

# TNS5800 Series Layer 3 Industrial Ethernet Switch User Manual

Version 03

Issue Date:2019-01-23

**Copyright © 2019 3onedata Co., Ltd. All rights reserved.**

No company or individual is allowed to duplicate or transmit this manual in any forms without written permission issued by 3onedata Co., Ltd.

## **Trademark statement**

 **3onedata**<sup>®</sup> and  **3One data**<sup>®</sup> are the registered trademark owned by 3onedata Co., Ltd. And other trademarks mentioned in this manual belong to their corresponding companies.

## **Notes**

Purchased product, service or features should be constrained by 3onedata commercial contracts and clauses. The whole or part product, service or features described in this document may beyond purchasing or using range. 3onedata won't make any statement or warranty for this document content unless any other appointment exists.

Due to product version upgrading or other reason, this document content will be upgraded periodically. Unless other appointment exists, this document only for usage guide, all statement, information and suggestion in this document won't constitute any warranty.



Embedded Industrial Ethernet Switch Modules  
Embedded Serial Device Server Modules

**Safety**

**3onedata**  
One-stop industrial communication products and solutions

**Reliability**



Layer 3 Industrial Ethernet Switch  
Managed DIN-Rail Ethernet Switch  
Managed Rackmount Ethernet Switch  
Industrial PoE Switch  
Industry Specific (Rail transit, Power...)



BlueEyes Switch Management Software  
VSP Virtual Serial Port Management Software



Modbus Gateway  
Serial Device Server  
Media Converter  
CAN Device Server  
Interface Converter

**Real time**

**3onedata Co., Ltd.**

Headquarter address: 3/B, Zone 1, Baiwangxin High Technology Industrial Park, Song Bai Road, Nanshan District, Shenzhen, 518108, China

Technology support: tech-support@3onedata.com

Service hotline: +86-400-880-4496

E-mail: sales@3onedata.com

Fax: +86-0755-26703485

Website: http://www.3onedata.com

## Preface

Layer 3 Industrial Ethernet Switch User Manual has introduced this series of switches:

- Product feature
- Network management method
- Network management relative principle overview

## Readers






This manual mainly suits for engineers as follows:

- Network administrator responsible for network configuration and maintenance
- On-site technical support and maintenance staff
- Hardware engineer

## Text Format Convention

Format	Description
“”	Words with "" represent the interface words. e.g.: "The port number".
>	Multi-level path is separated by ">". Such as opening the local connection path description: Open "Control Panel> Network Connection> Local Area Connection".
Light Blue Font	Represent the words click to achieve hyperlink. Font color as: "Light blue".
About This Chapter	The "About This Chapter" section provides links to each section and corresponding principles / operating chapters in this chapter.

## Icon Convention

Format	Description
 Notice	Reminder the announcements in the operation, improper operation may result in data loss or equipment damage.
 Warning	Pay attention to the notes on the mark, improper operation may cause personal injury.
 Note	Make a necessary supplementary instruction for operation description.
 Key	Configuration, operation, or tips for device usage.
 Tips	Pay attention to the operation or information to ensure success device configuration or normal working.

## Revision Record

Version No.	Revision Date	Revision Description
01	2017.08	Create document
02	2018.06	Add NAT
03	2019.01.24	Upgrade template

# Content

<b>PREFACE</b> .....	<b>1</b>
<b>CONTENT</b> .....	<b>1</b>
<b>THE FIRST PART: OPERATION</b> .....	<b>1</b>
<b>1 LOG IN THE WEB INTERFACE</b> .....	<b>1</b>
1.1 WEB BROWSING SYSTEM REQUIREMENTS .....	1
1.2 SETTING IP ADDRESS OF PC .....	1
1.3 LOG IN THE WEB CONFIGURATION INTERFACE .....	3
<b>2 SYSTEM CONFIGURATION</b> .....	<b>5</b>
2.1 SYSTEM INFORMATION .....	5
2.2 USER CONFIGURATION.....	7
2.3 DEVICE LOG MESSAGE .....	8
2.4 SSHD CONFIGURATION .....	9
2.5 TELNET CONFIGURATION .....	10
2.6 HTTPS SETTING .....	11
2.7 DIAGNOSTIC TEST .....	12
2.7.1 Ping .....	12
2.7.2 TRACEROUTE .....	13
2.7.3 Port Loopback.....	14
<b>3 PORT CONFIGURATION</b> .....	<b>16</b>
3.1 PORT SETTING.....	16
3.2 STORM CONTROL .....	18
3.3 PORT RATE LIMIT .....	20
3.4 MIRROR .....	21
3.5 ALARM SETTINGS.....	23
3.6 LINK AGGREGATION .....	24
3.6.1 Static Configuration .....	25
3.6.2 LACP Configuration .....	26
3.7 ISOLATE-PORT .....	28
3.8 PORT STATISTICS .....	29
3.8.1 Port Stats .....	29

3.8.2	Detail Port Stats.....	30
<b>4</b>	<b>LAYER 2 CONFIGURATION .....</b>	<b>32</b>
4.1	VLAN CONFIGURATION.....	32
4.1.1	PVlan Configuration .....	32
4.1.2	Trunk Configuration .....	34
4.1.3	VLAN Configuration .....	38
4.2	MAC CONFIGURATION .....	39
4.2.1	MAC Configuration .....	40
4.2.2	Static MAC .....	41
4.3	MAC ADDRESS LIMIT CONFIGURATION.....	42
4.4	SPANNING-TREE CONFIGURATION .....	43
4.4.1	Bridge Settings.....	43
4.4.2	Instance Configuration .....	45
4.4.3	Bridge Ports .....	46
4.4.4	Instance Port Configuration .....	47
4.5	IGMP-SNOOPING.....	49
4.5.1	IGMP-snooping.....	50
4.5.2	Static Multicast .....	51
4.6	SW-RING CONFIGURATION.....	51
4.6.1	Global Configuration .....	52
4.6.2	Node Configuration .....	52
4.7	GMRP CONFIGURATION.....	57
4.7.1	GMRP Global Configuration .....	58
4.7.2	GMRP Port Config .....	59
4.7.3	GMRP Group .....	60
<b>5</b>	<b>LAYER 3 CONFIGURATION .....</b>	<b>61</b>
<b>5.1</b>	<b>INTERFACE CONFIGURATION.....</b>	<b>61</b>
<b>5.2</b>	<b>ARP CONFIGURATION .....</b>	<b>64</b>
5.2.1	Show ARP.....	64
5.2.2	Static ARP .....	65
5.2.3	ARP Ageing Time.....	65
<b>5.3</b>	<b>VRRP.....</b>	<b>66</b>
<b>5.4</b>	<b>ND CONFIGURATION .....</b>	<b>69</b>
<b>6</b>	<b>ROUTER CONFIGURATION .....</b>	<b>71</b>
<b>6.1</b>	<b>SHOW ROUTER .....</b>	<b>71</b>
<b>6.2</b>	<b>STATIC CONFIGURATION .....</b>	<b>72</b>
<b>6.3</b>	<b>RIP CONFIGURATION .....</b>	<b>73</b>
6.3.1	RIP Global Configuration .....	73

6.3.2	RIP Network Setting .....	75
6.4	OSPF .....	76
6.4.1	OSPF Global Configuration .....	76
6.4.2	OSPF Network Configuration .....	78
6.4.3	MD5 Setting.....	79
6.5	BGP CONFIGURATION .....	80
6.6	MULTICAST ROUTE CONFIGURATION .....	82
7	NETWORK SECURITY .....	84
7.1	ACCESS CONTROL .....	84
7.2	ATTACK PROTECTION .....	85
7.3	ACL CONFIGURATION.....	87
7.3.1	ACL GROUP Configuration .....	87
7.3.2	Time Range Configuration.....	88
7.3.3	MAC ACL Configuration .....	90
7.3.4	IP ACL Configuration .....	91
7.4	NAT CONFIGURATION.....	93
7.4.1	NAT Rule Configuration.....	93
7.4.2	NAT Bind .....	94
8	ADVANCED CONFIGURATION.....	96
8.1	QOS CONFIGURATION .....	96
8.1.1	Global Configuration .....	96
8.1.2	Port Configuration .....	98
8.2	LLDP CONFIGURATION .....	99
8.2.1	Global Configuration .....	99
8.2.2	Port Configuration .....	101
8.2.3	LLDP Neighbors .....	102
8.3	SNMP CONFIGURATION .....	103
8.3.1	System Information.....	105
8.3.2	View .....	106
8.3.3	Community .....	107
8.3.4	V3 User .....	108
8.3.5	Trap .....	109
8.4	RMON CONFIGURATION .....	110
8.4.1	Event.....	111
8.4.2	Statistical.....	112
8.4.3	History .....	113
8.4.4	Alarm.....	114
8.5	DHCP SERVER CONFIGURATION .....	116



8.5.1	DHCP Server Configuration .....	116
8.5.2	DHCP Pool Configuration .....	117
8.5.3	Client List.....	119
8.5.4	Static Client Configuration .....	119
8.5.5	Port Address Binding Configuration .....	120
8.6	DHCP-SNOOPING .....	121
8.6.1	Global Configuration .....	122
8.6.2	Static Binding .....	123
8.6.3	Port Configuration .....	124
8.7	NTP CONFIGURATION .....	126
<b>9</b>	<b>SYSTEM MANAGEMENT.....</b>	<b>128</b>
9.1	MANAGEMENT FILE.....	128
9.1.1	View Launch Configuration.....	128
9.1.2	Management File .....	129
9.2	SAVE.....	130
9.3	REBOOT .....	131
9.4	RESTORE DEFAULT SETTING.....	131
9.5	ONLINE UPGRADE .....	132
	<b>THE SECOND PART: FREQUENTLY ASKED QUESTIONS .....</b>	<b>134</b>
<b>10</b>	<b>FAQ.....</b>	<b>134</b>
10.1	SIGN IN PROBLEMS .....	134
10.2	CONFIGURATION PROBLEM .....	135
10.3	ALARM PROBLEM.....	136
10.4	INDICATOR PROBLEM.....	136
<b>11</b>	<b>MAINTENANCE AND SERVICE.....</b>	<b>138</b>
11.1	INTERNET SERVICE .....	138
11.2	SERVICE HOTLINE .....	138
11.3	PRODUCT REPAIR OR REPLACEMENT .....	139

# The First Part: Operation

## 1 Log in the Web Interface

### 1.1 WEB Browsing System Requirements

While using managed industrial Ethernet switches, the system should meet the following conditions.

Hardware and Software	System Requirements
CPU	Above Pentium 586
Memory	Above 128MB
Resolution	Above 1024x768
Color	Above 256 color
Browser	Above Internet Explorer 6.0
Operating System	Windows XP Windows 7

### 1.2 Setting IP Address of PC

The switch default management as follows:

IP Setting	Default Value
IP Address	192.168.1.254

IP Setting	Default Value
Subnet Mask	255.255.255.0

While configuring the switch via Web:

- Before remote configuration, please make sure the route between computer and switch is reachable.
- Before local configuration, please make sure the computer IP address is on the same subnet as the one of switch.

Notes:

While first configuring the switch, if it is a local configuration mode, please make sure that the network segment of current PC is 1.

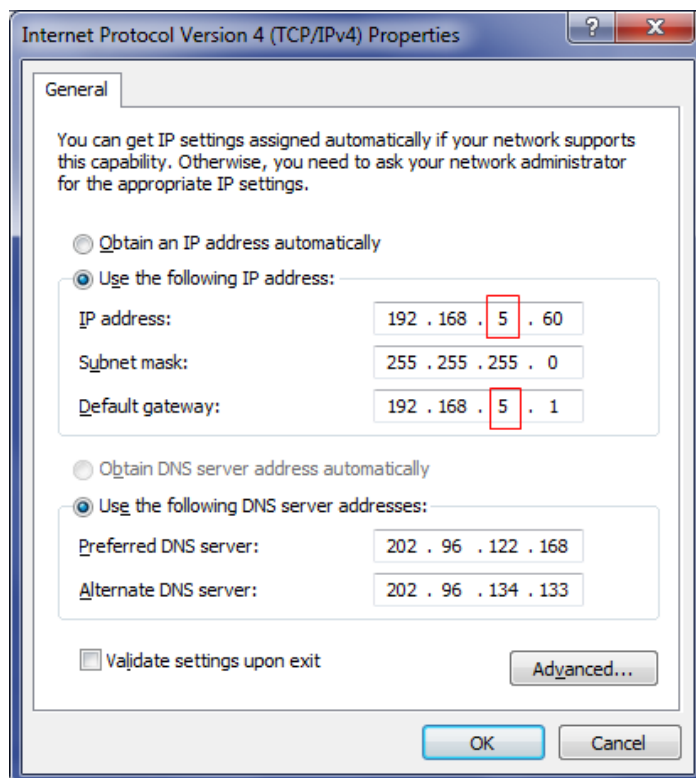
E.g.: Assume that the IP address of current PC is 192.168.5.60, change the network segment "5" of the IP address to "1".

### Operation Steps

Amendment steps as follows:

**Step 1** Open "Control Panel > Network Connection > Local Area Connection > Properties > Internet Protocol Version 4 (TCP/IPv4) > Properties".

**Step 2** Change the selected "5" in red frame of the picture below to "1".



**Step 3** Click “OK”, IP address is modified successfully.

**Step 4** End.



Notice

In windows system, if user adopts the advanced configuration function of IP address and accesses the switch device via setting IP dummy address, the following managed functions can't be achieved: IEEE 802.1x polling.

## 1.3 Log in the Web Configuration Interface

### Operation Steps

Login in the web configuration interface as follows:

**Step 1** Run the computer browser.

**Step 2** On the browser's address bar, type in the switch addresses "http://192.168.1.254".

**Step 3** Click the “Enter” key.

**Step 4** Pop-up a window as the figure below, enter the user name and password on the login window.



Notes:

- The default username and password are “admin123”; please strictly distinguish capital and small letter while entering.
- Default username and password have the administrator privileges.
- WebServer will provide 3 times opportunities to enter username and password. If enter the error information for 3 times, the browser will display an "Access denied" to reject access message. Refresh the page and try again.

**Step 5** Click "OK".

**Step 6** End.

After login in successfully, user can configure relative parameters and information according to demands.

Notes:

After login in the device, modify the switch IP address for usage convenience.

# 2 System Configuration

## 2.1 System Information

### Function Description

In "System Information" page, user can check "Device Information" and "Port Info".

### Operation Path

Open in order: "Main Menu > System Config > System Information".

### Interface Description

Device information interface as follows:

Device information			
Device model:	Industrial Switch	Running time:	0Day, 2 Hours, 3 Minutes
SN:	0123456789	Cpu usage :	4.2%
Device name:	switch	memory usage:	37% (free:155424 KB, total:245272 KB)
Hardware version:	1.0	Cpu MAC:	0022-6fcc-cccc
Software version:	V1.1.1 build 20181107R		

The main element configuration description of device information interface:

Interface Element	Description
Device model	The batch number used by the device to facilitate the management of device tags.
SN	SN code, product serial number.
Device name	Network identity used by the device.
Hardware version	Current hardware version information, pay attention to the

Interface Element	Description
	hardware version limits in software version.
Software version	Current using software version information, updated software version has more functions.
Running time	Current device running time after power on.
Cpu usage	Current device CPU utilization ratio.
memory usage	Current device memory utilization ratio.
Cpu MAC	Hardware address of device factory configuration.

Port information interface as follows:

Port info					
Port number	Connection state	Duplex	Rate	Flow control	Interface type
ge1/1	LOS	-	-	-	Light
ge1/2	LOS	-	-	-	Light
ge1/3	LINK	FULL	1000M	DISABLE	Light
ge1/4	LOS	-	-	-	Light
ge1/5	LOS	-	-	-	Electricity
ge1/6	LOS	-	-	-	Electricity
ge1/7	LOS	-	-	-	Electricity
ge1/8	LOS	-	-	-	Electricity
ge1/9	LOS	-	-	-	Electricity
ge1/10	LOS	-	-	-	Electricity
ge1/11	LOS	-	-	-	Electricity
ge1/12	LOS	-	-	-	Electricity
ge1/13	LOS	-	-	-	Electricity
ge1/14	LOS	-	-	-	Electricity
ge1/15	LOS	-	-	-	Electricity
ge1/16	LOS	-	-	-	Electricity
ge1/17	LOS	-	-	-	Electricity

The main element configuration description of port information interface:

Interface Element	Description
Port number	The corresponding port name of the device Ethernet port.
Connection state	Port connection state, display state as follows: <ul style="list-style-type: none"> <li>"LINK" represents connected port;</li> <li>"LOS" represents disconnected port.</li> </ul>

Interface Element	Description
Port state	Port work state, display state as follows: <ul style="list-style-type: none"> <li>"HALF" represents the corresponding port is in half-duplex state;</li> <li>"FULL" represents corresponding port is in full duplex state.</li> </ul>
Rate	Current port link rate, valid after port connection, display speed as follows: <ul style="list-style-type: none"> <li>10M;</li> <li>100M;</li> <li>1000M</li> </ul>
Interface type	Interface type, display port type as follows: <ul style="list-style-type: none"> <li>Fiber port;</li> <li>Copper port.</li> </ul>

## 2.2 User Configuration

### Function Description

On the "User Config" page, user is free to add and delete username, user needs to enter username and password to access the device, the initial username and password are: admin123.

### Operation Path

Open in order: "Main Menu > System Config > User Config".

### Interface Description

User configuration interface as follows:

User set

User name:  31 characters atmost. We have to modify the related password and authority if the user exists already.

Password:  no more than 31 characters

Privilege:  ▼

User name	Password	Privilege	
admin123	admin123	15	<input type="button" value="Delete"/>



The main element configuration description of user configuration interface:

Interface Element	Description
User name	Visitor's identification, it can't be empty. Notes: Maximum 31 characters, if the user has existed in system, user should modify relative password and privilege.
Password	Password used by visitor, it can't be empty, maximum 31 characters.
Privilege	The visitor's privilege is 1-15. Notes: <ul style="list-style-type: none"><li>• Privilege 1-2: Only conduct read-only operation in the command line;</li><li>• Privilege 3-15: It can conduct all operations.</li><li>• In this device, these privileges only work when user adopts Telnet or HyperTerminal to access the device. Any privilege in the WEB interface can perform all operations.</li></ul>

## 2.3 Device Log Message

### Function Description

On the "Device log message" page, user can view the log information of the device and upload the log information to the tftp server.

### Operation Path

Open in order: " Main Menu > System Configuration > Device log message".

### Interface Description

Log information interface as follows:

**log upload**

TFTP server address:

File name:  the name of the stored file on the server

**Log-infomation**

```

2019/01/23 13:52:03 SNMP: SNMP V1.1.1 build 20181107R starting
2019/01/23 13:52:03 RIP: RIPd V1.1.1 build 20181107R starting
2019/01/23 13:52:03 OSPF: OSPFd V1.1.1 build 20181107R starting
2019/01/23 13:52:03 VRRP: VRRP V1.1.1 build 20181107R starting
2019/01/23 13:52:03 NETMANAGER: netmanager V1.1.1 build 20181107R starting
2019/01/23 13:52:03 BGP: BGPd V1.1.1 build 20181107R starting
2019/01/23 13:52:12 ZEBRA: vlanif1 changes to UP
2019/01/23 13:52:12 MCWNO: gel/1 is up
2019/01/23 13:52:19 SNMP: switch coldstart
2019/01/23 13:52:39 ZEBRA: vlanif1 changes to DOWN
2019/01/23 13:52:40 MCWNO: gel/1 is down
2019/01/23 13:52:43 MCWNO: gel/1 is up
2019/01/23 13:52:43 ZEBRA: vlanif1 changes to UP
2019/01/24 14:43:46 MCWNO: Mono V1.1.1 build 20181107R starting
2019/01/24 14:43:47 SNMP: SNMFD V1.1.1 build 20181106R starting
2019/01/24 14:43:47 SNMP: srmpd receive 590 starting
2019/01/24 14:43:47 ZEBRA: Zebra V1.1.1 build 20181107R starting
2019/01/24 14:43:47 MSTP: MSTP V1.1.1 build 20181107R starting
2019/01/24 14:43:47 ICMFS: Igmps V1.1.1 build 20181107R starting
2019/01/24 14:43:47 LLDP: LLDP V1.1.1 build 20181107R starting
2019/01/24 14:43:47 RELAY: relay V1.1.1 build 20181107R starting
2019/01/24 14:43:47 LACP: LACP V1.1.1 build 20181107R starting
2019/01/24 14:43:47 DHCPSNOOP: Dhcp-snooping V1.1.1 build 20181107R starting
2019/01/24 14:43:47 SNMP: SNMP V1.1.1 build 20181107R starting
2019/01/24 14:43:47 RIP: RIPd V1.1.1 build 20181107R starting
2019/01/24 14:43:47 OSPF: OSPFd V1.1.1 build 20181107R starting
2019/01/24 14:43:47 VRRP: VRRP V1.1.1 build 20181107R starting
2019/01/24 14:43:47 NETMANAGER: netmanager V1.1.1 build 20181107R starting
2019/01/24 14:43:47 BGP: BGPd V1.1.1 build 20181107R starting
2019/01/24 14:44:03 SNMP: switch coldstart
                
```

The main element configuration description of log information interface:

Interface Element	Description
TFTP server address	Upload log TFTP server IP address.
File name	Log stored file name.

## 2.4 SSHD Configuration

### Function Description

On the "SSHD-config" page, enable/disable the SSH service function. The full English name of SSH is Secure Shell. SSH is the security protocol based on the application layer and transport layer. SSH is a currently reliable protocol that provides security protocol for remote login sessions and other web services. SSH protocol can effectively prevent the information leakage in the process of remote management issues, and DNS and IP spoofing. In addition, the transmitted data is compressed so that the transmission speed can be increased.

### Operation Path

Open in order: "Main Menu > System Config > SSHD-config".

### Interface Description

SSHD configuration interface as follows:

The main element configuration description of SSHD configuration interface:

Interface Element	Description
SSH service	SSH service function status, the options are as follows: <ul style="list-style-type: none"> <li>• Enable;</li> <li>• Disable.</li> </ul>

## 2.5 TELNET Configuration

### Function Description

On the "TELNET-config" page, enable TELNET service, TELNET terminal can be connected to the switch through the PC Telnet client.

### Operation Path

Open in order: "Main Menu > System Config > TELNET-config".

### Interface Description

TELNET configuration interface as follows:

The main element configuration description of TELNET configuration interface:

Interface Element	Description
TELNET service	TELNET service function status, the options are as follows: <ul style="list-style-type: none"> <li>• Enable;</li> <li>• Disable.</li> </ul>
Port	TELNET service port number, default port number is 23.

## 2.6 HTTPS Setting

### Function Description

On the "HTTPS-config" page, enable the HTTP or HTTPS protocol, PC can use browser to access the switch. HTTPS (Full name: Hypertext Transfer Protocol over Secure Socket Layer), is the HTTP channel which takes safety as the goal, is simply a safe version of HTTP. HTTPS provides data encryption services to prevent the attacker to intercept the transmitted message between the Web browser and web server, obtain some sensitive information, such as credit card numbers, passwords, etc.

### Operation Path

Open in order: "Main Menu > System Config > HTTPS-config".

