0	20000	Disabled	forwarding
G3	G3	*	0	128	0	20000	Disabled	forwarding
G4	G4	*	0	128	0	20000	Disabled	forwarding
G5	G5	*	0	128	0	20000	Disabled	forwarding
G6	G6	*	0	128	0	20000	Disabled	forwarding
G7	G7	*	0	128	0	20000	Disabled	forwarding
G8	G8	*	0	128	0	20000	Disabled	forwarding
G9	G9	*	0	128	0	20000	Disabled	forwarding
G10	G10	٠	0	128	0	20000	Disabled	forwarding

Interface configuration: Configure the ports enabled for spanning tree protocol and the enabled ports for BPDU

#### packets;

Global Config	Instance Co	nfig Interface In	stance Config	Interface						
Interface	Ports List	Enable Spanning-Tree	Root Guard	BPDU Guard	Admin	Edge	Oper Edge	Admin Po Poir	oint-to- It	Oper Point-to- Point
Select All		0	0	0	Auto	~		Auto	~	
G1	G1		0	0	Auto	~	NO	Auto	~	NO
G2	G2		0	0	Auto	~	NO	Auto	~	Yes
G3	G3		0	0	Auto	~	NO	Auto	~	NO
G4	G4		0	0	Auto	~	NO	Auto	~	NO
G5	G5		0	0	Auto	~	NO	Auto	~	NO
G6	G6		0	0	Auto	~	NO	Auto	~	Yes
G7	G7		0	0	Auto	~	NO	Auto	~	NO
G8	G8		0	0	Auto	~	NO	Auto	~	Yes
G9	G9		0	0	Auto	~	NO	Auto	~	NO
G10	G10		0	0	Auto	~	NO	Auto	~	Yes

## **4.6 ERPS**

#### [Function Description]

ERPS (Ethernet Ring Protection Switching): Ethernet multi-ring protection technology, the protocol standard is ITU-TG.8032 multi-ring standard. ERPS's pursuit of higher performance and more security is the eternal development direction of the network, and the Ethernet ring technology has become an important means of redundancy protection in the second-tier network.

In the two-layer network, the STP protocol is generally used for network reliability, as well as the loop protection protocol mentioned in the previous section. The STP protocol is a standard ring network protection protocol developed by IEEE and has been widely used. The application is limited by the size of the network, and the convergence time is affected by the network topology. STP generally takes a second to converge, and it takes longer when the network diameter is larger. Although RSTP/MSTP can reduce the convergence time to milliseconds, it still cannot meet the requirements for services with high service quality requirements such as 3G/NGN voice. In order to further shorten the convergence time into being.

ERPS is a link layer protocol specially applied to the Ethernet ring. It can prevent the broadcast storm caused by the data loop in the Ethernet ring; when a link on the Ethernet ring is disconnected, the backup link can be quickly activated to Restore communication between nodes on the ring network. Compared with the STP protocol, the ERPS protocol has the characteristics of fast topology convergence (less than 20ms) and the convergence time has nothing to do with the number of nodes on the ring network. The loop protection function is similar to STP and erps, but the loop protection does not have IEEE standards and belongs to a private protocol. The configuration is simple to use, and the convergence time is also in seconds. For simple ring network topologies and common network services, it has advantages in line backup It's also obvious. [Operation path]

Basic > ERPS

[Interface description]

## Figure 4-6-1 ERPS Global Config interface

Global Config	ERPS Profile Config	ERPS Ring Config	ERPS Instance Config	ERPS Sub-Ring Instance Config	ERPS Ring Instance Info
Enable ERF	•s			Set	
STG ID			1	~	
Vlan Mappe	ed		7.9.10	Separated by	a space, with '-' said range. Such as: 2 4
			Add		
Index	STG	B ID	Vlan I	Mapped	
1	C		1-4	1094	

# Figure 4-6-2 ERPS Profile Config interface

	nfig ERPS Profi	le Config ERPS	S Ring Config	ERPS Insta	nce Config ER	PS Sub-Ring Instance Config	ERPS Ring Inst	ance Info	
Profile	Name				test	Range: less	than 32 characters		
WTR 1	Timer				1	Range: 1-1	2, Unit: minute		
Hold-c	off Timer					Range: 0-1	0000, Unit: ms, Step: 1	00ms	
Guard	Timer					Range: 10-	2000, Unit: ms, Step: 1	Oms	
Rever	tive								
Rever	tive				Add				
Reven	tive Profile Name	WTR Timer (min	ute) Hold-of	f Timer (ms)	Add Guard Timer (ms	WTB Timer (ms)	Revertive		
Revent ndex 1	tive Profile Name Default	WTR Timer (min	ute) Hold-of	f Timer (ms) 0	Add Guard Timer (ms 500	WTB Timer (ms) 5500	Revertive	Set	Del

# Figure 4-6-3 ERPS Ring Config interface

lobal Config	ERPS Profile Config	ERPS Ring Config	ERPS Instance Config	ERPS Sub-Ring Instance Config	ERPS Ring Instance Info
Ring ID			1	~	
East Interfa	ace		X1	~	
West Interf	ace		X2	~	
			Add		
Index	Ring ID	E	East Interface	West Interface	
1	1		X1	X2	Del

Figure 4-6-4 ERPS Instance Config interface

Global Config	ERPS Profile C	config ERPS	Ring Config	ERPS Instance Config	ERPS Sub-Ring Insta	nce Config	ERPS Ring Instance I	nto					
Instance ID						1 Add	]	•					
Del Instance	Physical Ring ID	East Interface	West Interface	Node Role	Role Port	Profile Name	Ring Type	R-APS Channel	Data Reference STG	Data VLAN	R-APS Level	Protocol Version	Enable
0 1	1 •			Owner Node	East Interface	test 🗸	Major Ring 🗸	3001	0 ~		7 🗸	V2 •	
						Apply							

# Figure 4-6-5 ERPS Ring Instance Info interface

Global Config	ERPS Pro	ofile Config	ERPS	Ring Config	ERPS I	nstance Config	ERPS Sub-R	ing Instance Config	ERPS Ring In	stance Info				
Instance ID: 11	D	Physical Rin	ig ID	Enable E	RPS	Ring Typ	e ii	Instance State	Node Role		Data VLAN List	Attached Sub-Ring Instances	Attached to Major Instance	Virtual ID(Vlan ID : Ring ID)
1		None		*		Major Ri	g	Init	None		1.0			- 14 C
Interfa	асе Туре		Interf	face name		Interface	Role	Link S	itate	F	Forced Switch	Manual Sw	itch	Clear
East	Interface			-						F	orced Switch	Manual Sw	itch	Clear
West	Interface			1.5		121					orced Switch	Manual Sw	itch	Clear

# 4.7 Loop Protect

## [Function Description]

The loop protection function is similar to STP in terms of functions, but the loop protection does not have the IEEE standard and is a private protocol. It is simple to configure and use. It has obvious advantages in line backup for simple ring network topologies and common network services.

On the "Loop Protection" page, you can enable or disable the loop protection function and set related parameters.

[Operation path]

Basic > Loop Protect

[Interface description]

Figure 4-7-1 Loop protection Global Config

interface

Global Config Port Config	
Enable	0
Tx Interval	1 range : 1-10 s
Port Auto-Recover Time	3 s. Blocked port will recover if not received PDU while timer expires.
	Apply

Figure 4-7-2 Loop protect port config

interface

Global Config Po	ort Config			
Port	Enabled	tx	State	Loop
Select All				
G1			Down	*
G2			Down	*
G3			Down	*
G4			Down	*
G5			Down	*
G6			Forwarding	*
G7			Down	*
G8			Forwarding	*
G9			Down	*
G10			Forwarding	*

# 4.8 PTP

PTP enable: enable PTP function globally;

The PTP protocol defines the following three types of basic clock nodes: OC (Ordinary Clock): Only one PTP communication port clock is an ordinary clock.

BC (Boundary Clock): A clock with more than one PTP communication port.

