L3 Manage Switch

Web Configuration Manual

(Applicable to DH-PFS6428-24T)

Table of contents

Web Configuration Manual 1

1 Log-in web 4

1.1 System requirements 4
1.2 Login 5

2 System status 6

2.1 System information 6
2.2 Log information 7
2.3 Port statistics 9
2.4 Lacp status 11
2.5 View route 12
2.6 ERPS-Ring status 12
2.7 Power status 13

3 System setting 15

3.1 IP config 15
3.2 User config 15
3.3 Time setting 16

4 Port config 19

4.1 Port config 19
4.2 Rate limit 21
4.3 Port mirroring 22
4.4 Link aggregation 24

5 Advanced config 28

5.1 VLAN config 28
5.2 QinQ config 33
5.3 MAC config 34
5.4 ARP config 35
5.5 MSTP config 37
5.6 IGMP snooping 40
5.7 DHCP server 42
5.8 DHCP relay 45
5.9 DHCP snooping 46
5.10 QoS config 49

5.11 VRRP 51
6 Routing config 55
6.1 Interface config 55
6.2 Static routing 56
6.3 OSPF config 58
6.4 BGP config 62
6.5 RIP config 64
7 Network security 68
7.1 Anti-attack 68
7.2 MAC binding 68
7.3 ARP binding 69
7.4 ACL config 73
7.5 802.1X config 77
7.6 AAA 79
7.7 Port isolation 84
7.8 Storm control 85
7.9 ERPS-Ring config 87
7.10 ERPS-E config 89
7.11 IP source guard 91
8 Network management 95
8.1 HTTP config 95
8.2 SNMP config 96
9 System maintenance 100
9.1 Reboot 100
9.2 Restore factory 101
9.3 Online upgrade 102
9.4 Config management 103
9.5 Ping test 105
10 Diagnosis 106

1 Log-in web

1.1 System requirements

Using the DH-PFS6428-24T switch, the system shall meet the following conditions.

Hardware and software	System requirements
CPU	Pentium 586 above
Memory	128MB above
RP	1024x768 above
Colour	256 colors above
Browser	IE11/Firefox/Chrome/Opera etc
OS	1.Windows XP 2.Windows Vista 3.Windows 7 and above 5.Linux 6.Unix

Note:

Due to compatibility issues,we suggest the use of IE11 browser and Firefox browser.

1.2 Login

To log in to the WEB configuration interface for the DH-PFS6428-24T switch, users need to confirm the following conditions:

- Has the IP configuration of the switch, the default VLAN1 interface IP address is 192.168.1.110.
- To ensure that the local PC (the management host) card of ip address is 192.168.1.* network.
- Guarantee the local PC network cable connected to any one of the ports between 1-24.
- Has installed a Web browser host connected to the network,and the host can PING through the switch.

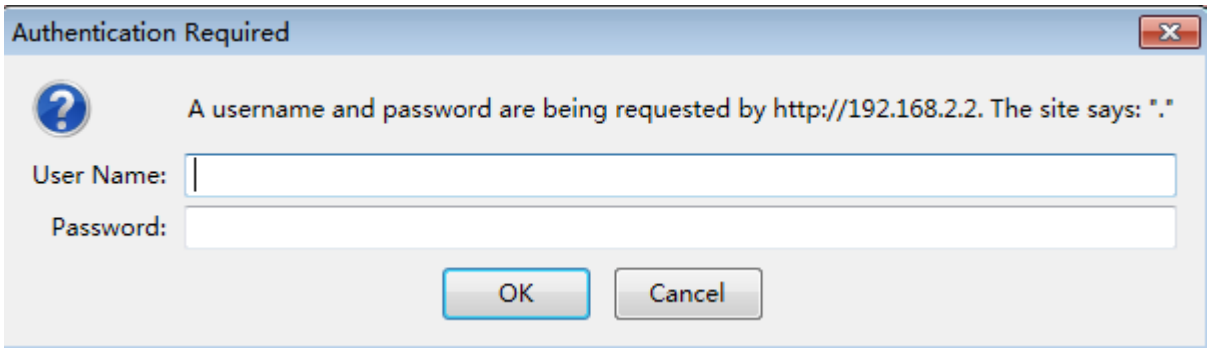
Login WEB configuration interface, the operation steps are as follows:

Step1 Run a computer browser.

Step2 Enter the address of the switch http://192.168.1.110 in the browser, then press the Enter key.

Step3 As shown in Figure 1-1, enter the user name and password in the login window (the default user name and password both are admin), then click"ok".

Figure 1-1 WEB interface login window



After successful login, you can configure the WEB interface related parameters and information as needed.

2 System status

2.1 System info

【Function description】

On the "information system" page , you can view the equipment type、hardware version、firmware version、device serial number and other information.

【Operation path】

System status>system information

【Interface description】

Figure 2-1 system information interface

Product Information	
Equipment Type	DH-PFS6428-24T
Hardware Version	V1.2.0
Firmware Version	V2.0.6-R1
Device Serial Number	A202026221610090
Console Port Baud Rate	115200

System Information	
Device MAC Address	ac-31-9d-16-b5-65
Running Time	0 days, 3 hours, 40 minutes
Current System Time	Fri Apr 29 14:34:27 2016
Software Compilation Time	Mon, 11 Apr 2016 11:00:43 +0800

Table 2-1 Main elements

Interface elements	Description
Equipment type	Display switch product model.
Hardware version	Display the hardware version number for the current use of the switch.
Firmware version	Display the software version number for the current use of the switch.

Device serial number	Display the serial number of the switch
Console port baud rate	Display the baud rate of the switch using Console to manage .
Device MAC address	Display the MAC address of the switch.
Running time	Displays the time of the switch from start up to the present.
Current system time	Display the current time of the system.
Software compilation time	Display software compile time.

2.2 Log info

【Function description】

On the "information log" interface , you can view and download the system log.

【Operation path】

System status > log information

【Interface description】

Figure 2-2-1 View interface

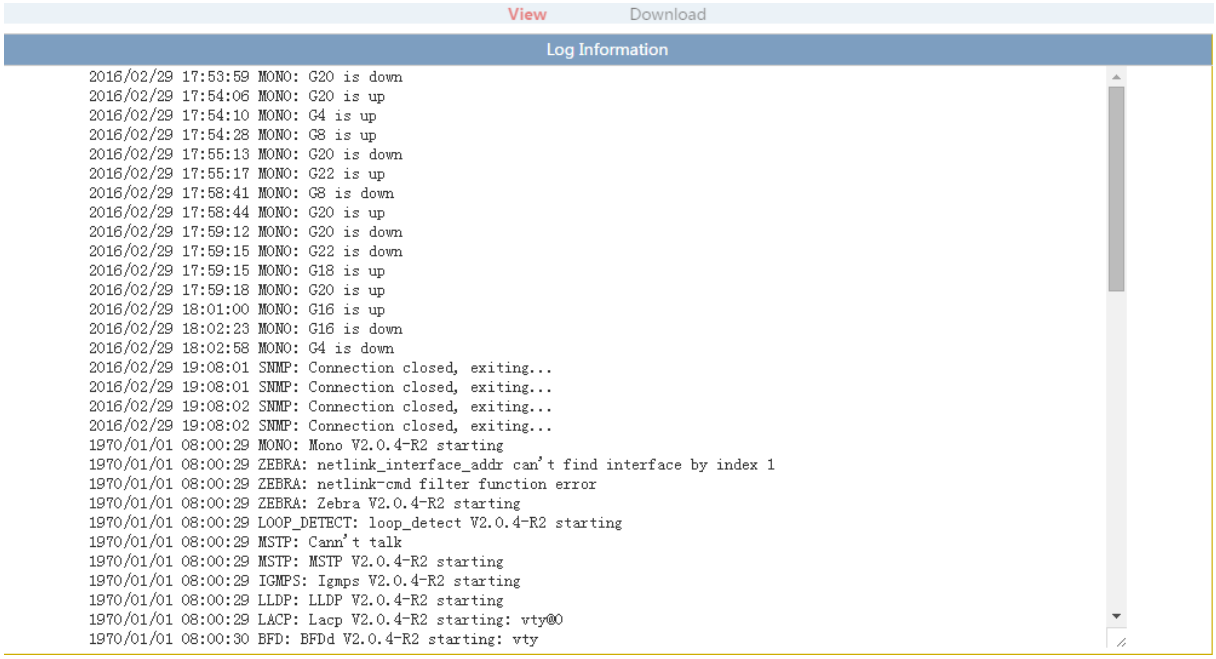


Table 2-2-1 Main elements

Interface elements	Description
Log information	Display the information for the current operation.
Clear	Click "clear" to clear the current system log.
Refresh	Click "Refresh"to refresh the current system log.

Figure 2-2-2 download interface

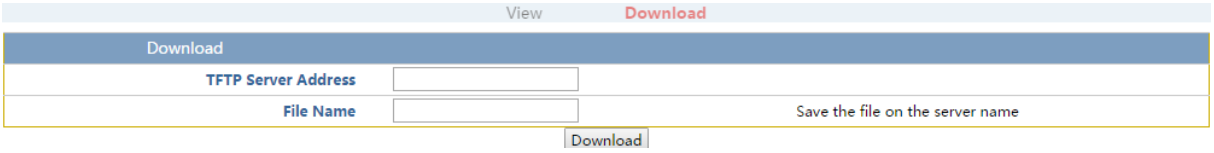


Table 2-2-2 Main elements

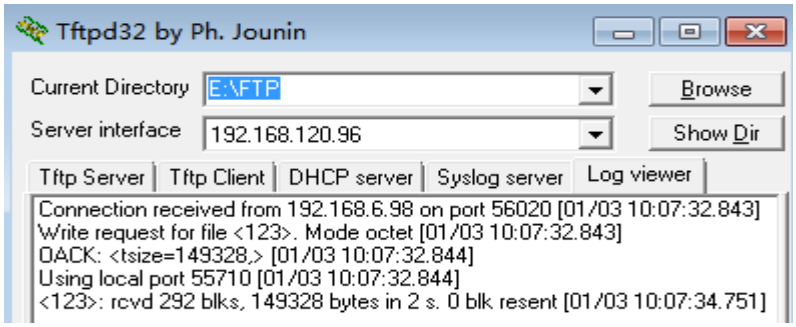
Interface elements	Description
TFTP server address	Enter the IP address of the server.
File name	Enter the name of the log file on the server.
Download	Click "download"to upload the system log to the server.

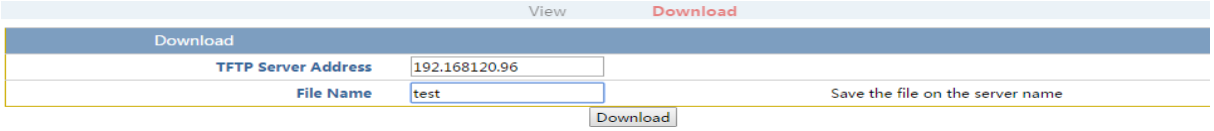
【Example】

1.Open tftp32 software;

2.Enter TFTP server address 192.168.120.96 and the file name in log download interface ;

3.Click the "download" button. As follows:





2.3 Port statistics

【Function description】

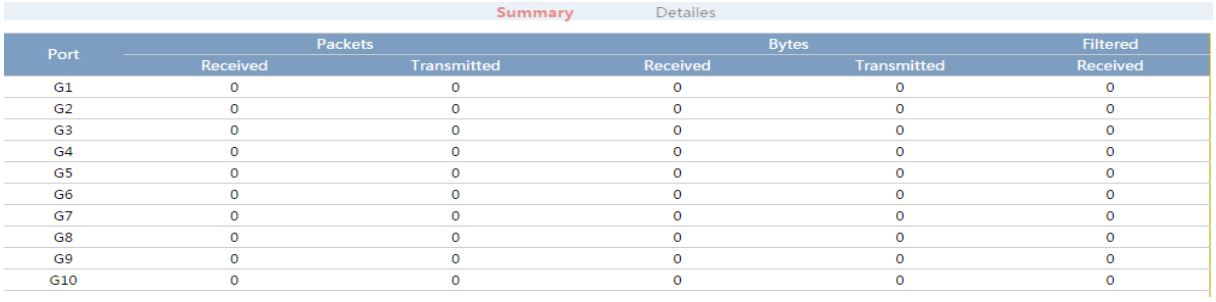
You can view port profile statistics and port details on the " port statistics "page .

【Operation path】

System status > port statistics

【Interface description】

Figure 2-3-1 summary interface



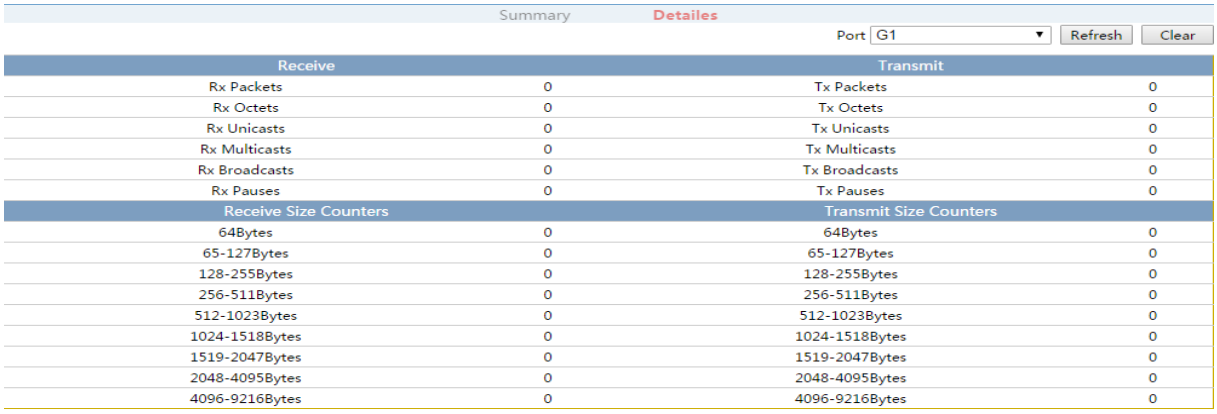
Summary Detailes

Port	Packets		Bytes		Filtered
	Received	Transmitted	Received	Transmitted	Received
G1	0	0	0	0	0
G2	0	0	0	0	0
G3	0	0	0	0	0
G4	0	0	0	0	0
G5	0	0	0	0	0
G6	0	0	0	0	0
G7	0	0	0	0	0
G8	0	0	0	0	0
G9	0	0	0	0	0
G10	0	0	0	0	0

Table 2-3-1 Main elements

Interface elements	Description
Port	Display the port name.
Packets	Display the number of send and received packets.
Bytes	Display the number of sent and received bytes.
Filtered	Display the number of packets to be filtered.

Figure 2-3-2 details interface



Receive		Transmit	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicasts	0	Tx Unicasts	0
Rx Multicasts	0	Tx Multicasts	0
Rx Broadcasts	0	Tx Broadcasts	0
Rx Pauses	0	Tx Pauses	0
Receive Size Counters		**Transmit Size Counters**	
64Bytes	0	64Bytes	0
65-127Bytes	0	65-127Bytes	0
128-255Bytes	0	128-255Bytes	0
256-511Bytes	0	256-511Bytes	0
512-1023Bytes	0	512-1023Bytes	0
1024-1518Bytes	0	1024-1518Bytes	0
1519-2047Bytes	0	1519-2047Bytes	0
2048-4095Bytes	0	2048-4095Bytes	0
4096-9216Bytes	0	4096-9216Bytes	0

Table 2-3-2 Main elements

Interface elements	Description
Port	Click the "port" drop-down list box to choose any one port to view the port details of the statistical information.
Refresh	Click "Refresh" to refresh port details.
Clear	Click "clear" to clear the port details of statistical information.
Receive	Display the number of packets received and bytes, and other related information.
Transmit	Display the number of packets and bytes which sent to the port, and other related information.

Receive Size Counters	Display statistics on the number of bytes received in 64~9216 bytes.
Transmit Size Counters	Display statistics on the number of bytes sent in 64~9216 bytes.

2.4 Lacp status

【Function description】

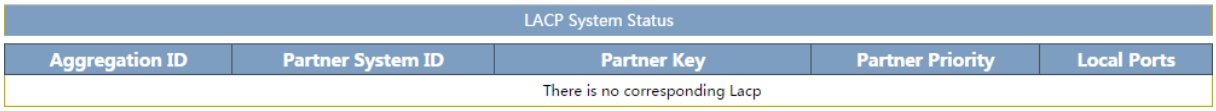
On the "status LACP" page, you can view the status information of the LACP system information.

【Operation path】

System status > lacp status

【Interface description】

Figure2-4 LACP status interface



LACP System Status				
Aggregation ID	Partner System ID	Partner Key	Partner Priority	Local Ports
There is no corresponding Lacp				

Table2-4 LACP Main elements

Interface elements	Description
Aggregation ID	Display the aggregation group ID of settings.
Partner system ID	Display the aggregation group member ID of terminal equipment.
Partner Key	Display the aggregation member key of the terminal device.
Partner Priority	Display the aggregation member priority of the terminal device.
Local Ports	Display the port number of the device that is added to the aggregation group.

2.5 View route

【Function description】

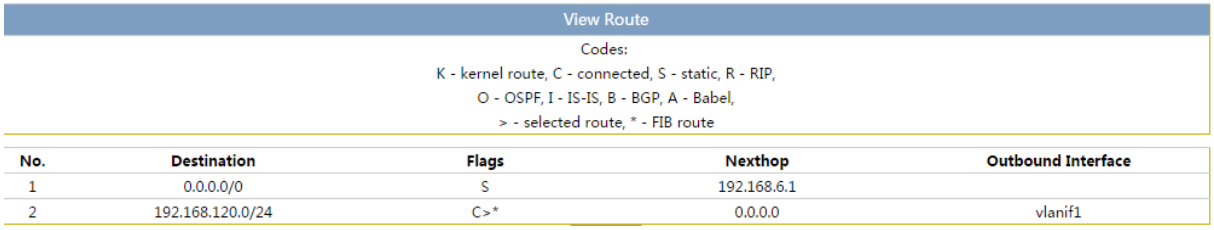
On“view route"page,you can view the router’s related information.

【Operation path】

System status >view route

【Interface description】

Figure2-5 View route interface



View Route

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

No.	Destination	Flags	Nexthop	Outbound Interface
1	0.0.0.0/0	S	192.168.6.1	
2	192.168.120.0/24	C>*	0.0.0.0	vlanif1

Table2-5 Main elements

Interface elements	Description
NO.	Display a number of routes.
Destination	Display destination address.
Flags	Display connection status.
Next hop	Display gateway (next hop).
Outbound interface	Display the name of the L3 interface.

2.6 ERPS-Ring status

【Function description】

On“ERPS-Ring status"page,you can view the ERPS status information.

【Operation path】

System status> erps-ring status

【Interface description】

Figure2-6 ERPS-Ring status interface

ERPS Status

Port	Action	Transmission Packets	Port Status	Loop
G1	Discarded Packets	Disabled	Down	-
G2	Discarded Packets	Disabled	Down	-
G3	Discarded Packets	Disabled	Down	-
G4	Discarded Packets	Disabled	Down	-
G5	Discarded Packets	Disabled	Down	-
G6	Discarded Packets	Disabled	Down	-
G7	Discarded Packets	Disabled	Down	-
G8	Discarded Packets	Disabled	Down	-
G9	Discarded Packets	Disabled	Down	-
G10	Discarded Packets	Disabled	Down	-
G11	Discarded Packets	Disabled	Down	-
G12	Discarded Packets	Disabled	Down	-

Table2-6 Main elements

Interface elements	Description
Port	Display the corresponding port number of the switch .
Action	Display the action performed of ports.
Transmission packets	Displays messages that allow or prohibit the transmission of ports.
Port status	Display port status is "up" or "down".
Loop	Display Loop information of ports.