### Interface Description

HTTPS configuration interface as follows:

The main element configuration description of HTTPS configuration interface:

Interface Element	Description
-------------------	-------------

Interface Element	Description
HTTP	Device HTTP protocol function status, enable checkbox. Notes: HTTP access format is: HTTP://192.168.1.254, Address is corresponding switch IP address.
HTTPS	Device HTTPS protocol function status, enable checkbox. Notes: HTTPS access format is: HTTPS://192.168.1.254, Address is corresponding switch IP address.
Port	HTTP protocol service port number, the default port number is 80, if the default port is modified, specify the port number in the browser address bar while accessing.

## 2.7 Diagnostic Test

### 2.7.1 Ping

#### Function Description

On the "Ping" page, Ping is used to check whether the network is open or network connection speed. Ping utilizes the uniqueness of network machine IP address to send a data packet to the target IP address, and then ask the other side to return a similarly sized packet to determine whether two network machines are connected and communicated, and confirm the time delay.

#### Operation Path

Open in order: "Main Menu > System Config > Diagnosis > Ping".

#### Interface Description

Ping information interface as follows:

The screenshot shows a web interface for the 'Ping' function. At the top, there is a blue header with the word 'Ping'. Below the header, there is a text label 'IP address:' followed by a text input field. To the right of the input field, there is a small text example 'eg:192.168.1.1, 2000:1'. Below the input field and example, there is a rectangular button labeled 'Test'.

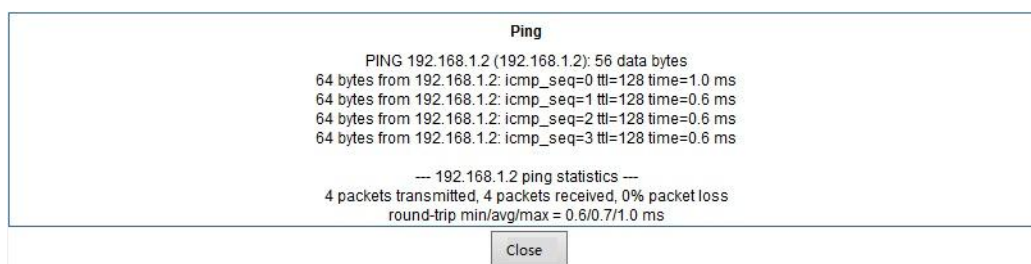
The main element configuration description of Ping configuration interface:

Interface Element	Description
IP Address	The IP address of the detected device, that is, the destination address. The device can check the network intercommunity to other devices via the ping command.

### Ping Configuration Steps:

**Step 1** Fill in the needed Ping IP address in the IP address text box;

**Step 2** Click the "Test" to see the Ping results;



**Step 3** End.

## 2.7.2 TRACEROUTE

### Function Description

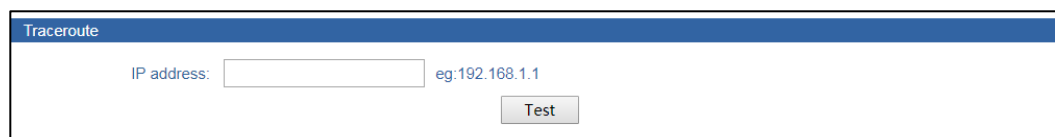
In the "Traceroute" page, users can test the network situation between the switch and the target host. Traceroute sends the data packet to destination device and measure the cost time. Each Traceroute will measure a route for three times. Output result includes each test time (ms), device name (if exists) and the IP address.

### Operation Path

Open in order: "Main Menu > System Config > Diagnosis > Traceroute".

### Interface Description

Traceroute interface as follows:



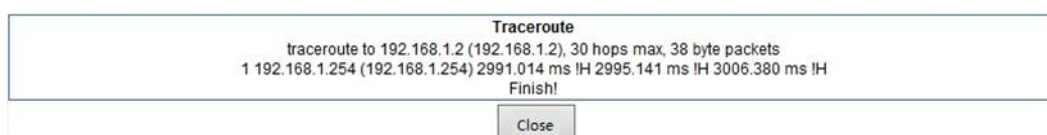
The main element configuration description of Traceroute interfaces:

Interface Element	Description
IP address	Destination device IP address, fill in the opposite device IP address that needs test.

### TRACEROUTE Configuration Steps:

**Step 1** Fill in the destination IP address in the "IP address" text box;

**Step 2** Click the "Test" to see the results, as the picture below.



Notes:

The picture above shows the time from device to IP address 192.168.1.2, after a jump, the three times were 2991.014ms, 2995.141ms and 3006.380ms.

**Step 3** End.

## 2.7.3 Port Loopback

### Function Description

On "Port Loopback" page, user can measure the loopback situation of the switch port PHY or MAC for the convenience of troubleshooting. Port loopback is a common method for the maintenance and troubleshooting of communication port line. Connect the sending end of tested device or line to its receiving end, then the tested device can judge whether the line or port exists breakpoint by receiving the signal sent by it. The test instrument hanged on the loopback route can also test the transmission quality of the loopback route.

### Operation Path

Open in order: "Main Menu > System Config > Diagnosis > Port Loopback".

### Interface Description

Port loopback interface as follows:

Port Loopback			
Port	Port Loopback	Port	Port Loopback
ge1/1	None ▼	ge1/2	None ▼
ge1/3	None ▼	ge1/4	None ▼
ge1/5	None ▼	ge1/6	None ▼
ge1/7	None ▼	ge1/8	None ▼
ge1/9	None ▼	ge1/10	None ▼
ge1/11	None ▼	ge1/12	None ▼
ge1/13	None ▼	ge1/14	None ▼
ge1/15	None ▼	ge1/16	None ▼
ge1/17	None ▼	ge1/18	None ▼
ge1/19	None ▼	ge1/20	None ▼

Attention: loopback may cause broadcast storm, the page won't be accessed. Please not use if not ensure

The main element configuration description of port loopback interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Port Loopback	Port loopback method, options as follows: <ul style="list-style-type: none"> <li>• None: that is the port disable port loopback function;</li> <li>• MAC: Data is looped back after transmitted to the MAC layer of Ethernet;</li> <li>• PHY: Data is looped back after transmitted to the physical layer of Ethernet.</li> </ul>



# 3 Port Configuration

---

## 3.1 Port Setting

### Function Description

On the "Port Setting" page, user can check port type, rate and connection state, set rate mode, duplex mode, port enable, flow control and other parameters.

### Operation Path

Open in order: " Main Menu > Port Config > Port Setting".

### Interface Description

Port setting interface as follows:

Port Setting								
PortName	Status	Medium	Rate	Duplex	Rate status	Flow control	Max-Frame	Enable
ge1/1	LOS	Light	Auto negotiation ▼	Auto ▼	-	disable ▼	1518	<input checked="" type="checkbox"/>
ge1/2	LOS	Light	Auto negotiation ▼	Auto ▼	-	disable ▼	1518	<input checked="" type="checkbox"/>
ge1/3	LINK	Light	Auto negotiation ▼	Auto ▼	1000M full	disable ▼	1518	<input checked="" type="checkbox"/>
ge1/4	LOS	Light	Auto negotiation ▼	Auto ▼	-	disable ▼	1518	<input checked="" type="checkbox"/>
ge1/5	LOS	Electricty	Auto negotiation ▼	Auto ▼	-	disable ▼	1518	<input checked="" type="checkbox"/>
ge1/6	LOS	Electricty	Auto negotiation ▼	Auto ▼	-	disable ▼	1518	<input checked="" type="checkbox"/>
ge1/7	LOS	Electricty	Auto negotiation ▼	Auto ▼	-	disable ▼	1518	<input checked="" type="checkbox"/>
ge1/8	LOS	Electricty	Auto negotiation ▼	Auto ▼	-	disable ▼	1518	<input checked="" type="checkbox"/>
ge1/9	LOS	Electricty	Auto negotiation ▼	Auto ▼	-	disable ▼	1518	<input checked="" type="checkbox"/>
ge1/10	LOS	Electricty	Auto negotiation ▼	Auto ▼	-	disable ▼	1518	<input checked="" type="checkbox"/>
ge1/11	LOS	Electricty	Auto negotiation ▼	Auto ▼	-	disable ▼	1518	<input checked="" type="checkbox"/>
ge1/12	LOS	Electricty	Auto negotiation ▼	Auto ▼	-	disable ▼	1518	<input checked="" type="checkbox"/>
ge1/13	LOS	Electricty	Auto negotiation ▼	Auto ▼	-	disable ▼	1518	<input checked="" type="checkbox"/>
ge1/14	LOS	Electricty	Auto negotiation ▼	Auto ▼	-	disable ▼	1518	<input checked="" type="checkbox"/>
ge1/15	LOS	Electricty	Auto negotiation ▼	Auto ▼	-	disable ▼	1518	<input checked="" type="checkbox"/>
ge1/16	LOS	Electricty	Auto negotiation ▼	Auto ▼	-	disable ▼	1518	<input checked="" type="checkbox"/>
ge1/17	LOS	Electricty	Auto negotiation ▼	Auto ▼	-	disable ▼	1518	<input checked="" type="checkbox"/>
ge1/18	LOS	Electricty	Auto negotiation ▼	Auto ▼	-	disable ▼	1518	<input checked="" type="checkbox"/>
ge1/19	LOS	Electricty	Auto negotiation ▼	Auto ▼	-	disable ▼	1518	<input checked="" type="checkbox"/>
ge1/20	LOS	Electricty	Auto negotiation ▼	Auto ▼	-	disable ▼	1518	<input checked="" type="checkbox"/>

The main element configuration description of port setting interface:

Interface Element	Description
Port Name	The corresponding port name of the device Ethernet port.
Status	Ethernet port connection status, display status as follows: <ul style="list-style-type: none"> <li>• LOS: represent the port is disconnected;</li> <li>• LINK: represent the port is connected.</li> </ul>
Medium	Ethernet port connection type, display medium as follows: <ul style="list-style-type: none"> <li>• Copper port;</li> <li>• Fiber port.</li> </ul>
Rate	Ethernet port working speed, optional speed as follows: <ul style="list-style-type: none"> <li>• Auto negotiation: that is 10/100/1000 M speed self-adaption;</li> <li>• 10M only;</li> <li>• 100M only;</li> <li>• 1000M only.</li> </ul>
Duplex	Under current Ethernet working mode, optional mode as follows: <ul style="list-style-type: none"> <li>• Auto negotiation;</li> <li>• Full duplex;</li> <li>• Half duplex</li> </ul>

Interface Element	Description
Rate status	Current Ethernet port working rate, display rate as follows: <ul style="list-style-type: none"> <li>• 10M;</li> <li>• 100M.</li> <li>• 1000M</li> </ul>
Flow control	Port flow control status, options as follows: <ul style="list-style-type: none"> <li>• Disable: Disable;</li> <li>• Tx: Enable port data sending flow control;</li> <li>• Rx: Enable port data receiving control;</li> <li>• Both: Enable port data sending or receiving flow control.</li> </ul>
Max-Frame	Ethernet port transmitted maximum data frame length, input range 64-16356.
Enable	Enable Ethernet port. Note: If user doesn't check the port "Enable" checkbox, the port won't be connected to use.

## 3.2 Storm Control

### Function Description

On the "Storm Control" page, user can set the maximum broadcast, multicast or unknown unicast packet flow the port allows. When the sum of each port broadcast, unknown multicast or unknown unicast flow achieves the value user sets, the system will discard the packets beyond the broadcast, unknown multicast or unknown unicast flow limit, so that the proportion of overall broadcast, unknown multicast or unknown unicast flow can be reduced to limited range, ensuring the normal operation of network business.

### Operation Path

Open in order: "Main Menu > Port Config > Storm control".

### Interface Description

Storm control interface as follows:

Storm control					
Port	Broadcast(kbps)		Unkown Multicast(kbps)		Unkown Unicast(kbps)
ge1/1	0		0		0
ge1/2	0		0		0
ge1/3	0		0		0
ge1/4	0		0		0
ge1/5	0		0		0
ge1/6	0		0		0
ge1/7	0		0		0
ge1/8	0		0		0
ge1/9	0		0		0
ge1/10	0		0		0
ge1/11	0		0		0
ge1/12	0		0		0
ge1/13	0		0		0
ge1/14	0		0		0
ge1/15	0		0		0
ge1/16	0		0		0
ge1/17	0		0		0
ge1/18	0		0		0
ge1/19	0		0		0
ge1/20	0		0		0

The main element configuration description of storm control interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Broadcast (kbps)	The port control for broadcast packet transmission speed, input value range 0-100000. Notes: Broadcast packet, namely, the destination address is FF-FF-FF-FF-FF-FF data frame.
Unknown Multicast (kbps)	The port control for unknown multicast data packet transmission speed, input value range 0-100000. Notes: Multicast packet, namely, the destination address is XX-XX-XX-XX-XX-XX data frame, the second X is odd number, such as: 1, 3, 5, 7, 9, B, D, F, other X represents arbitrary number.
Unknown Unicast (kbps)	The port control for unknown unicast data packet transmission speed, input value range 0-100000. Notes: Unknown unicast packet, namely, the MAC address of the data frame doesn't exist in the MAC address table of the device, which needs to be forwarded to all ports.

## 3.3 Port Rate Limit

### Function Description

On the "Port rate-Limit" page, User can limit the communication flow of each port or cancel the port flow limit. The device provides port speed limit, including entrance and exit speed limit. User can select a fixed speed, its range is: 0kbps~100Mbps (100M), the device will discard the packet or adopt flow control to limit the transmission speed or receiving speed of opposite device according to the flow control is enabled or not.

### Operation Path

Open in order: "Main menu > Port Config > Port rate-Limit".

### Interface Description

Port rate limit interface as follows:

Port rate-Limit				
Port	InputRate(kbps)	InputBurst(kbps)	OutputRate(kbps)	OutputBurst(kbps)
ge1/1	0	0	0	0
ge1/2	0	0	0	0
ge1/3	0	0	0	0
ge1/4	0	0	0	0
ge1/5	0	0	0	0
ge1/6	0	0	0	0
ge1/7	0	0	0	0
ge1/8	0	0	0	0
ge1/9	0	0	0	0
ge1/10	0	0	0	0
ge1/11	0	0	0	0
ge1/12	0	0	0	0
ge1/13	0	0	0	0
ge1/14	0	0	0	0
ge1/15	0	0	0	0
ge1/16	0	0	0	0
ge1/17	0	0	0	0
ge1/18	0	0	0	0
ge1/19	0	0	0	0
ge1/20	0	0	0	0

The main element configuration description of port rate limit interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Input Rate(kbps)	The port limit for all input data transmission speed, input

Interface Element	Description
	value range 0-100000.
Input Burst(kbps)	The port limit for input burst data transmission speed, maximum input burst is input rate, input value range is 0-100000.
Output Rate(kbps)	The port control for all output data transmission speed, input value range 0-100000.
Output Burst(kbps)	The port control for output burst data transmission speed, input value range 0-100000.



Note

- When using the port rate limit, flow control should be enabled, otherwise the rate between devices will no longer be a smooth curve;
- When using the port rate limit, packet loss should not occur unless the flow control is disabled. The fast or slow transmission speed represents packet loss;
- Port rate limit has a high quality requirement to network cable; otherwise there will occur a lot of conflict and broken packets.

## 3.4 Mirror

### Function Description

On the "Mirror" page, user can copy the data from the origin port to appointed port for data analysis and monitoring.

### Operation Path

Open in order: "Main Menu > Port Config > Mirror".

### Interface Description

Mirror interface as follows:

**Mirror**

SessionID:

SourcePort:  ge1/1  ge1/2  ge1/3  ge1/4  ge1/5  ge1/6  ge1/7  ge1/8  ge1/9  ge1/10  
 ge1/11  ge1/12  ge1/13  ge1/14  ge1/15  ge1/16  ge1/17  ge1/18  ge1/19  ge1/20

Destination port:

Direction:

SessionID	SourcePort	Destination port	Direction
<input type="button" value="Refresh"/>			

The main element configuration description of mirror interface:

Interface Element	Description
Session ID	Device mirror ID number, value is 1-4. Notes: The device supports maximum 4-way mirror sessions.
Source port	A set of monitored ports, which will collect data from these ports in the specified direction, and the mirror port can be one or more.
Destination port	A port for monitoring, and the device outputs data from the port to the specified direction.
Direction	This parameter specifies the direction of the monitoring port data, a total of "ingress", "egress", "both" three options. Monitor can choose according to their own needs. <ul style="list-style-type: none"> <li>ingress: import data, the packet received by the port will be mirrored to the destination port;</li> <li>egress: export data, the message sent by the port will be mirrored to the destination port;</li> <li>Both: all data, mirror the port receiving and sending packets at the same time.</li> </ul>

**Note**

- The function must be shut down in normal usage, otherwise all senior management functions based on port are not available, such as RSTP, IGMP, snooping, etc.
- Mirror function only deals with FCS normal packet; it cannot handle the wrong data frame

## 3.5 Alarm Settings

### Function Description

On the "Alarm Settings" page, user can set power supply alarm, port alarm function; when the equipment is in abnormal state, it can promptly notify the administrator, and quickly repair the equipment status to avoid excessive losses.

### Operation Path

Open in order: "Main Menu > Port Config > Alarm Settings".

### Interface Description

Alarm settings interface as follows:

Port Alarm Setting					
Port Numbers	Alarm Settings	Link Status	Port Numbers	Alarm Settings	Link Status
ge1/1	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Not connected	ge1/2	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Not connected
ge1/3	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Connection	ge1/4	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Not connected
ge1/5	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Not connected	ge1/6	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Not connected
ge1/7	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Not connected	ge1/8	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Not connected
ge1/9	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Not connected	ge1/10	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Not connected
ge1/11	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Not connected	ge1/12	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Not connected
ge1/13	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Not connected	ge1/14	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Not connected
ge1/15	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Not connected	ge1/16	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Not connected
ge1/17	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Not connected	ge1/18	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Not connected
ge1/19	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Not connected	ge1/20	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	Not connected

The main element configuration description of alarm setting interface:

Interface Element	Description
Alarm Settings	Power supply and port alarm function status, options: <ul style="list-style-type: none"> <li>• Enable;</li> <li>• Disable.</li> </ul>
Relay Output Type	Relay output type status, options as follows: <ul style="list-style-type: none"> <li>• Normally open: Relay is open circuit status in normal no</li> </ul>



Interface Element	Description
	<p>alarm, when there is an alarm, the alarm lamp is bright, and the relay is in a closed state.</p> <ul style="list-style-type: none"> <li>Normally closed: Relay is closed status in normal no alarm, when there is an alarm, the alarm light is bright, the relay is in the open state.</li> </ul>
<b>Port Alarm Setting</b>	<b>Port alarm setting column.</b>
Port Numbers	The corresponding port name of the device Ethernet port.
Alarm Settings	<p>Port alarm function status, options as follows:</p> <ul style="list-style-type: none"> <li>Enable;</li> <li>Disable.</li> </ul> <p>Notes: After enable port alarm, when port occurs abnormal status, such as connection break down, the device will output a signal to hint the abnormal operation of device.</p>
Link Status	<p>Port link status, display items as follows:</p> <ul style="list-style-type: none"> <li>No connection;</li> <li>Connected.</li> </ul>

## 3.6 Link Aggregation

Link aggregation is the shorter form of Ethernet link aggregation; it binds multiple Ethernet physical links into a logical link, achieving the purpose of increasing the link bandwidth. At the same time, these bundled links can effectively improve the link reliability by mutual dynamic backup.

The Link Aggregation Control Protocol (LACP) protocol based on the IEEE802.3ad standard is a protocol for implementing dynamic link aggregation. Devices running this protocol exchange LACPDUs (Link Aggregation Control Protocol Data Unit, Link Aggregation Control Protocol Data Unit) to exchange link aggregation related information.

Based on the enabling or disabling of LACP protocol, the link aggregation can be divided into two modes, static aggregation and dynamic aggregation.

## 3.6.1 Static Configuration

### Function Description

Under static aggregation mode, the member port in aggregation group disables LACP protocol, its port status is maintained manually.

### Operation Path

Open in order: "Main Menu > Port Config > Link Aggregation > Static Config".

### Interface Description

Static configuration interface as follows:

The screenshot shows a web-based configuration interface for static LACP aggregation. It is divided into three main sections:

- LACP setting:** Contains a text input field for 'LACP setting' with the value '32768' and a 'scope:0-65535,Default:32768'. Below the input are 'Apply' and 'Cancel' buttons.
- Add static LACP:** Features a 'Group ID' dropdown menu set to '1' and a 'Load balance mode' dropdown menu set to 'Src Mac'. Below these are two rows of checkboxes for ports 'ge1/1' through 'ge1/20'. At the bottom of this section are 'Add' and 'Delete' buttons.
- lACP list:** A table with columns for 'Group ID', 'Type', 'Status', 'Load balance mode', and 'Port member'. A 'Refresh' button is located below the table.

The main element configuration description of static configuration interface:

Interface Element	Description
<b>LACP setting</b>	<b>LACP setting column.</b>
LACP setting	LACP priority level setting, LACP setting range 0-65535, defaults to 32768. Notes: The smaller of interface LACP priority level value is, the higher priority level is, which is used for distinguishing the priority degree of selecting different ports as active port.
<b>Add static LACP</b>	<b>Add static aggregation group setting column.</b>
Group ID	Static aggregation link ID number, support maximum 16 groups, each group can configure 8 ports to join aggregation.
Load balance	Load balance mode is the flow load balance in aggregation

Interface Element	Description
mode	group, there exist 3 options: <ul style="list-style-type: none"> <li>• Src Mac: Conduct load balance according to the message MAC address, messages with the same source MAC addresses pass via the same port when , otherwise, messages pass via different ports;</li> <li>• Dst Mac: Conduct load balance according to the message destination MAC address, messages with the same destination MAC addresses pass via the same port, otherwise, messages pass via different ports;</li> <li>• Src&amp;Dst Mac: Conduct load balance according to the message source and destination MAC address, messages with the same source and destination MAC addresses pass via the same port, otherwise, messages pass via different ports;</li> </ul>
Port list	Device port list, check the port to join aggregation group.
<b>lACP list</b>	<b>LACP list column.</b>
Group ID	Added port aggregation group ID number.
Type	Aggregation group mode: <ul style="list-style-type: none"> <li>• Manual: Static aggregation;</li> <li>• LACP: Dynamic aggregation.</li> </ul>
Status	Aggregation group connection state: <ul style="list-style-type: none"> <li>• UP: Port member is connected;</li> <li>• DOWN: Port member is disconnected.</li> </ul>
Load balance mode	Load balance mode: <ul style="list-style-type: none"> <li>• Src Mac;</li> <li>• Dst Mac;</li> <li>• Src&amp;Dst Mac.</li> </ul>
Port member	Port member in the aggregation group.

## 3.6.2 LACP Configuration

### Function Description

Dynamic aggregation is an aggregation method in which system automatically creates or deletes aggregation group, the port addition and deleting in the dynamic

aggregation group is done automatically by LACP protocol. Only ports connected to the same device with same rate, duplex property, and basic configuration can create a dynamic aggregation. Even one port can also create dynamic aggregation, at this time, its single port aggregation. In dynamic aggregation, port LACP protocol is in enable state.