TC (Transparentclock): Compared with BC/OC, BC/OC needs to keep time synchronization with other clock nodes, while TC does not keep time synchronization with other clock nodes. TC has multiple PTP ports, but it only forwards PTP protocol packets between these ports and corrects the forwarding delay, and does not synchronize time through any one

port.

Global Config Port Config	
PTP Enable	0
PTP Clock	○ ordinary ○ boundary ○ transparent PTP Clock Type
	Apply

## Port configuration

Enable the PTP function of the designated port;

Global Config Port Config		
Port	Enabled	State
Select All		
G1		Down
G2		Down
G3		Down
G4		Down
G5		Down
G6		Forwarding
G7		Down
G8		Forwarding
G9		Down
G10		Forwarding

# 4.9 DHCP-snooping

### Global configuration: enable DHCP monitoring

### function;

Global Config	Static Binding	Port Config	
Enable DHC	P-Snooping		
			Apply

#### Static Binding: configure static monitoring port

MAC				For Example: 02-02-03-04-05-0
IP Address				For Example: 192.168.1.1
Port			G1 ~	•
		Add		

Port configuration: enable the DHCP monitoring function on the

port;

Global Config	Static Binding Port Config	
Port	Untrust	IPSG
Select All	0	0
G1	0	0
G2	0	0
G3	0	0
G4	0	0
G5	0	0
G6	0	0
G7	0	0
G8	0	0
G9	0	0
G10	0	0

## 4.10 **802.1X**

## [Function Description]

The 802.1X protocol was proposed by the IEEE802 LAN/WAN committee to solve the problem of wireless LAN network security. Later, the protocol was applied to Ethernet as a common access control mechanism for LAN ports, and was mainly used to solve the problems of authentication and security in the Ethernet. At the port level of the LAN access device, the connected equipment Authentication and control.

[Operation path]

Basic > 802.1X

[Interface description]

On the "Global Configuration" page, you can enable or disable the relevant parameters of the 802.1x authentication function.

Figure 4-1-1 Global configuration

interface

Global Config	RADIUS Server Config	Port-based Authentication	Authentication Host	
802.1X Settings				
Enable 802.1X			0	
Auth Method			Port-Auth	•
RADIUS Client Ac	idress			For Example : 192.168.200.1
RADIUS Client Po	ort		1812	range : 0-65535 , Defaults 1812
RADIUS Server K	ey			range : less than 64 characters
RADIUS Server R	etransmit		3	range: 1-100, Defaults 3
RADIUS Server Ti	imeout		5	range: 1-1000, Defaults 5
RADIUS Server D	eadtime		0	range: 0-1440, Defaults 0
			Apply	

## Figure 4-10-2 RADIUS Server Config

### interface

			No matching r	records found	
IP Addre	ess The Port	Number	Server Key	Retransmit	Timeout
Add RADIUS	Server				
obal Config	RADIUS Server Config	Port-based A	uthentication Authenti	cation Host	

Add RADIUS Server	×
RADIUS Server Address	For Example : 192.168.200.1
RADIUS Server Port	range: 0-65535, Defaults 1812
RADIUS Server Key	range : less than 64 characters
RADIUS Server Retransmit	range: 1-100, Defaults 3
RADIUS Server Timeout	range : 1-1000 , Defaults 5

Figure 4-10-3 Port-based Authentication Interface

Global Config	RADIUS Server Config	Port-based Authentication	Authentication Host	J							
Port Name	Port Auth Enable	Port Auth Mode	Ctrl Direction	Version	Auth Status	Quiet Period	Reauth Max	EAP Tx Period	Reauth Period	Reauthentication	Key Transmit
Select All	0	Force Unauthorized 🗸	Both-dir 👻	1 💌						0	0
G1	0	Auto 👻	In-dir 🗸	2 🗸	Uncontrolled	60	2	30	3600	0	0
G2	0	Auto 🗸	In-dir 🗸	2 🗸	Uncontrolled	60	2	30	3600	0	0
G3	0	Auto 👻	In-dir 🗸	2 🗸	Uncontrolled	60	2	30	3600	0	0
G4	0	Auto 🗸	In-dir 🗸	2 ~	Uncontrolled	60	2	30	3600	0	0
G5	0	Auto 👻	In-dir 🗸	2 ¥	Uncontrolled	60	2	30	3600	0	0
G6	0	Auto 🗸	In-dir 🗸	2 🗸	Uncontrolled	60	2	30	3600	0	0
G7	0	Auto 👻	In-dir 🗸	2 🗸	Uncontrolled	60	2	30	3600	0	0
G8	0	Auto 🗸	In-dir 🗸	2 🗸	Uncontrolled	60	2	30	3600	0	0
G9	0	Auto 🖌	In-dir 🗸	2 🗸	Uncontrolled	60	2	30	3600	0	0
G10	0	Auto	In-dir 🗸	2 ~	Uncontrolled	60	2	30	3600	0	0

#### Figure 4-10-4 Authtication Host Interface

Global Config	RADIUS Server Config	Port-based Authentication	Authentication Host		
Port-Auth Infor	mation				
User Na	me Port	Session Time	(S) Authentication Method	MAC Address	Session State and Reason
		Nor	matching records found		

# 5. Layer 3 Config

# 5.1 Interface Config

[Function Description]

On the "Interface Configuration" page, you can configure interface parameters.

[Operation path]

Layer3 > Interface

[Interface description]

Figure 5-1 Interface Config Interface

[Example]

As shown in the figure: set the interface name to vlanif20 and the IP to 192.168.20.1/32.

				Interface Name	vlanif20	✓ Interface Name	vlanif20	~	
Ę	Create Inte Delete Inter	rface face		IPV4 Address	AddIPV4	For Example: 10.1 1724 Address	AddIPV6	For Example	fe80:fe00::1/6
0	Interface	State	Mode	IPV	4 Address	IPV6 Addres	ss	MAC	Enable
	eth0	DOWN	Ethernet					ac-ac-ac-00-00-01	
	lo	UP	Loopback	12	27.0.0.1/8	.::1/128		00-00-00-00-00	1-1-
	vlanif1	UP	Unknown	192.168.10.12	/24 Set	fe80:fe00::1/64	Set	ac-90-00-40-3d-00	
	vlanif20	UP	Unknown	192,168,20,1/32	Set Del		Set Del	ac-90-00-40-3d-00	

Table 5-1 Main elements of the interface configuration interface

Interface elements	Description
Interface	Set the name of the Layer 3 interface, the format is vlanifX (X
	range 1-4094).
Enable	Enable or disable the Layer 3 interface function. Enabled by
	default.
IPV4 Address	Set the IP address and mask.
Set	After modifying the IP, click the Set button and the
	modification will be applied.

# 5.2 Route Config

[Function Description]

Static routing refers to routing information manually configured by users or network administrators. When the network topology or link status changes, the network administrator needs to manually modify the related static routing information in the routing table. Static routing information is private by default and will not be passed to other routers. Of course, the network administrator can also configure the router to be shared. Static routing is generally suitable for relatively simple network environments. In such an environment, network administrators can easily understand the network topology and set correct routing information.

【Operation path】

#### Layer3 > Route

### [Interface description]

# Figure 5-2-1 View IPv4 Route interface

View IPv4 Route	IPv4 Static Route	View IPv6 Route	IPv6 Static Route			
No	purpose		Mask	Sign	Gateway	Out Interface
1	127.0.0.0		8	C>*		ю
2	192.168.10	.0	24	C>*		vlanif1
3	192.168.20	.1	32	C>*		vlanif20

Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP, P - PIM, A - Babel, N - NHRP, > - selected route, \* - FIB route



# Figure 5.2.2 IPv4 Static Route Config interface

/iew IPv4 Ro	IPv4 Static Route	View IPv6 Route	IPv6 Static Route		
Destinati	on prefix			For Example:	10.1.1.0/24
Gateway				For Example: 10.0.0.1	
distance				range: 1-255	
			Add		
No	Destination prefix	Mask	Gateway	distance	
1 eg	192.168.30.0	24	192.168.20.2	1	De

#### Table 5-2-2 Main elements of static routing interface

Interface elements	Description
Destination Prefix	Fill in the destination network address.
Gateway	Fill in the address of the next hop.
distance	Fill in the management distance, the default is 1, and
	the range is 1-255.