2.7 Power status

【Function description】

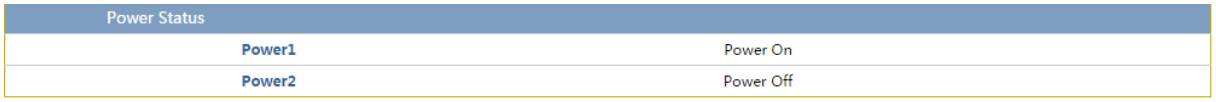
On"power status"page, you can view the status information of the power supply.

【Operation path】

System status>power status

【Interface description】

Figure2-7 power status interface



Power Status	
Power1	Power On
Power2	Power Off

Table2-7 Main elements

Interface elements	Description
Power1	Display the working state of power supply 1
Power2	Display the working state of power supply 2

3 System setting

3.1 IP config

【Function description】

On the IP configuration interface,you can configure the management IP address of the switch.

【Operation path】

System setting >ip config

【Interface description】

Figure3-1 IP config interface

Table3-1 Main elements

Interface elements	Description
IP address	Administrator IP address can be modified.

3.2 User config

【Function description】

On“user config"page,you can configure the user name, password, and permissions on the WEB interface of the login switch.

【Operating path】

System setting > user config

【Interface description】

Figure3-2 user config interface

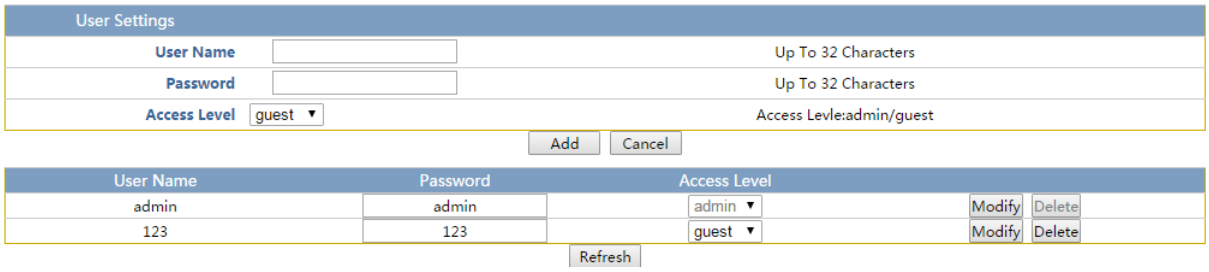


Table3-2 Main elements

Interface elements	Description
User name	The login switch WEB interface user name can be configured.
Password	The login switch WEB interface password can be configured.
Access level	The login switch WEB interface access level can be configured. 1.guest,2.admin.
Modify	Click "modify" to modify the user information which you configure.
Delete	Click "delete" to delete the user information which you configure.

3.3 Time setting

【Function description】

On“time setting"page,you can configure the NTP server address, so that the switch system time synchronization with the server. You can manually configure the current time.

【Operating path】

System setting > time setting

【Interface description】

Figure3-3-1 NTP config interface

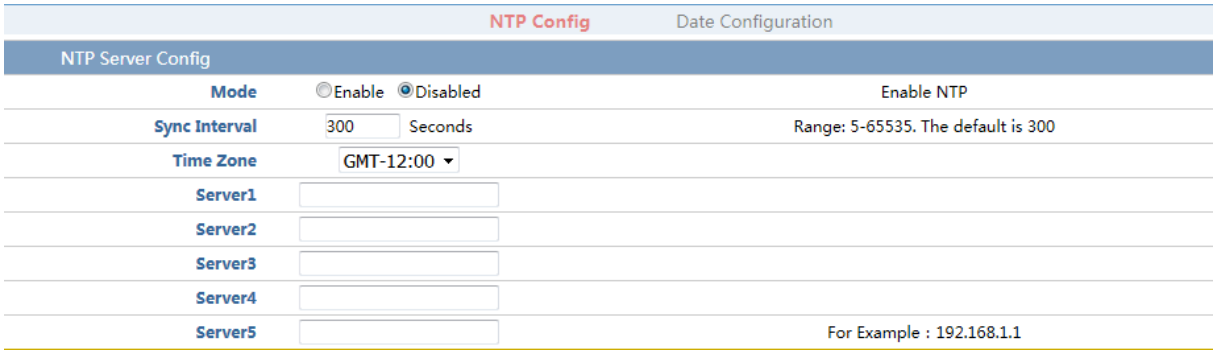


Table3-3-1 Main elements

Interface elements	Description
Mode	Function enable or disable
Enable	Select "enable", which indicates that the NTP function is enabled.
Disabled	Select "disable", which indicates that the NTP function is disabled.
Sync interval	The time interval between the switch and the NTP server.
Time zone	Select the time zone from the drop-down list.
Server	Allows up to 5 NTP server address can be configured .

Figure3-3-2 date configuration interface

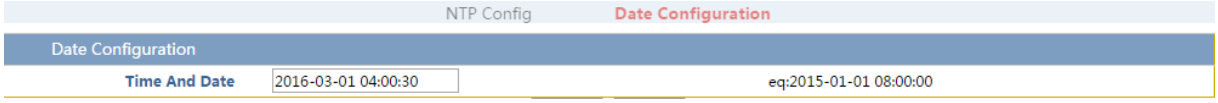
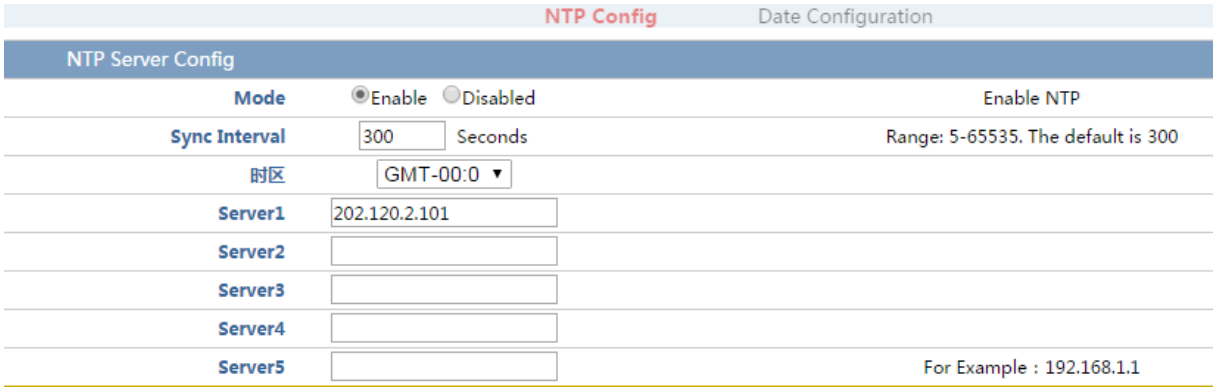


Table3-3-2 Main elements

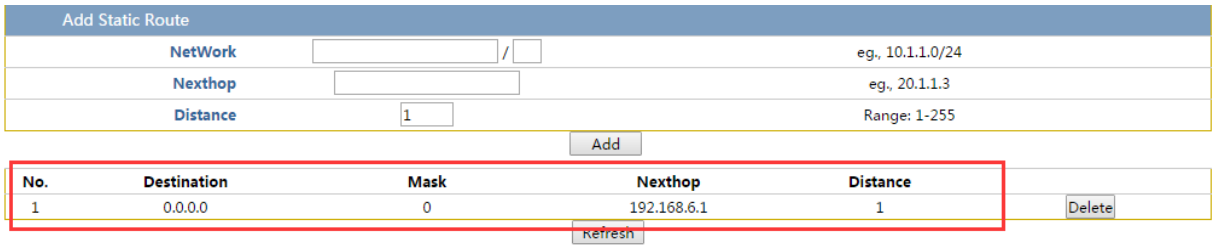
Interface elements	Description
Time and date	Set local time and date.

【Example】

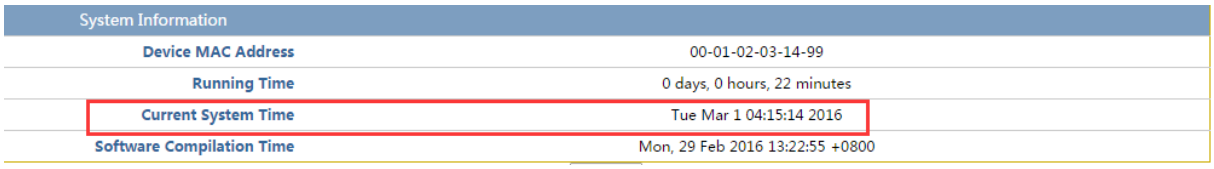
1.Enable NTP server,you can view the time interval default is 300s and the time zone set to 00:00 London time, then add NTP server 202.120.2.101 ,as shown in the following figure:



2.Set a route ,as shown in the following figure:



3.It can be seen in time to London time on the system information page,as shown in the following figure:



Tips:If the time doesn't change:

1. Please make sure that the switch is connected to the network (Routing is a path or not);

2. Please reboot the switch.

4 Port config

4.1 Port config

【Function description】

On“Port config"page,you can enable or disable ports, set port rates and flow control, or view the basic information of all ports.

【Operating path】

Port config > port config

【Interface description】

Figure4-1 Port config interface

Port	Port Description	Status	Media	Speed/Duplex	Speed	Duplex	Flow Control Config	Flow Control Status	Enable
*	-	-	-	<>	-	-	☑	-	☑
G1		DOWN	RJ45	1000M Full	1G	FULL	☑	✓	☑
G2		DOWN	RJ45	1000M Full	1G	FULL	☑	✓	☑
G3		DOWN	RJ45	1000M Full	1G	FULL	☑	✓	☑
G4		DOWN	RJ45	1000M Full	1G	FULL	☑	✓	☑
G5		DOWN	RJ45	1000M Full	1G	FULL	☑	✓	☑
G6		DOWN	RJ45	1000M Full	1G	FULL	☑	✓	☑
G7		DOWN	RJ45	1000M Full	1G	FULL	☑	✓	☑
G8		DOWN	RJ45	1000M Full	1G	FULL	☑	✓	☑
G9		DOWN	RJ45	1000M Full	1G	FULL	☑	✓	☑
G10		DOWN	RJ45	1000M Full	1G	FULL	☑	✓	☑
G11		DOWN	RJ45	1000M Full	1G	FULL	☑	✓	☑

Table4-1 Main elements

Interface elements	Description
Port	Display the port name.
Port description	Configure port description information (only including numbers, case letters and underscores).
Status	Display the port status.
Media	Display the port medium.
Speed/Duplex	Configure port rate and duplex mode.
Speed	Display the port rate.
Duplex	Display the port whether supports duplex mode.
Flow control config	Select the flow control configuration check box ,then enable port flow control function.
Flow control status	Display the port flow control state.(" ✕ " the state indicates that the port flow control function is not enabled or the port is not currently in place," ✓ " the state indicates that port flow control is in effect, it can normally send or receive pause frames)
Enable	Select the "enable" check box, then enable the corresponding port. Default enable.

【Example】

Port 1 and port 2 are described as T1, T2, selection rate for 100M full duplex and full duplex 1000M, open flow control,as shown in the following figure:

Port	Port Description	Status	Media	Speed/Duplex	Speed	Duplex	Flow Control Config	Flow Control Status	Enable
*	-	-	-	<>	-	-	☑	-	☑
G1	T1	DOWN	RJ45	100M Full	100M	FULL	☑	✓	☑
G2	T2	DOWN	RJ45	1000M Full	1G	FULL	☑	✓	☑
G3		DOWN	RJ45	Auto	1G	AUTO	☑	✓	☑
G4		DOWN	RJ45	Auto	1G	AUTO	☑	✓	☑
G5		DOWN	RJ45	Auto	1G	AUTO	☑	✓	☑

4.2 Rate limit

【Function description】

On“rate limit"page,you can configure egress rate and ingress rate of all ports.

【Operating path】

Port config > rate limit

【Interface description】

Figure4-2 rate limit interface

Port	Ingress Rate(kbps) (Range:0-10000000)	Egress Rate(kbps) (Range:0-10000000)
*	0	0
G1	0	0
G2	0	0
G3	0	0
G4	0	0
G5	0	0
G6	0	0
G7	0	0
G8	0	0
G9	0	0
G10	0	0
G11	0	0
G12	0	0
G13	0	0
G14	0	0

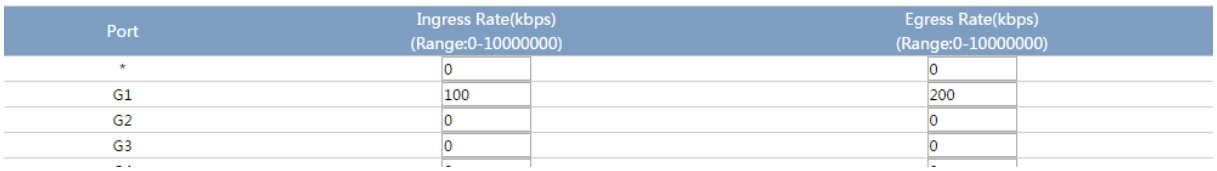
Table4-2 Main elements

Interface elements	Description
Port	Display the port name.
Ingress rate	Configure corresponding port ingress rate.

Egress rate	Configure corresponding port egress rate.

【Example】

In the port speed limit configuration page,set port 1 ingress rate is 100Kbps and the egress rate is 200Kbps,as shown in the following figure:



Port	Ingress Rate(kbps) (Range:0-10000000)	Egress Rate(kbps) (Range:0-10000000)
*	0	0
G1	100	200
G2	0	0
G3	0	0

4.3 Port mirroring

【Function description】

Port mirroring is also called port monitoring. Port monitoring is a data packet acquisition technology. It can be configured on a switch to copy data packets from one or more ports (mirror source ports) to a specified port (mirror destination port). The destination port is connected to a host installed with the packet analysis software. The software analyzes the collected packets to implement network monitoring and eliminating network faults.

【Operating path】

Port config > port mirroring

【Interface description】

Figure4-3 port mirroring interface

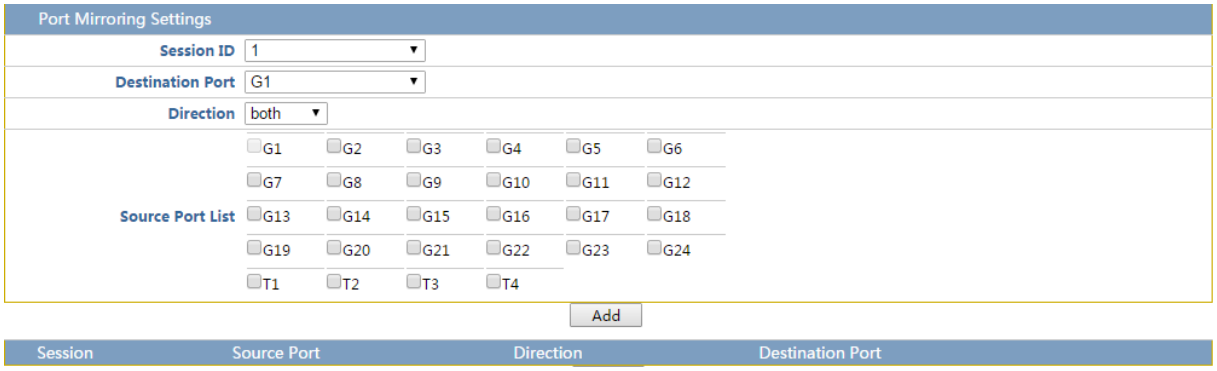
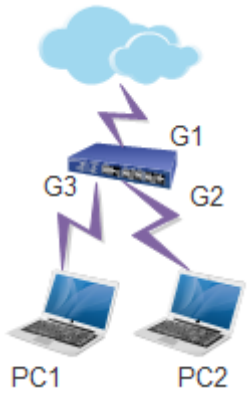
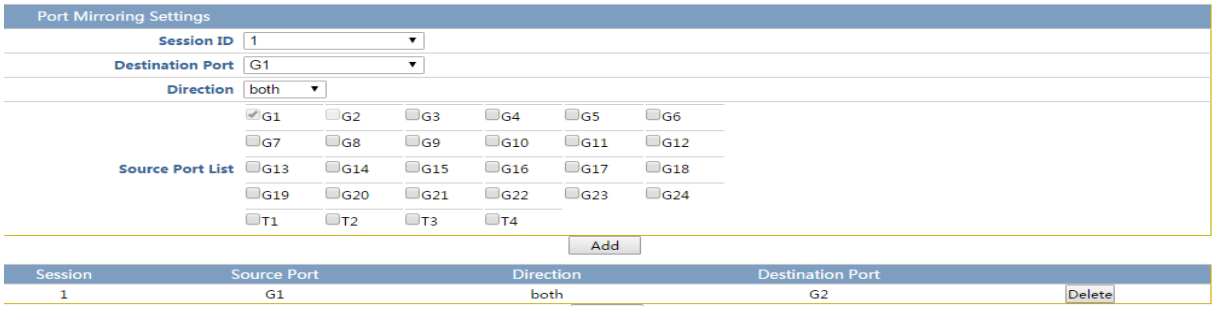


Table4-3 Main elements

Interface elements	Description
Session ID	Select the mirror session ID, up to 4, the range of 1-4.
Destination Port	Select the destination port of the mirror, it can only choose one.
Direction	Selection of monitoring inflows or outflows, inflows and outflows of image source port data stream, including egress, ingress and both three options egress:the data packet received by the switch port. ingress:the data packet sent by the switch port. both:the data packet received and sent by the switch port.
Source port list	Select mirror source port,you can have multiple choices.

【Example】





Set the source port and destination port are G1 and G2 respectively,capture in the G2,you can catch G1 related data package.

4.4 Link aggregation

【Function description】

In link aggregation, multiple physical ports of a switch are aggregated into one logical port. Multiple links in the same aggregation group can be treated as a logical link with higher bandwidth.

With link aggregation, communication traffic can be shared among member ports of an aggregation group to increase the bandwidth. In addition, member ports in the same aggregation group serve as dynamic backup for each other, which improves the link reliability.

Member ports in the same aggregation group must have consistent configurations, which include the STP, QoS, VLAN, port attributes, MAC address learning, ERPS configuration, loop protection configuration, mirror, 802.1x, IP filtering, MAC filtering, and port isolation. Tip: If a port is used for link aggregation, port parameters and other software functions should not be configured for this port.

Link aggregation is divided into static aggregation and dynamic aggregation (LACP). The peer device that participates in link aggregation of a switch is generally another switch or a network adapter.

4.4.1 Static aggregation

【Function description】

Static aggregation must be manually configured. Ports in an aggregation group cannot be automatically added or deleted by the system. The logic of static aggregation configuration is simple and is easy to understand and use.