### Operation Path

Open in order: "Main Menu > Port Config > Link Aggregation > LACP Config".

### Interface Description

LACP configuration interface as follows:

PortName	Type	Group ID	Mode	PortPriority
ge1/1	None	1	Active	32768
ge1/2	None	1	Active	32768
ge1/3	None	1	Active	32768
ge1/4	None	1	Active	32768
ge1/5	None	1	Active	32768
ge1/6	None	1	Active	32768
ge1/7	None	1	Active	32768
ge1/8	None	1	Active	32768
ge1/9	None	1	Active	32768
ge1/10	None	1	Active	32768
ge1/11	None	1	Active	32768
ge1/12	None	1	Active	32768
ge1/13	None	1	Active	32768
ge1/14	None	1	Active	32768
ge1/15	None	1	Active	32768
ge1/16	None	1	Active	32768
ge1/17	None	1	Active	32768
ge1/18	None	1	Active	32768
ge1/19	None	1	Active	32768
ge1/20	None	1	Active	32768

The main element configuration description of LACP configuration interface:

Interface Element	Description
Port Name	The corresponding port name of the device Ethernet port.

Interface Element	Description
Type	Setting port aggregation function: <ul style="list-style-type: none"> <li>• None: Represent the port disabling link aggregation function;</li> <li>• Static: Represent the port is static aggregation mode;</li> <li>• Dynamic (LACP): Represent the port is dynamic aggregation mode.</li> </ul>
Group ID	Group ID, the range is 1-16.
Mode	Mode refers to LACP negotiation mode, it's divided into: <ul style="list-style-type: none"> <li>• Active: The port sends LACP message periodically;</li> <li>• Passive: The port doesn't send LACP message in normal time, once receiving the LACP message of opposite terminal, it will normally send LACP message.</li> </ul>
Port Priority	Dynamic LACP port priority, defaults to 32768.

## 3.7 Isolate-port

### Function Description

Isolate-port is for achieving layer-2 isolation between messages, it can add different ports to different VLAN, but won't waste limited VLAN sources. Adopting isolate-port characteristics can achieve isolation of ports within the same VLAN. After adding the ports to isolation group, user can achieve the layer 2 data isolation of ports within isolation group. Port isolation function has provided safer and more flexible networking scheme for users.

### Operation Path

Open in order: "Main Menu > Port Config > Isolate-port Config".

### Interface Description

Isolate-port configuration interface as follows:

Isolate-port Config			
PortName	PortIsolation	PortName	PortIsolation
ge1/1	<input type="checkbox"/>	ge1/2	<input type="checkbox"/>
ge1/3	<input type="checkbox"/>	ge1/4	<input type="checkbox"/>
ge1/5	<input type="checkbox"/>	ge1/6	<input type="checkbox"/>
ge1/7	<input type="checkbox"/>	ge1/8	<input type="checkbox"/>
ge1/9	<input type="checkbox"/>	ge1/10	<input type="checkbox"/>
ge1/11	<input type="checkbox"/>	ge1/12	<input type="checkbox"/>
ge1/13	<input type="checkbox"/>	ge1/14	<input type="checkbox"/>
ge1/15	<input type="checkbox"/>	ge1/16	<input type="checkbox"/>
ge1/17	<input type="checkbox"/>	ge1/18	<input type="checkbox"/>
ge1/19	<input type="checkbox"/>	ge1/20	<input type="checkbox"/>

The main element configuration description of isolate-port config interface:

Interface Element	Description
Port Name	The corresponding port name of the device Ethernet port.
Port Isolation	Check the port isolation optional box to enable the port isolation function within the same VLAN.

## 3.8 Port Statistics

### 3.8.1 Port Stats

#### Function Description

On the "Port Stats" page, user can check the data packet and byte number that each port sends or receives,

#### Operation Path

Open in order: "Main Menu > Port Config > Port statistics > Port stats".

#### Interface Description

Port stats interface as follows:

Port stats					
PortName	Packet		Byte		Filter
	Receive	Send	Receive	Send	Receive
ge1/1	0	0	0	0	0
ge1/2	0	0	0	0	0
ge1/3	1459	1130	185497	909649	133
ge1/4	0	0	0	0	0
ge1/5	0	0	0	0	0
ge1/6	0	0	0	0	0
ge1/7	0	0	0	0	0
ge1/8	0	0	0	0	0
ge1/9	0	0	0	0	0
ge1/10	0	0	0	0	0
ge1/11	0	0	0	0	0
ge1/12	0	0	0	0	0
ge1/13	0	0	0	0	0
ge1/14	0	0	0	0	0
ge1/15	0	0	0	0	0
ge1/16	0	0	0	0	0
ge1/17	0	0	0	0	0
ge1/18	0	0	0	0	0
ge1/19	0	0	0	0	0
ge1/20	0	0	0	0	0

## 3.8.2 Detail Port Stats

### Function Description

On the "Detail port stats" page, user can check the data sum and message size classified statistic that each port sends or receives.

### Operation Path

Open in order: "Main Menu > Port Config > Port statistics > Detail port stats".

### Interface Description

Detail port stats interface as follows:

Detail port stats			
Port: <input type="text" value="ge1/1"/>		<input type="button" value="Refresh"/>	<input type="button" value="Clear"/>
ReceiveTotal		SendTotal	
ReceivePacket num	0	SendPacket num	0
ReceiveByte num	0	SendByte num	0
ReceiveUnicast num	0	SendUnicast num	0
ReceiveMulticast num	0	SendMulticast num	0
ReceiveBroadcast num	0	SendBroadcast num	0
ReceivePause frame	0	SendPause frame	0
ReceiveMessage size classification statistics		SendMessage size classification statistics	
Receive64Byte size packet num	0	Send64Byte size packet num	0
Receive65-127Byte size packet num	0	Send65-127Byte size packet num	0
Receive128-255Byte size packet num	0	Send128-255Byte size packet num	0
Receive256-511Byte size packet num	0	Send256-511Byte size packet num	0
Receive512-1023Byte size packet num	0	Send512-1023Byte size packet num	0
Receive1024-1518Byte size packet num	0	Send1024-1518Byte size packet num	0
Receive1519-2047Byte size packet num	0	Send1519-2047Byte size packet num	0
Receive2048-4095Byte size packet num	0	Send2048-4095Byte size packet num	0
Receive4096-9216Byte size packet num	0	Send4096-9216Byte size packet num	0



# 4 Layer 2 Configuration

## 4.1 VLAN Configuration

VLAN is Virtual Local Area Network. VLAN is the data switching technology that logically (note: not physically) divides the LAN device into each network segment (or smaller LAN) to achieve the virtual working group (unit).

VLAN advantages mainly include:

- Port isolation. Ports in different VLAN, even in the same switch, can't intercommunicate. Such a physical switch can be used as multiple logical switches.
- Network security. Different VLAN can't directly communicate with each other, which has eradicated the insecurity of broadcast information.
- Flexible management. Changing the network user belongs to needn't to change ports or connection; only needs to change the firmware configuration.

That is, ports within the same VLAN can intercommunicate; otherwise, ports can't communicate with each other. A VLAN is identified with VLAN ID, and ports with the same VLAN ID belong to a same VLAN.

### 4.1.1 PVlan Configuration

#### Function Description

On the "PVlan-config" page, user can configure the port VLAN mode (access, trunk), and VLAN ID: PVID.

#### Operation Path

Open in order: "Main Menu > Layer 2 Config > VLAN Config > PVlan-config".

## Interface Description

PVlan configuration interface as follows:

PVlan-config		
Port	VLANMode	PVID
ge1/1	access ▼	1
ge1/2	access ▼	1
ge1/3	access ▼	1
ge1/4	access ▼	1
ge1/5	access ▼	1
ge1/6	access ▼	1
ge1/7	access ▼	1
ge1/8	access ▼	1
ge1/9	access ▼	1
ge1/10	access ▼	1
ge1/11	trunk ▼	10
ge1/12	trunk ▼	10
ge1/13	trunk ▼	10
ge1/14	trunk ▼	10
ge1/15	trunk ▼	10
ge1/16	trunk ▼	10
ge1/17	trunk ▼	10
ge1/18	trunk ▼	10
ge1/19	trunk ▼	10
ge1/20	trunk ▼	10

The main element configuration description of PVlan configuration interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
VLAN Mode	Two port link types that the switch supports: <ul style="list-style-type: none"> <li>• Access: Port can only belong to 1 VLAN, which is generally used to connect user device. All default ports belong to access port.</li> <li>• Trunk: Ports can belong to multiple VLAN, receive and send multiple VLAN messages, generally used in the connection between network devices.</li> </ul>
PVID	Port0base Vlan ID is the port virtual LAN ID number, which is relative to the VLAN TAG mark when the port receives and sends data frame.

## 4.1.2 Trunk Configuration

### Function Description

On the "Trunk-config" page, user can configure the port Untagged and Tag port list.

### Operation Path

Open in order: "Main Menu > Layer 2 Config > VLAN Config > Trunk-config".

### Interface Description

Trunk configuration interface as follows:

**Vlan setting**

Vlan ID:  scope:1-4094. The port will automatically change to trunk mode.

Untag Port list:

ge1/1  ge1/2  ge1/3  ge1/4  ge1/5  ge1/6  ge1/7  ge1/8  ge1/9  ge1/10  
 ge1/11  ge1/12  ge1/13  ge1/14  ge1/15  ge1/16  ge1/17  ge1/18  ge1/19  ge1/20

Tag Port list:

ge1/1  ge1/2  ge1/3  ge1/4  ge1/5  ge1/6  ge1/7  ge1/8  ge1/9  ge1/10  
 ge1/11  ge1/12  ge1/13  ge1/14  ge1/15  ge1/16  ge1/17  ge1/18  ge1/19  ge1/20

VID	Untag Port list	Tag Port list
1	ge1/1 ge1/2 ge1/3 ge1/9 ge1/10	ge1/4 ge1/5 ge1/6 ge1/7 ge1/8
10	ge1/11 ge1/12 ge1/13 ge1/19 ge1/20	ge1/14 ge1/15 ge1/16 ge1/17 ge1/18

Total 2 Entry 20 entrys per page 1/1Page

The main element configuration description of Trunk configuration interface:

Interface Element	Description
Vlan ID	VLAN ID number, value range is 1-4094.
Untag Port list	Untagged port member to conduct untagged process to sending data frame.
Tag Port list	Tag port member to conduct tagged process to sending data frame.

### Process for Port Receiving and Sending Message

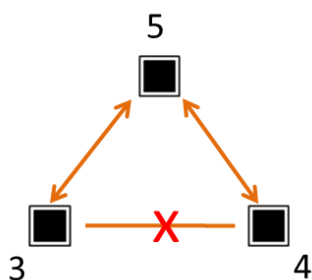
Port Type	Process for Receiving Message	
	When Receiving the untagged message	When Receiving Tagged Message
<b>Access Port</b>	Label the message with corresponding VLAN Tag of port default VLAN ID.	Label the message with corresponding VLAN Tag of port default VLAN ID.
<b>Trunk Port</b>	Label the message with corresponding VLAN Tag of port default VLAN ID.	Keep VLAN ID unchanged, without replacing.

Port Type	Process for Sending Message
<b>Untag</b>	Forward the untagged message during forwarding
<b>Tag</b>	Forward the tagged message during forwarding

Access port type can only be Untagged, Trunk port type can be Untagged or Tag.

### Example: Typical VLAN Configuration

Suppose that the switch port 3, 4 and 5 have the following requirements: Port 3 and Port 5 communicate with each other. Port 4 and Port 5 communicate with each other. Port 3 and Port 4 cannot communicate with each other, as the picture below. Do not consider other ports, how to set the VLAN?



### Example Analysis

Port3, Port 4 and Port 5 are set with different forwarding entries, and forwarding entries enable the communication between the ports.

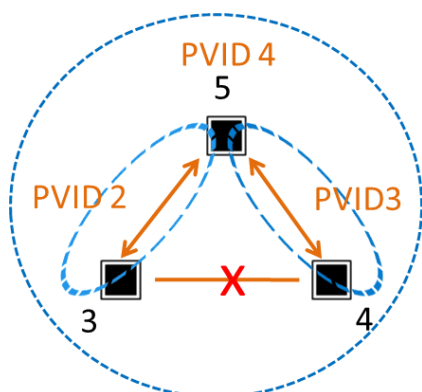
Analyze the port forwarding entries design as below:

- Port3

Port3 and Port5 communicate with each other. Port3 forwarding entries include Port3 and Port5. Therefore, a forwarding entry PVID2 is designed, including Port 3 and Port 5. Plan port 3 and port 5 as "Untag Port List".

- Port4  
Port4 and Port5 communicate with each other. Port3 forwarding entries include Port4 and Port5. Therefore, a forwarding entry PVID3 is designed, including Port 4 and Port 5. Plan Port4 and Port5 as "Untag Port List".
- Port5  
Port5 and Port3, Port4 communicate with each other, Port5 forwarding entries include Port3, Port4 and Port5. Therefore, design a forwarding entry PVID4, including Port3, Port 4 and Port 5. Plan port 3, port 4 and port 5 as "Untag Port List".

According to Port3, Port 4 and Port 5 forwarding entry analysis, the forwarding entry design picture as follows:



### Operation Steps

**Step 1** Access "Main Menu > Layer 2 Config > VLAN Config > Trunk-config".

**Step 2** Establish forwarding entry PVID2.

1. Enter 2 in "Vlan ID" text box;
2. Select the ports "fe1/3" and "fe1/5" checkbox under "Untag Port List";
3. Click "add" button.

**Step 3** Establish forwarding entry PVID3.

1. Enter 3 in "Vlan ID" text box;
2. Select the ports "fe1/4" and "fe1/5" checkbox under "Untag Port List";
3. Click "add" button.

**Step 4** Establish forwarding entry PVID4.

1. Enter 4 in "Vlan ID" text box;
2. Select the port "ge1/3", "ge1/4" and "ge1/5" checkbox under "Untag Port List";
3. Click "add" button, as the picture below.

**Vlan setting**

Vlan ID:  scope:1-4094. The port will automatically change to trunk mode.

Untag Port list:

ge1/1    ge1/2    ge1/3    ge1/4    ge1/5    ge1/6    ge1/7    ge1/8    ge1/9    ge1/10  
 ge1/11    ge1/12    ge1/13    ge1/14    ge1/15    ge1/16    ge1/17    ge1/18    ge1/19    ge1/20

Tag Port list:

ge1/1    ge1/2    ge1/3    ge1/4    ge1/5    ge1/6    ge1/7    ge1/8    ge1/9    ge1/10  
 ge1/11    ge1/12    ge1/13    ge1/14    ge1/15    ge1/16    ge1/17    ge1/18    ge1/19    ge1/20

VID	Untag Port list								Tag Port list
1	ge1/1 ge1/9	ge1/2 ge1/10	ge1/3	ge1/4	ge1/5	ge1/6	ge1/7	ge1/8	
2	ge1/3	ge1/5							
3	ge1/4	ge1/5							
4	ge1/3	ge1/4	ge1/5						
10	ge1/11 ge1/19	ge1/12 ge1/20	ge1/13	ge1/14	ge1/15	ge1/16	ge1/17	ge1/18	

**Step 5** Access "Main Menu > Layer 2 Config > VLAN Config > PVlan Config".

**Step 6** Port corresponding forwarding entry PVID;

1. Enter 2 in the "PVID" text box in "ge1/3" configuration bar of the port;
2. Enter 3 in the "PVID" text box in the "ge1/4" configuration bar of the port;
3. Enter 4 in the "PVID" text box in "ge1/5" configuration bar of the port;
4. Click "Apply" button, as the picture below.

PVlan-config		
Port	VLANMode	PVID
ge1/1	access ▼	1
ge1/2	access ▼	1
ge1/3	trunk ▼	2
ge1/4	trunk ▼	3
ge1/5	trunk ▼	4
ge1/6	access ▼	1
ge1/7	access ▼	1
ge1/8	access ▼	1
ge1/9	access ▼	1
ge1/10	access ▼	1
ge1/11	trunk ▼	10
ge1/12	trunk ▼	10
ge1/13	trunk ▼	10
ge1/14	trunk ▼	10
ge1/15	trunk ▼	10
ge1/16	trunk ▼	10
ge1/17	trunk ▼	10
ge1/18	trunk ▼	10
ge1/19	trunk ▼	10
ge1/20	trunk ▼	10

**Step 7** End.

### 4.1.3 VLAN Configuration

#### Function Description

On the "Vlan-config" page, user can configure the VLAN ID description.

#### Operation Path

Open in order: "Main Menu > Layer 2 Config > VLAN Config > Vlan-config".

#### Interface Description

Vlan configuration interface as follows:

**Vlan setting**

Vlan ID:  scope: 1-4094

Description:  Max number is 31

Multicast:

Vlan ID	Description	Unkown Multicast
1		Flood-unknown
2		Flood-unknown <input type="button" value="Delete"/>
3		Flood-unknown <input type="button" value="Delete"/>
4		Flood-unknown <input type="button" value="Delete"/>
10		Flood-unknown <input type="button" value="Delete"/>

Total 5 Entry 20 entrys per page 1/1Page

The main element configuration description of Vlan configuration interface:

Interface Element	Description
Vlan ID	VLAN ID number, value range is 1-4094.
Description	Vlan ID description, maximum 31 characters.
Multicast	Multicast process method; <ul style="list-style-type: none"> <li>Flood-all: Flooding all multicast packets;</li> <li>Flood-unknow: Flooding unknown multicast packets;</li> <li>Drop: Drop the multicast packets.</li> </ul>

## 4.2 MAC Configuration

MAC (Media Access Control) address is the hardware identity of network device; the switch forwards the message according to MAC address. MAC address has uniqueness, which has guaranteed the correct retransmission of message. Each switch is maintaining a MAC address table. In the table, MAC address is corresponding to the switch port. When the switch receives data frame, it filters the data frame or forwards it to corresponding port of the switch according to MAC address table. MAC address is the foundation and premise that switch achieves fast forwarding.



## 4.2.1 MAC Configuration

Each port in the switch is equipped with automatic address learning function, it stores the frame source address (source MAC address, switch port number) that port sends and receives in the address table. Ageing time is a parameter influencing the switch learning process; the default value is 300 seconds. When the timekeeping starts after an address record is added to the address table, if each port doesn't receive the frame whose source address is the MAC address within the ageing time, then these addresses will be deleted from dynamic forwarding address table (source MAC address, destination MAC address and their corresponding switch port number).

### Function Description

On the "MAC address setting" page, user can configure the ageing time of dynamic MAC address and check static and dynamic MAC address information.

### Operation Path

Open in order: "Main Menu > Layer 2 Config > MAC Config > MAC Config".

### Interface Description

MAC configuration interface as follows:

SerialNum	MAC	Vid	Interface	Type
1	00e0-6332-172b	1	ge1/3	dynamic

The main element configuration description of MAC configuration interface:

Interface Element	Description
MAC address aging-time	MAC address aging-time, unit is second, default value is 300, and range is 10-1000000.
SerialNum	MAC table size serial number.
MAC	Access the device MAC address.
Vid	VLAN ID number the data MAC address sending belongs to.

Interface Element	Description
Interface	Corresponding port number of the MAC address.
Type	MAC address type, dynamic MAC and static MAC address, display as follows: <ul style="list-style-type: none"> <li>• Dynamic;</li> <li>• Static.</li> </ul>

## 4.2.2 Static MAC

### Function Description

On the "Static Mac" page, user can manually configure the static MAC address and bind the source MAC address without aging.

### Operation Path

Open in order: "Main Menu > Layer 2 Config > MAC Config > Static Mac".

### Interface Description

Static MAC interface as follows:

MAC bind

MAC:  eg:0001-0001-0001

Vlan Id:  eg:1-4094

Port:  eg:ge1/1

SerialNum	MAC	Vlan Id	Port
Total 0 Entry 20 entrys per page			

1/1Page

The main element configuration description of static MAC interface:

Interface Element	Description
MAC	Fill in the MAC address that needs to bind the interface, such as 0001-0001-0001.
Vlan Id	VLAN ID number the data MAC address sending belongs to, such as 1-4094. Notes:

Interface Element	Description
	Input Vlan ID is the existing ID.
Port	Select the binding port number via the drop-down arrow.



Note

- The function is a sort of security mechanism, please carefully confirm the setting, otherwise, part of the devices won't be able to communicate;
- Please don't adopt multicast address as the entering address;
- Please don't enter reserved MAC address, such as the local MAC address.

## 4.3 MAC Address Limit Configuration

### Function Description

On the "MAC Address Limit Configuration" page, user can limit the mac address learning number of each port.

### Operation Path

Open in order: "Main Menu > Layer 2 Config > MAC Config > MAC Limit Config".

### Interface Description

MAC address limit configuration interface as follows:

MAC limit config			
PortName	MAC address learning limit	PortName	MAC address learning limit
ge1/1	0	ge1/2	0
ge1/3	0	ge1/4	0
ge1/5	0	ge1/6	0
ge1/7	0	ge1/8	0
ge1/9	0	ge1/10	0
ge1/11	0	ge1/12	0
ge1/13	0	ge1/14	0
ge1/15	0	ge1/16	0
ge1/17	0	ge1/18	0
ge1/19	0	ge1/20	0

The main element configuration description of MAC address limit configuration interface:

Interface Element	Description
Port Name	The Ethernet port name of the switch
Mac address learning limit	The limiting port mac address learning number

## 4.4 Spanning-tree Configuration

Spanning-tree protocol is a sort of layer 2 management protocol; it can eliminate the network layer 2 circuit via selectively obstructing the network redundant links. At the same time, it has link backup function. Here are three kinds of spanning-tree protocols:

- STP (Spanning Tree Protocol);
- RSTP (Rapid Spanning Tree Protocol);
- MSTP (Multiple Spanning Tree Protocol).

Spanning-tree protocol has two main functions:

- First function is utilizing spanning-tree algorithm to establish a spanning-tree that takes a port of a switch as the root to avoid ring circuit in Ethernet.
- Second function is achieving the convergence protection purpose via spanning-tree protocol when Ethernet topology changes.

Compared to STP, RSTP, MSTP can converge the network more quickly when network structure changes; MSTP is compatible with STP and RSTP, and is better than STP and RSTP. It can not only quickly converge but also send different VLAN along each path to provide better load sharing system for redundant link.

### 4.4.1 Bridge Settings

#### Function Description

On the "Bridge Settings" page, user can configure relative parameters of spanning-tree.

#### Operation Path

Open in order: "Main Menu > Layer 2 Config > Spanning-tree > Bridge Settings".

## Interface Description

Bridge settings interface as follows:

MSTP setting

EnableSpanning-tree:

Mode: stp rstp mstp

Priority:  scope:0-61440

Max age:  scope:6-40

Hello time:  scope:1-10

Forward delay:  scope:4-30

Max hop:  scope:1-40

Revision:  scope:0-65535

Name:  no more than 31 characters

The main element configuration description of bridge settings interface:

Interface Element	Description
Enable Spanning-tree	Enable Spanning-tree.
Mode	Three modes for spanning-tree protocol choice: <ul style="list-style-type: none"> <li>• STP: Spanning-tree;</li> <li>• RSTP: Rapid spanning tree;</li> <li>• MSTP: Multiple spanning-trees.</li> </ul>
Priority	Bridge priority level, value range is 0-61440. Notes: Smaller the priority level value is, higher the priority level is.
Max age	The maximum lifetime of the message in the device, range is 6-40. It's used to determine whether the configuration message times out.
Hello time	Message sending cycle, value range is 1-10. Notes: The spanning tree protocol sends configuration information every Hello time to check whether the link is faulty.
Forward delay	Port state transition delay, value range is 4-30.