Figure 5-2-3 View IPv6 Route Interface

w IPv4 Route	IPv4 Static Route View IP	Pv6 Route IPv6 Static Rou	te		
No	purpose	Mask	Sign	Gateway	Out Interfa
1	::1	128	C>*		lo
2	fe80::	64	C *		vlanif20
3	fe80::	64	C>*		vlanif1
4	fe80:fe00::	64	C>*		vlanif1
5	ff00::	8	K>*		vlanif20
ure 5.2. w IPv4 Route	4 IPv6 Static R	Oute Config Ir w IPv6 Route IPv6 Stat	Refresh Iterface ic Route		
ure 5.2.	4 IPv6 Static R	OUTE Config Ir w IPv6 Route IPv6 Stat	Refresh Iterface ic Route		
ure 5.2. w IPv4 Route	4 IPv6 Static R	oute Config Ir w IPv6 Route IPv6 Stat		J For	Example: 3ffe:506::/
ure 5.2. w IPv4 Route Destination pro Gateway	4 IPv6 Static R IPv4 Static Route Vie	oute Config Ir w IPv6 Route IPv6 Stat		For Example: 21	Example: 3ffe:506:://
ure 5.2. w IPv4 Route Destination pro Gateway	4 IPv6 Static R IPv4 Static Route Vie	oute Config Ir w IPv6 Route IPv6 Stat	Refresh hterface ic Route	For Example: 21	Example: 3ffe:506:://
ure 5.2. aw IPv4 Route Destination pro Gateway distance	4 IPv6 Static R IPv4 Static Route Vie	oute Config Ir w IPv6 Route IPv6 Stat	Refresh hterface ic Route	For Example: 21	Example: 3ffe:506::/{ 134:3e::1
ure 5.2. w IPv4 Route Destination pro Gateway distance	4 IPv6 Static R IPv4 Static Route Vie	oute Config Ir w IPv6 Route IPv6 Stat	Refresh terface ic Route	For Example: 21	Example: 3ffe:506::/( 134:3e::1
ure 5.2. <sup>w IPv4 Route</sup> Destination pro Gateway distance	4 IPv6 Static R	oute Config Ir w IPv6 Route IPv6 Stat	Refresh terface ic Route	For Example: 21	Example: 3ffe:506::// 134:3e::1

## 5.3 ARP

[Function Description]

On the ARP configuration page, you can configure the arp aging time or statically bind IP+MAC. One of the IP or MAC is different from the IP or MAC in the binding entry. It cannot access the CPU but can be forwarded; IP+MAC are all different Or if they are all the same, they can access the CPU, and they can also be forwarded.

[Operation path]

Layer3 > arp

[Interface description]

Figure 5-3-1 View ARP

interface

ARP View	Static ARP	ARP Aging Time				
No		IP Address	MAC Address	Out Interface	Mode	ARP Aging Time
1		192.168.10.18	4c-cc-6a-70-b4-60	vlanif1	dynamic	14240
2		192.168.10.88	00-26-9e-f6-93-f5	vlanif1	dynamic	14240

Table 5-3-1 Main elements of the View ARP configuration interface

Interface elements	Description
No	Serial number.
IP Address	The IP address of the ARP entry.
MAC Address	The MAC address of the ARP entry.
Out Interface	Display the bound virtual interface.
Mode	Shows whether the arp entry is dynamic or static.
ARP Aging Time	Display Arp aging time, the default is 14400s.

Figure 5-3-2 Static ARP Config interface

Set the IP address and MAC address to be

bound;

IP Address			For Example : 192.168.1.1
MAC Address		Add	For Example : 00-01-02-03-04-05
No	IP Address	MAC	
		No matching records found	

## Figure 5-3-3 ARP Aging Time Config interface

Aging Tim	State	Interface	No
14400	DOWN	eth0	1
14400	UP	ю	2
14400	UP	vlanif1	3
14400	UP	vlanif20	4

# 5.4 ND Config

## [Function Description]

On the ND configuration page, you can configure the ND aging time or statically bind IP+MAC. One of the IP or MAC is different from the IP or MAC in the binding entry. It cannot access the CPU but can be forwarded; IP+MAC are all different Or if they are all the same, they can access the CPU or forward them.

### [Operation path]

Layer3 > ND

[Interface description]

# Figure 5-4-1 View ND interface

ND View	Static ND	ND Aging Time				
No		IP Address	MAC Address	Out Interface	Mode	ND Aging Time
1		fe80::95a:6a30:7e0b:ae2c	00-26-9e-f6-93-f5	vlanif1	dynamic	14190
2		fe80::2156:41f4:8163:e630	4c-cc-6a-70-b4-60	vlanif1	dynamic	14190
3		fe80::5a41:20ff:fead:a6c4	58-41-20-ad-a6-c4	vlanif1	dynamic	11620

# Figure 5-4-2 Static ND interface

IP Address			For Example : fe80:fe00::fe0e
MAC Address			For Example : 00-01-02-03-04-0
Interface	<u>\</u>	/lanif1 ~	]
	Add		

# Figure 5-4-3 ND Aging Time Config interface

No	Interface	State	Aging Time(s
1	eth0	DOWN	14400
2	lo	UP	14400
3	vlanif1	UP	14400
4	vlanif20	UP	14400

# 5.5 DHCP Server

#### [Function Description]

On the "DHCP Server" page, you can configure the address pool and static binding configuration.

#### [Operation path]

Layer3 > DHCP Server

[Interface description]

## Figure 5-5-1 Global configuration interface

Add	Iress Pool Config	Client List	Static client config							
ļ	Enable DHCP Server					0				
	Max Lease Num					4096		range : 2048-10	0240, Defaults 4096	
					5	Set				
	] _									
Ad	d Address Pool Del	ete Address Pool								
	Address Pool Name	Subnet segme	ent Default Gateway	Begin IP	End IP	Lease time	DNS server 1	DNS server 2	Domain Name Service	NetBIOS server
				1	vo matchi	ng records fou	nd			

## Figure 5-5-2 Address Pool Setting

Interface

NetBIOS server	For Example: 192.168.0.1
Domain Name Service	For Example: 192.168.0.1
DNS server 2	For Example: 192.168.0.1
DNS server 1	For Example: 192.168.0.1
Default Gateway	For Example: 192.168.0.1
Lease time	Seconds
End IP	
Begin IP	
Subnet segment	For Example: 192.168.0.0/2
Address Pool Name	Less than 32 Bytes

## Table 5-5-2 Main elements of the address pool configuration interface

Interface elements	Description
Address Pool name	Fill in the name of the dhcp address pool.
Subnet Segment	Fill in the subnet segment
Begin IP	Fill in the starting address of the DHCP address pool
End IP	Fill in the end address of the DHCP address pool
Lease time	Fill in the lease time of the address.
Default gateway	Fill in the default gateway of the client. This will be the

	default gateway parameter assigned by the server to
	the client. The IP address of the default gateway must
	be on the same network as the IP address of the
	DHCP client.
DNS server 1	Fill in the primary DNS Server address
DNS server 2	Fill in the address of the standby DNS server
Domain Name	Fill in the server domain name
Service	
NetBIOS Server	Fill in NetBIOS Server

## Figure 5-5-3 Client List interface;

Address Pool Co	onfig Client List	Static client config			
Index	MAC Address	IP Address	User Name	Lease Time(s)	Expired Time(s)
			No matching records found		

## Figure 5-5-4 Static Client Config interface;

static DHCP Confi	g				
DHCP Pool				~	
IP Address				For	Example: 192.168.0.1
MAC Address				For	Example: 00-01-02-03-04-0
MAC Address			Add	For	Example: 00-01-02-03-04-0

## Table 5-5-4 Main elements of Static Client Config interface

Interface elements	Description
DHCP Pool	Select the DHCP address pool.
IP Address	Fill in the IP address to be bound.
MAC Address	Fill in the MAC address to be bound.