【Operating path】

Port config > link aggregation

【Interface description】

Figure4-4-1 Aggregation interface

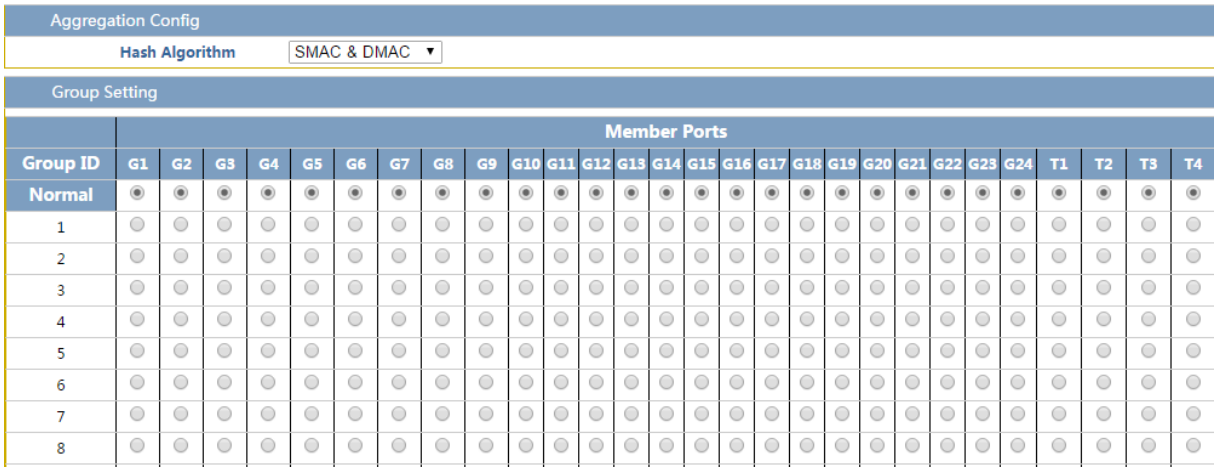


Table4-4-1Main elements

Interface elements	Description
Hash algorithm	Load balancing mode for selecting data stream. There are three kinds of: Source MAC Destination MAC SMAC&DMAC
Member ports	Select the port to be grouped into groups. The switch was created all groups by default, but port member is empty. To configure the member ports for the aggregation group, point to the corresponding aggregation group, you can achieve the port to join the aggregation group.

Tip:

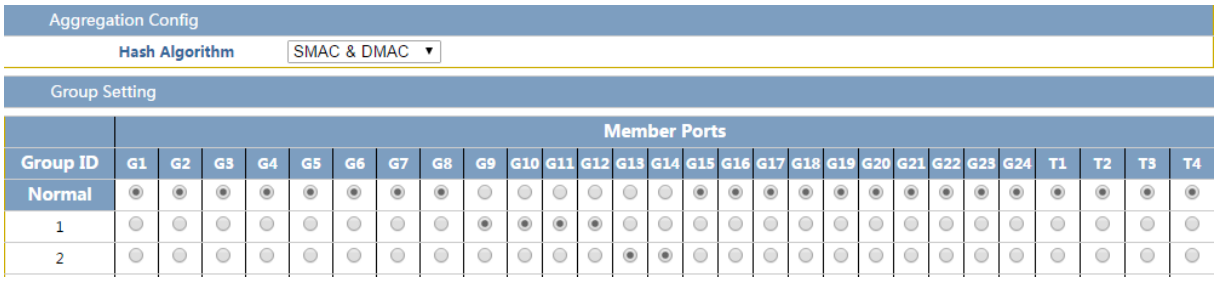
On the same port, only one type of aggregation (either static aggregation or dynamic lacp aggregation) can be configured.

Configurations of member ports in the same aggregation group must be consistent.

An aggregation group can contain two to eight member ports.

【Example】

Set the load balancing mode to SMAC&DMAC, and add ports 9 to 12 to aggregation group 1 and ports 13 to 14 to aggregation group 2, as shown in the following figure.



4.4.2 LACP config

【Function description】

Link Aggregation Control Protocol (LACP) implements dynamic aggregation and deaggregation of links based on the IEEE 802.3ad standard. Two aggregation devices exchange aggregation information through LACP data units (LACPDUs) to bundle matched links for data transmission. Addition or deletion of ports to/from an aggregation group is automatically completed by the protocol, which features good flexibility and provides the capability of load balancing.

After LACP is enabled on a port, the port notifies its peer of the following information about the local port: system priority, system MAC address, port priority, port number, and operation key (determined by the physical attribute, upper-layer protocol information, and management key of the port),port priority.

The end with a higher device priority takes the lead in aggregation or deaggregation. The device priority is determined by the system priority and system MAC address. A smaller value of the system priority indicates a higher device priority. If the system priorities are the same, the device with a smaller system MAC address has a higher device priority. The end with a higher device priority selects ports for aggregation based on the port priority, port number, and operation key. Only ports with the same operation key can be added to the same aggregation group. In an aggregation group, the port with a smaller port priority value will be preferentially selected. If the port priorities are the same, the port with a smaller port number will be preferentially selected. After two ends exchange the aggregation information, the selected ports will be aggregated to send or receive data.

【Operating path】

Port config > link aggregation

【Interface description】

Figure 4-4-2 LACP config interface

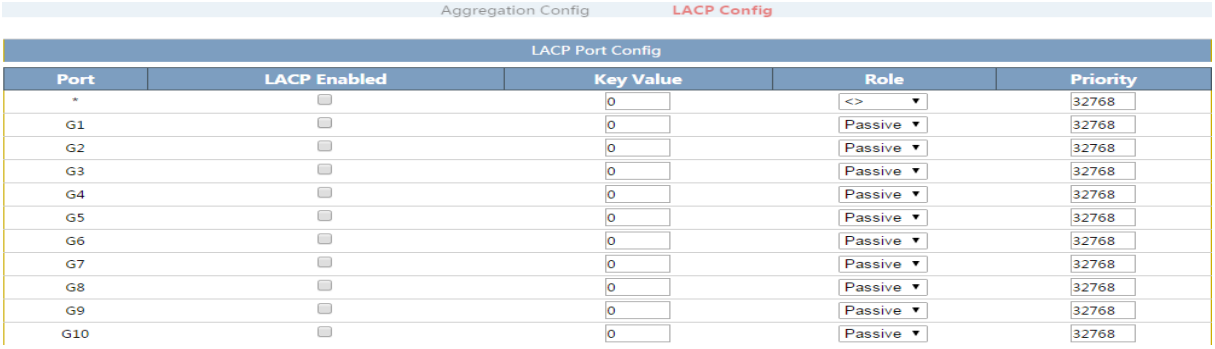
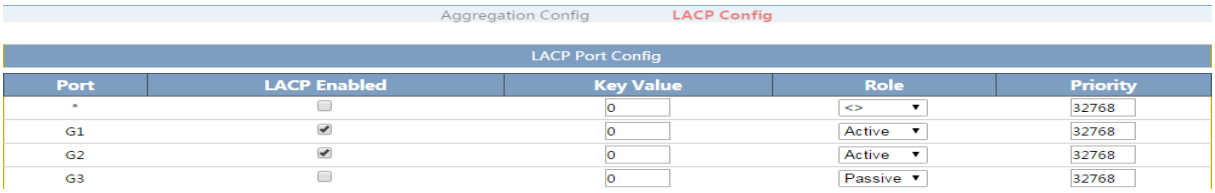


Table4-4-2 Main elements

Interface elements	Description
Port	Display the port number of the switch.
LACP Enabled	Enable or disable LACP ports.
Key value	Members of the same group, need to configure the same management Key (manual configuration, a llowable value range 1-65535), the default is 0.
Role	Configure port role information. Optional: Active and Passive. Participate in dynamic aggregation of the device at one end to choose Active mode and the other end to choose Passive mode.Default is passive.
Priority	Configuring LACP port priority. Default is 32768.

【Example】

Set G1 and G2 LACP Enabled.role selection:active, other default.On the end of the switch to select 2 ports enabled LACP too, other default.G1,G2 and the ports which enabled LACP on the end of the switch are connected..as shown in the following figure:



5 Advanced config

5.1 VLAN config

【Function description】

Ethernet is a shared communication media based on the Carrier Sense Multiple Access/Collision Detect (CSMA/CD) technology. A LAN built using the Ethernet technology is not only a collision domain, but also a broadcast domain. When the number of hosts on the network is large, the collision becomes serious, broadcast flooding occurs, and the performance is significantly degraded. Even worse, the network is unavailable. Deployment of bridges or L2 switches on the Ethernet can resolve the problem of serous collision, but still cannot isolate broadcast packets. To address this issue, the Virtual Local Area Network (VLAN) technology emerges. This technology can divide a physical LAN into multiple logical LANs, that is, VLANs. Hosts located in the same VLAN can directly communicate with each other, but hosts located in different VLANs cannot communicate with each other. In this way, broadcast packets are confined in the same VLAN. That is, each VLAN is a broadcast domain.

Advantages of VLAN are as follows:

Improve network performance. Broadcast packets are confined in the VLAN, which effectively controls broadcast storms of the network, saves the network bandwidth, and improves the network processing capability.

Enhance network security. Devices in different VLANs cannot access each other, and hosts in different VLANs cannot directly communicate with each other. Packets must be forwarded at L3 through network layer devices, such as routers or L3 switches.

Simplify network management. Hosts in the same virtual work group are not limited to a certain physical range, which simplifies network management, and makes it convenient for people in different areas to set up work groups.

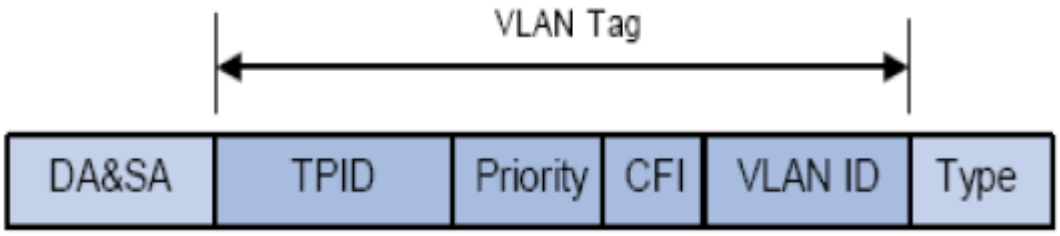
Division of VLANs is not restricted by physical locations. Hosts in different physical locations may belong to the same VLAN. Users of one VLAN can connect to the same switch or different switches. This switch supports the 802.1Q VLAN, MAC-based VLAN, IP Subnet-based VLAN, and protocol VLAN. The protocol VLAN is effective only for untagged packets and packets with the priority tag. When a packet meets the requirements of the 802.1Q VLAN, MAC-based VLAN, IP subnet-based VLAN, and protocol VLAN, the switch will process the packet in the following order: MAC-based VLAN, IP subnet-based VLAN, protocol VLAN, and Port VLAN ID (PVID), and forward this packet in the corresponding

VLAN.

802.1Q VLAN:

A common switch works at the data link layer of the OSI model. To enable the switch to identify packets of different VLANs, the data link layer of the packets must be encapsulated. Therefore, the VLAN tag field is added to the data link layer encapsulation.

To standardize the VLAN implementation solution, the structure of packets with the VLAN tag is defined in IEEE 802.1Q. According to the protocol, a 4-byte VLAN tag is encapsulated after the source and destination MAC addresses to identify the VLAN-related information. The VLAN tag contains four fields, including the Tag Protocol Identifier (TPID), Priority, Canonical Format Indicator (CFI), and VLAN ID, as shown in the following figure.



TPID:

This field indicates that the data frame contains the VLAN tag. It is a 16-bit field. According to the protocol, the default value of TPID is **0x8100**.

Priority:

This field indicates the transmission priority of the packet.

CFI:

On an Ethernet switch, CFI is always set to **0**. Due to the compatibility feature, CFI is often used between the Ethernet and token ring networks. If CFI of a frame received on an Ethernet port is set to 1, the frame is not forwarded because this Ethernet port is an untagged port.

VLAN ID:

This field identifies the ID of the VLAN to which the packet belongs. It is a 12-bit field. The value ranges from 0 to 4095. As 0 and 4095 are reserved values and generally not assigned to users, the VLAN ID generally ranges from 1 to 4094. The VLAN ID is abbreviated as VID.

A switch uses the VLAN ID to identify the VLAN to which a packet belongs. If a received packet does not contain a VLAN tag, the switch encapsulates the default VLAN ID of the receive port in the packet, and transmits the packet in the default VLAN of the receive

port.

In this manual, a packet that contains the VLAN tag field is called tagged frame, and a packet that does not contain the VLAN tag field is called untagged frame. A frame with the priority tag refers to a packet that contains the VLAN tag field, but the VLAN ID is 0.

Three link types of a port:

When creating a 802.1Q VLAN, you need to configure the link type of a port based on the device connected to the port. Three links types of a port are available:

Access: A port can belong to only one VLAN. The rule for sending packets over a port is UNTAG. An access port is often connected to a user terminal. When an access port is added to another VLAN, it automatically exits from the original VLAN.

Trunk: A trunk port allows packets of multiple VLANs to pass through, and can receive or send packets of multiple VLANs. It is often used for cascading of network devices. A VLAN often spans different switches on the network. For a trunk port, the default rule for sending packets over a port is TAG. When default VLAN data of the port is forwarded, the VLAN information is removed; when other types of VLAN data is forwarded, the VLAN information is retained.

Hybrid: A hybrid port allows packets of multiple VLANs to pass through, and can receive or send packets of multiple VLANs. It is often used for connection between network devices or connection with user devices. The rule for sending packets over a hybrid port can be flexibly configured based on the device connected to the port.

Processing relationship between the PVID and VLAN packets:

PVID is the default VLAN ID of a port. When a packet received on a port of a switch does not contain the VLAN tag, the switch inserts a VLAN tag to the packet based on the PVID value of the receive port, and then forwards the packet.

When VLANs are divided in a LAN, the PVID is an important parameter for each port. It indicates the VLAN to which the port belongs by default. Two functions of the PVID are as follows:

When an untagged packet is received on a port, the switch inserts a VLAN tag to the packet based on the PVID.

The PVID specifies the default broadcast domain of a port. That is, when a UL or broadcast packet is received on a port, the switch broadcasts this packet in the default VLAN of the port.

You configure the IEEE802.1Q VLAN on three interface s, including the VLAN configuration, VLAN status, and VLAN port configuration interface s.

【Operating path】

Advanced config> vlan config

【Interface description】

Figure5-1-1 VLAN config interface

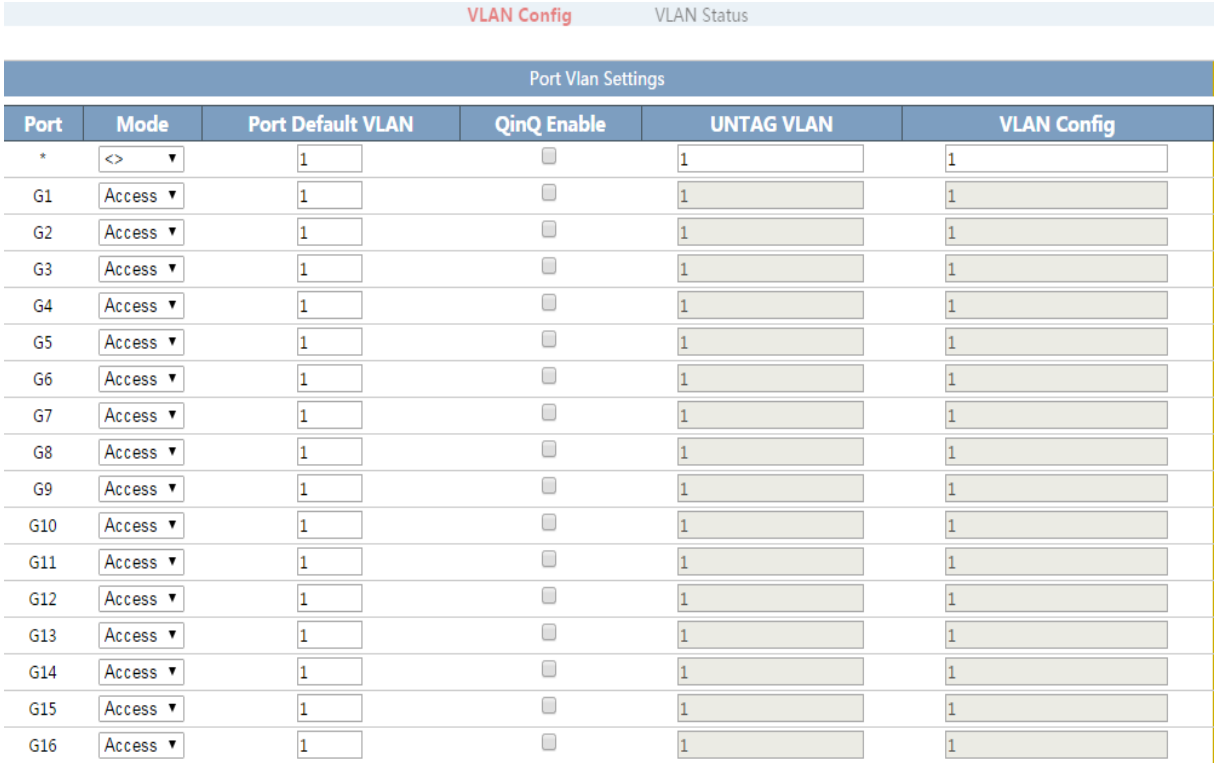


Table5-1-1 Main elements

Interface elements	Description
Port	Display port name.
Mode	configure port mode:Access/Trunk/Hybrid
QinQ enable	Configure port QinQ enable/disable
Port default VLAN	Enter the ID value,set port PVID value.
UNTAG VLAN	Configure VLAN export labels:tag/untag.

VLAN config	Enter the VLAN ID(1-4094),configure the VLAN that belongs to this port.

Figure5-1-2 VLAN status interface

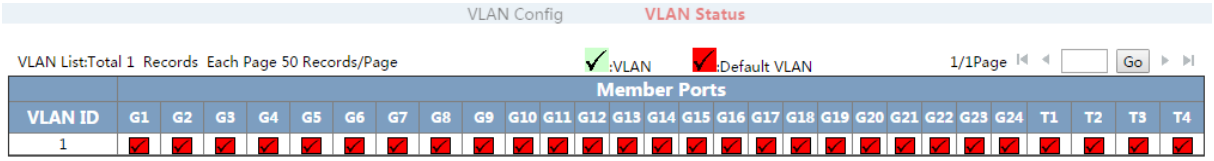
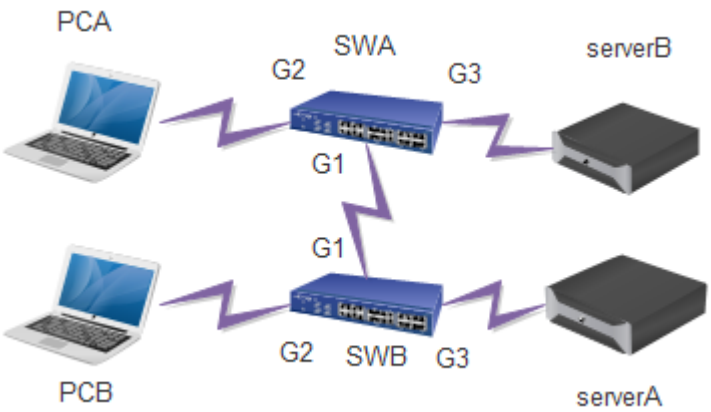


Table5-1-2 Main elements

Interface elements	Description
Member ports	Display all port VLAN information.

【Example】



Networking requirement: Switch A is connected to PC A and server B. Switch B is connected to server A and PC B. PC A and server A belong to one department, and PC B and server B belong to another department. Two VLANs are defined respectively for the two departments, and the two departments cannot communicate with each other.

Step 1:

Configure switch A as follows: Add the port G3 to VLAN 3, and set the port type to Access. Add the port G2 to VLAN 2, and set the port type to Access. Add the port G1 to VLANs 1–3, and set the PVID to 1, port type to Trunk, and Egress Tagging to Tag All. The following figure shows the configuration results.