Interface Element	Description
Max hop	The maximum hop in MST region, value range is 1-40. Notes: The maximum hop in MST region has limited the size of MST region. The maximum hop configured on a domain root will be used as the maximum hop in MST region.
Revision	MSTP revision level, value range is 0-65535. Notes: When the MST region name, revision level, instance-to-VLAN mapping relation are the same, the two or more bridges will belong to a same MST region.
Name	MST domain name, up to 31 characters.

## 4.4.2 Instance Configuration

### Function Description

On the "Instance Configuration" page, user can configure instance-to-VLAN mapping. Multiple Spanning Tree Regions (MST Regions) are composed of multiple devices in the switched network and the network segments between them.

In a MST region, multiple spanning trees can be generated through MSTP. Each spanning tree is independent to others and corresponding to special VLAN. Each spanning tree is called an MSTI (Multiple Spanning Tree Instance).

VLAN mapping table is an attribute of MST region, and it's used to describe the mapping relation between VLAN and MSTI.

### Operation Path

Open in order: "Main Menu > Layer 2 Config > Spanning-tree > Instance Config".

### Interface Description

Instance configuration interface as follows:

MSTI setting

MSTI ID:

Priority:  Priority range is 0-61440, default is 32768, step is 4096

Vlan Mapped:  separated by ',' is scope,such as 2,4-7,9,10-15

Instance	Priority	Vlan Mapped
<input type="button" value="Refresh"/>		

The main element configuration description of instance configuration interface:

Interface Element	Description
MSTI ID	Multiple Spanning-tree instance ID number.
Priority	Device priority level, value range is 0-61440, default to 32769, step is 4096. Notes: The priority of a device participates in spanning tree calculation. Its size determines whether the device can be selected as the root bridge of a spanning tree.
Vlan Mapped	VLAN mapping table is separated by commas, such as: 4, 5, 6, 7; "-" represents range, such as: 4-7. Notes: VLAN mapping table is an attribute of MST region, and it's used to describe the mapping relation between VLAN and MSTI. MSTP achieves load balancing based on the VLAN mapping table.

## 4.4.3 Bridge Ports

### Function Description

On the "Bridge Port" page, user can enable port to participate in spanning-tree and configure port type, link type and BPDU protection function.

### Operation Path

Open in order: "Main Menu > Layer 2 Config > Spanning-tree > Bridge Ports".

### Interface Description

Bridge ports interface as follows:

Port Config				
Port	Enable	BPDU Guard	Edge	Point-to-Point
ge1/1	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	Auto ▼
ge1/2	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	Auto ▼
ge1/3	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	Auto ▼
ge1/4	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	Auto ▼
ge1/5	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	Auto ▼
ge1/6	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	Auto ▼
ge1/7	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	Auto ▼
ge1/8	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	Auto ▼
ge1/9	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	Auto ▼
ge1/10	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	Auto ▼
ge1/11	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	Auto ▼
ge1/12	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	Auto ▼
ge1/13	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	Auto ▼
ge1/14	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	Auto ▼
ge1/15	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	Auto ▼
ge1/16	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	Auto ▼
ge1/17	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	Auto ▼
ge1/18	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	Auto ▼
ge1/19	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	Auto ▼
ge1/20	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▼	Auto ▼

The main element configuration description of bridge ports interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Enable	Enable checkbox to participate in spanning-tree.
BPDU Guard	BPDU (Bridge Protocol Data Unit) protection function.
Edge	Configure port type: <ul style="list-style-type: none"> <li>• Auto: Automatic system detection;</li> <li>• Force True: Edge port;</li> <li>• Force False: No edge port.</li> </ul>
Point-to-Point	Port link type: <ul style="list-style-type: none"> <li>• Auto: Automatic system detection;</li> <li>• Force True: Point-to-point link;</li> <li>• Force False: Non point-to-point link.</li> </ul>

## 4.4.4 Instance Port Configuration

### Function Description

On the "Inst Port Config" page, user can configure port priority level and cost.



## Operation Path

Open in order: "Main Menu > Layer 2 Config > Spanning-tree > Inst Port Config".

## Interface Description

Instance port configuration interface as follows:

Inst Port Config							
MSTID: <input type="text" value="0"/> <input type="button" value="Refresh"/>							
Port	Enable	Instance	Priority	AdminCost	Cost	Role	Status
ge1/1	Yes	0	128	20000	20000	Disa	forw
ge1/2	Yes	0	128	20000	20000	Disa	forw
ge1/3	Yes	0	128	20000	20000	Disa	forw
ge1/4	Yes	0	128	20000	20000	Disa	forw
ge1/5	Yes	0	128	20000	20000	Disa	forw
ge1/6	Yes	0	128	20000	20000	Disa	forw
ge1/7	Yes	0	128	20000	20000	Disa	forw
ge1/8	Yes	0	128	20000	20000	Disa	forw
ge1/9	Yes	0	128	20000	20000	Disa	forw
ge1/10	Yes	0	128	20000	20000	Disa	forw
ge1/11	Yes	0	128	20000	20000	Disa	forw
ge1/12	Yes	0	128	20000	20000	Disa	forw
ge1/13	Yes	0	128	20000	20000	Disa	forw
ge1/14	Yes	0	128	20000	20000	Disa	forw
ge1/15	Yes	0	128	20000	20000	Disa	forw
ge1/16	Yes	0	128	20000	20000	Disa	forw
ge1/17	Yes	0	128	20000	20000	Disa	forw
ge1/18	Yes	0	128	20000	20000	Disa	forw
ge1/19	Yes	0	128	20000	20000	Disa	forw
ge1/20	Yes	0	128	20000	20000	Disa	forw

The main element configuration description of instance port configuration interface:

Interface Element	Description
MSTID	Choose multiple Spanning-tree ID number.
Port	The corresponding port name of the device Ethernet port.
Enable	Port enable status: <ul style="list-style-type: none"> <li>Yes: Enable, participate in spanning-tree;</li> <li>No: Disable, not participate in spanning-tree.</li> </ul>
Instance	Instance ID number port belongs to.
Priority	Port priority level. Notes: Port priority level in bridge, port priority level is higher when the value is smaller. Port with higher priority level is more possible to become root port.

Interface Element	Description
Admin Cost	Path cost from bridge to root bridge.
Cost	Cost from current port to root bridge.
Role	Port role. <ul style="list-style-type: none"> <li>• unkn: Unknown;</li> <li>• root: Root port;</li> <li>• desg: Designated port;</li> <li>• altn: Alternate port;</li> <li>• back: Backup port;</li> <li>• disa: Disable port.</li> </ul>
Status	Port status in spanning-tree: <ul style="list-style-type: none"> <li>• Disable: Port close status;</li> <li>• Blocking: Blocked state;</li> <li>• Listening: Monitoring state.</li> <li>• Learning: Learning state;</li> <li>• Forwarding: Forwarding state;</li> </ul>

## 4.5 IGMP-snooping

IP host applies for joining (or leaving) multicast group to nearby routers through the Internet Group Management Protocol (IGMP). IGMP Snooping is a multicast suppression mechanism that manages and controls multicast group by listening and analyzing IGMP messages exchanged between host and multicast devices.

The working process of IGMP Snooping is: The switch intercepts the messages exchanged between the host and router, and traps the multicast information and requested port. When the switch intercepts the IGMP Report (request) sent by the host toward router, the switch adds the port to multicast forwarding table. When the switch intercepts the IGMP Leave message sent by the host, the router sends a Group-Specific Query message of the port. If other hosts need the multicast, they will respond with the IGMP Report message. If the router can't receive any response from the host, the switch deletes the port from the multicast forwarding table. The router sends IGMP Query messages periodically. After receiving the IGMP Query messages,

the switch deletes the port from the multicast table if the device does not receive IGMP Report messages from the host within a certain period of time.

## 4.5.1 IGMP-snooping

### Function Description

On the "IGMP-snooping Configuration" page, users can enable/disable IGMP and configure the host aging time.

### Operation Path

Open in order: "Main Menu > Layer 2 Config > IGMP-snooping > IGMP-snooping".

### Interface Description

IGMP-snooping configuration interface as follows:

The main element configuration description of IGMP-snooping port configuration interface:

Interface Element	Description
Enable IGMP-snooping	Enable IGMP-snooping configuration checkbox.
Host age-time	Host aging time, value range is 200-1000s.
SerialNum	IGMP-Snooping list serial number.
Vlan Id	Port number VLAN ID number.
Multicast source	Multicast source IP address.
Multicast address	Multicast IP address.
Port list	The corresponding port name of the device Ethernet port.

## 4.5.2 Static Multicast

### Function Description

On the "Static multicast" page, user can add or delete static multicast.

Main function of static multicast: Add certain ports to a multicast group; these ports can receive data when data is sent to this multicast address.

### Operation Path

Open in order: "Main Menu > Layer 2 Config > IGMP-snooping > Static multicast".

### Interface Description

Static multicast interface as follows:

The main element configuration description of static multicast interface:

Interface Element	Description
VLAN Id	VLAN ID number, value range is 1-4094.
multicast addr	Multicast IP address information, such as: 225.1.2.3.
Port list	Check the box and select the device port to form a multicast group.

## 4.6 SW-Ring Configuration

SW-Ring provides automatic recovery and reconnection mechanism for the disconnected Ethernet network, which has link redundancy and self-recovery ability in case of network interruption or network failure.

The core of SW-Ring technology is without master station setting. In a multi-ring network of up to 250 switches, the network self-recovery time is less than 20 milliseconds. Each port in this series of switches can be used as a ring port and connected with other switches. When an interruption occurs in the network connection, the relay for fault alarm will be activated and the SW-Ring redundant mechanism enables the backup link to quickly recover the network communication.

## 4.6.1 Global Configuration

### Function Description

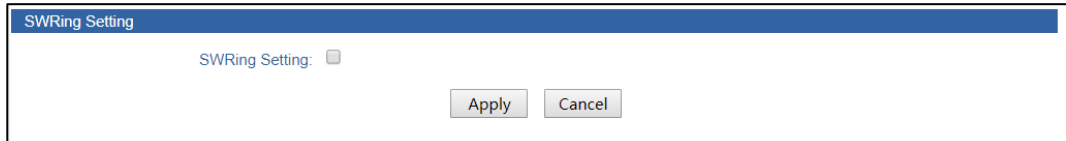
On the "Local Configuration" page, user can enable/disable the ring network.

### Operation Path

Open in order: "Main Menu > Layer 2 Config > SWRing Config > Global Config".

### Interface Description

Global configuration interface as follows:



The main element configuration description of global configuration interface:

Interface Element	Description
SWRing Setting	SWRing setting checkbox, enable SWRing network function after checking.

## 4.6.2 Node Configuration

### Function Description

On the "Node Configuration" page, user can enable/disable the ring network.

### Operation Path

Open in order: "Main Menu > Layer 2 Config > SWRing Config > Node Config".

## Interface Description

Node configuration interface as follows:

SWRing Setting

Ring Group:

Network ID:  The network identity range [0--255]

Ring Type:

Ring Port 1:

Ring Port 2:

HelloTime:  ×100ms(0~300)

Master/Slave:

Ring Group	Network ID	Ring Port 1	Ring Port1 Status	Ring Port 2	Ring Port2 Status	Ring Type	HelloTime	Master/Slave
<input type="button" value="Refresh"/>								

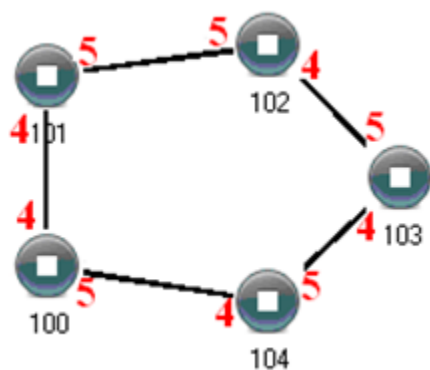
The main element configuration description of node configuration interface:

Interface Element	Description
Ring Group	Support ring group 1-4, it can create 4 ring networks at the same time.
Network ID	When multiple switch devices constitute a ring network, the current ring identification of the ring is network identification; the network identifications of different ring network are different.
Ring Type	<p>According to the scene environment requirement, choose different ring type.</p> <ul style="list-style-type: none"> <li>Single: Single ring, it adopts a continuous ring to connect each device together.</li> <li>Couple: Coupling ring is a redundant structure proposed to connect two independent networks.</li> <li>Chain: The chain, it enhances the flexibility that user builds any type of redundant network topology structure via a kind of advanced software technology.</li> <li>Dual-homing: Two adjacent rings share a switch; users can carry the same switch on two different networks or two different switching devices on the same network.</li> </ul>

Interface Element	Description
Ring port 1	The network port 1 on the switch device used to form the ring network. Notes: When the ring network type is “Couple”, it displays “coupling port”. Coupling port is the port that connects different network identities.
Ring port 2	Network port 2 on the switch device that is used to form the ring network. Notes: When the ring network type is “Couple”, it displays “console port”. Console port is the port in the chain where two rings intersect.
Hello Time	Hello_time is the sending time interval of Hello packet; via the ring port, CPU sends information packet to adjacent device for confirming the connection is normal or not.

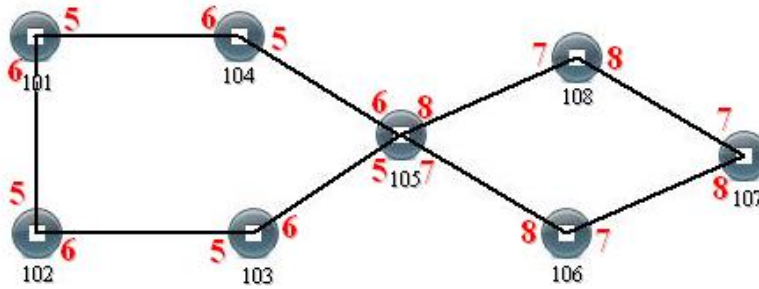
### Single Ring Configuration

Enable Single, enable ring group 1 (other ring group is OK), Set the device port 4 and port 5 to ring port, and set other switches to the same configuration as the switch above, Enable these devices, and adopt network cable to connect port 4 and port 5 of the switch, then search it via network management software, the ring topology structure picture as below:



### Double Ring Configuration

Double ring as shown below, in the figure, double ring is the tangency between two rings, and the point of tangency is NO. 105 switch.

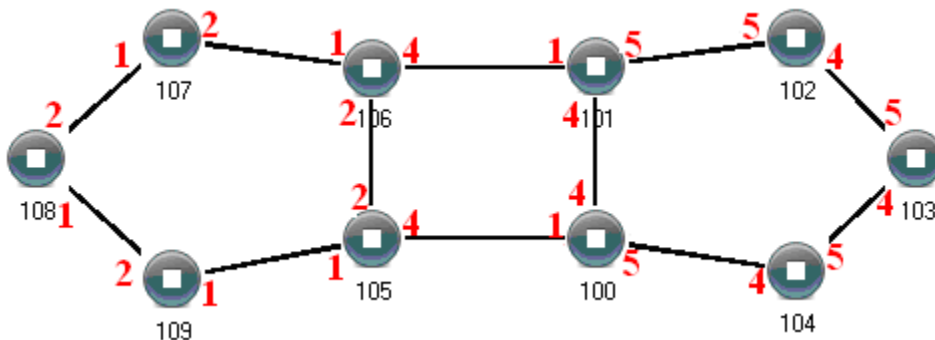


**Configuration Method:**

- Step 1** Adopt single ring configuration method to configure port 5 and port 6 of NO. 101, 102, 103, 104, 105 switches as the ring port, and the ring group is 1;
- Step 2** Adopt single ring configuration method to configure port 7 and port 8 of NO. 105, 106, 107 and 108 switches as the ring ports and the ring group 2;
- Step 3** Adopt network cable to connect the ring group 1;
- Step 4** Adopt network cable 2 to connect the ring group 2;
- Step 5** Search the topology structure picture via network management software;  
Since NO. 105 devices belong to two ring groups, the network IDs of the two ring groups cannot be the same.

**Coupling Ring Configuration**

Coupling ring basic framework as the picture below:



**Operation method:**

- Step 1** Enable ring group 1 and ring group 2; (Hello\_time is disable, but setting time can't cause too fast sending of Hello packet, otherwise, it will seriously influence CPU dealing speed);
- Step 2** Set the ring port of NO. 105, 106 device ring group to port 1 and port 2, network identification to 1, ring type to Single; Set the coupling port of ring group 2 to port 4,



console port to 2, ring identification to 3, ring type to Coupling.

**Step 3** Set the ring port of NO. 100, 101 device ring group 1 to port 4 and port 5, network identification to 2, ring type to Single; Set the coupling port of ring group 2 to port 1, console port to port 4, ring identification to 3, ring type to Coupling.

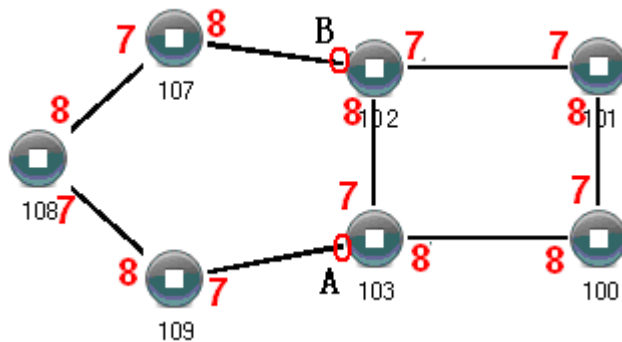
**Step 4** Set the ring port of NO. 107, 108 and 109 device ring group 1 to port 1 and port 2, network identification to 1, ring type to Single; Set the ring port of NO. 102, 103 and 104 device ring group 1 to port 4 and port 5, network identification to 2, ring type to Single.

**Step 5** Connect the port 4 and port 5 of five devices NO. 100-104 to the single ring in turn, adopt network cable to connect the port 1 and port 2 of four devices NO. 105-109 to the single ring in turn, Then adopt Ethernet cable to connect port 4 of NO. 106 device to port 1 of NO. 101 device, port 4 of NO. 105 device to port 1 of NO. 100 device, coupling ring combination is completed.

Console ports are two ports connected to NO. 105 device and NO. 106 device in the above picture. The two ports connected to NO. 100 device and NO. 101 device are also called console ports.

### Chain Configuration

Chain basic framework as the picture below:



#### Operation method:

**Step 1** Enable the ring group 1; (Hello\_time can be disable, but setting time can't cause too fast sending of Hello packet, otherwise it will seriously influence CPU dealing speed);

**Step 2** Set the ring port of NO. 100, 101, 102 and 103 device ring group 1 to port 7 and port 8, network identification to 1, ring type to Single. Set the ring port of NO. 107, 108 and 109 devices ring group 1 to port 7 and port 8, network identification to 2, ring type to

Chain.

**Step 3** Adopt network cable to connect the port 7 and port 8 of three devices NO. 107-109, adopt network cable to connect the port 7 and port 8 of four devices NO. 100-103 to the single ring in turn, Then adopt network cable to connect port 7 of NO. 107 device and port 7 of NO. 109 device to normal ports of NO. 102 and 103 device, chain combination is complete.



Note

- Port that has been set to port aggregation can't be set to rapid ring port, and one port can't belong to multiple rings;
  - Network identification in the same single ring must be consistent, otherwise it cannot form a normal ring or normal communicate;
  - Network identification in different ring must be different;
  - When forming double ring and other complex ring, user should notice whether the network identification in the same single ring is consistent, and network identification in different single ring is different.
- 

## 4.7 GMRP Configuration

GMRP multicast registration protocol is an application of the universal attribute registration protocol, it mainly provides a limited multicast diffusion function similar to IGMP probing technology. GMRP allows bridge and end station to dynamically register group membership information to MAC bridges connected to the same LAN segment, and this information can be propagated to all bridge systems in a bridging LAN supporting extended filtering server. GMRP software runs on the host and switch.

When a host wants to join an IP multicast group, it needs to send an IGMP join information, The information evolves as a GMRP join information, once receiving GRMP join information, switch will add the port receiving the information to proper multicast group, Switch sends GMRP join information to other hosts in VLAN, among which one host as the multicast source, When the multicast source sends multicast information, switch will send the multicast information via the port that joins in the

multicast group before. In addition, switch will periodically send GMRP query, if the host stays in the multicast group, it will response to GMRP query, In this case, the switch does nothing, and if the host does not want to stay in the multicast group, it can either send a leave message or not respond to periodic GMRP query. Once the host receives the leave message or does not receive a response message during the timer setting period, it deletes the host from multicast group.

Enable the function is OK while adopting this function, If the switch receives the host IGMP join information, then switch will build a multicast group according to IGMP join information, and add the port that receives IGMP join information to the multicast group, At this time, if the data destination address is the multicast address, then the data can only be forwarded from the multicast group member.

## 4.7.1 GMRP Global Configuration

### Function Description

On the "GMRP Global Set" page, user can enable/disable the GMRP.

### Operation Path

Open in order: "Main Menu > Layer 2 Config > GMRP Config > GMRP Global Config".

### Interface Description

GMRP global configuration interface as follows:

The main element configuration description of GMRP global configuration interface:

Interface Element	Description
GMRP enable	Enable GMRP multicast registration protocol.

## 4.7.2 GMRP Port Config

### Function Description

On the "GMRP Port Config" page, user can configure relative parameters of GMRP port.

### Operation Path

Open in order: "Main Menu > Layer 2 Config > GMRP Config > GMRP Port Config".

### Interface Description

GMRP port config interface as follows:

GMRP Port Config						
PortName	Enable	JoinTime	LeaveTime	LeaveAllTime	Registration	
ge1/1	<input type="checkbox"/>	20	60	1000	Normal ▼	
ge1/2	<input type="checkbox"/>	20	60	1000	Normal ▼	
ge1/3	<input type="checkbox"/>	20	60	1000	Normal ▼	
ge1/4	<input type="checkbox"/>	20	60	1000	Normal ▼	
ge1/5	<input type="checkbox"/>	20	60	1000	Normal ▼	
ge1/6	<input type="checkbox"/>	20	60	1000	Normal ▼	
ge1/7	<input type="checkbox"/>	20	60	1000	Normal ▼	
ge1/8	<input type="checkbox"/>	20	60	1000	Normal ▼	
ge1/9	<input type="checkbox"/>	20	60	1000	Normal ▼	
ge1/10	<input type="checkbox"/>	20	60	1000	Normal ▼	
ge1/11	<input type="checkbox"/>	20	60	1000	Normal ▼	
ge1/12	<input type="checkbox"/>	20	60	1000	Normal ▼	
ge1/13	<input type="checkbox"/>	20	60	1000	Normal ▼	
ge1/14	<input type="checkbox"/>	20	60	1000	Normal ▼	
ge1/15	<input type="checkbox"/>	20	60	1000	Normal ▼	
ge1/16	<input type="checkbox"/>	20	60	1000	Normal ▼	
ge1/17	<input type="checkbox"/>	20	60	1000	Normal ▼	
ge1/18	<input type="checkbox"/>	20	60	1000	Normal ▼	
ge1/19	<input type="checkbox"/>	20	60	1000	Normal ▼	
ge1/20	<input type="checkbox"/>	20	60	1000	Normal ▼	

The main element configuration description of GMRP port config interface:

Interface Element	Description
Port Name	The corresponding port name of the device Ethernet port.
Enable	Port enables checkbox.
Join Time	Join timer time, it will send Join message outward after timeout.
Leave Time	Leave timer time, when the entity that receives the leave message does not receive the Join message after timeout;

Interface Element	Description
	the attribute information should be canceled.
Leave All Time	The default value of Leave All Time timer is 1000 centiseconds, which is 10 seconds, Each GMRP application entity periodically sends a Leave All Time Message after the Leave All Time timer timeout, all VLAN information in the entity should be canceled.
Registration	Registration state, options as follows: <ul style="list-style-type: none"> <li>• Normal;</li> <li>• Fixed;</li> <li>• Forbidden.</li> </ul>

## 4.7.3 GMRP Group

### Function Description

On the "GMRP group" page, user can check GMRP group information.