# 5.6 DHCP Relay

### [Function Description]

If the DHCP client and the DHCP server are on the same physical network segment, the client can correctly obtain the dynamically allocated ip address. If they are not in the same physical network segment, a DHCP Relay Agent is required. The DHCP Relay agent can eliminate the need for a DHCP server in each physical network segment. It can deliver messages to DHCP servers that are not on the same physical subnet, or send messages from the server back to those that are not on the same physical subnet. Net's DHCP client.

[Operation path]

Layer3 > dhcp relay

[Interface description]

Figure 5-6 DHCP relay interface

DHCP Relay		
Enable DHCP Relay		O Set
Interface		~
DHCP Server		For Example: 192.168.1.1
		Add
Index	Interface	DHCP Server
		No. and the second formal

#### Table 5-6 Main elements of the DHCP relay interface

Interface elements	Description
Enable DHCP Relay	Enable the DHCP Relay function.
Interface	Select the corresponding Layer 3 interface.
DHCP Server	Configure the server IP address.

## 5.7 RIP

[Function Description]

RIP is a protocol based on the Distance-Vector algorithm. It exchanges routing

information through UDP packets and uses a port number of 520.

RIP uses the number of hops to measure the distance to the destination address, and the number of hops is called the metric value. In RIP, the number of hops from a router to the network directly connected to it is 0, the number of hops to reach another network through the router connected to it is 1, and the rest can be deduced by analogy. To limit the convergence time, RIP specifies that the metric value is an integer between 0 and 15. The number of hops greater than or equal to 16 is defined as infinity, that is, the destination network or host is unreachable. Due to this limitation, RIP is not suitable for large-scale networks.

[Operation path]

Layer3 > RIP

[Interface description]

Figure 5-7-1 RIP Global Config interface

F	RIP Global Config	RIP Network Config	RIP Interface Config	RIP Route Info	]			
	Enable RIP				0			
	RIP Version			tx	v2, rx: v1&v2	2 🗸		
	Send Update Tin	ne			30 ra	inge: 1-86400,	Defaults: 30	
	Route Timeout 1	īme			180 ra	nge:1-86400,	Defaults : 180	
	Garbage Collect	Time			120 ra	inge: 1-86400,	Defaults: 120	
	Suppress Interfa	ice Route Update			0			
	Allow Equal Cos	t MultiPath			0			
	Redistribute							
	Default Metric				1 ra	inge: 1-16, Del	faults : 1	
	Redistribute Def	ault Route			0			
	Redistribute Cor	nnected Route			0			
Fi	gure 5-7-2	2 RIP Networ	k Config					
int	erface							
F	RIP Global Config	RIP Network Config	RIP Interface Config	RIP Route Info	]			
	RIP Enable Netwo	rk		_				
	Network					/	For Example: 1	0.1.1 <mark>.0/</mark> 24
				Add				
	Ne			Madarate				
	NO			Network				

No matching records found

Figure 5-7-3 RIP Interface Config interface

Characters

т г	menae									
L	RIP Global C	onfig RIP Network Con	fig RIP Inter	face Config R	IP Route Info					
	No	Destination Network	Route Type	Route Sub-Type	Next Hop	Metric	From	External Metric	Route Tag	Route remain time
				No	matching record	s <mark>found</mark>				

# 5.8 OSPF

[Function Description]

The full English name of OSPF is Open Shortest Path First (Open Shortest Path First). It is a link state routing protocol that uses bandwidth-based metrics. OSPF uses the SPF algorithm to calculate routes, which guarantees no routing loops algorithmically, maintains routes through neighbor relationships, and avoids bandwidth consumption for periodic updates. OSPF has high routing update efficiency and fast network convergence, which is suitable for large and medium-sized networks. On the "OSPF" page, you can configure OSPF parameters.

[Operation path]

Layer3 > OSPF

[Interface description]

Figure 5-8-1 OSPF Global Config interface

Enable OSPF		0		
Router ID		F	For Example: 192.168.1.1	
Suppress Interface	Route Update	0		
Redistribute				
Default Metric		1 range : 0-16777	7214	
Redistribute Default	t Route	O Metric Type:	External Type 1 V Metric:	range : 0-167772
Redistribute Conne	cted Route	O Metric Type:	External Type 1 🗸 Metric:	range : 0-167772
Redistribute Static	Route	O Metric Type:	External Type 1 V Metric:	range : 0-167772
Redistribute RIP Ro	ute	O Metric Type:	External Type 1 V Metric:	range : 0-167772

## Table 5-8-1 Main elements of OSPF Global Config interface

Interface elements	Description
Enable OSPF	Enable or disable OSPF.
Route ID	Fill in the router ID number.
Suppress Interface Route	Enable/disable.
Update	
Default Metric	Set the cost of importing external routes (range:
	0-16777214)
Redistribute Default Route	Redistribute Default Route (range: 0-16777214)
Redistribute Connected Route	(range: 0-16777214)
Redistribute Static Route	(range: 0-16777214)
Redistribute RIP Route	(range: 0-16777214)

# Figure 5-8-2 OSPF Network Config interface

OSPF Global Config	OSPF Network Config	OSPF Interface Config	OSPF Area Config	OSPF Neighbor Info	OSPF Route Info	
Network					For Example: 10.1.1.0/24	
Area				A.B.C.D or	0-4294967295(0.0.0.0-255.25	5.255.255
			Add			
No		OSPE Netw	vork		Area	
		No n	natching records found		rieu -	

## Table 5-8-2 Main elements of OSPF Network Config interface

Interface elements	Description
Network	Fill in the routing network segment address and mask.
Area	Fill in the area information.

# Figure 5-8-3 OSPF Interface Config interface

	Route Info	OSPF R	PF Neighbor Info	Config OS	OSPF Area	terface Config	OSPF Int	F Network Config	al Config O	OSPF Glob
Authentica Character	Type of Certification	Transmit Delay(s)	Retransmit Interval(s)	Dead Interval(s)	Hello Interval(s)	Router Priority	Cost	Area	Network Type	Interface
	not-set 🗸								Broadcast 🗸	Select All
				found	matching records	No				

Table 5-8-3 Main elements of OSPF	Interface Config interface
-----------------------------------	----------------------------

Interface elements	Description						
interface	Display the interface name.						
Network Type	Select the type of OSFP:						
	P2P: Hello packets are sent to the multicast address						
	224.0.0.5, neighbors can be discovered automatically,						
	DR/BDR is not elected, the default Hello timer is 10 seconds,						
	and the Dead timer is 40 seconds.						
	Broadcast: Hello packets are sent to the multicast address						
	224.0.0.5, neighbors can be automatically discovered,						
	DR/BDR elections, the default Hello timer is 10 seconds, and						
	the Dead timer is 40 seconds.						
	NBMA: Hello packets are sent by unicast. Neighbors need to						
	be manually specified. DR/BDR is not elected. By default,						
	the Hello timer is 30 seconds and the Dead timer is 120						
	seconds.						
	P2MP: Hello packets are sent to the multicast address						

	224.0.0.5, neighbors can automatically discover that they do
	not elect DR/BDR, the default Hello timer is 30 seconds, and
	the Dead timer is 120 seconds.
Area	Area Name
Cost	Cost
Router Priority	Priority, the default is 1, the range (0-255).
Hello Interval	The interval for sending hello packets, the default is 10s
Dead Interval	The number of seconds to wait for the Hello packet sent by
	the router to declare that the OSPF router has disappeared
	(shut down) without being seen by the neighbor. The default
	is 40s.
Retransmit Interval	Retransmit after failure, the default interval is 5s
Authentication type	Area-based authentication types: 1. No authentication; 2.
	Simple password authentication; 3. MD5 authentication. No
	authentication by default.
key	Fill in the authentication key value.