VLAN配置 VLAN状态

端口Vlan设置

端口	模式	端口默认VLAN	QinQ 使能	UNTAG VLAN	VLAN配置
*	<>	1		1	1-3
G1	Trunk	1		1	1-3
G2	Access	2		2	2
G3	Access	3		3	3

Step 2:

Configure switch B as follows: Add the port G3 to VLAN 2, and set the port type to Access. Add the port G2 to VLAN 3, and set the port type to Access. Add the port G1 to VLANs 1–3, and set the PVID to 1, port type to Trunk, and Egress Tagging to Tag All. The following figure shows the configuration result.

VLAN配置 VLAN状态

端口Vlan设置

端口	模式	端口默认VLAN	QinQ 使能	UNTAG VLAN	VLAN配置
*	<>	1		1	1-3
G1	Trunk	1		1	1-3
G2	Access	3		3	3
G3	Access	2		2	2
G4	Access	1		1	1
G5	Access	1		1	1

5.2 QinQ config

【Function description】

QinQ Technology (also known as Stacked VLAN or double VLAN) is refers to the user on private network VLAN tag package in the public network VLAN tag so that packets with two layer VLAN tag through the backbone network operators, in public only according to the spread of the outer VLAN tag, private network VLAN tag is blocked, so that not only logarithmically with the according to flow were distinguished and transparent transmission due to private network VLAN tag, different users' VLAN tag can repeated use, only the outer VLAN label can only in the public network, actually it also expanded the use of VLAN tag number.

【Operating path】

Advanced config > QinQ config

【Interface description】

Figure5-2 QinQ config interface

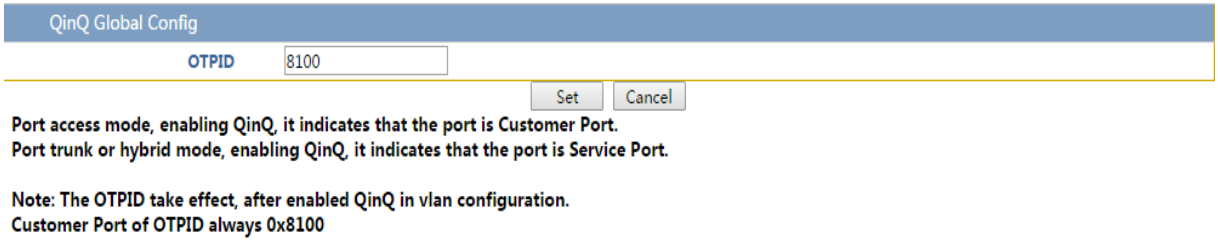
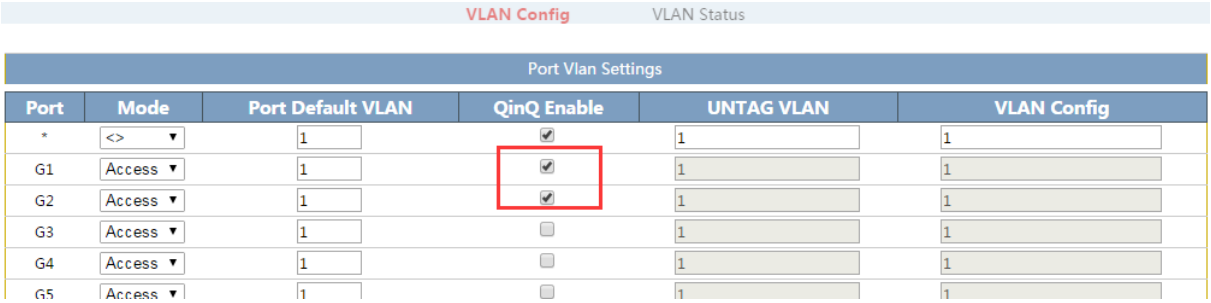


Table5-2 Main elements

Interface elements	Description
OTPID	Set the outer tag protocol ID.Default is 8100.It can be set to be compatible with other devices' TPID, such as TPID 88a8.

【Example】

1.On VLAN config page,enable QinQ function of port1 and port2,pvid=1,the default of OTPID is 8100. Injection packets of tag=2 on the port1 , capture on port 2,you can catch packets of tag=2.



5.3 MAC config

【Function description】

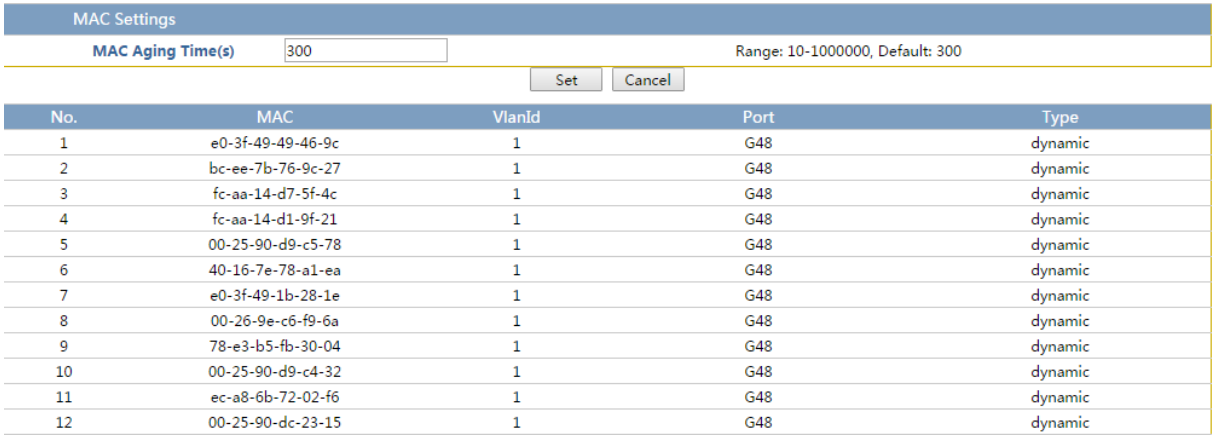
On"MAC config"page,you can configure the aging time of the MAC address and view the port's MAC address information.

【Operating path】

Advanced config > mac config

【Interface description】

Figure5-3 MAC config interface



No.	MAC	VlanId	Port	Type
1	e0-3f-49-49-46-9c	1	G48	dynamic
2	bc-ee-7b-76-9c-27	1	G48	dynamic
3	fc-aa-14-d7-5f-4c	1	G48	dynamic
4	fc-aa-14-d1-9f-21	1	G48	dynamic
5	00-25-90-d9-c5-78	1	G48	dynamic
6	40-16-7e-78-a1-ea	1	G48	dynamic
7	e0-3f-49-1b-28-1e	1	G48	dynamic
8	00-26-9e-c6-f9-6a	1	G48	dynamic
9	78-e3-b5-fb-30-04	1	G48	dynamic
10	00-25-90-d9-c4-32	1	G48	dynamic
11	ec-a8-6b-72-02-f6	1	G48	dynamic
12	00-25-90-dc-23-15	1	G48	dynamic

Table5-3 Main elements

Interface elements	Description
MAC aging time	Set the MAC aging time, the value range is 10-1000000s. Default is 300s.

5.4 ARP config

【Function description】

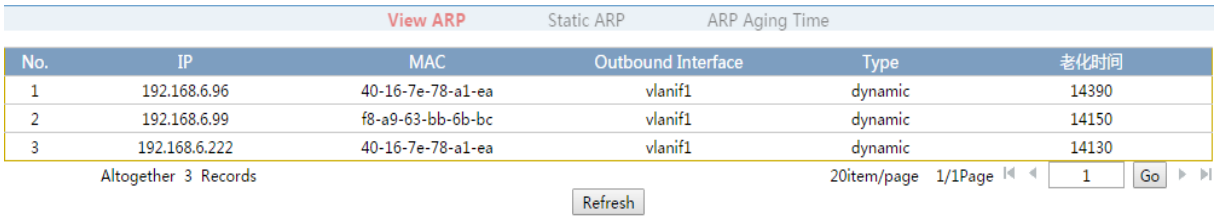
On ARP config page,you can configure the ARP aging time or static binding IP+MAC, one of IP or MAC is different from the IP or MAC in the binding entry, cannot access CPU,but can be forwarded. IP and MAC are different or the same can be accessed CPU, also can be forwarded.

【Operating path】

Advanced config > arp config

【Interface description】

Figure5-1-1 view ARP interface



No.	IP	MAC	Outbound Interface	Type	老化时间
1	192.168.6.96	40-16-7e-78-a1-ea	vlanif1	dynamic	14390
2	192.168.6.99	f8-a9-63-bb-6b-bc	vlanif1	dynamic	14150
3	192.168.6.222	40-16-7e-78-a1-ea	vlanif1	dynamic	14130

Table5-4-1 Main elements

Interface elements	Description
NO.	Display entry number.
IP	IP address of arp entry.
MAC	MAC address of arp entry.
Outbound interface	Display bound virtual interface.
Type	Display that the arp entry is dynamic or static.
Aging time	Display arp aging time, the default is 14400s.

Figure5-2-2 Static ARP interface

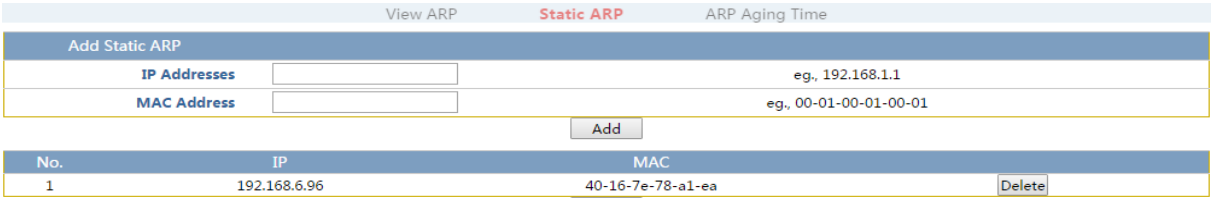


Table5-4-2 Main elements

Interface elements	Description
IP Address	Configure the IP address that needs to be bound.
MAC Address	Configure the MAC address that needs to be bound.

Figure5-3-3 ARP aging time interface

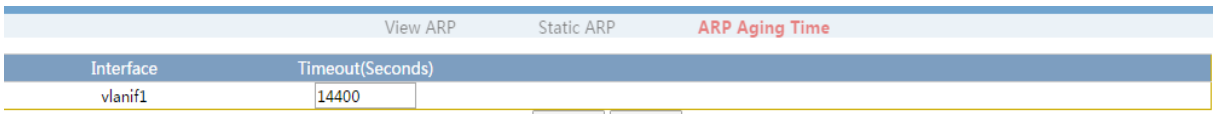
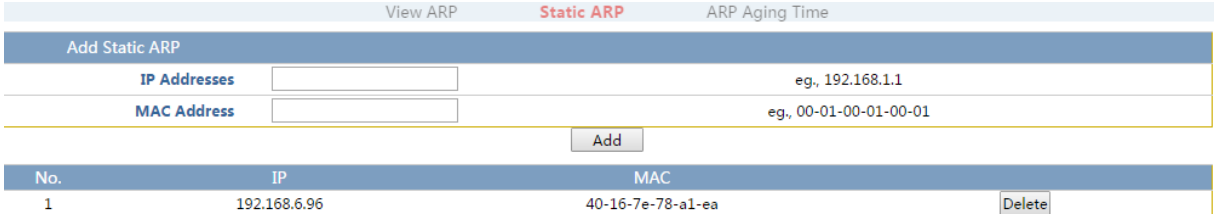


Table5-4-3 Main elements

Interface elements	Description
Interface	Display ARP aging time of corresponding to the interface.

Timeout(s)	Configure ARP aging time,default is 14400s.rang is 60-86400s

【Example】



After Binding PCA's MAC and IP, PCA can ping through SWB, it can also Ping through PCB. Modify PCA's IP for non 192.168.6.96, then you can not Ping through SWB, but you can access the PCB.

5.5 MSTP config

【Function description】

STP is developed based on IEEE 802.1D, and is a protocol used to eliminate physical loops at the data link layer in the LAN. STP-enabled devices exchange information to detect loops on the network, and selectively block some ports to change a loop topology into a loop-free tree topology. This prevents continuous growing and infinite loop of packets on the loop network, and prevents occurrence of problems such as degraded packet processing capability of devices caused by repeated receiving of the same packets.

The STP function of the device is simple configuration.Select the relevant agreement (STP or RSTP) after enabled the STP functions ,then it can be used.MSTP only need to configur the example after enabled the function ,then it can be used.

【Operating path】

Advanced config > mstp config

【Interface description】

Figure5-5-1 Global config interface

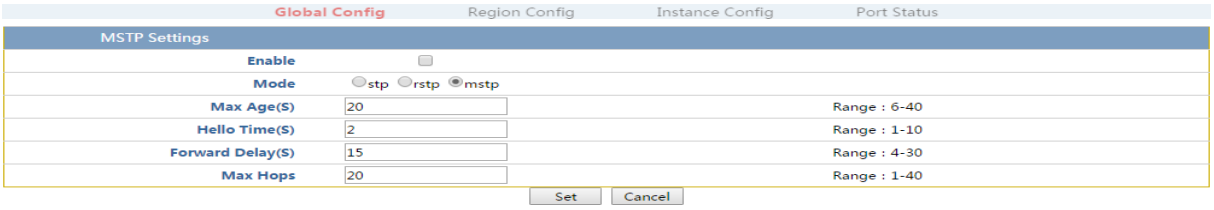


Table5-5-1 Main elements

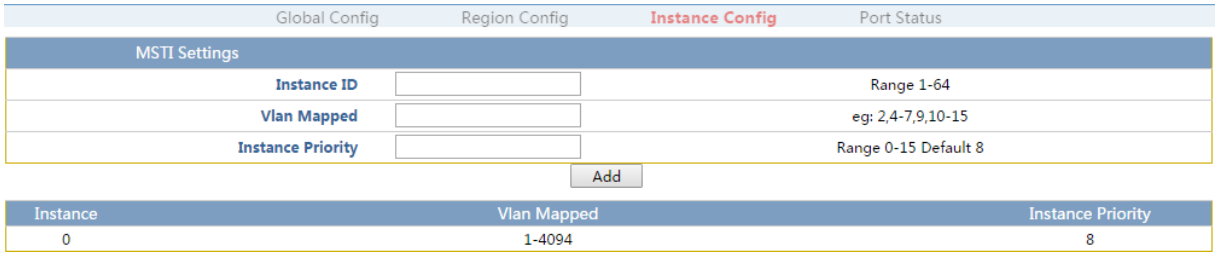
Interface elements	Description
Enabled	Check the box then STP enabled, otherwise not enabled.
Mode	Select spanning tree protocol mode, optional STP, RSTP, and MSTP.
Max age	Aging time, numerical range of 6-40 seconds. If it does not received BPDU packets from the root bridge after over aging time, the switch will send BPDU packets to all other switches to recalculate the spanning tree. the default is 20 seconds.
Hello time	The time of connection,numeric range for 1-10 seconds, the time interval of the BPDU packet sent by the root bridge to all other switches, used for the switch to detect whether the link is fault. Default is 2 seconds.
Forward delay	Transmission delay, numeric range for 4-30seconds, refers to the time when the port state of the switch is migrated.Default is 15 seconds.
Max hops	Max hops, numerical range of 1-40 hops,Default is 20 hops.

Figure5-4-2 Instance config interface

Table5-1-2 Main elements

Interface elements	Description
Revision	Configuration revision number, Default is 0.(range: 0-65535)
Region name	Configuration region name, Default MAC address is 000066111133, maximum length is 31 bits.

Figure5-5-3 Instance config interface



MSTI is a property of the MST domain, which is used to describe the mapping relationship between the VLAN and the spanning tree. VLAN can be assigned to different instances, each instance is a "VLAN group", is not affected by other instances and public spanning tree.

Table5-2-3 Main elements

Interface elements	Description
Instance ID	Set instance number.
Vlan Mapped	Set Vlan mapping.

Figure5-5-4 Port status interface

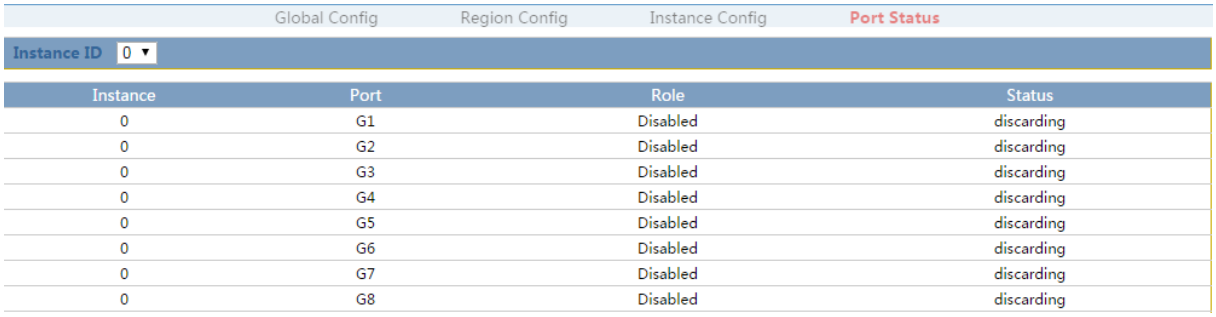
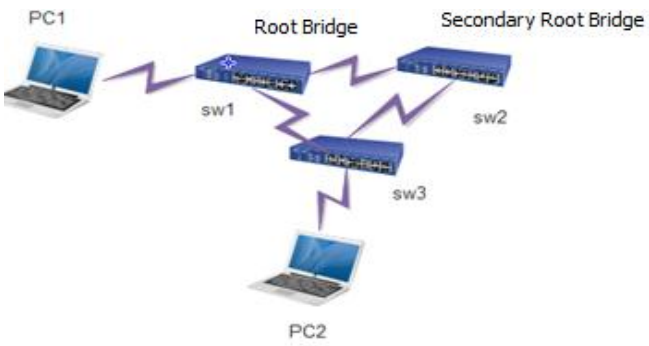


Table5-5-4 Main elements

Interface elements	Description
Instance ID	Select instance ID.
Instance	Display instance number.
Port	Display the port number corresponding to each instance.
Role	Display port role information.
Status	Display port status information.

【Example】



1. SW1,SW2,SW3 enable STP,SW1 is the root bridge election,SW2 is the secondary root bridge；
2. When the SW3 and the root bridge direct line interruption,STP can quickly switch, does not affect the network communication.

5.6 IGMP snooping

【Function description】

Internet Group Management Protocol (IGMP) snooping is a multicast restraining mechanism that runs on L2 devices. It is used to manage and control multicast groups. By analyzing received IGMP packets, an IGMP snooping L2 device sets up a mapping relationship between ports and MAC multicast addresses, and forwards multicast data based on this mapping relationship.

On"IGMP Snooping" page,You can make global configuration,static multicast configuration.

【Operating path】

Advanced config>igmp snooping

【Interface description】

Figure5-6-1 igmp snooping interface

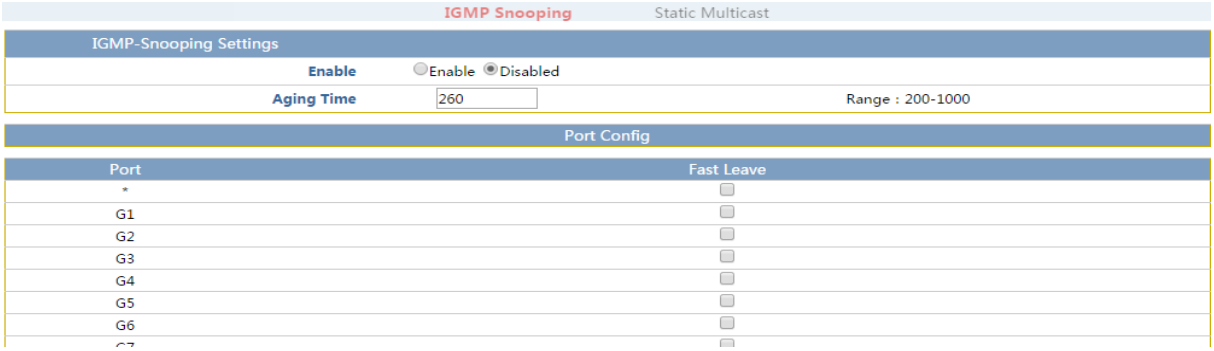


Table5-6-1 Main elements

Interface elements	Description
Enabled	Select"enable",enabled IGMP Snooping,select"disabled" then disabled IGMP Snooping.
Aging time	Configure host aging time.Range :200-1000s. Default is 260s.
Port	Display port information.
Fast leave	Configure port to quickly leave.