### Operation Path

Open in order: "Main Menu > Layer 2 Config > GMRP Config > GMRP group".

### Interface Description

Check GMRP group interface as below:

GMRP group				
SerialNum	MAC	Vlan Id	Port	Type
Total 0 Entry 20 entrys per page				
				1/1Page << < > >> Go >>>

The main element configuration description of GMRP group interface:

Interface Element	Description
SerialNum	GMRP group serial number.
MAC	Multicast source MAC address.
Vlan Id	Vlan ID number.
Port	The corresponding port name of the device Ethernet port.
Type	Multicast address type.

# 5 Layer 3 Configuration

## 5.1 Interface Configuration

Interface configuration mainly refers to setting the device interface IPV4 address. The interface configuration only supports manual configuration, doesn't support automatic acquisition (DHCP). User chooses the interface, and fill in IPV4 address is ok. IPV6 address setting can be achieved via command line.

### IPV4 address:

The IP address is a 32-bit address assigned to the device connected to Internet. IP address is composed of two fields: Network number field (net-id) and host number field (host-id). IP addresses are allotted by the Network Information Center (NIC) of U.S. Defense Data Network. IP addresses are divided into five categories for the convenience of IP address management. As the table below:

Network Type	Address Range	Usable IP Network Range
A	0.0.0.0~126.255.255.255	1.0.0.0~126.0.0.0
B	128.0.0.0~191.255.255.255	128.0.0.0~191.254.0.0
C	192.0.0.0~223.255.255.255	192.0.0.0~223.255.254.0
D	224.0.0.0~239.255.255.255	-
E	240.0.0.0~246.255.255.255	-
Other addresses	255.255.255.255	255.255.255.255

Thereinto, category A, B, C address are unicast address; category D address is multicast address; category E address is reserved address for the future special purpose. Now, most of the using IP addresses belong to category A, B, C address.

IP address adopts dotted decimal notation recording mode. Each IP address is expressed as four decimal integers separated by radix point, each integer is corresponding to a byte, such as 10.110.50.101.

### **IPv6 address:**

IPv6 (Internet Protocol Version 6) is the second standard protocol of network layer protocol, also called IPng (IP Next Generation); it's a set of standards designed by IETF (Internet Engineering Task Force) and is the upgrade version of IPv4. The most significant difference between IPv4 and IPv6: IP address length is increased from 32 bits to 128 bits.

IPv6 address is expressed as a series of 16 bits hexadecimal number separated by colon. Each IPv6 address is divided into eight groups, 16 bits in each group is expressed by four hexadecimal numbers, two groups are separated by colon, such as: 2001:0000:130F:0000:0000:09C0:876A:130B. In order to simplify the expression of IPv6 address, "0" in IPv6 address can be handled in the following way: The leading "0" in each group can be omitted, that is above address can be written as 2001:0:130F:0:0:9C0:876A:130B. If the address contains two or more successive 0 group, it can be replaced by double colon "::", that is, above address can be written as 2001:0:130F::9C0:876A:130B.



Notice

One IPv6 address can only use the double colon "::" once, otherwise, when the device changes "::" to 0 for restoring 128 bits address, 0 number represented by "::" won't be able to confirm.

---

IPv6 address is composed of two parts: address prefix and interface identification. Thereinto, address prefix is the network number field part in IPv4 address, interface identification is the host number part in IPv4 address.

The expression method of address prefix is: IPv6 address/prefix length. Thereinto, IPv6 address is any form listed before, and prefix length is a decimal number, it represents how many bits in the leftmost of IPv6 address is the address prefix.

## Function Description

On the "Interface Config" page, user can configure the interface IP address.

## Operation Path

Open in order: "Main Menu > L3 forward Config > Interface Config".

## Interface Description

Interface configuration interface as follows:

The main element configuration description of interface configuration interface:

Interface Element	Description
<b>Interface Add</b>	<b>Interface addition configuration column.</b>
Interface Name	Layer 3 interface names, such as, vlanif1.
Enable	Interface configuration enabling checkbox.
IPv4 address	IPv4 address and subnet mask, such as 10.1.1.0/24.
Enable	Directional broadcasting enabling checkbox.
<b>Ip address setting</b>	<b>IP address setting column.</b>
Interface Add	Interface pull-down list, added interface is optional; mode pull-down list only supports static mode; blank textbox is used for configuring the interface IPv4 address.



## 5.2 ARP Configuration

ARP (Address Resolution Protocol) is the protocol that resolves IP address into Ethernet MAC address (or physical address).

In local area network, when the host or other network device sends data to another host or device, it must know the network layer address (IP address) and MAC address of the opposite side. So it needs a mapping from IP address to the physical address. ARP is the protocol to achieve the function.

### 5.2.1 Show ARP

#### Function Description

On the "show ARP" page, user can check the IP address, MAC, Output port and other parameters.

#### Operation Path

Open in order: "Main Menu > L3 forward Config > ARP Config > show ARP".

#### Interface Description

Check ARP interface as below:

ARP				
IP address	MAC	Output port	Mode	ARP age-time
192.168.1.61	00e0-6332-172b	vlanif1	Dyn	14145
Total 1 Entry 20 entries per page				
			1/1Page	Go

The main element configuration description of show ARP interface:

Interface Element	Description
IP address	IP address of accessing device.
MAC	MAC address of accessing device.
Output port	Output port of accessing device data transmission.
Mode	ARP mode of accessing device.
ARP age-time	ARP age-time of accessing device.

## 5.2.2 Static ARP

### Function Description

On the "Static ARP" page, user can conduct static ARP configuration.

### Operation Path

Open in order: "Main Menu > L3 forward Config > ARP Config > Static ARP".

### Interface Description

Static ARP interface as follows:

The screenshot shows a web interface for adding static ARP entries. At the top, there's a title bar 'Add static ARP'. Below it, there are two input fields: 'IP address:' with a text box and 'eg:192.168.1.1' next to it, and 'MAC:' with a text box and 'eg:0001-0001-0001' next to it. An 'Add' button is positioned below the MAC field. Below the form is a table with three columns: 'SerialNum', 'IP address', and 'MAC'. The table is currently empty, showing 'Total 0 Entry' and '20 entrys per page'. At the bottom right of the table area, there are pagination controls: '1/1Page', a left arrow, a search box, a 'Go' button, a right arrow, and a double right arrow.

The main element configuration description of static ARP interface:

Interface Element	Description
IP address	IP address of accessing device, such as 192.168.1.1.
MAC	MAC address of accessing device, such as 0001-0001-0001.

## 5.2.3 ARP Ageing Time

### Function Description

On the "ARP age-time" page, user can conduct ARP age-time configuration.

### Operation Path

Open in order: "Main Menu > L3 forward Config > ARP Config > ARP age-time".

### Interface Description

ARP age-time interface as follows:

ARP age-time	
Interface	timeout( Seconds)
vlanif1	14400

The main element configuration description of ARP age-time interface:

Interface Element	Description
Interface	Interface Name.
timeout	Ageing time setting, valid input range is 120-2147483 (second).

## 5.3 VRRP

VRRP (Virtual Router Redundancy Protocol) is a fault-tolerant protocol. In general, all hosts in a network will set a default route, when the destination address of the message sent by host isn't in the network segment; the message will be sent to the Router A via default router, achieving the communication between the host and external network. When the Router A breaks down, all hosts that takes Router A as default router in the network segment will disconnect communication to the outside, generating single point of failure. VRRP is proposed to solve the problem above, and it's designed for the local area network (such as: Ethernet) with multicast or broadcast capability.

VRRP organizes a set of routers (including a Master, that is the active router and several Backup, that is the standby router) in the local area network into a virtual router, which is called a backup team. The virtual router possesses its own IP address 10.100.10.1 (The IP address can be same to a router interface address in the backup team, it's called IP owner), routers in the backup team have their own IP address (such as IP address of Master is 10.100.10.2, IP address of Backup is 10.100.10.3). Hosts in the local area network only knows the virtual router IP address is 10.100.10.1, it doesn't know that the specific Master router IP address is 10.100.10.2 and Backup router IP address is 10.100.10.3. Hosts set their own default router next hop address to the virtual router IP address 10.100.10.1. Thereupon, hosts in the network start to communicate with other networks via the virtual router. If the Master router in backup

team breaks down, Backup router will elect a new Master router via election strategy and provide router service for hosts in the network. Therefore, hosts in the network can uninterruptedly communicate with outside network.

### **Principle of realization**

A VRRP router has the only identification: VRID, range is 0-255. The router has only one virtual MAC address, and the address format is 00-00-5E-00-01-[VRID]. Master router is responsible for replying the ARP request by MAC address. Regardless of the switching, it's ensured to give the only consistent IP and MAC address to the terminal device, declining the switching influence to terminal device.

VRRP control message includes only one type: VRRP announce (advertisement). It's packaged by IP multicast data packet, the multicast address is 224.0.0.18, issue range can be only in the same local area network. It has ensured that VRID can be repeatedly used in different network. In order to decrease the network bandwidth consumption, only the master router can periodically send VRRP announce message. Backup router will start new VRRP election if it can't receive VRRP in three consecutive announce intervals or receives announce with 0 priority.

In the VRRP router group, master router is elected according to the priority, and the priority range in VRRP protocol is 0-255. If VRRP router IP address is the same to virtual router interface IP address, then the virtual router is called IP address owner in VRRP group; IP address owner automatically has the highest priority: 255. Priority 0 is usually used when IP address owner forwardly gives up the master role. Configurable priority range is 1-254. Priority configuration principle is set according to the link speed and cost, router performance and reliability, and other management strategies. In the election of master router, virtual router with high priority wins; therefore, if there exists IP address owner in VRRP group, it will appear as the master router. Candidate router with the same priority can be elected according to IP address size order. VRRP has also provided priority preemption strategy, if the strategy is configured, backup router with high priority will deprive current master router with low priority and become the new master router.

In order to ensure the safety of VRRP protocol, two safety certification measures are provided: Plaintext authentication and IP header authentication. Plaintext authentication method requirements: User must provide the VRID and plaintext password while joining a VRRP router. It suits for avoiding the configuration error in the local area network but can't prevent gaining the password via network monitoring method. IP header authentication method has provided higher security, and it can prevent message replay and modification attack.

### Function Description

On the "VRRP Config" page, user can configure VRRP parameters.

### Operation Path

Open in order: "Main Menu > L3 forward Config > VRRP Config".

### Interface Description

VRRP interface as below:

VRRP

Interface:  Interface choice

VRID:  Range: 1-255

Virtual IP:  Virtual IP

Broadcast Interval time:  scope:1-10 Seconds

Priority:  scope:1-254, Default:100

Preempt:  enable  disable

Dealy of preempt:  scope:0-1000 Seconds

Interface	Virtual RouterID	Virtual IP	Status	Broadcast Interval time	Priority	Effective priority	Preempt	Dealy of preempt
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

The main element configuration description of VRRP interfaces:

Interface Element	Description
Interface	Interface pull-down list.
VRID	Virtual router ID, valid range is 1-255.
Virtual IP	Virtual router IP address, such as 192.168.1.1.
Broadcast interval time	Annunciate time interval, valid range is 1-10 seconds.
Priority	Priority defaults to 100, valid range is 1-254.
Preempt	Preemption mode check box, options as follows: <ul style="list-style-type: none"> <li>• enable;</li> </ul>

Interface Element	Description
	<ul style="list-style-type: none"> <li>disable.</li> </ul>
Delay of preempt	Preemption delay time, valid range is 1-1000 seconds.

## 5.4 ND Configuration

IPv6 Neighbor Discovery Protocol (IPv6 ND, ND for short) is a basic IPv6 protocol. It adopts NA, NS, RA, RS and redirection ICMPv6 messages to confirm neighbor node relationship and address information, achieving address resolution, reachable neighbor authentication, duplicated address detection, router discovery/prefix discovery, address auto configuration and redirection functions.

Neighbor Discovery Protocol has replaced IPv4 ARP, ICMP Router Discovery and ICMP Redirect Message and provided a series of enhancements to guarantee the device security.

### Function Description

On the "ND Config" page, user can configure static ND parameters.

### Operation Path

Open in order: "Main Menu > L3 forward Config > ND Config".

### Interface Description

ND configuration interface as follows:

The main element configuration description of ND configuration interface:

Interface Element	Description
IP	IPv6 address of accessing device, such as 2000::1.
MAC	MAC address of accessing device, such as

Interface Element	Description
	0001-0001-0001.
Output port	Interface pull-down list.

# 6 Router Configuration

## 6.1 Show Router

### Function Description

On the "Show route" page, user can check various router configuration methods.

### Operation Path

Open in order: "Main Menu > Route Config > Show route".

### Interface Description

Show route interface as below:

Show route						
Codes: K - kernel route, C - connected, S - static, R - RIP, O - OSPF, I - IS-IS, B - BGP, A - Babel, > - selected route, * - FIB route						
SerialNum	Destination	Mask	Mark	Gateway	Output port	
1	192.168.1.0	24	C>*		vlanif1	
Total 1 Entry 20 entrys per page				1/1Page <input type="text"/> Go		

The main element configuration description of show route interface:

Interface Element	Description
SerialNum	Serial number.
Destination	Destination IP addresses.
Mask	Subnet mask.
Mark	Mark, corresponding full name relationship as below: K - kernel route; C - connected; S – static; R – RIP; O – OSPF; I - IS-IS; B – BGP; A – Babel; > - selected route; * - FIB



Interface Element	Description
	route.
Gateway	Gateway addresses information.
Output port	Interface name.

## 6.2 Static Configuration

Static route refers to the route information that user or network administrator manually configures. When the network topology structure or link status changes, network administrator needs to manually modify relative static route information in the routing table. Static route usually adapts to simple network environment, under this environment, network administrator can clearly know the network topology structure, which is convenient for setting correct route information.

### Function Description

On the "Static Config" page, user can configure static route.

### Operation Path

Open in order: "Main Menu > Route Config > Static Config".

### Interface Description

Static configuration interface as follows:

Add static route

Destination prefix:  /  eg:10.1.1.0/24

Gateway:  eg:20.1.1.3

Distance:  scope:1-255

SerialNum	Destination prefix	Mask	Gateway	Distance
Total 0 Entry 20 entrys per page				

1/1Page

The main element configuration description of static configuration interface:

Interface Element	Description
Destination prefix	Destination network IP address, input subnet masks information in the textbox after "/", such as destination

Interface Element	Description
	address is 10.1.1.0/24.
Gateway	Next hop gateway address, such as 20.1.1.3.
Distance	Management distance, defaults to 1, valid input range is 1-255.

## 6.3 RIP Configuration

RIP (Routing Information Protocol) is a simple Interior Gateway Protocol (IGP) and mainly used in small network, such as Campus Network and Local Area Network with simple structure. RIP isn't used in more complex environment and large network.

RIP is simple to achieve and easier in configuration and maintenance than OSPF or IS-IS, so it's widely used in actual networking.

### 6.3.1 RIP Global Configuration

#### Function Description

On the "RIP Global Config" page, user can conduct RIP global relative parameters configuration.

#### Operation Path

Open in order: "Main Menu > Route Config > RIP Config > RIP Global Config".

#### Interface Description

RIP global configuration interface as follows:

**RIP Global setting**

RIP Enable:

RIP version:

Distribute:  Distribut default route

metric:  1-16,Default:1.

passive:  Restrain route Interface

Update:  Update timer of RouteTable.5-2147483647,Default:30.

Timeout:  RouteInfo timeout.5-2147483647,Default:180.

LOOP:  Collection Timer of reclaim .5-2147483647,Default:120.

Connected Direct line

Redistribute:  Static Static route setting

OSPF (OSPFv2)

The main element configuration description of RIP global configuration interface:

Interface Element	Description
RIP Enable	Enable RIP function check box.
RIP version	Compatible RIP protocol version, options as follows: <ul style="list-style-type: none"> <li>v1: RIP-1 is Classful Routing Protocol, it only supports releasing protocol message via broadcast mode.</li> <li>v2: RIP-2 is Classless Routing Protocol, and it supports broadcast mode and multicast mode.</li> <li>v1&amp;2.</li> </ul>
Distribute	Distribute check box, control default route distribution.
metric	Hop count distance from device to destination address, metric value defaults to 1, valid input range is 1-16.
passive	Passive check box, restrain the route updating interface.
Update	Routing table update time defaults to 30, valid input range is 5-2147483647.
Timeout	Route information timeout time defaults to 180, valid input range is 5-2147483647.
LOOP	Garbage collection time defaults to 120, valid input range is 5-2147483647.
Redistribute	Redistribution route type, options as follows: <ul style="list-style-type: none"> <li>Connected: connection (direct-connected subnet or host);</li> <li>Static: static route configuration;</li> </ul>

Interface Element	Description
	<ul style="list-style-type: none"> <li>OSPF: Open Shortest Path First (OSPFv2).</li> </ul>

## 6.3.2 RIP Network Setting

### Function Description

On the "RIP network setting" page, user can conduct RIP network parameters configuration.

### Operation Path

Open in order: "Main Menu > Route Config > RIP Config > RIP network setting".

### Interface Description

RIP network setting interface as follows:

The main element configuration description of RIP network setting interface:

Interface Element	Description
Network	RIP network check box, network IP address, such as 10.1.1.0/24.
Interface	RIP interface check box, interface name pull-down list.
<b>RIP network/interface</b>	<b>RIP network/interface display list</b>
Interface	Interface name.
Horizon	Horizon check box. Notes: Route that RIP learns from an interface, it won't be sent from the interface to neighbor router. It can not only reduce bandwidth consumption but also prevent routing loops.

Interface Element	Description
Send version	RIP protocol version of sending data, options as follows: <ul style="list-style-type: none"> <li>• auto;</li> <li>• v1;</li> <li>• v2;</li> <li>• v1&amp;2.</li> </ul>
Receive version	RIP protocol version of receiving data, options as follows: <ul style="list-style-type: none"> <li>• auto;</li> <li>• v1;</li> <li>• v2;</li> <li>• v1&amp;2.</li> </ul>
Auth type	Authentication type, options as follows: <ul style="list-style-type: none"> <li>• No auth;</li> <li>• Simple;</li> <li>• MD5.</li> </ul>
Auth character	Authentication character information.

## 6.4 OSPF

OSPF (Open Shortest Path First) is an Interior Gateway Protocol, IGP for short; it's used for route decision in the single autonomous system, AS for short. It's the realization of link status route protocol, and subordinate to Interior Gateway Protocol, so it's operated in the interior autonomous system. It adopts Dijkstra algorithm to calculate the shortest path.

OSPF is the IGP route protocol developed by OSPF working team of IETF. OSPF designed for IP network supports IP subnet and exterior route information mark, and it allows message authentication and IP multicast.

### 6.4.1 OSPF Global Configuration

#### Function Description

On the "OSFP global Config" page, user can conduct OSPF global parameters configuration.

## Operation Path

Open in order: "Main Menu > Route Config > OSPF Config > OSPF global Config".

## Interface Description

OSPF global configuration interface as follows:

The main element configuration description of OSPF global configuration interface:

Interface Element	Description
OSPF Enable	Enable OSPF function check box.
Route ID	Router ID number, similar to IP address format.
Distribute D	Default distribution check box, force ASBR to generate default route and access OSPF routing domain.
metric Default metric	Redistribute router metric value, valid input range is 0-16777214.
passive	Passive check box, restrain the route updating interface.
spf timer	Set the calculated router time delay, initial interval, maximum interval in a domain. Delay: delay time, defaults to 200. Init hold: initial hold time, defaults to 1000. Max hold: Maximum hold time, defaults to 10000.
Redistribute	Route type redistribution, options as follows: <ul style="list-style-type: none"> <li>Connected: connection (direct-connected subnet or host);</li> <li>Static: static route configuration;</li> <li>RIP: route information protocol.</li> </ul>

Interface Element	Description
Metric-Type	Metric type, defaults to 2.
Metric	Metric value of bringing in exterior route, valid input range is 0-16777214.

## 6.4.2 OSPF Network Configuration

### Function Description

On the "OSPF network Config" page, user can conduct OSPF network parameters configuration.

### Operation Path

Open in order: "Main Menu > Route Config > OSPF Config > OSPF network Config".

### Interface Description

OSPF network configuration interface as follows:

Interface	Network	Cost	Hello Interval	Dead Interval	Priority	Auth type	Auth character

The main element configuration description of OSPF network configuration interface:

Interface Element	Description
Network	Router network segment address and subnet mask, such as 10.1.1.0/24.
Area	Area information, valid range is 0-4294967295.
<b>OSPF Network</b>	<b>OSPF network display list</b>
Interface	Interface name.
Network	OSPF network type.
Cost	Interface cost.
Hello Interval	Time interval of sending hello message.

Interface Element	Description
Dead Interval	Waiting response time after sending hello message.
Priority	Port priority.
Auth type	Authentication type, options as follows: <ul style="list-style-type: none"> <li>• No auth;</li> <li>• Simple;</li> <li>• MD5.</li> </ul>
Auth character	Authentication character information.

## 6.4.3 MD5 Setting

### Function Description

On the "MD5 setting" page, user can conduct MD5 authentication parameters setting.

### Operation Path

Open in order: "Main Menu > Route Config > OSPF Config > MD5 setting".

### Interface Description

MD5 setting interface as follows:

MD5 setting

Network:  eg:vlanif1

MD5 id:  eg:(1-255)

Auth character:  eg:abc123

SerialNum	Interface	Auth type	MD5 id	Auth character
Total 0 Entry 20 entrys per page				

1/1Page

The main element configuration description of MD5 setting interface:

Interface Element	Description
Network	Network/interface name.
MD5 id	MD5 serial number, valid input range is 1-255.
Auth character	Authentication character information.



## 6.5 BGP Configuration

Border Gateway Protocol (BGP) is an autonomous system router protocol running on TCP. BGP is the only protocol for dealing with the network like Internet and multi-line connection between irrelevant router domains. BGP is established upon EGP. The main function of BGP system is exchanging network reachable information with other BGP system. Network reachable information includes listed autonomous system (AS) information. The information has validly established AS interlinked topological graph, eliminated the routing loops, and implemented strategies.