# Figure 5-8-4 OSPF Area Config interface

i	OSPF Route Info	Neighbor Info	OSPF Area Config OSP	OSPF Interface Config	twork Config	OSPF Ne	SPF Global Config
Virtual Li	utting Mode	Type of Certification Shortcutti		Default Cost	Summary	Area Type	Area ID A
			atching records found	No m			

# Figure 5-8-5 OSPF Neighbor Info interface

OSPF Glob	al Config	OSPF Network C	onfig OSPF	F Interface Config	OSPF /	Area Config	OSPF Neighbor Info	OSPF Route Info	
No	Neighbo ID	r Router Priority	Neighbor State	Interface State	Dead Time	Neighbor Address	Area Interface	Designated Router	Backup Designated Router
				No	matching rea	cords found			

Figure 5-8-6 OSPF Route Info interface

OSPF Global Confi	g OSPF Network Config	OSPF Interface Config	OSPF Are	a Config	OSPF Neig	ghbor Info	OSPF Route Info	
			Network Route	e Info				
No	Destination Network	Destination Type	Pat	h Type	Cost	Area ID	Next Hop	Out Interface
			Border Router	r Info				
No	Destination Network	Destination Type	Path Type	Cost	Area ID	LSA Flag	Next Hop	Out Interface
LSA Flag: ABR Are	ea Border Router, ASBR Autor	nomous System Boundary Ro	outer.					
			External Route	e Info				
No	Destination Network	Destination Type	Path Type	Cost	Type2 Cost	Route Tag	Next Hop	Out Interface

# 5.9 RIPng

#### Figure 5-9-1 RIPng Global Config interface RIPng Global Config RIPng Network Config RIPng Interface Config RIPng Route Info 0 Enable RIPng Send Update Time 30 range: 1-86400, Defaults: 30 Route Timeout Time 180 range : 1-86400 , Defaults : 180 range: 1-86400, Defaults: 120 Garbage Collect Time 120 0 Allow Equal Cost MultiPath Redistribute range: 1-16, Defaults: 1 Default Metric 1 0 Redistribute Default Route 0 Redistribute Connected Route 0 Redistribute Static Route Redistribute OSPFv3 Route 0

#### Figure 5-9-2 RIPng Network Config interface

RIPng Global Config	RIPng Network Config	RIPng Interface Config	RIPng Route Info		
RIPng Enable Netw	ork				
Network			Add	For Example: 213	34:3e::/64
No		Ne	etwork		
		Nom	atching records found		

Figure 5-9-3 RIPng Interface Config interface

Interface	Enable RIPng	Split Horizon	Suppress Interface Route Update
Select All	0	None 💌	0
vlanif1	0	Split Horizon	0
vlanif20	0	Split Horizon	0

### Figure 5-9-4 RIPng Route Info interfaceRIPng Route Info

RIPng Globa	I Contig RIPng Network C	Config RIPng Inte	rface Config R	IPng Route Into				
No	Destination Network	Route Type	Route Sub-Typ	e Next Hop	Metric	From	Route Tag	Route remain time
			No matchin	ng records found				

# 5.10 OSPFv3

Figure 5-10-1 OSPFv3 Global Config interface

OSPFv3 Global Config	OSPFv3 Interface Config	OSPFv3 Neighbor Info	OSPFv3 Route Info	
Enable OSPFv3			0	
Router ID				For Example : 192.168.1.1
Redistribute				
Redistribute Connect	ed Route		0	
Redistribute Static Ro	oute		0	
Redistribute RIPng Re	oute		0	
			Apply	

## Figure 5-10-2 OSPFv3 Interface Config interface

Interface	Enable OSPFv3	Network Type	Area	Cost	Router Priority	Hello Interval(s)	Dead Interval(s)	Retransmit Interval(s)	Transmit Delay(s)	Suppress Interface Route Update
Select All	0	Broadcast 🗸								0
				No mat	tching records	found				

## interface

DSPFv3 Gl	obal Config	OSPFv3 Interfa	ace Config	OSPFv3 Neighbo	r Info	OSPFv3 Route Info				
No	Neighbor ID	Router Priority	Neighbor State	Interface State	Dead Time	Neighbor Address	Area In	terface	Designated Router	Backup Designated Router
				N	o matching	g records found				

Figure 5-10-3 OSPFv3 Route Info interface

OSPFv3 Gl	obal Config 05	SPFv3 Inte	erface Config	OSP	Fv3 Neighbo	or Info	OSPFv3 F	toute Info					
						Network	Route Info						
No	Destination Ne	twork	Destination	Туре	Path Type	Cost	Area ID	Origin Type	e Origir	ID Or	igin Router	Next Hop	Out Interface
						Border	Router Info						
No	Destination Net	work	Destination Typ	e Pat	h Type Co	ost Area	ID LSA F	lag Origir	туре О	rigin ID	Origin Router	Next Hop	Out Interface
SA Flag: AB	R Area Border Ro	uter, ASB	R Autonomou	s Systen	Boundary F	Router.							
						Externa	I Route Info						
No	Destination	C	Destination	Path	Cost	Type2	Route	Area	Origin	Origin	n Origin	Next	Out
	Network		Туре	Type		Cost	Tag	ID	Type	ID	Router	Нор	Interface

# 6. Multicast Management

# 6.1 IGMP Snooping

### [Function Description]

IGMP Snooping is the abbreviation of Internet Groupmanagement Protocol snooping (Internet Multicast Management Protocol Detection), which is a multicast restriction mechanism running on Layer 2 devices to manage and control multicast groups. The Layer 2 device running IGMP snooping analyzes the received IGMP messages, establishes a mapping relationship between ports and MAC multicast addresses, and forwards multicast data according to this mapping relationship.

On the "IGMP Snooping Config" page, you can perform global configuration and static multicast configuration.

[Operation path]

Multicast > IGMP Snooping

[Interface description]

Figure 6-1-1 IGMP Snooping Global Config

interface

Shooping Clobal Coning	IGMP Shooping VLAN Coming	IF V4 Static Municast			
Enable			0		
Member Port Aging Time			300 ra	inge: 200-1000(Defaults: 300)	
Router Port Aging time			105 U	nit: seconds Range: 1-1000 (Default: 10	05)
		Sat			
		oct			

# Figure 6-1-2 IGMP Snooping VLAN Config

## interface

Vlan Id	1	~	
Port Fast Leave	0		
Query Source Address		For Example	e: 192.168.1.254
Query Interval	10	Unit: second	ls Range: 2-300
Max Response Time	10	Unit: second	ls Range: 1-25 (default: 10)
Last-Member Query Interval	1	Unit: second	ls Range: 1-5 (default: 1)
	Set	Ď	

Figure 6-1-3 IPv4 Static Multicast Config

interface

IGMP Snooping	Global Config	IGMP Snooping ∖	/LAN Config	IPv4 Static	Multicast						
Vian Id			1	Ý	•]						
Multicast Sour	ce Address				For Exa	imple: 192	2.168. <mark>1</mark> .1				
Multicast Grou	p Address				For Exa	imple: 225	i.1.2.3				
Port List		Select All					G14 G16	G18	G20 G19 G10	622 G24	X4
					Add						
Index	Vian Id	Multic	ast Source Ad	dress M	Aulticast	Group Ac	idress	Stati	c Memb	er Ports	
				No mat	ching rec	ords found	d				

## 6.2 MLD Snooping

MLD Snooping global configuration: configure MLD monitoring enable and set MLD function

attributes;

MLD Snooping G	Global Config MLD	⊃ Snooping ∨LAN Config	IPv6 Static Multicast	]		
Enable				0		
Member Por	t Aging Time			300 ran	ge: 200-1000(Defaults: 300)	
Router Port	Aging time			105 Uni	t: seconds Range: 1-1000 (Default: 1)	05)
			Set			
						Dynamic Member
Index	Vlan Id	Multicast Source A	ddress Multicast	Group Address	Static Member Ports	Ports(Aging time)
			No matching rec	ords found		