Figure5-6-2 Static multicast interface

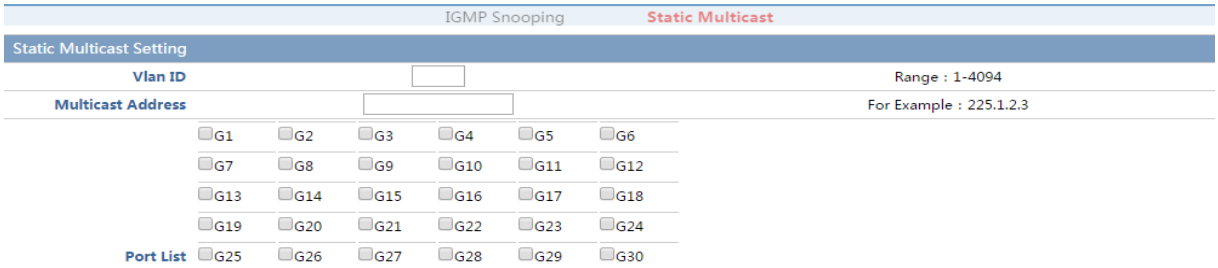
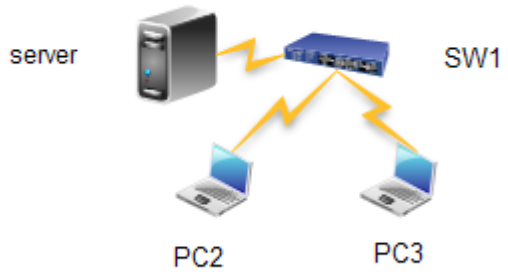


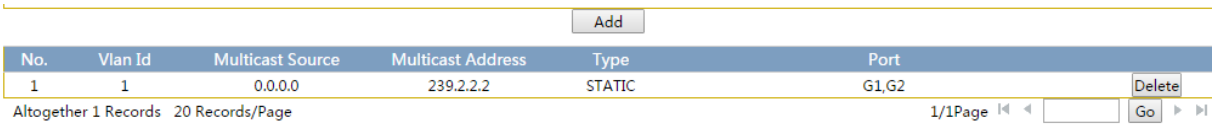
Table5-6-2 Main elements

Interface elements	Description
Vlan ID	Fill in VLAN ID .Range :1-4094.
Multicast address	Fill in the multicast IP address of the static binding.
Port list	Select multicast group member port.

Static binding means that the Multics source can only be received by a limited individual port, can not be received by the port which is not bound. Non statically bound Multics source can be received by the bound port.

【Example】





Server is the Multics source 239.2.2.2,SW1 port 1 and port 2 join Multics group. PC2 and PC3 direct port 1, port 2.

PC2 and PC3 can receive Multics streams. Multics stream cannot be received by the port which is not added the Multics group.

5.7 DHCP server

【Function description】

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

【Operating path】

Advanced config > dhcp server

【Interface description】

Figure5-7-1 Global config interface

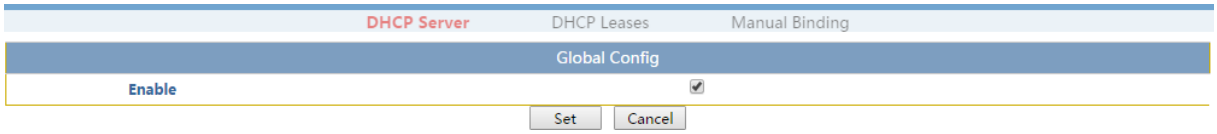


Table5-7-1 Main elements

Interface elements	Description
Enabled	Enable or disabled the DHCP.

Figure5-7-2 DHCP Leases interface

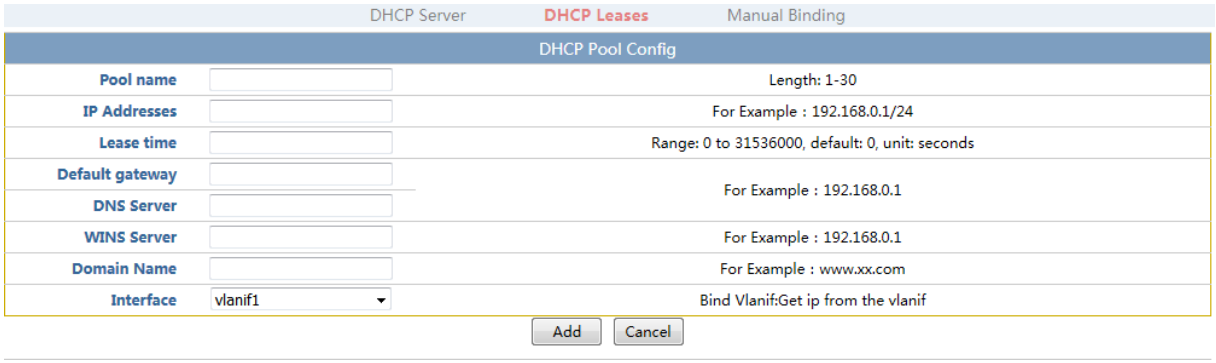


Table5-7-2 Main elements

Interface elements	Description
Pool name	Fill in the name of the DHCP address pool.
IP addresses	Fill in the DHCP address pool range.
Lease time	Fill in the lease time of the address.
Default gateway	Fill in client's default gateway.This will be used as the default gateway parameter for the server assigned to the client. The IP address of the default gateway must be in the same network as the IP address of the DHCP client.
DNS Server	Fill in DNS Server address.
WINS server	Fill in WINS DNS Server address.
Domain name	Fill in Domain name.
Interface	Select L3 interface for binding.

Figure5-7-3 Manual binding interface

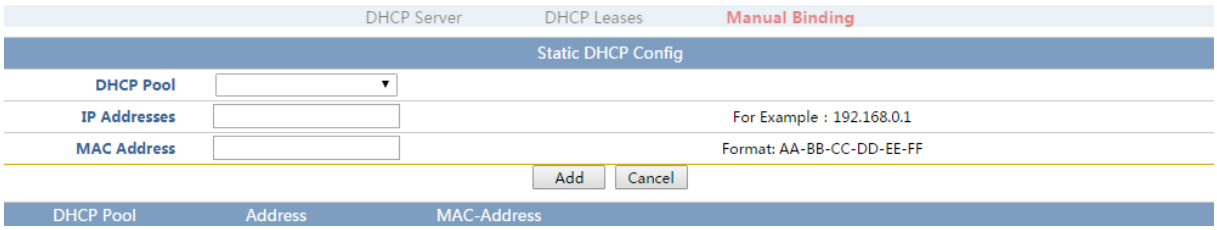
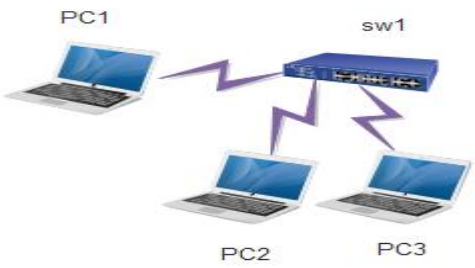
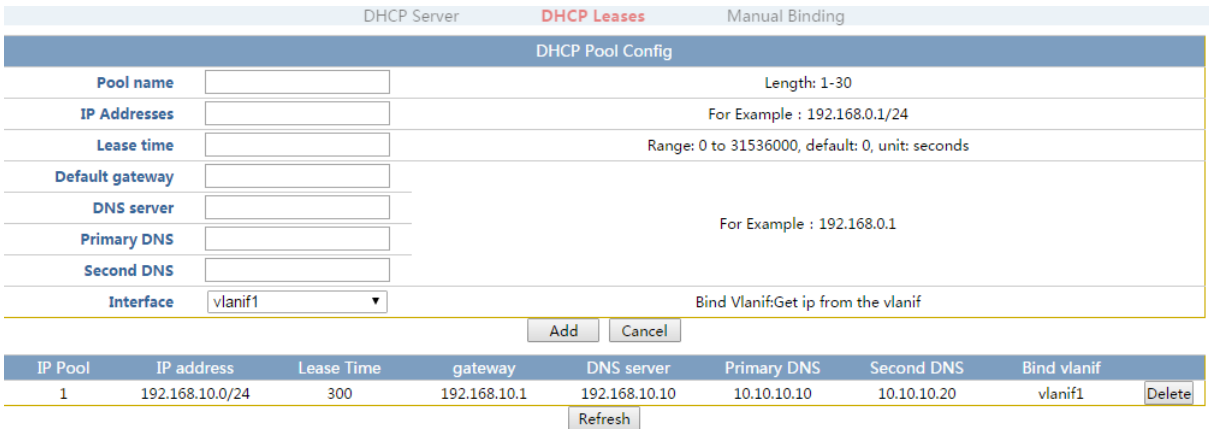


Table5-7-3 Main elements

Interface elements	Description
DHCP pool	Select DHCP pool.
IP addresses	Fill in the IP address that needs to be bound.
MAC address	Fill in the MAC address that needs to be bound.

【Example】





As shown in the figure above,SW1configure DHCP server pool,PC1、PC2、PC3 automatic access to the address, they can get to the address from the DHCP server pool.

5.8 DHCP relay

【Function description】

If the DHCP client and the DHCP server on the same physical network segment, the client can correctly obtain the IP address of dynamic allocation. If they are not in the same physical network, they need DHCP Relay Agent (relay agent). DHCP Relay agent can be removed to the necessary of DHCP server should be in each physical segment, It can deliver messages to the DHCP server that is not in the same physical subnet,it can also send a message back to the DHCP client that is not in the same physical subnet.

【Operating path】

Advanced config > dhcp relay

【Interface description】

Figure5-8 DHCP relay interface

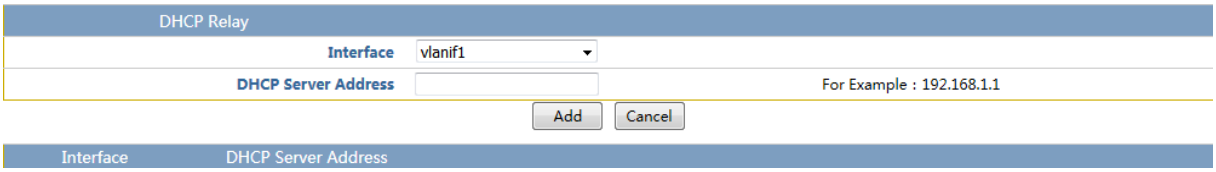
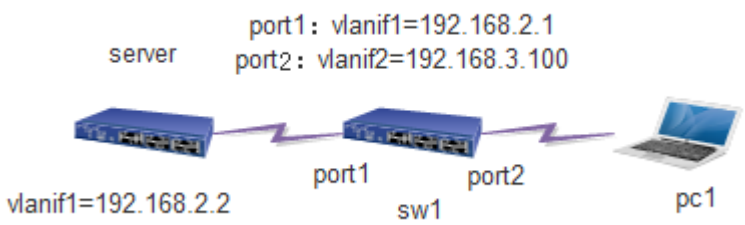


Table5-8 Main elements

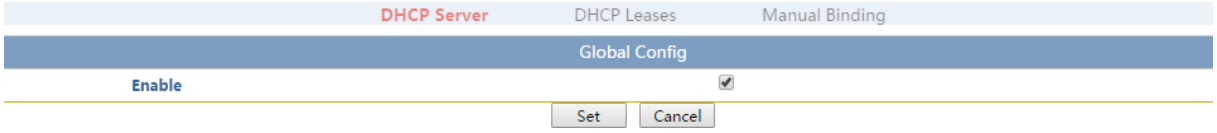
Interface elements	Description
Interface	Select the corresponding L3 interface.
Dhcp server address	Configure server's IP address.

【Example】

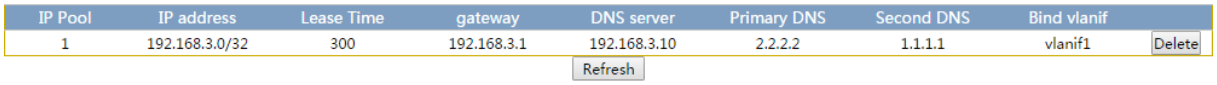


Configure server:

1.Enable dhcp(Note: this button is not a DHCP server enabled button, but a DHCP global enabled button . sw1 must also be turned on.)



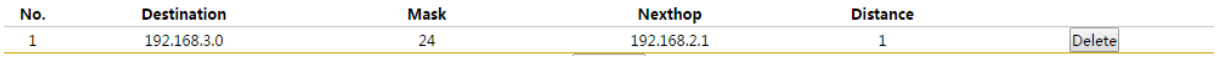
2.Set the address pool 1. As shown in the following figure:



IP Pool	IP address	Lease Time	gateway	DNS server	Primary DNS	Second DNS	Bind vlanif	
1	192.168.3.0/32	300	192.168.3.1	192.168.3.10	2.2.2.2	1.1.1.1	vlanif1	Delete

Refresh

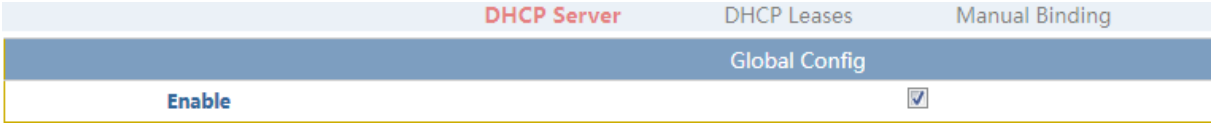
3.Setting static routes on server.As shown in the following figure:



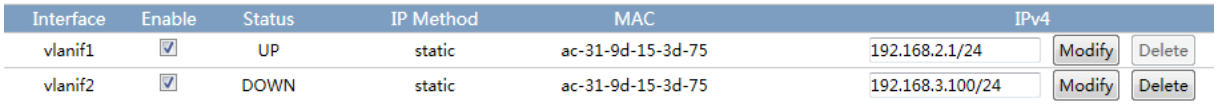
No.	Destination	Mask	Nexthop	Distance	
1	192.168.3.0	24	192.168.2.1	1	Delete

SW1:

1.Enable dhcp on SW1

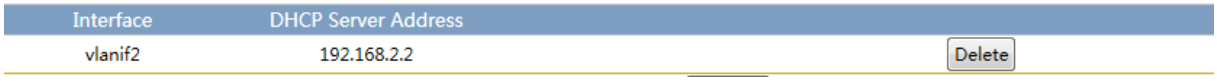


2.Configure L3 interface:vlanif1=192.168.2.1,vlanif2=192.168.3.100



Interface	Enable	Status	IP Method	MAC	IPv4		
vlanif1	☑	UP	static	ac-31-9d-15-3d-75	192.168.2.1/24	Modify	Delete
vlanif2	☑	DOWN	static	ac-31-9d-15-3d-75	192.168.3.100/24	Modify	Delete

3.Configure relay server:IP address in vlanif2 :192.168.2.2



Interface	DHCP Server Address	
vlanif2	192.168.2.2	Delete

4.Set port2’s pvid=2 on SW1, connect PC1.

5.PC1 automatic acquisition IP=192.168.3.3.

5.9 DHCP snooping

【Function description】

DHCP snooping is a security feature of DHCP, and provides the following functions:

1. Ensure that a client obtains its IP address from an authorized server.

If an unauthorized DHCP server that is built privately exists on the network, the DHCP clients may obtain incorrect IP addresses and network configuration parameters, and

consequently cannot implement communication normally. To ensure that DHCP clients can obtain IP addresses from an authorized DHCP server, the DHCP snooping security mechanism supports configuration of ports as trusted or untrusted ports.

a.A trusted port can forward received DHCP packets normally.

b.On receiving the DHCP-ACK and DHCP-OFFER packets from the DHCP server, an untrusted port drops the packets.

On the DHCP snooping device, the port connected to the DHCP server must be configured as a trusted port, and other ports must be configured as untrusted ports. In this way, DHCP clients can obtain IP addresses only from an authorized DHCP server, and unauthorized DHCP servers cannot allocate IP addresses to DHCP clients.

2. Record the mapping between IP addresses and MAC addresses of DHCP clients.

By monitoring the DHCP-REQUEST packets and the DHCP-ACK packets received from trusted ports, the DHCP snooping device records the DHCP snooping entries, which contain information such as the MAC address of the client, IP address allocated by the DHCP server to the DHCP client, port connected to the DHCP client, and VLAN. Based on such information, the switch can implement:

Address Resolution Protocol (ARP) inspection: Check whether the user sending the ARP packet is an authorized user based on the DHCP snooping entries, thus preventing the ARP attacks initiated by unauthorized users.

IP source guard: By dynamically obtaining the DHCP snooping entries, the switch filters packets forwarded by a port to prevent invalid packets from passing through the port.

【Operating path】

Advanced config > dhcp snooping

【Interface description】

Figure5-9-1 Global configuration interface

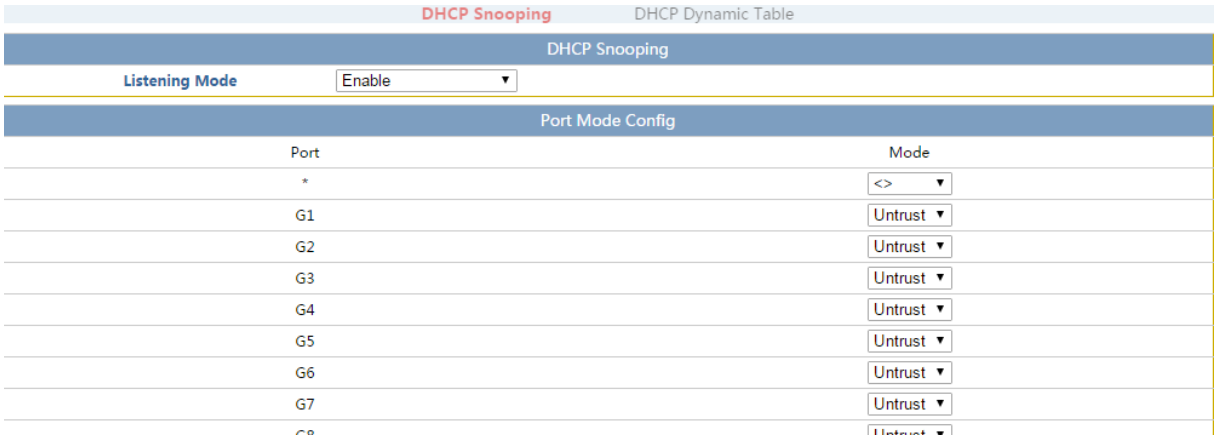
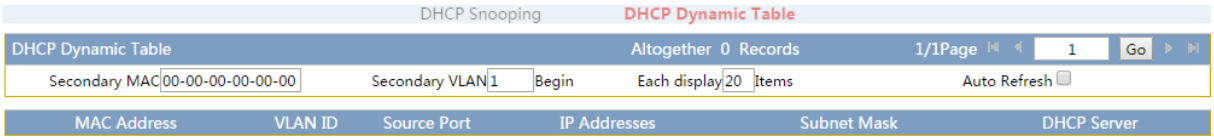


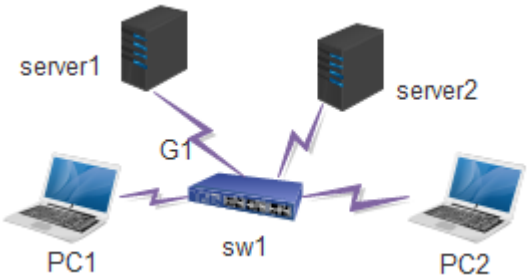
Table5-9-1 Main elements

Interface elements	Description Description
Listening Mode	Disable or enable DHCP Snooping.
Port	Display port information.
Mode	Configure port mode, optional trust, distrust.