Although BGP protocol is designed for router selection between autonomous systems, it can also be used in the interior autonomous system and is a dual routing protocol. Two BGP neighbor nodes that can communicate with each other in the autonomous system must be in the same physical link. BGP routers in the same autonomous system can communicate with each other, which can ensure the consistency of all information in the autonomous system. After exchanging the information, they decide which BGP router in the autonomous system as the connection point to receive the exterior information in autonomous system.

Some autonomous system is only a data transmission channel; this autonomous system is neither the data transmitting end nor the receiving end. BGP protocol must communicate with the router protocol within these autonomous system interior to guarantee the data passing. The route refresh message of BGP protocol is composed of "Network number: autonomous system path", each autonomous system path is a series of name character string of autonomous system; it has recorded the network to the ultimate target. The route refresh message of BGP protocol is transmitted via Transmission Control Protocol TCP. The initial data exchange between two routers is the routing table of whole BGP protocol. With the continuous change of routing table, the refresh message frequency of sending router becomes more and more. Unlike some other routing protocols, BGP protocol doesn't require periodic refresh to the whole routing table; on the contrary, router that runs BGP protocol possesses the newest version routing table. BGP protocol possesses the routing table of all paths to the specific target. The route metric method of BGP protocol can be a number of arbitrary units, it indicates the reference degree of a special path, and these metric

methods are usually configured by network administrator via the configuration documents. Reference degree can be based on any numerical criterion, such as final system counting (the path is better when the counting is smaller), data link type.

**Function Description**

On the "BGP Config" page, user can configure BGP parameters.

**Operation Path**

Open in order: "Main Menu > Route Config > BGP Config".

**Interface Description**

BGP configuration interface as follows:

The main element configuration description of BGP configuration interface:

Interface Element	Description
<b>BGP</b>	<b>BGP configuration column</b>
BGP Enable	Enable BGP function check box.
AS	Autonomous domain serial number, valid input range is 1-4294967295.
KeepAlive Interval	Time interval of sending keep-alive message, defaults to 180, valid input range is 1-65535.
Hold Time	Valid time length of sender information, defaults to 180, valid

Interface Element	Description
	input range is 1-65535.
Redistribute	Route type redistribution, options as follows: <ul style="list-style-type: none"> <li>• Connected: Connection line (direct-connected subnet or host);</li> <li>• Static: static route configuration;</li> <li>• RIP: route information protocol;</li> <li>• OSPF: Open Shortest Path First (OSPFv2).</li> </ul>
<b>Neighbor addr</b>	<b>Neighbor IP address configuration column</b>
Remote IP	Neighbor IP address.
Remote AS	Neighbor AS serial number.

## 6.6 Multicast Route Configuration

### Function Description

On the "Multicast routing Config" page, user can configure the multicast route parameters.

### Operation Path

Open in order: "Main Menu > Route Config > Multicast routing Config".

### Interface Description

Multicast route configuration interface as follows:

Multicast routing Config

RuleID:  eg:1-100

VLAN:  eg:(1-4094)

Multicast IP:  eg:(224.1.2.3)

Source IP:  eg:(192.168.1.1)

Interface Name:  Interface choice

SerialNum	RuleID	VLAN	Multicast IP	Source IP	Interface Name
Total 0 Entry 20 entries per page					
					1/1Page <input type="button" value="Go"/>

The main element configuration description of multicast route configuration interface:

Interface Element	Description
Rule ID	Rule ID number, such as 1-100.

Interface Element	Description
VLAN	VLAN ID, such as 1-4094.
Multicast IP	Multicast IP address, such as 224.1.2.3
Source IP	Multicast source IPv4 address, such as 192.168.1.1
Interface Name	The drop-down list of interface name.

# 7 Network Security

## 7.1 Access Control

### Function Description

On the "Access Control" page, user can configure access rules and filtering rule.

### Operation Path

Open in order: "Main Menu > Network security > Access Control".

### Interface Description

Access control interface as follows:

**Filtering rule**

Configure access policy,default is disabled.If specify **allowed**, all host which not matched rule list will be forbidden. Please add rule list first.

Disable  
 IP listed below, **allowed** access this device.  
 IP listed below, **forbidden** access this device.

---

**Access rules**

IP address:  eg:192.168.0.1/24

Service:

SerialNum	IP address	Service
Total 0 Entry 20 entries per page		

1/1Page

The main element configuration description of access control interface:

Interface Element	Description
Filtering rule	Set filtering rule, default to disable, that is disable access filtering function. Options as follows: <ul style="list-style-type: none"> <li>• Disable;</li> <li>• Hosts that meet the following rules are allowed to access the equipment corresponding service;</li> <li>• Hosts that meet following rules are forbidden to access the equipment corresponding service.</li> </ul>
<b>Access rules</b>	<b>Access rules setting column.</b>
IP address	Enable/disable device to access the switch IP address.
Service	Methods of enabling/disabling device to access the switch. Options as follows: <ul style="list-style-type: none"> <li>• ALL: Support HTTP and TELNET access;</li> <li>• HTTP: Support WEB interface access;</li> <li>• TELNET: Support Telnet client command line access;</li> </ul>



Notice

- Please first add the rules, and then set the access rules, otherwise it may cause the current web can't be accessed.

## 7.2 Attack Protection

### Ping attack

Ping attack refers to constantly sending data packets to appointed IP address and doesn't receive the reply, this kind of attack disaggregates the operating system via sending ICMP packet more than 65536 bytes. It usually won't send ICMP packet more than 65536 bytes, but it can segment the packets to fragments and then recombine the fragments on the destination host. Finally it will cause the buffer area overflow of embattled target.

### SYN DOS attack

In normal case, TCP connection needs three times handshakes, that is:

1. Initiator of TCP connection request sends SYN packet to target server;

2. After receiving SYN packet, target server will establish TCP semi-join in the SYN\_RECEIVED status and reply SYN ACK packet to initiator, then waiting for the reply of initiator;
3. After receiving SYN ACK packet, the initiator will reply ACK packet, and then TCP connection is established.

Through the establishing process of TCP connection, some vicious attacker can conduct SYN Flood attack. Attacker sends lots of SYN packets of requesting to establish TCP connection to the server, but doesn't reply SYN ACK packet of the server, causing lots of TCP semi-join in the server. Thus, the server source is consumed, which causes the server can't deal with normal business.

SYN Cookie function is used for preventing SYN Flood attack. When the server receives TCP connection request, it won't establish TCP semi-join, but directly reply SYN ACK packet to the initiator. After receiving the ACK packet replied by the initiator, the server starts to establish connection and enter into ESTABLISHED status. Through this kind of method, lots of TCP semi-join can avoid to be established in the server, preventing the server from SYN Flood attack.

### Function Description

On the "Attack protection" page, user can enable attack prevention function.

### Operation Path

Open in order: "Main Menu > Network security > Attack protection".

### Interface Description

Attack protection interface as follows:

Attack protection

Ignore PING:  Enable  Disable Ignore local device PING

SYN DOS attack protection:  Enable  Disable TCP SYN ATTACK protection

CPU receive threshold:  pps scope: 0-100000 (default is 0, no rate limit)

Apply Cancel

The main element configuration description of attack protection interface:

Interface Element	Description
Ignore PING	Ignore icmp request that the destination address is the device, options as below: <ul style="list-style-type: none"> <li>• Enable;</li> <li>• Disable.</li> </ul>
SYN DOS attack	Defense TCP SYN attack to the device. <ul style="list-style-type: none"> <li>• Enable;</li> <li>• Disable.</li> </ul>
CPU receive threshold	CPU receiving data packet threshold value, defaults to 0, it represents no speed limit, valid input range is 0-10000.

## 7.3 ACL Configuration

Access Control List (ACL) is the aggregation of single or multiple rules, which is used to identify the message flow. Rule refers to the judgment statement describing the message matching condition. These conditions may be the source address, destination address, port number of message. Network devices identify specific messages according to these rules and process the messages according to pre-defined strategies.

### 7.3.1 ACL GROUP Configuration

#### Function Description

On the "ACL GROUP Config" page, user can set MAC access list ID and IP access list ID for the port.

#### Operation Path

Open in order: "Main Menu > Network security > ACL Config > ACL GROUP Config".

#### Interface Description

ACL GROUP Configuration interface as follows:



ACL GROUP Config		
Port	MACACL ListID	IPACL ListID
ge1/1	<input type="text" value="0"/>	<input type="text" value="0"/>
ge1/2	<input type="text" value="0"/>	<input type="text" value="0"/>
ge1/3	<input type="text" value="0"/>	<input type="text" value="0"/>
ge1/4	<input type="text" value="0"/>	<input type="text" value="0"/>
ge1/5	<input type="text" value="0"/>	<input type="text" value="0"/>
ge1/6	<input type="text" value="0"/>	<input type="text" value="0"/>
ge1/7	<input type="text" value="0"/>	<input type="text" value="0"/>
ge1/8	<input type="text" value="0"/>	<input type="text" value="0"/>
ge1/9	<input type="text" value="0"/>	<input type="text" value="0"/>
ge1/10	<input type="text" value="0"/>	<input type="text" value="0"/>
ge1/11	<input type="text" value="0"/>	<input type="text" value="0"/>
ge1/12	<input type="text" value="0"/>	<input type="text" value="0"/>
ge1/13	<input type="text" value="0"/>	<input type="text" value="0"/>
ge1/14	<input type="text" value="0"/>	<input type="text" value="0"/>
ge1/15	<input type="text" value="0"/>	<input type="text" value="0"/>
ge1/16	<input type="text" value="0"/>	<input type="text" value="0"/>
ge1/17	<input type="text" value="0"/>	<input type="text" value="0"/>
ge1/18	<input type="text" value="0"/>	<input type="text" value="0"/>
ge1/19	<input type="text" value="0"/>	<input type="text" value="0"/>
ge1/20	<input type="text" value="0"/>	<input type="text" value="0"/>

The main element configuration description of ACL GROUP Configuration interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
MAC ACL List ID	Rule ID of MAC address device accessing the device. MAC discards or forwards the message according to the MAC access rule.
IP ACL List ID	Configuration rule ID of IP address accessing the device. IP MAC discards or forwards the message according to IP access rule.

## 7.3.2 Time Range Configuration

When ACL rule is valid only for a certain period of time, user can set time-based ACL filtering. Therefore, first user can configure one or more time periods, and then reference the time periods in the rule, the rule will be valid only for the specified time period.

Users can adopt the same name to configure multiple time segments with different contents. After gain the union of each cycle time period and each absolute time period, the intersection of each union will become the final valid time range.

### Function Description

On the "Time Range Config" page, user can add or delete the absolute time and cycle time.

### Operation Path

Open in order: "Main Menu > Network security > ACL Config > Time Range Config".

### Interface Description

Time Range configuration interface as follows:

The main element configuration description of Time Range configuration interface:

Interface Element	Description
<b>Add Time Range</b>	<b>Add Time Range setting column</b>
Name	Time period range name entering.
<b>Time Config</b>	<b>Configuration time setting column</b>
Time-Range Name	Time-Range name filling, select relative time method: <ul style="list-style-type: none"> <li>Absolute time: It represents the rule is valid in appointed time range (such as 8 o'clock 1st January 2017 to 18 o'clock 3rd January 2017).</li> <li>Cycle time: It represents the rule is valid in the cycle of a week (such as 8 o'clock to 12 o'clock per Monday).</li> </ul>
start	Starting time of absolute time, format: HH: MM (Hour:

Interface Element	Description
	minute); YYYY-MM-DD (Year-month-day).
end	End time of absolute time, format: HH: MM (Hour: minute); YYYY-MM-DD (Year-month-day).
Time	Time range of cycle time, format: HH: MM (Hour: minute).
Week	Cycle date of cycle time; take one week as a cycle.

### 7.3.3 MAC ACL Configuration

MAC ACL is used to identify the destination MAC address in the message flow. Identify the specific message according to the rules in MAC ACL and process the messages according to the preset strategies.

#### Function Description

On the "MAC ACL Config" page, user can add or delete MAC access list.

#### Operation Path

Open in order: "Main Menu > Network security > ACL Config > MAC ACL Config".

#### Interface Description

MAC ACL configuration interface as follows:

The main element configuration description of MAC ACL configuration interface:

Interface Element	Description
<b>MAC ACL Config</b>	<b>MAC ACL configuration column.</b> Note: Add MAC address access rules list group ID.
Group ID	Group ID serial number, support 1-99.
<b>rule Config</b>	<b>Rule configuration column.</b> Note: MAC address access rule configuration.
Group ID	Corresponding MAC address access list group ID.
Rule ID	Different rule ID number under group ID, value range is 1-127.
ACTION	MAC address access rule operation: <ul style="list-style-type: none"> <li>Deny: Access denied;</li> <li>Permit: Access allowed.</li> </ul>
Source MAC	Access the source MAC address of data information Notes: If no input, anything is valid.
Dest MAC	Access the destination MAC address of data information Notes: If no input, anything is valid.
Time-Range Name	Time range name. Notes: Any time is valid if no input.

## 7.3.4 IP ACL Configuration

IP ACL is used to identify the destination MAC address in the message flow for access control. The specific message is identified according to the rules in MAC ACL and is processed according to a preset strategy.

### Function Description

On the "IP ACL Config" page, user can add or delete MAC access list.

### Operation Path

Open in order: "Main Menu > Network security > ACL Config > IP ACL Config".

### Interface Description

IP ACL configuration serial setting interface as follows:

**IP ACL Config**

Group ID:  scope:100-999

---

**rule Config**

Group ID:  scope:100-999  
RuleID:  scope:1-127  
ACTION:  ACTION  
protocol:  ACTION  
SourceIP:  format: XXX.XXX.XXX.XXX or any  
SourceMask:  format: XXX.XXX.XXX.XXX or any  
SourcePort:  scope is 0-65535,any port if no input  
DestIP:  format: XXX.XXX.XXX.XXX or any  
DestMask:  format: XXX.XXX.XXX.XXX or any  
DestPort:  scope is 0-65535,any port if no input  
Time-RangeName:  any time is valid if no input

Group ID	RuleID	ACTION	protocol	SourceIP	SourceMask	SourcePort	DestIP	DestMask	DestPort	TimeRange
<input type="button" value="Refresh"/>										

The main element configuration description of IP ACL Configuration interface:

Interface Element	Description
<b>IP ACL Config</b>	<b>Add IP address access rules list group ID.</b>
Group ID	Group ID serial number, support 1-99.
<b>rule Config</b>	<b>IP address access rules configuration.</b>
Group ID	Corresponding IP address access list group ID.
Rule ID	Different rule ID number under group ID, value range is 1-127.
ACTION	IP address access rule operation: <ul style="list-style-type: none"> <li>• Deny: Access denied;</li> <li>• Permit: Access allowed.</li> </ul>
protocol	Protocol data packet access rule operation: <ul style="list-style-type: none"> <li>• Any: any protocol data;</li> <li>• Icmp: Control message protocol data;</li> <li>• Icmp: Internet group management protocol data;</li> <li>• TCP: Transmission control protocol data;</li> <li>• UDP: User data message protocol.</li> </ul>
Source IP	Access the source IP address of data information. Notes: If no input, anything is valid.

Interface Element	Description
Source Mask	Access the source mask address of data information. Notes: If no input, anything is valid.
Source Port	Access the source port information of data information. Notes: If no input, anything is valid.
Dest IP	Access the destination IP address of data information. Notes: If no input, anything is valid.
Dest Mask	Access the destination mask address of data information. Notes: If no input, anything is valid.
Dest port	Access the destination port information of the data. Notes: If no input, anything is valid.
Time-Range Name	Time range name. Notes: Any time is valid if no input.

## 7.4 NAT Configuration

Network Address Translation (NAT), legal IP address that maps IP address to external network can slow down the IP address space consumption.

### 7.4.1 NAT Rule Configuration

#### Function Description

On the "NAT Rule Config" page, user can configure the NAT rule.

#### Operation Path

Open in order: "Main Menu > Network security > NAT Config > NAT Rule Config".

#### Interface Description

NAT rule configuration interface as follows:

The main element configuration description of NAT rule configuration interface:

Interface Element	Description
Name	NAT rule name, no more than 31 characters.
protocol	Mapping port protocol, options as follows: <ul style="list-style-type: none"> <li>all;</li> <li>tcp;</li> <li>udp.</li> </ul>
Incar IP	Interior IP address and port number, port number valid input range is 0-65535, not fill represents arbitrary port number.
Outcar IP	External IP address and port number, port number valid input range is 0-65535, not fill represents arbitrary port number.

## 7.4.2 NAT Bind

### Function Description

On the "NAT Bind" page, user can bind NAT rule and interface.

### Operation Path

Open in order: "Main Menu > Network security > NAT Config > NAT Bind".

### Interface Description

NAT bind interface as follows:

Bind			
NAT Name:	<input type="text"/>	NAT interface choice	
Incar interface Name:	<input type="text" value="vlanif1"/>	Interface choice	
Outcar interface Name:	<input type="text" value="vlanif1"/>	Interface choice	
<input type="button" value="Add"/>			
SerialNum	NAT Name	Incar interface Name	Outcar interface Name
Total Entry 20 entrys per page			
			1/1Page <input type="button" value="Go"/>

The main element configuration description of NAT bind interface:

Interface Element	Description
NAT Name	NAT rule name pull-down list.
Incar interface Name	Interior IP address corresponding interface name pull-down list.
Outcar interface Name	External IP address corresponding interface name pull-down list.



# 8 Advanced Configuration

## 8.1 QOS Configuration

Quality of Service (QoS) is the service quality. As for network business, service quality includes transmission bandwidth, transfer delay, data packet loss rate and so on. In network, user can improve the service quality by ensuring the transmission bandwidth, reducing transfer delay, data packet loss rate, delay jitter and other measures.

Network resources are always limited, as long as there exists the case of snatching network resources, there will be service quality requirements. Quality of service is relative to the network business, while ensuring the service quality of a certain type of business; it may damage the service quality of other businesses. For example, in the case of total network bandwidth is fixed, if a type of business occupies more bandwidth, other businesses will be able to use less bandwidth, which may influence the usage of other businesses. Therefore, network managers need to make rational planning and distribution of network resources according to the characteristics of various businesses, so that network resources can be efficiently utilized.

### 8.1.1 Global Configuration

QoS function provides 8 internal queues, each queue supports 4 different levels traffic, High-priority data packets stay on the switch for a short period of time, and some latency-sensitive traffic supports lower latency. According to 802.1p priority level tag, IP TOS, the device can classify packets to a certain level.

## Function Description

On the "Global Config" page, user can configure QOS scheduling policies, COS queue mapping, and DSCP queue mapping.

## Operation Path

Open in order: "Main Menu > Advanced Config > QOS Config > Global Config".

## Interface Description

Global configuration interface as follows:

The screenshot displays the Global Configuration interface with three main sections:

- Policy:** Features radio buttons for **SP** (selected) and **WRR**. Below are seven input fields labeled W0 through W7, each with a small square next to it. **Apply** and **Cancel** buttons are positioned below the fields.
- COSCos map queue:** Includes a dropdown menu for **COS** (set to 0) and a dropdown for **Queue** (set to 0), followed by an **Apply** button. Below this are eight mapping options: 0->0, 1->1, 2->2, 3->3, 4->4, 5->5, 6->6, and 7->7.
- DSCPCos map queue:** Features dropdown menus for **DSCP** (set to 0), **New DSCP** (set to 0), and **Cos** (set to 0), followed by an **Apply** button. Below are 64 mapping options in an 8x8 grid, ranging from 0->0->0 to 63->0->0.

The main element configuration description of global configuration interface:

Interface Element	Description
<b>Policy</b>	<b>SP strict priority and WRR weighted round robin scheduling algorithm two scheduling strategies.</b>
SP	SP functional status, check to enable this strategy. Notes: SP is strict priority. SP schedule sends the higher-priority queues strictly according to the priority level from high to low. Queue 7 has the highest priority level and queue 0 has the lowest priority level.
WRR	Gain the resource special gravity equivalent, value range is

Interface Element	Description
	0-100. Notes: Weighted Round Robin (WRR) is a weighted round robin (WRR) scheduling algorithm. WRR can configure the scheduled packets number in each queue, and conduct schedule between queues in turn.
<b>COS Cos map queue</b>	<b>IEEE802.1p priority level and queue mapping relation.</b>
COS	Grade of service, value range is 0-7. Notes: The service level value is larger, the level is lower, for example, "7" represents the highest priority level and "0" represents the lowest priority level.
Queue	QoS internal priority level queue, value range is 0-7.
<b>DSCP Cos map queue</b>	<b>Mapping relation between DSCP priority level and COS queue.</b>
DSCP	DSCP priority level value is 0-63, 63 is the highest priority level, 0 is the lowest priority level.
New DSCP	In the drop-down list, New DSCP priority level 0-63 is optional.
Cos	In the drop-down list, COS priority level 0-7 is optional.

## 8.1.2 Port Configuration

### Function Description

On the "Port Config" page, user can configure the port default COS.

### Operation Path

Open in order: "Main Menu > Advanced Config > QOS Config > Port Config".

### Interface Description

Port configuration interface as follows:

Port Config					
Port	Default COS	Port	Default COS	Port	Default COS
ge1/1	<input type="text" value="0"/>	ge1/2	<input type="text" value="0"/>	ge1/3	<input type="text" value="0"/>
ge1/4	<input type="text" value="0"/>	ge1/5	<input type="text" value="0"/>	ge1/6	<input type="text" value="0"/>
ge1/7	<input type="text" value="0"/>	ge1/8	<input type="text" value="0"/>	ge1/9	<input type="text" value="0"/>
ge1/10	<input type="text" value="0"/>	ge1/11	<input type="text" value="0"/>	ge1/12	<input type="text" value="0"/>
ge1/13	<input type="text" value="0"/>	ge1/14	<input type="text" value="0"/>	ge1/15	<input type="text" value="0"/>
ge1/16	<input type="text" value="0"/>	ge1/17	<input type="text" value="0"/>	ge1/18	<input type="text" value="0"/>
ge1/19	<input type="text" value="0"/>	ge1/20	<input type="text" value="0"/>		

The main element configuration description of port configuration interface:

Interface Element	Description
Port	Ethernet port number of the switch.
Default COS	Port default COS priority level. Notes: Value range is 1-7.

## 8.2 LLDP Configuration

LLDP is a layer 2 topology discovery protocol, its basic principle is: Devices in network send the status information message to adjacent device, and each port in the device stores its own information, if there is change in the status of local device, it can also send updated information to the adjacent device directly connected to it. Adjacent devices will store the information in standard SNMP MIB bank. The network management system could inquiry the connection status of current layer 2 from SNMP MIB bank. It should be noted that LLDP is only a remote device status information discovery protocol, which cannot complete the network device configuration, port control and other functions.

### 8.2.1 Global Configuration

#### Function Description

On the "Global Config" page, user can configure LLDP relative parameters.

#### Operation Path

Open in order: "Main Menu > Advanced Config > LLDP Config > Global Config".