MLD Snooping VLAN configuration: Configure static multicast

VLAN;

Vlan Id				1	~	
Port Fast	t Leave			0		
Query Sc	ource Addre	SS			For Example	: fe80:fe00::1
Query Int	terval			10	Unit: second:	s Range: 2-300
Max Res	ponse Time			10	Unit: second:	s Range: 1-25 (default: 10)
Last-Men	nber Query	Interval		1	Unit: second	s Range: 1-5 (default: 1)
				Set		
ndex	Vian Id	Port Fast Leave	Query Source Addres	s Query Interval	Max Response Time	Last-Member Query Intr

IPv6 static multicast: configure static multicast function, and enable port static

#### multicast

#### function;

MLD Snooping Global Co	nfig MLD	Snooping VL	AN Config	IPv6 St	atic Mu	lticast									
Vlan Id			1		~										
Multicast Source Addre	ess					For Exa	imple :	fe80:fe0	0::1						
Multicast Group Addre	55					For Exa	imple :	ff1E::01							
Port List		Select All					G12	G14	G16				G24		
			61 65	65		Add		013	015	617	Gia	621	623	~1	A3
Index V	'lan Id	Multio	cast Source A	ddress	M	ulticast	Group	Addres	5	Stati	c Memt	per Por	ts		
				N	o matc	hina rec	ords fou	Ind							

# 6.3 IP Multicast

IP multicast global configuration: multicast routing is enabled;

IP Multicast Global Config	IP Multicast Interface Config	
Enable Multicast Routing	9	0
		Apply

IP multicast interface configuration:

/IF name	VIF index	Module Name	TTL threshold	Local Address	Remote Address	VIF Uptime
Select All						

## 6.4 **IGMP**

IGMP global configuration: Configure the maximum number of IGMP group records, the range is 0-2097152, the default is 0,

IGMP Global Config	IGMP Interface Config	IGMP Static Group Config	IGMP Group Info	
Max Group Record	d Num		Set	range : 0-2097152 , Defaults : 0
IGMP interface	e configuration:		,	

IGMP Global Config	IGMP Interf	ace Config IGN	IP Static Group Con	fig IGMP Group Info								
Interface name	Enable IGMP	IGMP Version	Last Member Query Count	Last Member Query Interval(ms)	Max Group Record Num	Other-Querier Interval(s)	Query Interval(s)	Query Response Time(s)	Startup Query Count	Startup Query Interval(s)	Robustness Variable	RA Option Validation
Select All	0	3 🗸										0
vlanif1	0	3 ~	2	1000	0	255	125	10	2	31	2	0
vlanif20	0	3 🗸	2	1000	0	255	125	10	2	31	2	0

#### IGMP static group configuration,

IGMP Global Config	IGMP Interfac	e Config	GMP Stati	c Group Config	IGM	P Group Info	1					
Static Group Config						Join Group C	onfig					
Interface name	vlani	f1	~			Interface nam	ne	vlanif1		~		
Multicast Group Add	dress		Fo	r Example: 225.*	1.2.3	Multicast Gro	oup Address			For I	Example: 22	5.1.2.3
ssm-map						Multicast Sou	urce Addres	s		For	Example: 19	2.168 <mark>.</mark> 1.1
Multicast Source Ad	dress		Fo	r Example: 192.	168.1.1							
		Add							Add			
4												
Del	rface name			Group Type		Multic	ast Group A	ddress	Mu	ulticast Sou	urce Addres	55
				No ma	atching red	cords found						
IGMP group	1											
information:												
IGMP Global Config	IGMP Interfac	ce Config I	GMP Stat	ic Group Config	IGM	1P Group Info						
Interface name Addr	up Group ess Mode	Group Record Uptime	Group Record Expires	Last Reporter	Include Source Count	Exclude Source Count	Source Mode	Source Address	Source Record Uptime	V3 Expires	Forward	Source Type

Flags: R - Remote, M - SSM Mapping, S - Static, L - Local

No matching records found

Count

Uptime Expires

Uptime

# 7. Advance

# 7.1 QOS

[Function Description]

QoS (Quality of Service) refers to a network that can use various basic technologies to provide better service capabilities for specified network communications. It is a technology used to solve problems such as network delay and congestion. When the network is overloaded or congested, QoS can ensure that important services are not delayed or discarded, while ensuring the efficient operation of the network.

[Operation path]

Advance > QOS

[Interface description]

Figure 7-1-1 Global Config interface

Set the Scheduling Policy, while policy is WRR/WFQ/DRR set Queue Weights(Range 1-127, if set 0, means 3	P+WRR/WFQ/DRR).
Policy	
Weight	W0: 0 W1: 0 W2: 0 W3: 0
	W4: 0 W6: 0 W6: 0 W7: 0
	Set
Maps to different queues based on the CoS(0-7) in packet. If the packet doesn't carry VLAN TAG(802.1p), packet.	rt default CoS is used.
CoS-Queue Map	CoS 0 • -> Queue 0 • Set
Current Map	0->0 1->1 2->2 3->3 4->4 5->6 6->6 7->7
Maps to new DSCP & CoS based on the DSCP in packet IP header. By default, DSCP & CoS Mapping are no	changed.
DSCP-CoS Map	DSCP 0 • -> New DSCP 0 • -> CoS 0 • Set
	0->0->0 1->1->0 2->2->0 3->3->0 4->4->0 5->5->0 6->6->0 7->7->0
	8->8->1 9->9->1 10->10->1 11->11 12->12->1 13->13->1 14->14->1 15->15->1
	16->16->2 17->17->2 18->18->2 19->19->2 20->20->2 21->21->2 22->22->2 23->23->2
2022 0-0 Mar	24->24->3 25->25->3 26->26->3 27->27->3 28->28->3 29->29->3 30->30->30->3 31->31->3
DSCP-Cos Map	32->32->4 33->33->4 34->34->4 35->35->4 36->36->4 37->37->4 38->38->4 39->39->4
	40->40->5 41->41->5 42->42->5 43->43->5 44->44->5 45->45->5 46->46->5 47->47->5
	48->48->6 49->49->6 50->50->6 51->51->6 52->52->6 53->53->6 54->54->6 55->55->6
	56->56->7 57->57->7 58->58->7 59->59->7 60->60->7 61->61->7 62->62->7 63->63->7

Figure 7-1-2 Port Config

interface

Port	Default CoS	Trust Mode
Select All	0 ~	Trust CoS 🗸
G1	0 ~	Trust CoS 🗸
G2	0 ~	Trust CoS 🗸
G3	0 🗸	Trust CoS 🗸
G4	0 ~	Trust CoS 🗸
G5	0 ~	Trust CoS 🗸
G6	0 ~	Trust CoS 🗸
G7	0 ~	Trust CoS 🗸
G8	0 🗸	Trust CoS 🗸
G9	0 ~	Trust CoS 🗸
G10	0 ~	Trust CoS 🗸

#### Table 7-1-2 Main elements of Port Config interface

Interface elements	Description
Port	Show port number
Default cos	Configure the default priority. The default is 0 (0-7). The
	larger the value, the higher the priority.
Trust Mode	1 Cos, 2 dscp, 3 all (when all is selected, dscp is effective,
	and dscp has a higher priority than cos).

## 7.2 ACL

### [Function Description]

ACL, Access Control List, access control list. ACL is the function of packet filtering by configuring matching rules and processing operations on packets. The ACL rules applied on the port analyze the fields of the packet, and after identifying a specific packet, it is based on a preset operation (Allow/Prohibit Passing, Speed Limiting, Redirection, Port Closing, etc.) for corresponding processing. On the "ACL Configuration" page, you can match the protocol fields of the L2-L4 layer of the data packet. By defining the time period, you can set the effective time of ACL rules. Configure MAC ACL and IP ACL to process data packets that match ACL rules.