Figure5-9-2 DHCP dynamic table interface



【Example】



The port G1 of the switch is cascaded with the DHCP server. All PCs connected to the switch must obtain IP addresses from this server. Other ports of the switch may be connected to devices with the DHCP server function. Configure data so that PCs connected to the switch can obtain IP addresses only from the DHCP server connected to G1.

Enable DHCP snooping globally. Set the port mode of G1 to Trusted, and the port mode of other ports to Untrusted. The following figure shows the configuration results.

5.10 QoS config

【Function description】

QoS(Quality of Service) refers to a network can use a variety of basic technology and provid better service capabilities for designated network communications. It is a technique that used to solve the problem of network delay and congestion.When the network overload or congestion, QoS can ensure that the important traffic is not delayed or discarded,while ensuring the efficient operation of the network.

【Operating path】

Advanced config> QoS config

【Interface description】

Figure5-10-1 Port priority interface

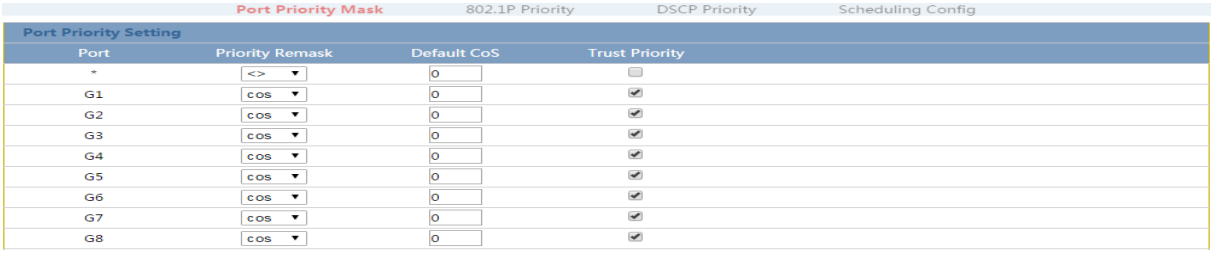


Table5-10-1 Main elements

Interface elements	Description Description
Port	Display port name.
Priority remask	Select priority remask type. 1 Cos,2 dscp,3 all (Select all,the entry into force of the DSCP, DSCP priority is higher than cos).
Default cos	Configure default priority. Default is 0 (0-7). The higher the

	value, the higher the priority.
Trust priority	Configure trust priority,check indicate to represent the priority of a trusted packet, uncheck indicate to trust the default cos which can be configured.

Figure5-10-2 802.1P priority interface

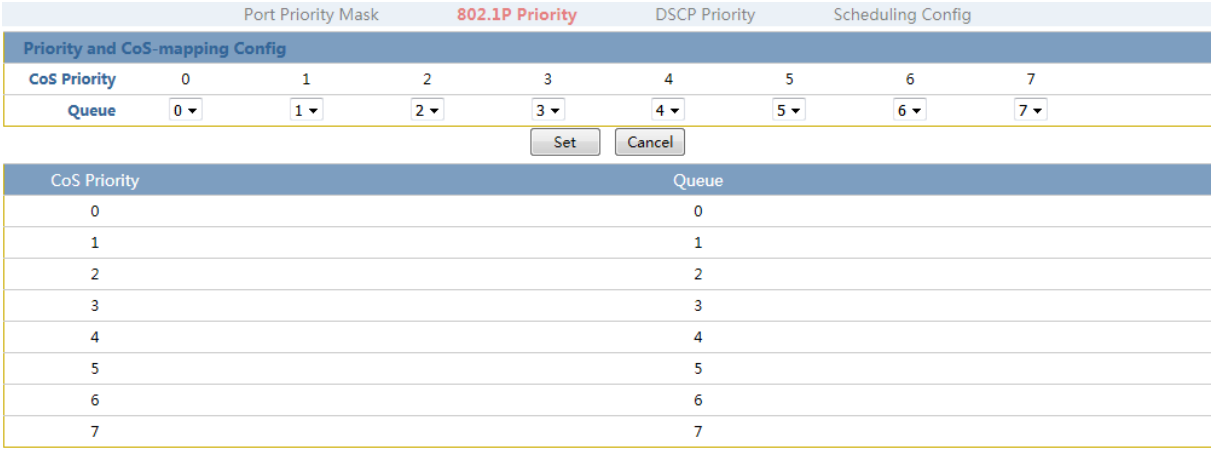


Table5-10-2 Main elements

Interface elements	Description Description
Cos priority	Display cos priority (0-7).
queue	Select cos priority corresponding to queue (0-7), Default cos priority(0-7)and queue(0-7)are corresponding one by one.

Figure5-10-3 DSCP priority interface

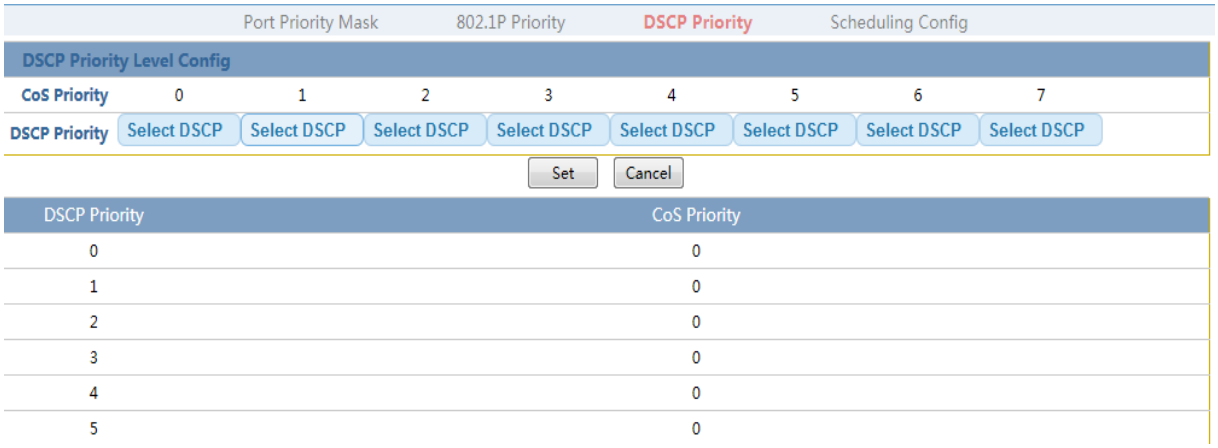


Table5-10-3 Main elements

Interface elements	Description Description
Cos priority	Display cos priority (0-7).
DSCP priority	Select the cos priority corresponding to the DSCP priority (0-63) to do the mapping. The default DSCP priority 0-7 corresponds to the cos priority 0, DSCP priority 8-15 corresponding to Cos priority 1,and so on, DSCP priority 56-63 corresponding to Cos priority 1.

Figure5-10-4 scheduling config interface

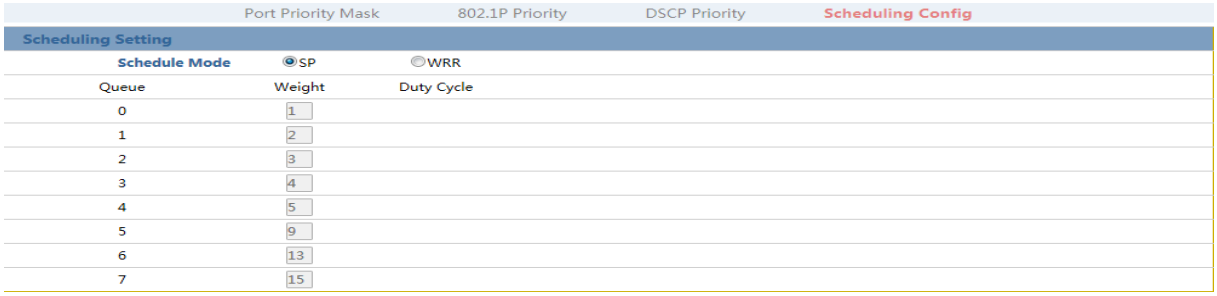


Table5-10-4 Main elements

Interface elements	Description Description
Schedule Mode	Select scheduling policy SP or WRR.
queue	Display queue number.
weight	Configur weights, it can be configured when you select WRR, the weight value is fixed when you select SP.
Duty cycle	Display weights corresponding width ratio,chang the size of the queue weight, the width ratio of the queue will also change.

5.11 VRRP

【Function description】

VRRP is a selection protocol,it can assign a virtual router's responsibility to one of the VRRP routers in a local area network..It can assign a virtual router's responsibility to a VRRP router in a local area network. It is responsible for forwarding packets to these virtual IP addresses. Once the main router is not available, this selection process provides a dynamic fault transfer mechanism, which allows the IP address of the virtual router can be used as the default first hop router. This is a LAN access device backup protocol. A default gateway is set

for all hosts in a local area network, then the messages which from the host and their destination addresss are not in this network segment, will be sent through the default gateway to the L3 switch, so the communication of the host and the external network is realized.

VRRP is a routing fault tolerance protocol, which can also be called backup routing protocol. A default route is set for all hosts in a local area network, when the destination address in the network from the host are not in the network segment, the message will be sent to the external router through the default route, so that the communication between the host and the external network is realized. The internal host will not be able to communicate with the external after the default router down off (port is closed), If the router set up VRRP, then the virtual router will enable the backup router at this time,so can achieve the whole network communication.

【Operating path】

Advanced config> vrrp

【Interface description】

Figure5-11 VRRP interface

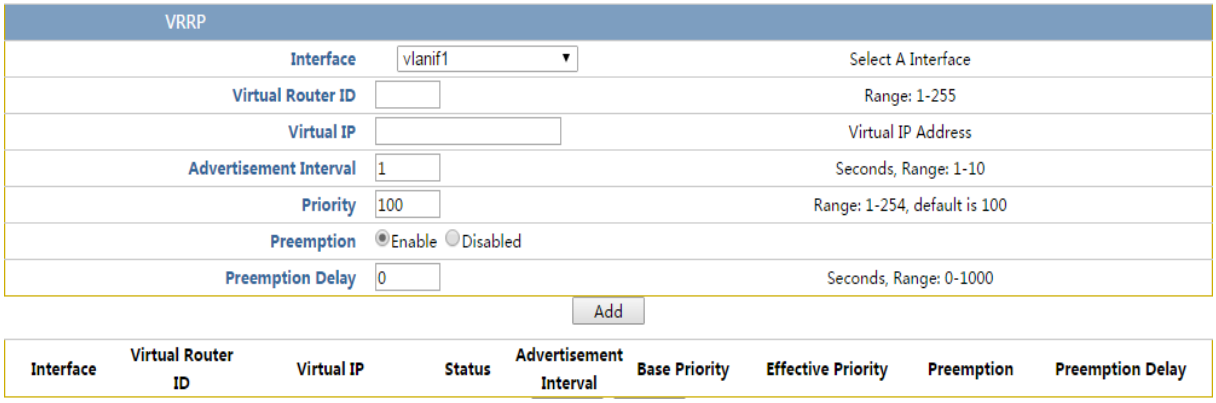
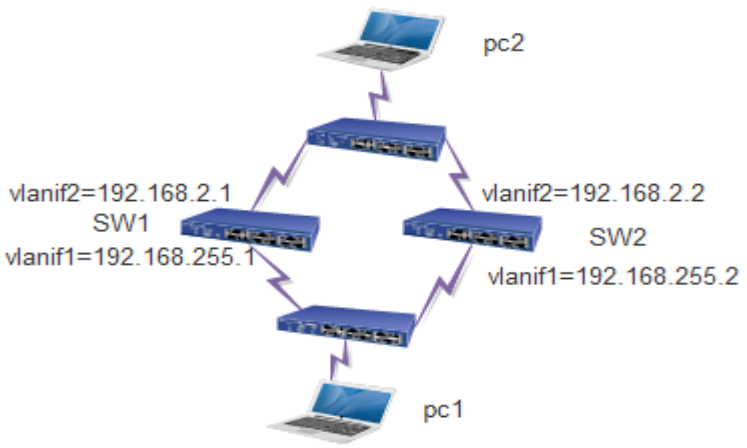


Table5-11 Main elements

Interface elements	Description Description
Interface	Select interface.
Virtual router ID	Configure virtual routing ID ,range is 1-255.
Virtual IP	Configure virtual IP.
Advertisement Interval	Configuration notification interval time, range is 1-10s.
Priority	The default configuration priority is 100, the range is 1-254.

Preemption	Enable /Disable "preemption" function.
Preemption Delay	Configure the preemption delay ,range is 1-1000s.

【Example】



SW1 :

vlan1=192.168.255.1,vlan2=192.168.2.1

Vlan1 virtual ID=100,virtual IP=192.168.255.100,other default.

Vlan2 virtual ID=200,virtual IP=192.168.2.100,other default.

Interface	Enable	Status	IP Method	MAC	IPv4		
vlanif1	☑	UP	static	ac-31-9d-15-3d-75	192.168.255.1/24	Modify	Delete
vlanif2	☑	DOWN	static	ac-31-9d-15-3d-75	192.168.2.1/24	Modify	Delete

Set Cancel

Interface	Virtual Router ID	Virtual IP	Status	Advertisement Interval	Base Priority	Effective Priority	Preemption	Preemption Delay	
vlanif2	200	192.168.2.100	INIT	1	100	0	enable	0	Delete
vlanif1	100	192.168.255.100	MASTER	1	100	100	enable	0	Delete

Set Cancel

SW2 :

vlan1=192.168.255.2,vlan2=192.168.2.2

Vlan1 virtual ID=100,virtual IP=192.168.255.100, set priority to 50,other default.

Vlan2 virtual ID=200,virtual IP=192.168.2.100, set priority to 50,other default.

Interface	Enable	Status	IP Method	MAC	IPv4		
vlanif1	☑	UP	static	ac-31-9d-15-3d-75	192.168.255.2/24	Modify	Delete
vlanif2	☑	DOWN	static	ac-31-9d-15-3d-75	192.168.2.2/24	Modify	Delete

Interface	Virtual Router ID	Virtual IP	Status	Advertisement Interval	Base Priority	Effective Priority	Preemption	Preemption Delay	
vlanif2	200	192.168.2.100	INIT	1	50	0	enable	0	Delete
vlanif1	100	192.168.255.100	MASTER	1	50	100	enable	0	Delete

Set Cancel

PC1:IP=192.168.255.5 Default gateway =192.168.255.100

PC2:IP=192.168.2.5 Default gateway =192.168.2.100

Tips:

Our equipment don’t support the routing protocol now, so both sides need to do VRRP networking mode. Moreover ,if you want to perfect use of VRRP standby backup function, it also need to link with the use of BFD detection protocol,We don't support these agreements for the moment, So, VRRP standby backup function, only a simulation of the situation of power equipment.

6 Routing config

6.1 Interface config

【Function description】

On the "config interface" page, you can configure the interface parameters.

【Operating path】

Routing config > interface config

【Interface description】

Figure6-1 interface config interface

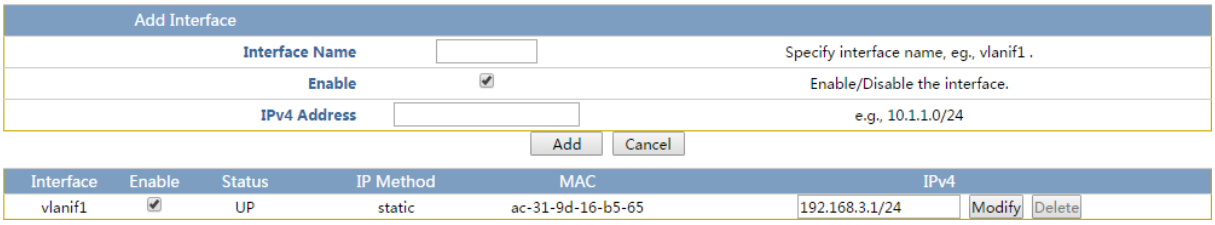


Table6-1 Main elements

Interface element	Description
Interface name	Set the name of the L3 interface,Format for vlanifX(the range of X is 1-4094).
Enabled	Enable/Disable L3 interface.default is Enable.
IPV4 address	Set the IP address and mask.
Modify	After modifying the IP, click the Modify button to modify the IP successfully.

6.2 Static routing

【Function description】

Static routing is a routing information that is manually configured by a user or network administrator. When the topology of the network or the state of the link changes, the network administrator needs to manually modify the routing table in the relevant static routing information.Static routing information is private by default and will not be passed to other routers.Of course, the network administrator can also be set to make the router to be shared.

Static routing is generally applicable to a relatively simple network environment, in this environment, the network administrator can easily understand the topology of the network, easy to set up the correct routing information.

【Operating path】

Routing config> static routing

【Interface description】

Figure6-2 static routing interface

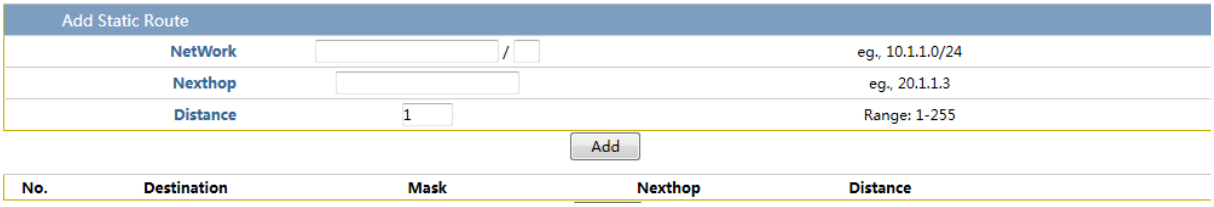
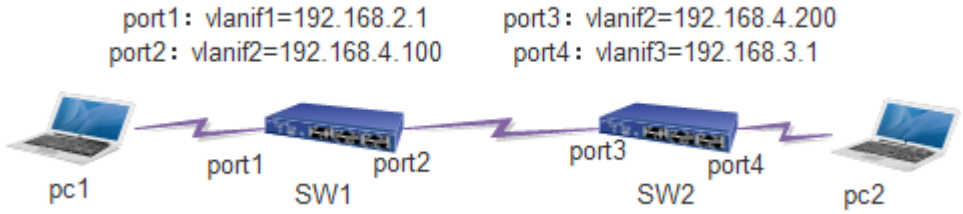


Table6-2 Main elements

Interface element	Description
network	Fill in the destination network address.
nexthop	Fill in the address of the next hop.
distance	Fill in the management distance, the default is 1, the range is 1-255.

【Example】



1.Set ip address and MAC address on PC.

PC1:ip=192.168.2.100,gateway=192.168.2.1

PC2:ip=192.168.3.100,gateway=192.168.3.1

1.Set the ip address and port pvid of the switch.