## Interface Description

Global configuration interface as follows:

The screenshot shows the 'LLDP Config' window. At the top, there's a title bar 'LLDP Config'. Below it, the 'LLDP' status is set to 'Disable' (radio button selected). There are four input fields: 'Send cycle' (30), 'Hold Time' (120), 'Send interval' (2), and 'Reinit delay' (2). Each field has a 'scope' value: 'scope:5-65535' for Send cycle and Hold Time, and 'scope:2-5' for Send interval and Reinit delay. At the bottom, there are checkboxes for 'TLV Optional to send' with the following options checked: Management address, Port description, System property, System description, and System name. There are 'Apply' and 'Cancel' buttons at the bottom right.

The main element configuration description of global configuration interface:

Interface Element	Description
LLDP	LLDP function status, options as follows: <ul style="list-style-type: none"> <li>• Enable;</li> <li>• Disable.</li> </ul>
Send cycle	LLDP send cycle range is 5-65535. Notes: When no device status changes, the device periodically sends LLDP packets to its adjacent nodes. The interval is called the period for sending LLDP packets.
Hold Time	LLDP hold time range is 5-65535. Notes: Hold time can control the aging time of device information in the adjacent device.
Send interval	LLDP send interval range is 2-5, that is the delay time of LLDP continuous message sending.
Reinit delay	Reinit delay time range is 2-5. Notes: When LLDP work mode of the port changes, port will conduct initialization operation to the protocol state machine, Re-enable the delay time via configuration to avoid continuous initialization of port due to the frequent changes in working mode.
TLV Optional to send	TLV sends information, options below are optional: <ul style="list-style-type: none"> <li>• Management address;</li> <li>• Port description;</li> <li>• System property;</li> <li>• System description;</li> </ul>

Interface Element	Description
	<ul style="list-style-type: none"> <li>System name.</li> </ul> <p>Notes: TLV is a unit that makes up LLDPDU. Each TLV represents a piece of information. LLDPDU is the data unit encapsulated in the data part of LLDP packet.</p>

## 8.2.2 Port Configuration

### Function Description

On the "Port Config" page, user can configure the sending and receiving mode and management address of the port.

### Operation Path

Open in order: "Main Menu > Advanced Config > LLDP Config > Port Config".

### Interface Description

Port configuration interface as follows:

Port Config			
Port	Send	Receive	Management address
ge1/1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ge1/2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ge1/3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ge1/4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ge1/5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ge1/6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ge1/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ge1/8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ge1/9	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ge1/10	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ge1/11	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ge1/12	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ge1/13	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ge1/14	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ge1/15	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ge1/16	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ge1/17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ge1/18	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ge1/19	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
ge1/20	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

The main element configuration description of port configuration interface:

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.
Send	The device won't receive LLDP information from adjacent device but will send LLDP information.
Receive	The device won't send LLDP information, but will receive and analyze LLDP information from adjacent device.
Management address	Corresponding LLDP management IP address of the port. Notes: LLDP management address is the address to be marked and managed by network management system. Management address can definitely mark a device, which is beneficial to the drawing of network topology and network management. Management address is encapsulated in Management Address TLV field of LLDP message and sent to adjacent nodes.

## 8.2.3 LLDP Neighbors

### Function Description

On the "LLDP Neighbors" page, user can look over the relative information of neighbors.

### Operation Path

Open in order: "Main Menu > Advanced Config > LLDP Config > LLDP Neighbors".

### Interface Description

LLDP neighbors interface as below:

LLDP Neighbors shows								
Capability Codes:								
(R)Router,(B)Bridge,(C)DOCSIS Cable Device,(T)Telephone								
(W)WLAN Access Point,(P)Repeater,(S)Station,(O)Other								
SerialNum	System name	Chassis-ID	managementIP	Local interface	Vlan	Hold Time	Port ID	System property
<input type="button" value="Refresh"/>								

The main element configuration description of LLDP neighbors interface:

Interface Element	Description
SerialNum	LLDP neighbors information display serial number.

Interface Element	Description
System name	System name of neighbor devices.
Chassis-ID	Bridge MAC address of neighbor device or port.
management IP	Management IP address of neighbor device or port.
Local interface	Local port number of local switch connected to adjacent devices.
Vlan	Local switch port VLAN PVID number.
Hold Time	LLDP hold time of neighbor device.
Port ID	Neighbor device port ID number.
System property	System property, abbreviated code as below: <ul style="list-style-type: none"> <li>• R: Router;</li> <li>• B: Bridge;</li> <li>• C: DOCSIS Cable Device;</li> <li>• T: Telephone;</li> <li>• W: WLAN Access Point;</li> <li>• P: Repeater;</li> <li>• S: Station;</li> <li>• O: Other.</li> </ul>

## 8.3 SNMP Configuration

### SNMP Introduction

Now, the broadest network management protocol in network is SNMP (Simple Network Management Protocol). SNMP is the industrial standard that is widely accepted and comes into use, it's used for guaranteeing the management information transmission between two points in network, and is convenient for network manager search information, modify information, locate faults, complete fault diagnosis, conduct capacity plan and generate a report. SNMP adopts polling mechanism and only provides the most basic function library, especially suit for using in minitype, rapid and low price environment. SNMP implementation is based on connectionless transmission layer protocol UDP, therefore, it can achieve barrier - free connection to many other products.

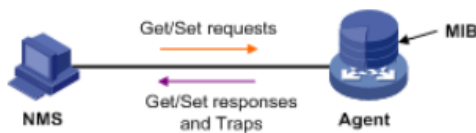
### SNMP Working Mechanism



SNMP is divided into NMS and Agent:

- Network Management Station (NMS) is the work station that runs client procedure, at present, common network management platforms include Quid View, Sun Net Manager and IBM Net View. Agent is the server software that runs in network device.
- NMS can send Get Request, Get Next Request and Set Request messages to Agent, after receiving these request messages from NMS, Agent will conduct Read or Write operation, generate Response message and return messages to NMS according to the message type. When the device appears abnormal situation or the state changes (such as device resets), Agent will forwardly send Trap message to NMS and report occurred event to NMS.

Any managed resource is represented as an object, called a managed object. MIB (Management Information Base, management information base) is the collection of managed objects. NMS manages the device via MIB. MIB has defined the hierarchical relationship between the nodes and a set of properties of objects, such as objects' name, access privilege and data type, etc. Each Agent has its own MIB. Managed device has its own MIB files; compiling these MIB files in NMS can generate MIB of the device. NMS conducts read/write operation according to access privilege, and achieves Agent management. Relationship of NMS, Agent and MIB as the picture below.



MIB is organized according to a tree structure, consisting of a number of nodes; each node represents a managed object that can be uniquely identified by a string of path-specific numbers starting from the root, this string of OID (Object Identifier) ".

SNMP supports three basic operations:

- **Get operation:** Manager adopts the operation to inquire a variable value of Agent;
- **Set operation:** Manager adopts the operation to set a variable value of Agent;
- **Trap operation:** Agent adopts the operation to send abnormal alarm information to manager.

### SNMP Protocol Version

At present, SNMP Agent in the device supports SNMP v1 version, SNMP v2c and SNMP v3 version. SNMP v1, SNMP v2c adopt community name authentication, SNMP message of community name without device authentication will be discarded. SNMP community name is used for defining the relationship of SNMP, NMS and SNMP Agent. Community name plays a role similar to password, and can limit SNMP Agent in SNMP NMS access device. User can choose and appoint one or more characters relative to community name:

- Define MIB view that community name can access.
- Configure MIB object access privilege of community name as read-write privilege or read-only privilege. Community name with read-only privilege can only inquire the device information; community name with read-write privilege can configure the device.
- Set the basic access control list appointed by community name.

## 8.3.1 System Information

### Function Description

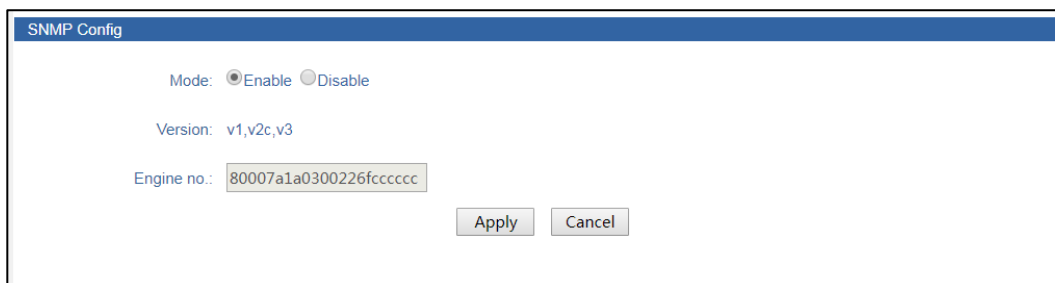
On the "System Information" page, user can choose enable or disable SNMP function.

### Operation Path

Open in order: "Main Menu > Advanced Config > SNMP Config > System Information".

### Interface Description

System Info interface as follows:



The screenshot shows the "SNMP Config" interface. It features a blue header bar with the text "SNMP Config". Below the header, there are three configuration options: "Mode" with radio buttons for "Enable" (selected) and "Disable"; "Version" with a text field containing "v1,v2c,v3"; and "Engine no." with a text field containing "80007a1a0300226fcccccc". At the bottom right of the interface, there are two buttons: "Apply" and "Cancel".

The main element configuration description of system information interface:

Interface Element	Description
Mode	SNMP function state: <ul style="list-style-type: none"> <li>• Enable;</li> <li>• Disable.</li> </ul>
Version	Compatible with v1, v2c, v3 versions.
Engine no.	The engine no. of the device

## 8.3.2 View

### Function Description

On the "View" page, user can add/delete view.

### Operation Path

Open in order: " Main Menu > Advanced Config > SNMP Config > View".

### Interface Description

View interface as below:

The main element configuration description of view interface:

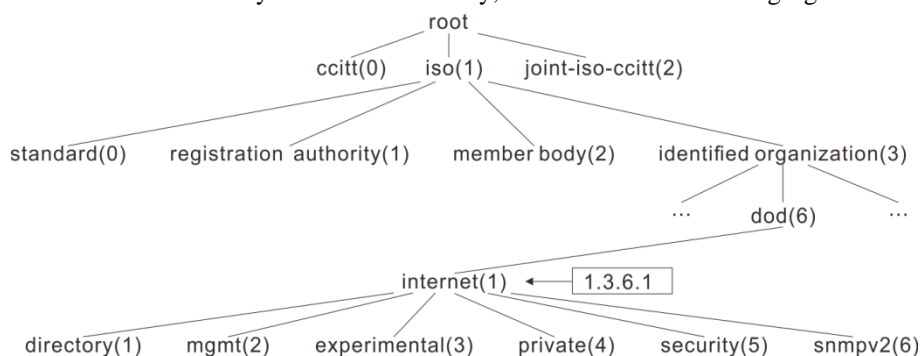
Interface Element	Description
Name	SNMP view name definition, support 32 characters input. Note: Name can't be empty or contain "&" or ";" or " or ' or "\" or "/"
Model	Node OID dealing method, options as below: <ul style="list-style-type: none"> <li>• Included: It contains all objects under the node subtree;</li> <li>• Excluded: Eliminate all objects beyond the node subtree.</li> </ul>
OID	Node location information of MIB tree where the device resides. Notes:

Interface Element	Description
	OID object identifier, a component node of MIB, uniquely identified by a string of numbers that represent the path.



Note

- In the SNMP view configuration, if user configures the "Node OID" to ".1.3.6.1", that is the INTERNET layer under MIB library, as shown in the following figure:



- When "Model" is "included", it contains all objects under MIB library 1.3.6.1 subtree;
- When "Model" is "excluded", it represents eliminating all objects beyond MIB library 1.3.6.1 subtree.
- It is recommended that non-professionals fill in ".1" in "OID". That is, OID is 1, indicating all objects under MIB library 1 subtree.

## 8.3.3 Community

### Function Description

On the "Community" page, user can add/delete community. Define MIB view that community name can access, set MIB object access privilege of community name as read-write privilege or read-only privilege.

### Operation Path

Open in order: " Main Menu > Advanced Config > SNMP Config > Community".

### Interface Description

Community interface as below:

The main element configuration description of community interface:

Interface Element	Description
Name	Community name definition. Note: The name needs to be same to view name.
Read View	Read only privilege view name selection.
Write View	Read-write privilege view name selection.

### 8.3.4 V3 User

SNMPv3 adopts User-Based Security Model (USM) authentication mechanism. Network manager can configure authentication and encryption function. Authentication is used to verify the validity of the packet sender and prevent unauthorized users from accessing it. Encryption encrypts the transmission packet between NMS and Agent to prevent eavesdropping. It adopts authentication and encryption function to provide higher security for the communication between NMS and Agent.

#### Function Description

On the "V3 User" page, user can configure SNMP V3 user information.

#### Operation Path

Open in order: " Main Menu > Advanced Config > SNMP Config > V3 User".

#### Interface Description

V3 user interface as follows:

Name	Engine no.	Authentication Type	Passphrase	Privacy Type	Passphrase	Read View	Write View

The main element configuration description of V3 user interface:

Interface Element	Description
Name	SNMP v3 version user name definition, combination of letters and numbers.
Engine no.	The engine number of the device
Authentication	Authentication information filling, two authentication methods optional: <ul style="list-style-type: none"> <li>• Md5: Information abstract algorithm 5;</li> <li>• Sha: Secure hash algorithm.</li> </ul>
Privacy	V3 user data encryption algorithm, options as follows: <ul style="list-style-type: none"> <li>• Des: Adopt data encryption algorithm;</li> <li>• Aes: Adopt advanced encryption standard;</li> <li>• None: No encryption.</li> </ul>
Read View	Read only privilege view name selection.
Write View	Read-write privilege view name selection.

### 8.3.5 Trap

Base on TCP/IP protocol, SNMP usually adopts UDP port 161 (SNMP) and 162 (SNMP-traps), SNMP protocol agent exists in the network device and adopts information specific to the device (MIBs) as the device interface; these network devices can be monitored or controlled via Agent. When a trap event occurs, the

message is transmitted by SNMP Trap. At this point, an available trap receiver can receive the trap message.

### Function Description

On the "Trap" page, user can configure the Trap information.

### Operation Path

Open in order: " Main Menu > Advanced Config > SNMP Config > Trap".

### Interface Description

Trap interface as below:

The main element configuration description of Trap interface:

Interface Element	Description
Address	IP address of SNMP management device, such as PC.
Version	SNMP management device version, options as below: <ul style="list-style-type: none"> <li>v1;</li> <li>v2c;</li> </ul>

## 8.4 RMON Configuration

RMON (Remote Network Monitoring) mainly achieves statistics and alarm functions, which are used for remote monitoring and management of management device to managed devices. Statistical function refers to that managed device can periodically or continuously keep track of all the traffic information on the network segment connected to the port , For example, the total number of packets received on a network segment in a period of time, or the total number of received super long packets. Alarm function refers to the managed device can monitor the value of

specified MIB variables, When the alarm threshold is reached (for example, the port rate reaches specified value or the broadcast packet reaches specified rate), the system will automatically log and send Trap messages to the management device.

## 8.4.1 Event

### Function Description

On the "Event" page, user can add, delete or check the configuration information of event.

### Operation Path

Open in order: "Main Menu > Advanced Config > RMON Config > Event".

### Interface Description

Check event interface as below:

Event Config			
SerialNum:	<input type="text"/>	The event group number between 0-1024(Only fill this item while deleting)	
Describe:	<input type="text"/>		
ACTION:	<input type="text" value="none"/>		
		<input type="button" value="Add"/>	<input type="button" value="Delete"/>
SerialNum	Describe	ACTION	Recent time
<input type="button" value="Refresh"/>			

The main element configuration description of event interface:

Interface Element	Description
SerialNum	Triggered event serial number when monitoring MIB object exceeds threshold value. Notes: This serial number corresponds to the rising event index and falling event index set in RMON alarm configuration information.
Describe	Some description information for describing the event.
ACTION	Event dealing method, options as below: <ul style="list-style-type: none"> <li>• None: No dealing;</li> <li>• log: Record the event in the log table when the event is triggered;</li> <li>• trap: Send Trap information to management station for informing the occurring of event when the event is</li> </ul>



Interface Element	Description
	triggered; • Log, trap: Record the event in the log table and produce a trap information when the event is triggered.

## 8.4.2 Statistical

### Function Description

On the "Statistical" page, user can add, delete or check the configuration information of statistical.

### Operation Path

Open in order: "Main Menu > Advanced Config > RMON Config > Statistical".

### Interface Description

Statistical interface as below:

The screenshot shows the 'Statistical Config' page. At the top, there is a header 'Statistical Config'. Below it, there are two input fields: 'SerialNum:' with a text box and a tooltip 'Statistical group number between 0-1024(Only fill this item while deleting)', and 'Port:' with a dropdown menu showing 'ge1/1' and a tooltip 'Statistical port'. There are 'Add' and 'Delete' buttons. Below these is a table with two columns: 'SerialNum' and 'PortName'. A 'Refresh' button is located below the table.

The main element configuration description of statistical interface:

Interface Element	Description
SerialNum	Serial number is used to identify a special application interface, when the serial number is same to the application interface serial number set before, previous configuration will be replaced.
Port	Set a port number (physical interface) as the receiving end of monitoring data information.

## 8.4.3 History

### Function Description

On the "History" page, user can add, delete or check the configuration information of history.

### Operation Path

Open in order: "Main Menu > Advanced Config > RMON Config > History".

### Interface Description

History interface as below:

History Config

SerialNum:  History team number between 0-1024(Only fill this item while deleting)

Sampling port:

Sampling interval:  Sampling interval between 5-65535, unit:sec

Sample maximum:  Sample maximum between 0-100

SerialNum	Sampling port	Sampling interval( Seconds)	Sample maximum
<input type="button" value="Refresh"/>			

The main element configuration description of history interface:

Interface Element	Description
SerialNum	Serial number is used to identify a special application interface, when the serial number is same to the application interface serial number set before, previous configuration will be replaced.
Sampling port	Set a physical interface as the receiving end of monitoring information.
Sampling interval	The interval time of gaining statistics data each two times.
Sample maximum	Table entries needed to be reserved.

## 8.4.4 Alarm

### Function Description

On the "Alarm" page, user can add, delete the alarm or check the alarm configuration information.

Alarm type adopts absolute to directly monitor MIB object value; Alarm type adopts delta to monitor changes in MIB object values between two samples;

- When monitoring MIB object reaches or surpasses the rising threshold value, it will trigger corresponding event of rising event index;
- When monitoring MIB object reaches or surpasses declining threshold value, it will trigger corresponding event of declining event index;

### Operation Path

Open in order: "Main Menu > Advanced Config > RMON Config > Alarm".

### Interface Description

Alarm interface as below:

Alarm Config

SerialNum:  The alarm set serial number between 0-1024(Only fill this item while deleting)

Sampling port:

Alarm parameters:

Sampling interval:  Sampling interval between 5-65535, unit:sec

Sampling type:

Rising threshold:  The threshold value between 0-4294967295

Falling threshold:

Rising event:  Event group index, when the alarm is triggered, corresponding event in the event group

Falling event:  will be activated, range is 0-1024

SerialNum	Sampling port	Alarm parameters	Sampling interval	Sampling type	Rising threshold	Falling threshold	Rising event	Falling event
<input type="button" value="Refresh"/>								

The main element configuration description of alarm interface:

Interface Element	Description
SerialNum	Serial number is used to identify special alarm configuration information, when the serial number is same to the applied serial number set before, previous configuration will be

Interface Element	Description
	replaced.
Sampling port	Set a physical interface as the receiving end of monitoring information.
Alarm parameters	Alarm parameters, options as follows: <ul style="list-style-type: none"> <li>• DropEvents: Falling edge event;</li> <li>• Octets: Byte.</li> <li>• Pkts: Data packet.</li> <li>• BroadcastPkts: Broadcast packet;</li> <li>• MulticastPkts: Multicast packet;</li> <li>• CRCAAlignErrors: CRC alignment errors;</li> <li>• UndersizePkts: Ultra short packet number, less than 64 bytes;</li> <li>• OversizePkts: Ultra-long packet number, more than 1518 bytes;</li> <li>• Fragments: Fragment frame data;</li> <li>• Jabbers: Invalid huge frame data, more than 1518 bytes;</li> <li>• Collisions: Conflicts occur;</li> <li>• Pkts64Octets: 64 bytes data packet;</li> <li>• Pkts65to127Octets: 65-127 bytes data packet;</li> <li>• Pkts128to255Octets: 128-255 bytes data packet;</li> <li>• Pkts256to511Octets: 256-511 bytes data packet;</li> <li>• Pkts512to1023Octets: 512-1023 bytes data packet;</li> <li>• Pkts1024to1518Octets: 1024-1518 bytes data packet.</li> </ul>
Sampling interval	Sampling time interval value, value range is 5-65535, unit: second.
Sampling type	Two sampling methods, options as follows: <ul style="list-style-type: none"> <li>• Absolute: When alarm variable value reaches alarm threshold value, an alarm is triggered; If the second sampling is same to last sampling alarm type, alarm isn't triggered again;</li> <li>• Delte: When alarm variable value reaches alarm threshold value during each sampling, an alarm is triggered.</li> </ul>
Rising threshold	Alarm variable value, upper limit alarm, threshold value is 0-4294967295. Notes:

Interface Element	Description
	In the rising process of alarm variable value, when the variable value surpasses rising threshold, an alarm occurs at least one time.
Falling threshold	Alarm variable value, lower limit alarm, threshold value is 0-4294967295. Notes: In the falling process of alarm variable value, when the variable value reaches falling threshold, an alarm occurs at least one time.
Rising event	Event index, when alarm variable value reaches or surpasses the rising event threshold value, it will activate corresponding event in event group, value range is 0-1024.
Falling event	Event index, when alarm variable value reaches or is less than the falling threshold value, it will activate corresponding event in event group, value range is 0-1024.

## 8.5 DHCP Server Configuration

Dynamic Host Configuration Protocol (DHCP) is usually applied in large LAN network environment, its main functions include intensively manage, distribute IP address, make the host in network environment actively gain IP address, Gateway address, DNS server address and other information, and improve the address utilization rate.

### 8.5.1 DHCP Server Configuration

#### Function Description

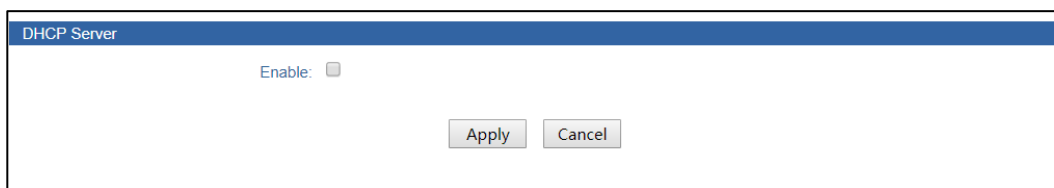
On the "DHCP Server Config" page, user can enable/disable DHCP Server.

#### Operation Path

Open in order: "Main Menu > Advanced Config > DHCP Server Config > DHCP Server Config".

#### Interface Description

DHCP Server configuration interface as follows:



The main element configuration description of DHCP Server configuration interface:

Interface Element	Description
DHCP Server	After enable DHCP Server function, set the device as a DHCP server by setting static allocation address table, the device can distribute IP address to devices connected to it.