[Operation path]

Advance > ACL

## [Interface description]

## Figure 7-2-1 MAC ACL Config

## interface

MAC ACL CONFIG	IP ACL CONFIG	Time Range Config ACL G		
Entry ID				range : 0-31
Rule ID Action			deny	range : 0-127
Source MAC				For example: 02-02-03-04-05-06, do not fill, that "any"
Source MAC M	ASK			For example: fc-ff-ff-00-00, do not fill, that "any"
Destination MA	с			For example: 02-02-03-04-05-06, do not fill, that "any"
Destination MA	C Mask			For example: fc-ff-ff-00-00, do not fill, that "any"
Time-Range Na	me		A	<ul> <li>It is empty, indicating that it is effective anytime</li> <li>Add</li> </ul>
Entry ID	Rule ID	Action	Source MAC	Destination MAC Time-Range
			No matching	hing records found

## Table 7-2-1 Main elements of MAC ACL Config interface

Interface elements	Description
Entry ID	Enter the ACL group number to be configured, the value
	range is 1-99.
Rule ID	Enter the rule number, the value range is 1-127.
Action	Select how the switch handles data packets that meet
	the matching rules. Deny means discarding data
	packets, and permit means forwarding data packets.
Source MAC	Enter the source MAC address information included in
	the rule.
Source MAC MASK	Enter the source MAC address mask information
	included in the rule.
Destination MAC	Enter the destination MAC address information included
	in the rule.
Destination MAC Mask	Enter the destination MAC address mask information
	included in the rule.
Time-Range Name	

## Figure 7-2-2 IP ACL Config

## interface

MAC ACL CONFIG	ACL CONFIG	Time Range Config	ACL GROUP CONFIG	]					
Entry ID						range : 0-31			
Rule ID						ange : 0-127			
Action				C	leny 🗸				
Protocol				a	iny 🗸				
Source IP						For example: xxx.xxx.xx	cx.xxx, do not fill, that "an	Ŋ"	
Source mask						For example: xxx.xxx.xx	x.xxx, do not fill, that "an	ıy"	
Source Port						Range: 0-65535, is emp	ty, meaning any port		
Destination IP						For example: xxx.xxx.xx	x.xxx, do not fill, that "an	ly"	
Purpose mask						For example: xxx.xxx.xx	ox.xxx, do not fill, that "an	ly"	
Destination Port						Range: 0-65535, is emp	ty, meaning any port		
Time-Range Name					Ŷ	It is empty, indicating that	at it is effective anytime		
					Add				
Entry ID Rule II		ction Prot	ocol Source IP	Source mask	Source Port	Destination IP	Purpose mask	Destination Port	Time-Range
			dourde in	Louide mask	matching records found				

## Table 7-2-2 Main elements of IP ACL Config interface

Interface elements	Description
Entry ID	Enter the ACL group number to be configured, the
	value range is 100-999.
Rule ID	Enter the rule number, the value range is 1-127.
Action	Select how the switch handles data packets that
	meet the matching rules. Deny means discarding
	data packets, and permit means forwarding data
	packets.
Protocol	Select the switch data transmission rule.
Source IP	Enter the source IP address information.
Source mask	Enter the mask of the source IP address, the mask is
	set to 1 to indicate a strict match.
Source Port	Enter the TCP/UDP source port number.
Destination IP	Enter the destination IP address information.
Destination mask	Enter the mask of the destination IP address. Set the
	mask to 1 to indicate a strict match.

Destination Port	Enter the TCP/UDP destination port number.
Time-Range Name	

Figure 7-2-3 Time Range Config

#### interface

AC ACL CONFIG	IP ACL CONFIG	Time Range Config	ACL GROUP CONFIG	
ADD Time Range				
Name				Add
Config the time				
Time Dance Mana				↓ Del
lime-kange Name				●Absolute ○ Periodic
Start Time				yyyy-MM-dd HH:mm
End Time				yyyy-MM-dd HH:mm
Time				HH:mm - HH:mm
Week				Sun Mon Tue Wed Thu Fri Sat
				Add
Na	me		State	Time
				No matching records found

### Figure 7-2-4 ACL GROUP CONFIG

#### interface

MAC ACL CONFIG	IP ACL CONFIG	Time Range Config	ACL GROUP CONFIG			
Port MAC ACL IP ACL				G1 V	G1     S blank, indicating that the rules applied to delete the pr     S blank, indicating that the rules applied to delete the pr     Set	ort (if any exist
	Port		MAC access list ID		IP access list ID	
	G1					
	G2					
	G3					
	G4					
	G5					
	G6					
	G7					
	G8					
	G9					
	G10					

# 7.3 SNMP

## [Function Description]

SNMP is currently the most widely used network management protocol in UDP/IP networks.

It provides a management framework to monitor and maintain Internet devices.

SNMP network elements are divided into two types: NMS and Agent:

NMS (Network Management Station) is a workstation running SNMP client programs, which can provide a very friendly human-computer interaction interface to facilitate network administrators to complete most network management tasks.

Agent is a process that resides on the device and is responsible for receiving and processing request messages from NMS. In some emergency situations, such as interface status changes, the Agent will also notify the NMS.

NMS is the manager of SNMP network, and Agent is the managed person of SNMP network. NMS and Agent exchange management information through SNMP protocol.

SNMP provides four basic operations:

Get operation: NMS uses this operation to query the value of one or more objects of the Agent.

Set operation: NMS uses this operation to reset the value of one or more objects in the Agent database (MIB, Management Information Base).

Trap operation: The agent uses this operation to send alarm information to the NMS.

Inform operation: NMS uses this operation to send alarm information to other NMSs. SNMP protocol version:

Currently, the SNMP Agent of the device supports SNMP v2c version and is compatible with SNMP v1 version.

SNMP v1 uses community name (Community Name) authentication. The community name is used to define the relationship between SNMP NMS and SNMP Agent. If the community name carried in the SNMP packet is not recognized by the device, the packet will be discarded. The community name plays a role similar to a password and is used to restrict the SNMP NMS's access to the SNMP Agent.

SNMP v2c also uses community name authentication. It is compatible with SNMP v1 while expanding the functions of SNMP v1: it provides more operation types (GetBulk and InformRequest); it supports more data types (Counter64, etc.); it provides richer error codes, Can distinguish errors in more detail.

#### Introduction to MIB:

Any managed resource is represented as an object, called a managed object. MIB (Management Information Base (Management Information Base) is a collection of managed objects. It defines a series of attributes of the managed object: the name of the object, the access rights of the object, and the data type of the object. Each agent has its own MIB. The NMS can perform read/write operations on the objects in the MIB according to the permissions. The relationship between NMS, Agent and MIB is shown in the figure



MIB is stored in a tree structure. The nodes of the tree represent managed objects, which can be uniquely identified (OID) by a path from the root. As shown in the figure below, the managed object B can be uniquely identified by a string of numbers {1.2.1.1}, which is the OID (Object Identifier) of the managed object.