Sw1:

vlanif1=192.168.2.1,vlanif2=192.168.4.100

set pvid to 2 for port2

Sw2:

vlanif3=192.168.3.1,vlanif2=192.168.4.200

set pvid to 2 for port3,set pvid to 3 for port4

3.Set the static route to switches.

SW1:as follows:

No.	Destination	Mask	Nexthop	Distance	
1	192.168.3.0	24	192.168.4.200	19	Delete

SW2:as follows:

No.	Destination	Mask	Nexthop	Distance	
1	192.168.2.0	24	192.168.4.100	19	Delete

4.PC1 ping PC2,the two sides can communicate with each other.

6.3 OSPF config

【Function description】

OSPF is a link state routing protocol that uses bandwidth based metrics.OSPF uses the SPF algorithm to calculate the route,no routing loop is guaranteed from the algorithm,maintain route through neighbor relationship,Avoid periodic updates on bandwidth consumption.OSPF routing update rate is high, and the network convergence is fast,it is Suitable for large and medium sized networks.

【Operating path】

Routing config >ospf config

【Interface description】

Figure6-3-1 OSPF global config interface

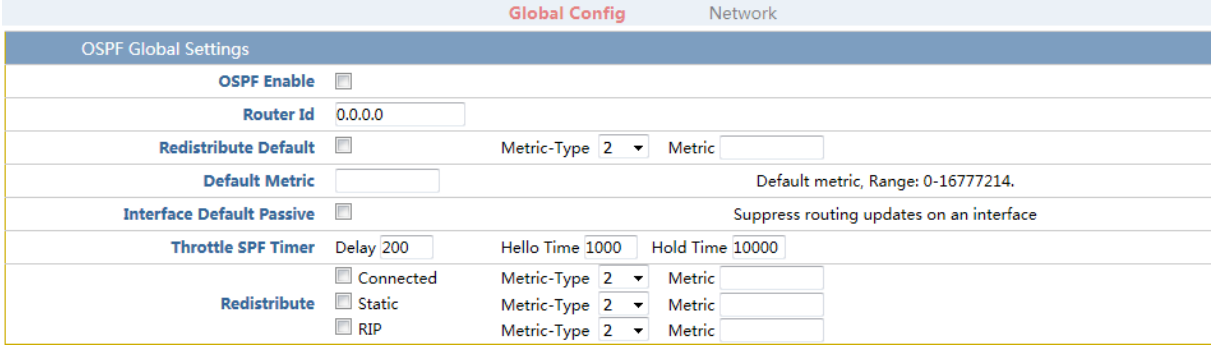


Table6-3-1 Main elements

Interface element	Description
OSPF enable	Enable/disable OSPF function.
Router ID	Fill in the router ID.
Redistribute default	Enable/disable default distribution function.
Metric-type	Select the overhead type, default type is 2.
Metric	Configure overhead when setting external routes.(range is 0-16777214)
Default metric	Fill in the default value for OSPF.(range is 0-16777214)
Interface default passive	Enable/disable passive interface.

Delay	Fill in throttle SPF timer delay time,default is 200ms.(range is 1-600000ms)
Hello time	Initial hold time (msec) between consecutive SPF calculations,default is 1000ms.(range is 1-600000ms)
Hold time	Maximum hold time (msec),default time is 10000ms.(rang is 1-600000ms)
Redistribute	Select the route type for republication. 1.connected,2.static,3.rip

Figure6-3-2 OSPF network interface

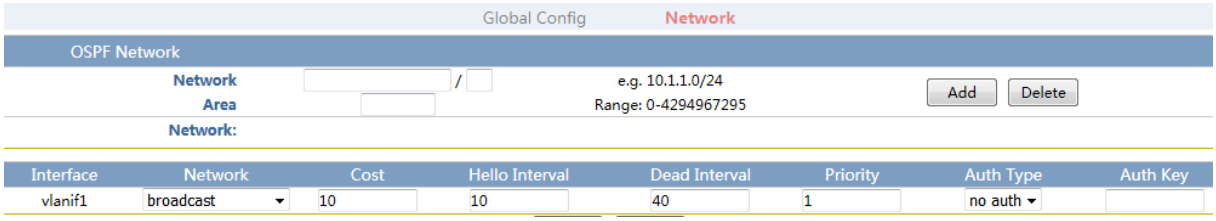
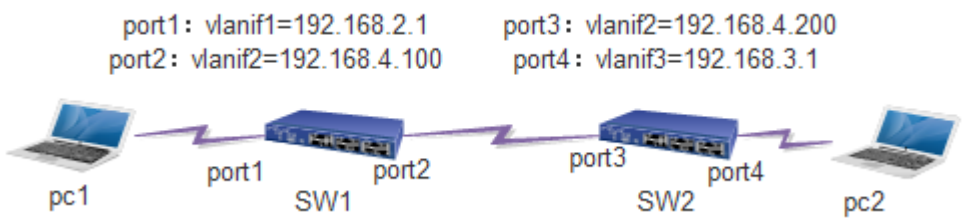


Table 6-3-2 Main elements

Interface element	Description
Network	You can fill in the routing network address and mask.
Area	You can fill in regional information.
OSPF network	Display the information of the network routing.
Interface	Display the interface name.
Network	Select the type of OSPF: **Point-to-point**: Hello packets sent to the multicast address 224.0.0.5, neighbors can automatically find, do not elect DR/BDR, the default Hello timer for 10 seconds, Dead timer for 40 seconds. **Broadcast**: Hello packets sent to the multicast address 224.0.0.5, neighbors

	can be found automatically, the election DR/BDR, the default Hello timer for 10 seconds, Dead timer for 40 seconds. **Non-broadcast**: Hello packets are sent by unicast, neighbors need to manually specify, do not elect DR/BDR, the default Hello timer for 30 seconds, Dead timer for 120 seconds. **Point-to-multipoint**: Hello message is sent to the multicast address 224.0.0.5, neighbors can automatically find no election DR/BDR, the default Hello timer for 30 seconds, Dead timer for 120 seconds.
Cost	Configuration interface overhead, default is 10.
Hello interval	Configuration time interval for sending Hello messages,default time is 10s.
Dead interval	The seconds to wait that the hello packet sent by the router has not been seen by a neighbor and claims that the OSPF router has lost.default time is 40s.
Priority	Interface priority, the default is 1, range is 0-255.
Auth type	authentication type based region : 1 no authentication; 2 simple password authentication; 3.MD5 authentication; 4.no authentication.
Auth key	You can fill in the key value of authentication.

【Example】



1.Enable OSPF function on SW1 and SW2.

2.Set ip address and MAC address on PC.

PC1:ip=192.168.2.100,gateway=192.168.2.1

PC2:ip=192.168.3.100,gateway=192.168.3.1

3.Set the IP and port PVID of the switch.

SW1:

vlanif1=192.168.2.1,vlanif2=192.168.4.100,

Set pvid to 2 for port2.

SW2:

vlanif3=192.168.3.1,vlanif2=192.168.4.200,

set pvid to 2 for port3,set pvid to 3 for port4.

4.Configure ospf network.

Sw1:router id=1.1.1.1

network 192.168.2.0/24 area 0,network 192.168.4.0/24 area 0

Sw2:router id=2.2.2.2

network 192.168.3.0/24 area 0,network 192.168.4.0/24 area 0

6.4 BGP config

【Function description】

The border gateway protocol (BGP) is a routing protocol that runs on TCP, which is a kind of autonomous system. BGP is the only protocol that is used to deal with the network size of the Internet, and is the only protocol that can properly handle the multi connection between the routing domain.BGP is built on the experience of EGP.The main function of the BGP system is to exchange network reachability information with other BGP systems.The network reachability information includes information of the autonomous system (AS) listed.These information effectively construct the topology of AS interconnection and thus clears the routing loop,At the same time, the AS level can be implemented in strategic decision-making.

【Operating path】

Routing config >bgp config

【Interface description】

Figure6-4-1 BGP global config interface

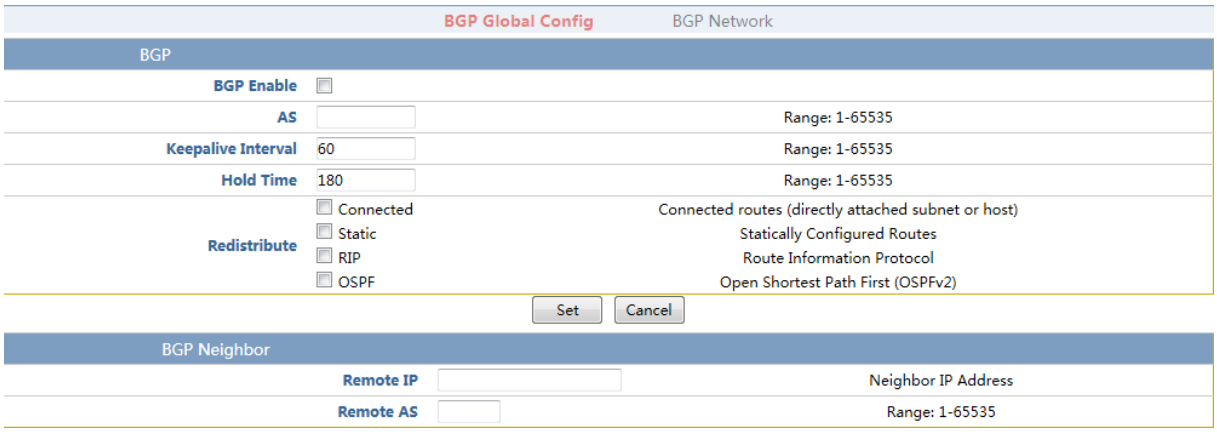


Table6-4-1 Main elements

Interface element	Description
BGP enable	Enable/disable BGP function.
AS	Number of autonomous domains (range 1-65535).
Keepalive interval	Sends the time interval to keep the active state packet,the default time is 60s,and the range is 1-65535s.

Hold time	BGP neighbors think the effective length of the sender information, the default time is 180s,range is 1-65535s.
Redistribute	Select the route type for republication.
BGP neighbor	
Remote IP	Fill in the neighbor's IP address.
Remote AS	Fill in the neighbor's AS number.

Figure6-4-2 netwrok interface

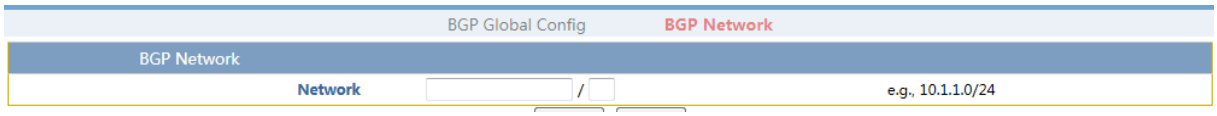
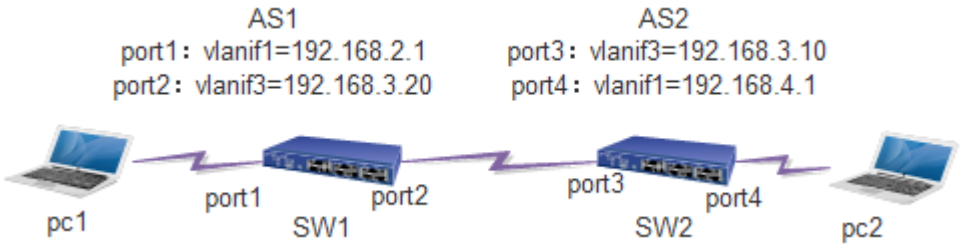


Table6-4-2 Main elements

Interface element	Description
Network	Fill in the static routing address and mask number.

【Example】



1.Set gateway and IP on PC.

PC1:IP=192.168.2.96,GW=192.168.2.1

PC2:IP=192.168.4.99,GW=192.168.4.1

2.Set the IP and port PVID of the switch.

SW1:vlanif1=192.168.2.1,vlanif3=192.168.3.20,set pvid to 3 for port2

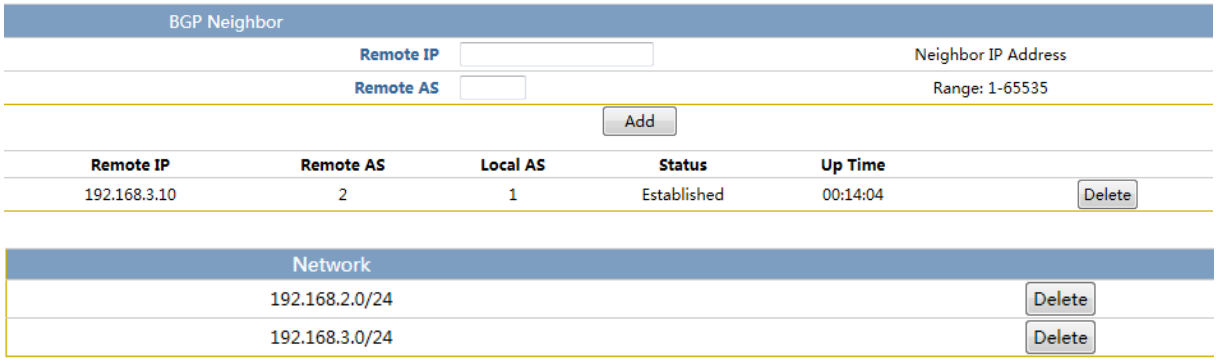
SW2:vlanif1=192.168.4.1,vlanif3=192.168.3.10,set pvid to 3 for port3

3.Enable bgp,set the neighbor and network of the switch.and others is default.

SW1:AS=1,neighbor=192.168.3.10,remote AS=2.

network=192.168.2.0/24,network=192.168.3.0/24,

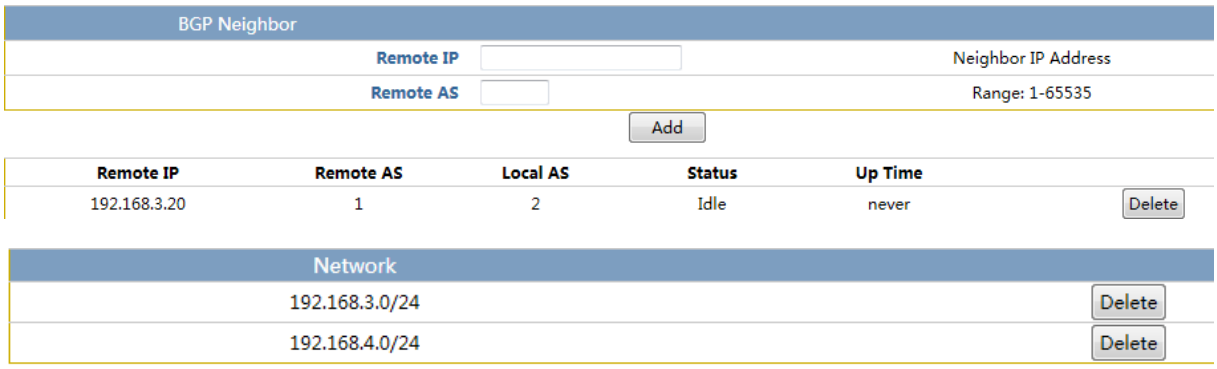
As follows:



SW2:AS=2,neighbor=192.168.3.20,remote as=1.

network=192.168.4.0/24,network=192.168.3.0/24

As follows:



6.5 RIP config

【Function description】

RIP is Interior Gateway Protocol that more common used and used earlier.It is suitable for small and similar network,and it is a typical distance vector protocol.RIP exchange routing information through broadcast UDP messages,and it is send routing information update every 30 seconds.RIP provides count Hop (hop count) as a scale to measure routing distance.The hop count is the number of routers that a packet must pass to reach the target.If the same target has two different speed or bandwidth of the router, but the same hop count.Then RIP thinks that the two route is equal distance.RIP maximum support of the number of hops is 15,the number of hops 16 indicates that it is not reachable.

【Operating path】

Routing config >rip config

【Interface description】

Figure6-5-1 RIP global config interface

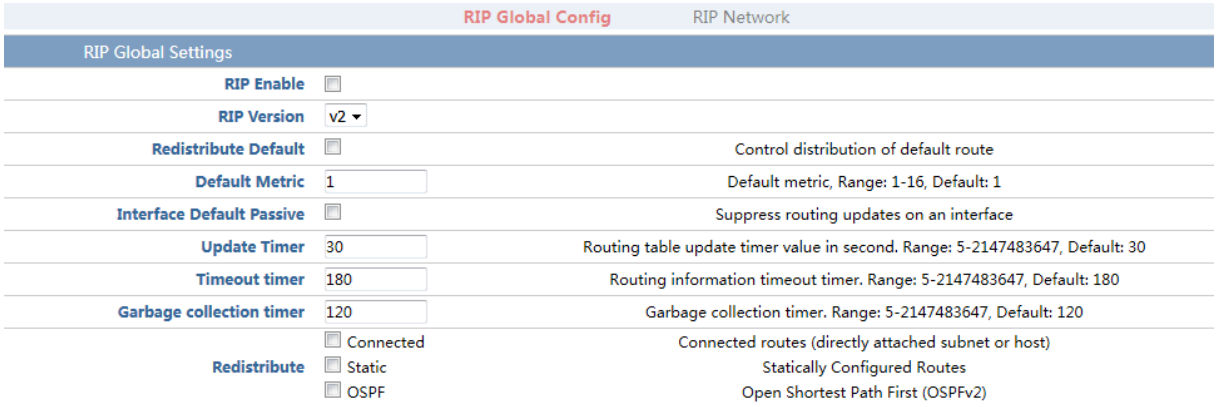


Table6-5-1 Main elements

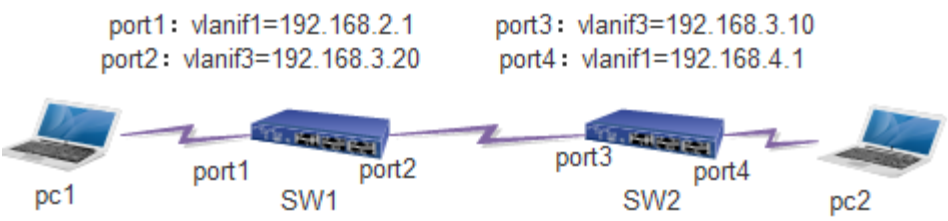
Interface element	Description
RIP enable	Check is enabled RIP, do not check is disabled RIP.
Rip version	Select the RIP version number, including V1 and V2.
Redistribute default	Enable/disable default distribution.
Default metric	Fill in the default hop count of RIP (range: 1-16).
Interface default passive	Enable/disable the passive interface.
Update timer	Routing table update timer, default time is 30s.
Timeout timer	Route timeout timer, default time is 180s.
Garbage collection timer	Garbage collection timer, the default time is 120s.
Redistribute	Select the route type for re publication.

Figure6-5-2 RIP netwrok interface

Table6-5-2 RIP Main elements

Interface element	Description
Network	The configuration, RIP routing subnet address and mask.
Interface	Select the three layer interface, the default vlanif1.
Rip network/interface	Display configuration of routing and interface information.
Interface	Display interface information.
Split horizen	Set interface level split, default enabled.
Send version	Send the rip version of the interface mode, the default auto, optional V1 or V2.
Receive version	Receive the rip version of the interface mode, the default version is auto, you can choose V1 or V2.
Auth type	Authentication type: 1 non authentication; 2 simple password authentication; 3.MD5 value authentication.
Auth key	Fill in the authentication key value.

【Example】



2.Set IP address and MAC address on PC.