## 8.5.2 DHCP Pool Configuration

After user defines DHCP range and exclusion range, surplus addresses constitute an address pool; addresses in the address pool can be dynamically distributed to hosts in network. Address pool is valid only for the method of automated IP acquisition; manual IP configuration can ignore this option only if conforming to the rules.

DHCP server chooses and distributes IP address and other relative parameters for client-side from address pool.

DHCP server adopts tree structure: Tree root is the address pool of natural network segment. Branch is the subnet address pool of the network segment. Leaf node is the manually binding client address. Same level address pool order is decided by the configuration order. This kind of tree structure has realized the inheritance of configuration, that is, subnet configuration inherits the configuration of natural network segment, and client configuration inherits the subnet configuration. Therefore, as for some common parameters (such as DNS server address), user only needs to configure in the natural network segment or subnet. Specific inheritance situation as follows:

1. When the parent-child relationship is established, sub address pool will inherit the existing configuration of parent address pool.
2. After the parent-child relationship is established, parent address pool is configured, sub-address pool will inherit or not, two situations as follows:

- If the child address pool doesn't include the configuration, it will inherit the configuration of parent address pool;
- If the child address pool has included the configuration, it won't inherit the configuration of parent address pool.

### Function Description

On the "DHCP Pool Config" page, user can add, delete the address pool and look over the configuration information of address pool.

### Operation Path

Open in order: "Main Menu > Advanced Config > DHCP Server Config > DHCP Pool Config".

### Interface Description

DHCP address pool configuration interface as follows:

The screenshot shows the DHCP Pool Config interface with the following fields and buttons:

- Pool name:  length:1-31
- Subnet mask:  eg:192.168.0.1/24
- Lease time: 1 Day 0 Hours 0 Minutes
- Default gateway:
- Name server:  eg:192.168.0.1
- Domain server:
- NetBIOS Server:
- Buttons: Add, Cancel
- Table header: Pool name, Subnet mask, Lease time, Default gateway, Name server, Domain server, NetBIOS Server
- Button: Refresh

The main element configuration description of DHCP pool configuration interface:

Interface Element	Description
Pool name	Address pool name, length range is 1-48.
Subnet mask	Address pool distributes the IP address network segment of client-side, for example: 192.168.0.1/24.
Lease time	IP address utilization valid time of client-side, range is 0-999 days.
Default gateway	Default gateway address of client-side.
DNS server	DNS server IP address of client-side.

Interface Element	Description
Domain server	DNS server domain address of client-side.
NetBIOS Server	NetBIOS server IP address of client-side.

## 8.5.3 Client List

### Function Description

On the "Client List" page, user can look over the information of DHCP client-side.

### Operation Path

Open in order: "Main Menu > Advanced Config > DHCP Server Config > Client List".

### Interface Description

Client list interface as follows:

Leases List			
SerialNum	MAC address	IP address	Ageing time
Total 0 Entry 20 entrys per page			1/1Page << < > >> Go
Refresh			

The main element configuration description of client list interface:

Interface Element	Description
SerialNum	Serial number name of DHCP client-side.
MAC address	MAC address of DHCP client-side device.
IP address	IP address of DHCP client-side device.
Ageing time	Ageing time of the client-side address.

## 8.5.4 Static Client Configuration

### Function Description

On the "Static Leases Config" page, user can add, delete the static client-side and look over the configuration information of static client-side.



The client MAC address is bound to the address assigned by DHCP server; therefore, each address obtained by the client from server is a binding IP address.

### Operation Path

Open in order: "Main Menu > Advanced Config > DHCP Server Config > Static Leases Config".

### Interface Description

Static Client Configuration interface as follows:

The main element configuration description of static client configuration interface:

Interface Element	Description
DHCP Pool	Corresponding list name of DHCP address pool.
IP address	IP address that DHCP address pool distributes, client-side needs to gain the static IP address.
MAC address	MAC address of DHCP client.

## 8.5.5 Port Address Binding Configuration

### Function Description

On the "Port binding config" page, user can bind IP address relation port distributes.

Device A enables DHCP Server function and sets 2 static distribution address tables: 192.168.1.19 corresponding port is 1; 192.168.1.20 corresponding port is 2. After device B enables IP address automated acquisition function, if device A is connected to device B via port 1, device B can automatically gain IP address 192.168.1.19; If

device A is connected to device B via port 2, device B can automatically gain IP address 192.168.1.20.

### Operation Path

Open in order: "Main Menu > Advanced Config > DHCP Server Config > Port binding config".

### Interface Description

Port binding configuration interface as follows:

The main element configuration description of port binding configuration interface:

Interface Element	Description
DHCP Pool	Corresponding list name of DHCP address pool.
Port	The corresponding port name of the device Ethernet port.
IP address	IP address that DHCP address pool distributes, the IP addresses that client-side gains in the port.

## 8.6 DHCP-snooping

DHCP Snooping is layer 2 snooping function of DHCP service, after enable DHCP Snooping function, the device can extract and record IP address and MAC address information from received DHCP-ACK and DHCP-REQUEST messages.

For security reasons, security department needs to record the IP address used by user to access the Internet, and confirm the correspondence between IP address applied by user and MAC address of the host used by user. User can snoop

DHCP-REQUEST messages and DHCP-ACK messages via DHCP Snooping function, and record IP address information user gains.

## 8.6.1 Global Configuration

### Function Description

On the "Global Config" page, user can configure DHCP-Snooping parameters information.

### Operation Path

Open in order: "Main Menu > Advanced Config > DHCP-snooping > Global Config".

### Interface Description

Global configuration interface as follows:

The main element configuration description of global configuration interface:

Interface Element	Description
Enable DHCP-snooping	Enable DHCP-Snooping function checkbox.
Enable Information	Enable information function checkbox, after checking; enable Option 82 relay agent function which has recorded the location information of DHCP client.
Write Delay	Write delay range is 1-1440; unit is minute, default to 0, which represents not writing.
Tftp Server	Upload database to IP address of TFTP server, for example 10.0.0.2.

Interface Element	Description
Tftp File name	Folder name of database uploading to TFTP server.
Enable DAI	Enable DAI optional box, after checking, forward ARP sent by legitimate host according to DHCP Snooping table items.
Enable IPSPG	Enable IPSPG optional box, after checking, forward IP message sent by legitimate host via dynamically gaining DHCP Snooping table items.

## 8.6.2 Static Binding

### Function Description

On the "Static Binding" page, user can bind static MAC and port.

### Operation Path

Open in order: "Main Menu > Advanced Config > DHCP-snooping > StaticBinding".

### Interface Description

Static binding interface as follows:

StaticBinding

MAC:  eg:0001-0001-0001

Vlan Id:  eg:1-4094

IP address:  eg:192.168.1.1

Port:  eg:ge1/1

SerialNum	MAC	Vlan Id	IP	Type	Ageing time	Port
Total 0 Entry 20 entrys per page						

1/1Page

The main element configuration description of static binding interface:

Interface Element	Description
MAC	Binding MAC address, for example: 0001-0001-0001.
Vlan Id	Binding VLAN ID information, for example: 1-4096.
IP address	Binding IP address, for example: 192.168.1.1.

Interface Element	Description
Port	The corresponding port name of the device Ethernet port.

## 8.6.3 Port Configuration

### Function Description

On the "Port Config" page, user can configure DHCP Snooping port information. DHCP Snooping trust function can provide users with further security, and ensure that DHCP Snooping trust function can control the source of DHCP server response messages, preventing existing spurious or forbidden DHCP server distributing IP address and other configuration information for other hosts.

DHCP Snooping trust function divides ports into trust port and distrustful port:

- Trust port is the port that is directly or indirectly connected to legitimate DHCP server. Trust port normally forwards received DHCP messages to ensure that DHCP client can gain correct IP address.
- Distrustful port is the port that isn't connected to legitimate DHCP server. DHCP-ACK, DHCP-NAK and DHCP-OFFER messages received from distrustful port in response to DHCP server are discarded, preventing DHCP client obtaining the wrong IP address.

### Operation Path

Open in order: "Main Menu > Advanced Config > DHCP-snooping > Port Config".

### Interface Description

Port configuration interface as follows:

Port Config								
PortName	Trust	Trust-DAI	Trust-IPSG	Policy(Op82)	Circuit-type	Circuit-id	Remote-type	Remote-id
ge1/1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Replace ▾	Normal ▾		Normal ▾	
ge1/2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Replace ▾	Normal ▾		Normal ▾	
ge1/3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Replace ▾	Normal ▾		Normal ▾	
ge1/4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Replace ▾	Normal ▾		Normal ▾	
ge1/5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Replace ▾	Normal ▾		Normal ▾	
ge1/6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Replace ▾	Normal ▾		Normal ▾	
ge1/7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Replace ▾	Normal ▾		Normal ▾	
ge1/8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Replace ▾	Normal ▾		Normal ▾	
ge1/9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Replace ▾	Normal ▾		Normal ▾	
ge1/10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Replace ▾	Normal ▾		Normal ▾	
ge1/11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Replace ▾	Normal ▾		Normal ▾	
ge1/12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Replace ▾	Normal ▾		Normal ▾	
ge1/13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Replace ▾	Normal ▾		Normal ▾	
ge1/14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Replace ▾	Normal ▾		Normal ▾	
ge1/15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Replace ▾	Normal ▾		Normal ▾	
ge1/16	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Replace ▾	Normal ▾		Normal ▾	
ge1/17	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Replace ▾	Normal ▾		Normal ▾	
ge1/18	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Replace ▾	Normal ▾		Normal ▾	
ge1/19	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Replace ▾	Normal ▾		Normal ▾	
ge1/20	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Replace ▾	Normal ▾		Normal ▾	

The main element configuration description of port configuration interface:

Interface Element	Description
Port Name	The corresponding port name of the device Ethernet port.
Trust	Trust checkbox, trust port.
Trust-DAI	Trust-DAI checkbox, trust port ARP dynamic snooping.
Trust-IPSG	Trust-IPSG checkbox, trust port IP source address examination.
Policy (Op82)	Option 82 dealing strategy, options as follows: <ul style="list-style-type: none"> <li>Replace: Keep Option 82 in messages unchanged and forward.</li> <li>Keep: Adopt different modes to fill Option 82, replace prime Option 82 in message and forward, filling modes will be described as below.</li> <li>Drop: Discard messages.</li> </ul>
Circuit-type	Circuit ID sub-option filling type, options as follows: <ul style="list-style-type: none"> <li>Normal: Normal mode;</li> <li>String: Detailed mode.</li> </ul>
Circuit-id	Circuit ID sub-option filling content, support ASCII and HEX mode.
Remote-type	Remote ID sub-option filling type, options as follows: <ul style="list-style-type: none"> <li>Normal: Normal mode;</li> </ul>

Interface Element	Description
	<ul style="list-style-type: none"> <li>• Sysname: Directly adopt device system name to fill Option 82;</li> <li>• String: Detailed mode.</li> </ul>
Remote-id	Remote ID sub-option filling content, support ASCII and HEX mode.

## 8.7 NTP Configuration

The full name of NTP protocol is Network Time Protocol. Its destination is to transmit uniform and standard time in international Internet. Specific implementation scheme is appointing several clock source websites in the network to provide user with timing service, and these websites should be able to mutually compare to improve the accuracy. It can provide millisecond time correction, and is confirmed by the encrypted way to prevent malicious protocol attacks.

### Function Description

On the "NTP Config" page, user can configure the device time and NTP server information.

### Operation Path

Open in order: "Main Menu > Advanced Config > NTP Config".

### Interface Description

NTP configuration interface as follows:

The screenshot displays the NTP configuration interface. At the top, there is a 'device Time' section with a text input field containing '2019-1-24 17:58:47' and a 'Set Time equal PC' button. Below this is the 'NTP Config' section. It features a 'Mode' section with radio buttons for 'Enable' and 'Disable', where 'Disable' is selected. A note states 'Enable the NTP automatically pair'. The 'Pair interval' is set to '300' with the unit 'Sec/time' and a 'scope:5-65535 Default:300'. There are five input fields for 'The server1' through 'The server5', with 'The server1' having a hint 'eg:192.168.1.1'. At the bottom right, there are 'Apply' and 'Cancel' buttons.

The main element configuration description of NTP configuration interface:

Interface Element	Description
device Time	The device own time, which can be synchronized to current computer time.
Timezone selection	Time standard of global different regions.
<b>NTP Config</b>	<b>NTP protocol server configuration.</b>
Mode	NTP automatic pair function status, options as follows: <ul style="list-style-type: none"> <li>• Enable;</li> <li>• Disable.</li> </ul>
Pair interval	Pair time interval, value range is 5-65535, default value is 300.
The server1	IP address of NTP-sync server1, for example: 192.168.1.1.
The server2	IP address of NTP-sync server2, for example: 192.168.1.1.
The server3	IP address of NTP-sync server3, for example: 192.168.1.1.
The server4	IP address of NTP-sync server4, for example: 192.168.1.1.
The server5	IP address of NTP-sync server5, for example: 192.168.1.1.



# 9 System Management

---

## 9.1 Management File

### 9.1.1 View Launch Configuration

#### Function Description

On the "View launch config" page, user can view current configuration information.

#### Operation Path

Open in order: "Main Menu > System management > Management File > View launch config".

#### Interface Description

View launch configuration interface as follows:

```

View launch config
!
ip http-server all
ip telnet-server
timezone gmt + 08:00
no spanning-tree
!
username admin123 password admin123
!
vlan 1
!
vlan 10
!
interface ge1/1
!
interface ge1/2
!
interface ge1/3
!
interface ge1/4
!
interface ge1/5
!
interface ge1/6
!
interface ge1/7
!
interface ge1/8
!
interface ge1/9
!
interface ge1/10
!
interface ge1/11
 switchport mode trunk
 switchport pvid 10
 switchport trunk untag 10
!
interface ge1/12
 switchport mode trunk
 switchport pvid 10
 switchport trunk untag 10
!

```

## 9.1.2 Management File

### Function Description

On the "Management File" page, user can download and upload configuration file.

### Operation Path

Open in order: "Main Menu > System management > Management File > Management File".

### Interface Description

Management file interface as follows:

The screenshot shows a web interface titled "Management File". It contains a text input field labeled "File path:" followed by a "Select file" button. To the right of the input field is the text "(Download, do not need to fill in this)". Below these elements are two buttons: "Download" and "Upload".

The main element configuration description of management file interface:

Interface Element	Description
-------------------	-------------

Interface Element	Description
File path	Locally uploading configuration file path, click "Select File" to select required configuration file.
Download	Download the configuration file of current device, format: .conf.
Upload	Upload configuration file.



Note

- After finishing update, the device will automatically open a new page to "System State", and uploading configuration file will be valid after the device is reset.

## 9.2 Save

### Function Description

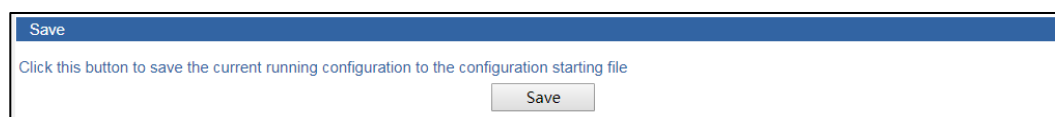
On the "Save" page, user can save the configuration file of current device.

### Operation Path

Open in order: "Main Menu > System management > Save".

### Interface Description

Save configuration interface as follows:



The main element configuration description of save configuration interface:

Interface Element	Description
Save	Save current configuration file.

## 9.3 Reboot

### Function Description

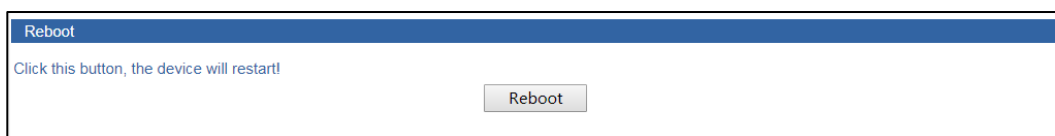
On the "Reboot" page, user can reset the device.

### Operation Path

Open in order: "Main Menu > System management > Reboot".

### Interface Description

Reboot interface as follows:



The main element configuration description of reboot interface:

Interface Element	Description
Reboot	Click the button to reset the device.

## 9.4 Restore Default Setting

### Function Description

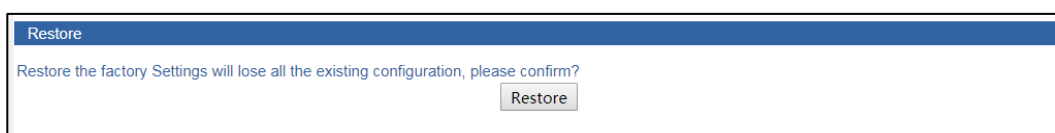
On the "Restore" page, user can restore the device to default setting.

### Operation Path

Open in order: "Main Menu > System management > Restore".

### Interface Description

Restore interface as follows:



The main element configuration description of restore interface:

Interface Element	Description
Restore	Click the button, the device will lose all existing configuration and restore to default setting.

## 9.5 Online Upgrade

### Function Description

On the "Online Upgrade" page, user can update and upgrade the device procedure via TFTP server.

### Operation Path

Open in order: "Main Menu > System management > Online Upgrade".

### Interface Description

Online upgrade interface as follows:

The main element configuration description of online upgrade interface:

Interface Element	Description
Upgrade file path	Name and file format ".bin" of upgrade file where TFTP server is stored.
TFTP server address	TFTP server IP addresses that upgrade file stores.

**Step 1** Online upgrade: place the upgrade file in TFTP server;

Note:

If there is no TFTP server, user can adopt TFTP tool to create server on PC.

**Step 2** In the "Upgrade file path" textbox, enter the upgrade file name and file format ".bin";

**Step 3** In the "TFTP server address" textbox, enter the IP address of TFTP server;

**Step 4** Click "Upload" button;

**Step 5** End.



Note

- Load factory default will cause all configurations to be the factory status, IP address is the static IP address "192.168.1.254".
  - While uploading configuration file, if the static IP in configuration file isn't in the same network segment to the computer IP, the webpage won't be able to open.
  - While uploading configuration file, if dynamic IP is used in the configuration file and there is no DHCP server in the network segment, relative IP portion won't be updated.
-

# The Second Part: Frequently Asked Questions

## 10 FAQ

---

### 10.1 Sign in Problems

- 1. Why the webpage displays abnormally when browsing the configuration via WEB?**

Before access the WEB, please eliminate IE cache buffer and cookies. Otherwise, the webpage will display abnormally.
- 2. How about forgetting the login password?**

For forgetting the login password, the password can be initialized by restoring factory setting, specific method is adopt BlueEyes\_II software to search and use restore factory setting function to initialize the password. Both of the initial user name and password are "admin".
- 3. Is configuring via WEB browser same to configuring via BlueEyes\_II software?**

Both configurations are the same, without conflict.

## 10.2 Configuration Problem

### 1. How to configure the device restore default setting via DIP switch?

Turn the DIP switch 2 to ON position, and restore default setting after power on again.

### 2. Why the bandwidth can't be increased after configure Trunking (port aggregation) function?

Check whether the port attributes set to Trunking are consistent, such as rate, duplex mode, VLAN and other attributes.

### 3. What's the difference between RING V2 and RING V3?

RING V2 and RING V3 are our company's ring patents. RING V2 only supports single ring and coupling ring. RING V3 supports single ring, coupling ring, chain and Dual\_homing, and Hello\_Time can be set to detect port connection status.

### 4. How to deal with the problem that part of switch ports are impassable?

When some ports on the switch are impassable, it may be network cable, network adapter and switch port faults. User can locate the faults via following tests:

- Connected computer and switch ports keep invariant, change other network cable;
- Connected network cable and switch port keep invariant, change other computers;
- Connected network cable and computer keep invariant, change other switch port;
- If the switch port faults are confirmed, please contact supplier for maintenance.

### 5. How about the order of port self-adaption state detection?

The port self-adaption state detection is conducted according to following order: 1000Mbps full duplex, 100Mbps full duplex, 100Mbps half-duplex, 10Mbps full duplex, 10Mbps half-duplex, detect from high to low, connect automatically in supported highest speed.



## 10.3 Alarm Problem

1. **When the device alarms, except BlueEyes\_II software nether alarm information display area will display alarm information, is there any other way to notify technical staffs?**

When the device alarms, the computer buzzer for host monitoring will continue to emit alarm sounds.

## 10.4 Indicator Problem

1. **Power indicator isn't bright, what's the reason?**

Possible reasons include:

- Not connected to the power socket; troubleshooting, connected to the power socket.
- Power supply or indicators faults; troubleshooting, change the power supply or device test.
- Power supply voltage can't meet the device requirements; troubleshooting, configure the power supply voltage according to the device manual.

2. **Link/Act indicator isn't bright, what's the reason?**

Possible reasons include:

- The network cable portion of Ethernet copper port is disconnected or bad contact; troubleshooting, connect the network cable again.
- Ethernet terminal device or network card works abnormally; troubleshooting, eliminate the terminal device fault.
- Not connected to the power socket; troubleshooting, connected to the power socket.
- Interface rate doesn't match the pattern; troubleshooting, examine whether the device transmission speed matches the duplex mode.

3. **Ethernet copper port and fiber port indicator are connected normally, but can't transmit data, what's the reason?**

When the system is power on or network configuration changes, the device and switch configuration in the network will need some time. Troubleshooting, after

the device and switch configuration are completed, Ethernet data can be transmitted; if it's impassable, power off the system, and power on again.

**4. The switch halts after communicate for a period time, and returns to normal after reboot, what's the reason?**

Reasons may include:

- Surrounding environment disturbs the product; troubleshooting, product grounding adopts shielding line or shields the interference source.
- Site wiring is not normative; Troubleshooting, optical fiber, network cable, optical cable cannot be arranged with power line and high-voltage line.
- Network cable is disturbed by static electricity or surge; Troubleshooting, change the shielded cable or install a lightning protector.
- High and low temperature influence; troubleshooting, check the device temperature usage range.

# 11 Maintenance and Service

Since the date of product delivery, our company provides five-year product warranty. According to our company's product specification, during the warranty period, if the product exists any failure or functional operation fails, our company will be free to repair or replace the product. However, the commitments above do not cover damage caused by improper usage, accident, natural disaster, incorrect operation or improper installation.

In order to ensure that consumers benefit from our company's managed switch products, consumers can get help and solutions in the following ways:

- Internet service;
- Call technical support office;
- Product repair or replacement;

## 11.1 Internet Service

More useful information and tips are available via our company website. Website:  
<http://www.3onedata.com>

## 11.2 Service Hotline

Users using our company products can call technical support office. Our company has professional technical engineers to answer the questions and help solve the products or usage problems ASAP. Free service hotline: **+86-400-880-4496**

## 11.3 Product Repair or Replacement

As for the product repair, replacement or return, customers should firstly confirm with the company technical staff, and then contact the company salesmen and solve the problem. According to the company's handling procedure, customers should negotiate with our company's technical staff and salesmen to complete the product maintenance, replacement or return.



## 3onedata Co., Ltd.

Headquarter address: 3/B, Zone 1, Baiwangxin High Technology Industrial Park, Song Bai Road, Nanshan District, Shenzhen

Technology support: [tech-support@3onedata.com](mailto:tech-support@3onedata.com)

Service hotline: +86-400-880-4496

Official Website: <http://www.3onedata.com>