[Operation path]

Advance > SNMP

[Interface description]

#### Figure 7-3-1 SNMP Global Config

interface



Figure 7-3-2 SNMP Group Config

#### interface

omation Group V3 User Alarm		
SNMP Community Config		
Name		
Community Attributes	rocommunity ~	
	Add	
Name	Community Attributes	
public	rocommunity	De
private	rwcommunity	De

## Figure 7-3-3 SNMP v3 User

#### Config

3 User Config	
ame	
ser Attribute	rouser
ertification Information	MD5 •
ncrypt information	DES V

Index	Name	User Attribute	Authentication Mode	Authentication password	Encryption mode	Encryption password
1	admin	rouser				
2	admin	rwuser				

## Figure 7-3-4 SNMP Alarm Config interface

Configure the TRAP trap receiving address and the corresponding SNMP protocol

#### version;

frap Conf	fig			
Address				
ersions			V1	~
			Add	

Address	versions
0.0.0	V1
0.0.0.0	V2C

# 7.4 RMON

Figure 7-4-1 Event Group Config interface

Event group: query and add event groups monitored

remotely;

Event Group	Statistics Group	History Group	Alarm Group			
Index				item)	Event group number: 0-1024	(delete, just fill in this
Description						
Action				none	~	
				Add		
Inde	c	Descriptio	n	Action	Recent Time	
			No	matching records found		

Figure 7-4-2 Statistics Group Config interface

Statistics group: query the statistics information of a specific event after the

interruption;

Event Group	Statistics Group	History Group	Alarm Group	]		
Index Port				item) G1	~	Event group number: 0-1024 (delete, just fill in this
				Add		
	Index			Name		
				No matching records found		

Figure 7-4-3 History Group Config interface

History group: Add to query the history records of specific events when they occur on the

port;

Index	item)		(ucicie, just ill ill ill
Sample Port	G1	~	
sampling Interval		range : 5-65535(Seconds)	
Max Sample Number		Max Sample Number : 0-100	)
	Add		

#### Figure 7-4-4 Alarm Group Config interface

Alarm group: add the attributes of the alarm event to be queried on the

port;									
Event Group Statist	ics Group History Gr	oup Alarm Group							
Index						Event group number	0-1024 (delete, just fill in this	; item)	
Sample Port					G1	•			
Alarm Parameters					DropEvents	•			
sampling Interval						range : 5-65535(Sec	onds)		
Sampling Type					absolute	~			
Rising Edge Thresho	ld					range : 0-429496729	35		
Falling Edge Thresho	bld					range : 0-429496729	95		
Rising Edge Event					Event group index, when	the alarm is triggered, the	corresponding event of the e	vent group will be activated	, Range: 0-1024
Falling Event					Event group index, when	the alarm is triggered, the	corresponding event of the e	vent group will be activated	, Range: 0-1024
					Add				
Index	Sample Port	Alarm Parameters	sampling Interval	Sampling Type	Rising Edge Threshold	Falling Edge Threshold	Rising Edge Event	Falling Event	
				No matching	g records found				

# 7.5 LLDP

Figure 7-5-1 LLDP Global Config interface Global configuration: enable and configure the LLDP function;

Global Config Port Config LLDP Neighbor	
LLDP	
Tx interval	30 range: 5-32768 Seconds
Tx Delay	2 range: 1-8192 Seconds
Tx Hold Times	4 range: 2-10
Port Reinit Delay	2 range: 2-5 Seconds
Manage Address	For Example: 192.168.1.1
TLV optional to send	
Manage Address TLV	
Port Description TLV	
System Capability TLV	
System Description TLV	
System Name TLV	
	Apply

## Figure 7-5-2 Port Config interface

## Port configuration: configure port LLDP function

#### attributes;

Global Config Port Config LLE	DP Neighbor	
Port	tx	rx
Select All		
G1		
G2		
G3		
G4		
G5		
G6		
G7		
G8		
G9		
G10		
G11		
G12		

Figure 7-5-3 LLDP Neighbor Information Interface

LLDP neighbor: query LLDP neighbor

### information;

Global Co	nfig Port Config	LLDP Nei	ghbor							
Index	Chassis-ID	PortID	Holdtime	Port Description	System Name	System Description	System Capability	Manage Address	Local Port	vlan id
1	MAC: 00:00:00:00:61:35	Locally Assigned - 4	120	Port #4		SMBStaX (standalone) 2019-09- 02T13:11:58+08:00 R2:03 2019-09- 02T13:11:58+08:00	Bridge/Switch (enabled)	192.168.10.200	G6	1

# 7.6 NTP

[Function Description]

On the "NTP Config" page, you can configure the NTP server address to synchronize the switch system time with the server.

[Operation path]

Advance > NTP

[Interface description]

Figure 7-6-1 NTP Global Config interface

Global configuration: configure NTP function enable, time zone selection and

modification of check time

interval;

NTP Global Config NTP Server Config	
Mode	
Time Zone Settings	(GMT+08:00) Irkutsk Uli 🗸
Time Interval	300 Second / time range: 5-65535 Defaults: 300

Figure 7-6-2 NTP Server Config interface

NTP server configuration: configure the NTP server address and view the NTP

#### server

status;

\$erver	For Example: 202.112.29.82
Commonly used server	
China	120.25.108.11 202.112.29.82
America	158.69.48.97 216.218.254.202
Singapore	202.73.57.107 218.186.3.36
Germany	46.4.106.197 141.82.25.203
ndia	162.159.200.1 157.119.108.165
ran	77.104.104.100 194.225.150.25
Brazil	188.165.236.162 200.160.0.8
ndex Server	State

# 7.7 Secure

Figure 7-7-1 Scure configuration interface

Distributed denial of service attack (DDOS) and anti-PING function (Icmp-echo) can be turned

on;	
DDOS	
Icmp-echo	0
	Apply

# 8. System Management

# 8.1 User Config

### [Function Description]

On the "User Config" page, you can configure the user name, password, and permissions for logging in to the switch's WEB interface.

[Operation path]

System > User

[Interface description]

Figure 8-1 User Config interface

Modify the user's login password, the account name cannot be changed nor can

the user be

added;

Administrator	admin
New Password	16 characters at most
Retype Password	16 characters at most
	Apply

## 8.2 Network

[Function Description]

The management IP address of the switch can be configured on the "Network" page.

[Operation path]

System > Network

[Interface description]

Figure 8-2-1 IPv4 Config interface

IPV4 configuration: modify the IPV4 address of the switch, you cannot add an IP

address;

Manage Interface	vlanif1	
IPV4 Address	192.168.10.12/24	For Example : 10.0.0.2/2
Default Gateway		For Example: 10.0.0.1
Preferred DNS Server		For Example : 10.0.0.1
Alternative DNS Server		For Example : 10.0.0.1

Figure 8-2-2 IPv6 Config interface

IPV6 configuration: Modify the IPV6 address of the switch, but also cannot add

the IPV6

address;

Manage Interface	vlanif1	
PV6 Address	fe80:fe00::1/64	For Example : fe80:fe00::1/6
Default Gateway		For Example : fe80:fe00::1

# 8.3 Service Config

Figure 8-3-1 Service Config interface

Configure the switch Telnet, SSH, HTTP version protocol and service port;

Telnet Service	
TELNET Port	23
SSH Service	
SSH Port	22
HTTP Service	HTTP
HTTP Port	80
	Apply

# 8.4 Configration management

Used to reset, upload and download switch

5	
Restore factory settings	Restore factory settings
Upload Config	Choose File No file chosen Upload
Download Config	Download

# 8.5 Firmware Upgrade

Used to upgrade the firmware version currently used by the

switch;

configuration;

Product Model	YH6824GST4-SFP
Hardware Version	V1
Firmware Version	V1.0.0.1-gd06e45122
New Firmware File	Choose File No file chosen
	Upload

# 8.6 Diagnostic

Ping detection: Use the ping function of the switch to detect whether the link between the switch itself and other IP devices is

reachable;

ing Detection	Tracert Detection	Cable Detection	
Address			Ping
PING 192.	168.10.200 (192.168.	10.200): 56 data bytes	
64 bytes	from 192.168.10.200:	seq=0 ttl=64 time=2.761 ms	
64 bytes	from 192.168.10.200;	seq=2 ttl=64 time=0.804 ms	
64 bytes	from 192.168.10.200:	seq=3 ttl=64 time=0.807 ms	
192.1 4 packets round-tri	68.10.200 ping stati transmitted, 4 pack p min/avg/max = 0.79	stics ets received, 0% packet loss 7/1.292/2.761 ms	

#### Tracert detection:

#### Traceroute;

Address	192.168.10.200 Traceroute	J
		J

Ethernet cable detection: detection of all network port cable properties of of the

switch

Tracert Detection		
G8	~	
	G8	G8 V

## 8.7 Restart

reboot the switch

Restart