PC1:IP=192.168.2.96,GW=192.168.2.1

PC2:IP=192.168.4.99,GW=192.168.4.1

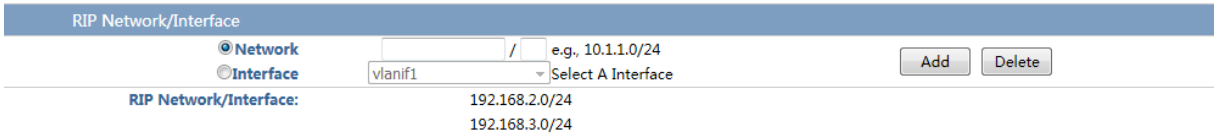
2.Set the IP and port PVID of the switch.

SW1:vlanif1=192.168.2.1,vlanif3=192.168.3.20,set pvid to 3 for port2.

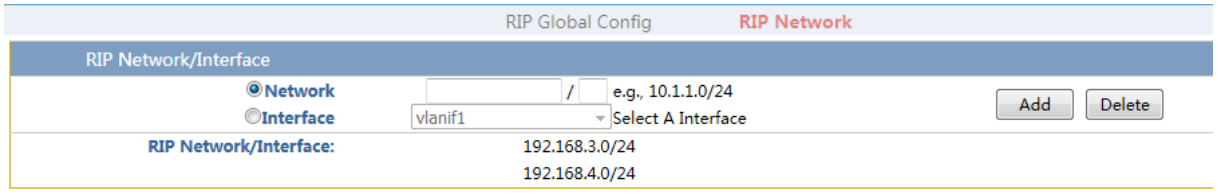
SW2:vlanif1=192.168.4.1,vlanif3=192.168.3.10,set pvid to 3 for port3.

3.Enable rip,set the network of the switch.and others is default.

SW1:network=192.168.2.0/24,network=192.168.3.0/24,as follows:



SW2:network=192.168.4.0/24,network=192.168.3.0/24,as follows:



7 Network security

7.1 Anti-attack

【Function description】

You can enable or disable ignore ping package function and you can Set the CPU packet reception threshold on"Anti-Attack"page.

【Operating path】

Network Security > anti-Attack

【Interface description】

Figure7-1 Anti-Attack interface

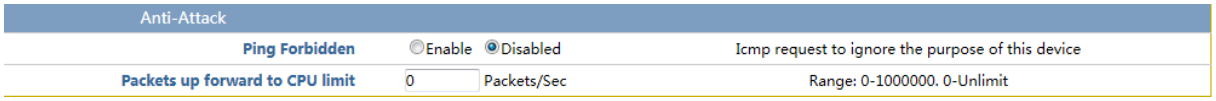


Table7-1 Main elements

Interface element	Description
Ping Forbidden	enable or disable ignore ping package function.
Packets up forward to CPU limit	Set the CPU packet reception threshold.

7.2 MAC binding

【Function description】

You can bind the port and MAC address on"MAC Binding"page.The MAC device can only communicate in this port after MAC and port binding ,and not communicate in other ports.But other mac devices can communicate normally in this port.

【Operating path】

Network Security > mac binding

【Interface description】

Figure7-2 MAC Binding interface

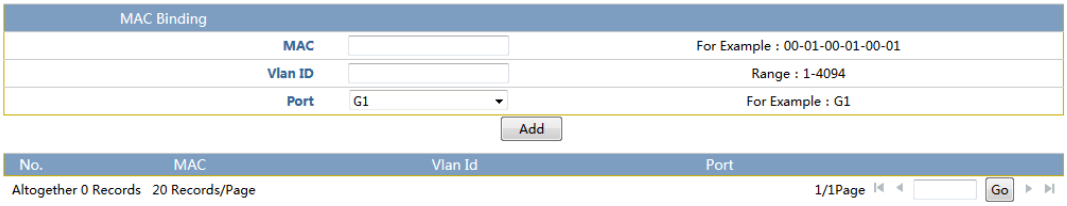


Table7-2 Main elements

Interface element	Description
MAC	Enter the MAC address that needs to be bound.
Vlan ID	Enter Vlan ID that needs to be bound.
Port	Select port that you need to be bound.

7.3 ARP binding

【Function description】

You can view the switch ARP information, configure the IP address and MAC address of the static arp, and you can scan the port arp on the "Binding ARP" page.

【Operating path】

Network Security > arp binding

【Interface description】

Figure7-3-1 ARP Global interface

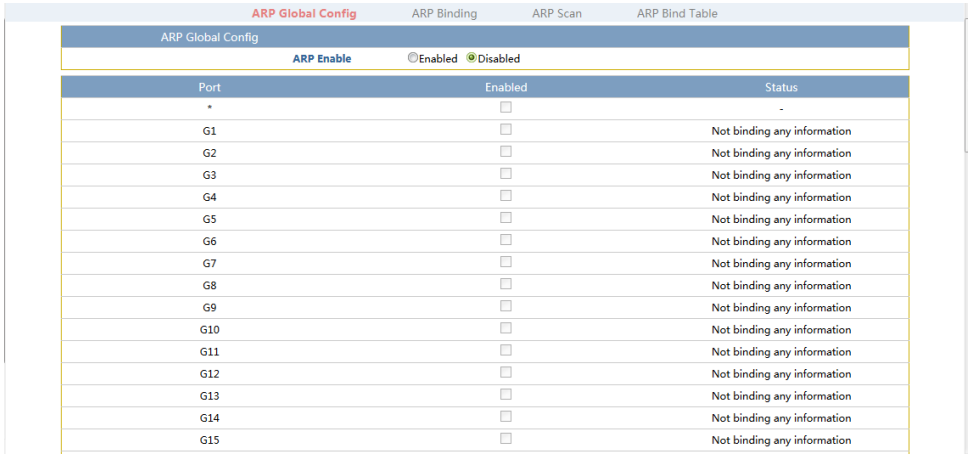


Table7-3-1 Main elements

Interface element	Description
ARP Enable	You can enable ARP binding function.

Figure7-3-2 ARP Binding interface

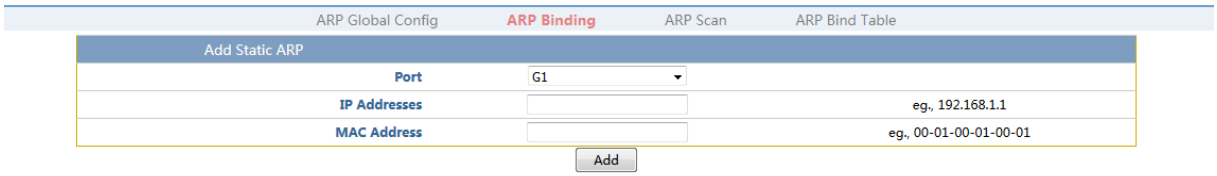
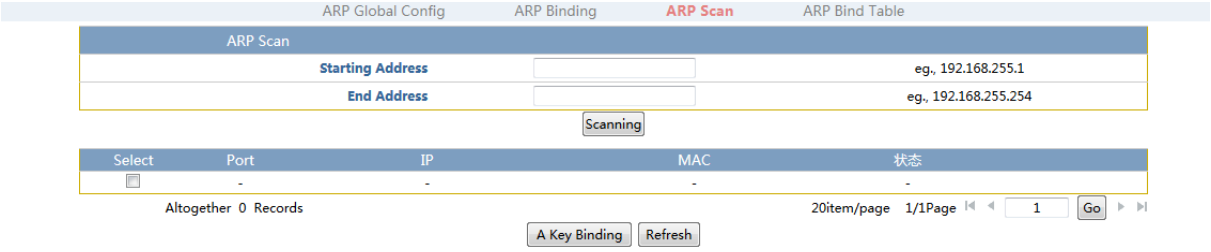


Table7-3-2 Main elements

Interface element	Description
Port	Select the port to bind ARP.
IP Address	Configure the IP address that needs to be bound.
MAC Address	Configure the MAC address that needs to be bound.

Figure7-3-3 ARP Scan interface



Note: this feature can only be implemented in web, the command line can not be achieved.

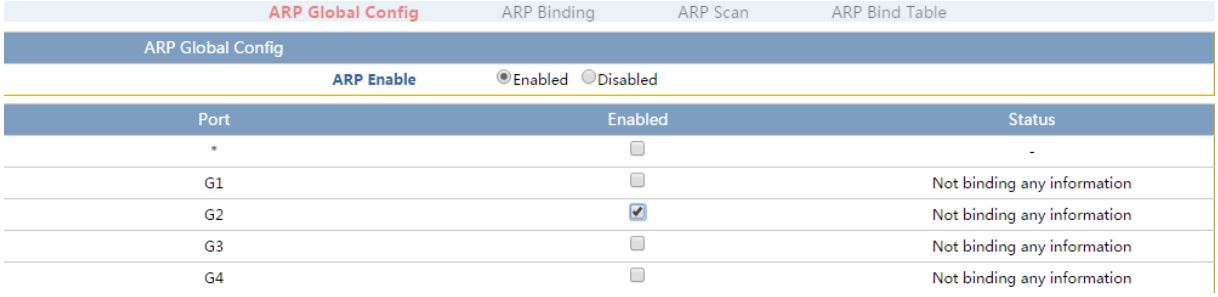
Table7-3-3 Main elements

Interface element	Description
Starting Address	Enter the starting ip address of the query.
End Address	Enter the ending IP address of the query.

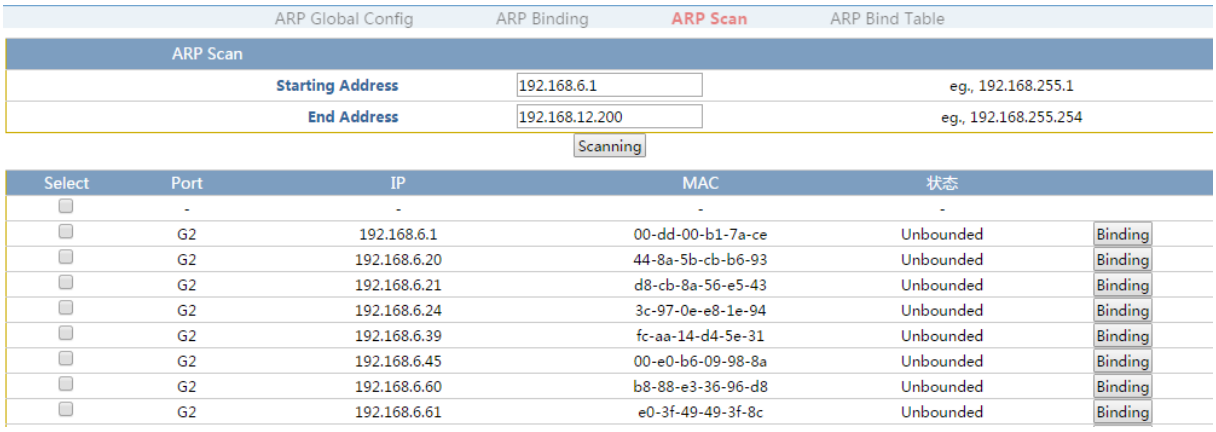
【Example1】

ARP scan:

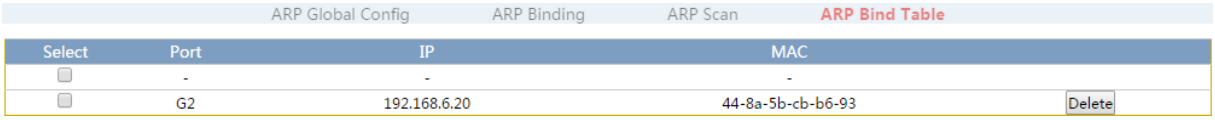
1.Enable ARP binding function,Enable ARP binding function of G2 port . As follows:



2.Enter starting ip address and end ip address,click"scanning" button.As follows:



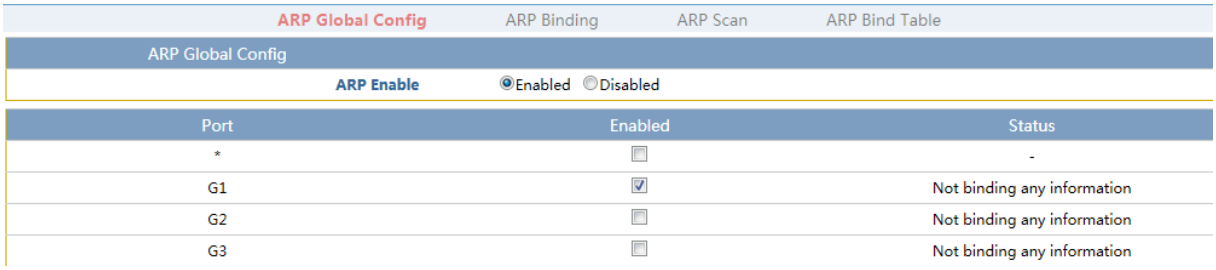
3. You can click"binding" button which you need to bind.and then the entry what you selec and binding could be seen in the ARP bind table.



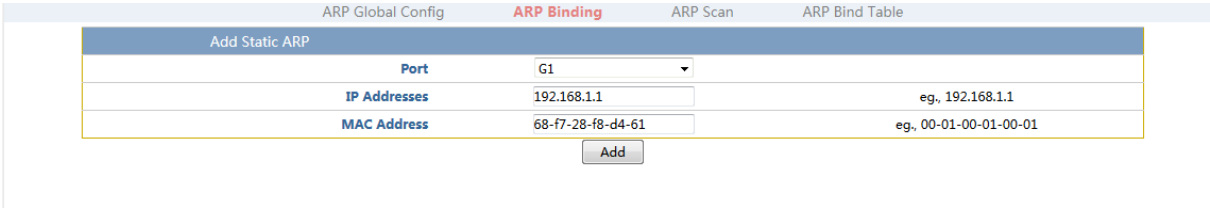
【Example2】

ARP binding:

Enable ARP binding function,Enable ARP binding function of G1 port .



Add ip address 192.168.1.1 and MAC address 68-f7-f8-d4-61 to G1 port,In addition to bind the MAC related terminal,Other MAC related terminals can not communicate through this port.



7.4 ACL config

【Function description】

ACLs are used to filter packets based on the configured packet matching rules and processing operations. After an ACL is applied to a port, fields in each packet are analyzed. After matched packets are identified, these packets are processed according to the preset operations, such as permit, deny, rate limiting, redirection, or port shutdown.

【Operating path】

Network Security > acl config

【Interface description】

Figure7-4-1 ACL Group interface

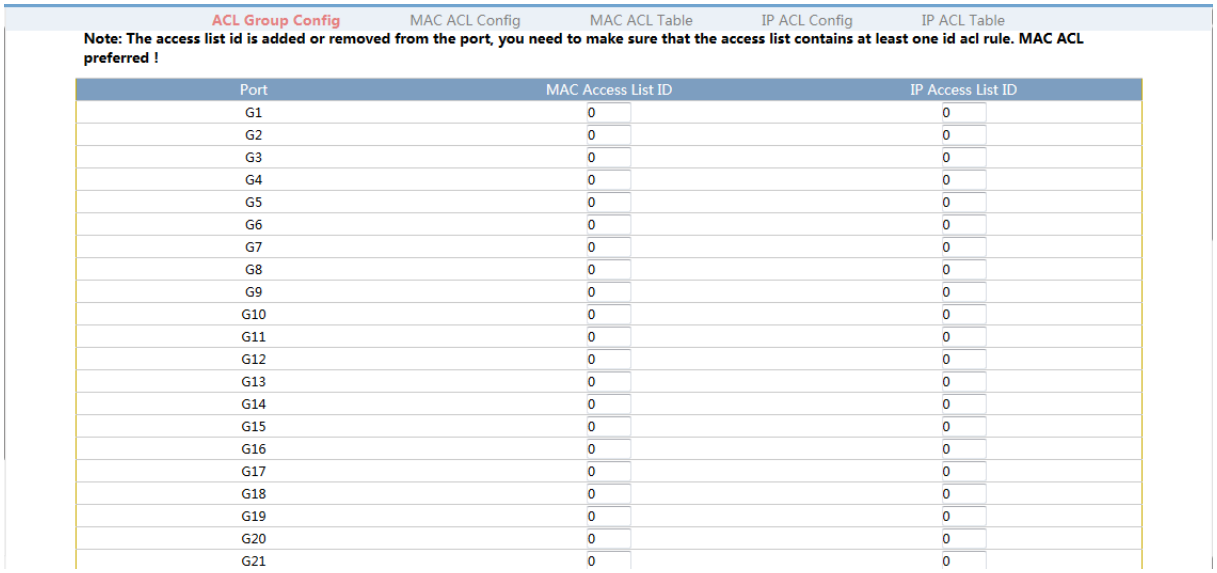


Table7-4-1 Main elements

Interface element	Description
Port	Shows the port name of the switch.
MAC access list ID	Configure the MAC ACL group ID for the corresponding port.
IP access list ID	Configure the IP ACL group ID for the corresponding port.

Figure7-4-2 MAC ACL Config interface

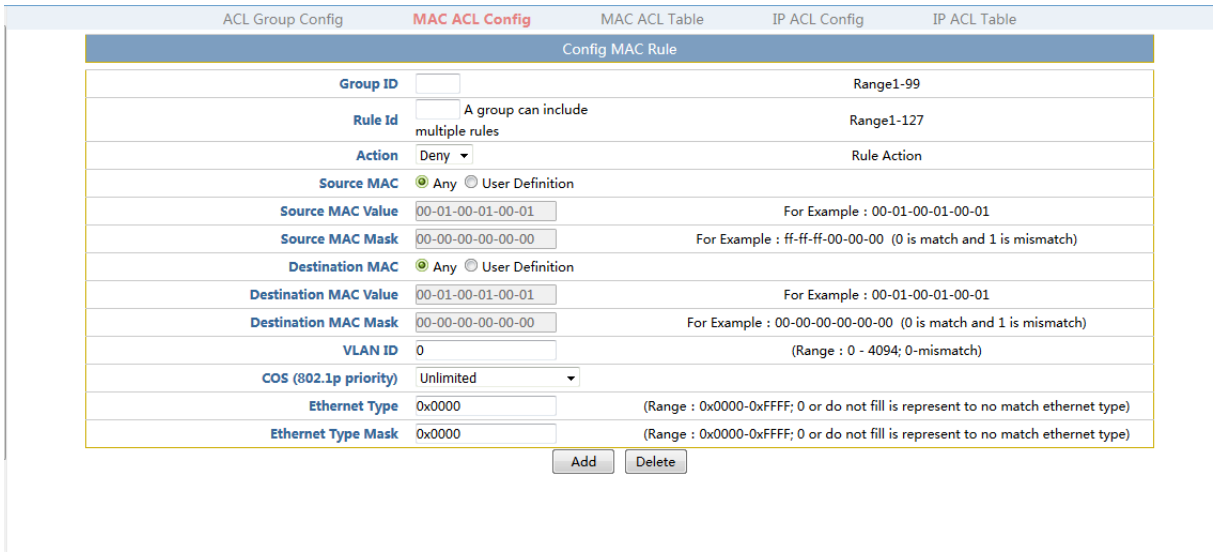


Table7-4-2 Main elements

Interface element	Description
Group ID	Configure ACL group id.Range of values is 1-99.
Rule ID	Configure rule id.Range of values is 1-127.
Action	Select rules of the data packet processing ,deny or permit.
Source Mac Value	Configuration source MAC address.
Soucre Mac Mask	Configuration source MAC address mask.
Destination Mac Value	Configuration destination MAC address.
Destination Mac Mask	Configuration destination MAC address mask.
VLAN ID	Configuration VLAN ID.
COS (802.1p priority)	Select the priority of cos.
Ethernet Type	Configure ethernet type.
Ethernet Type Mask	Configure ethernet type mask.

Figure7-4-3 MAC ACL Table interface

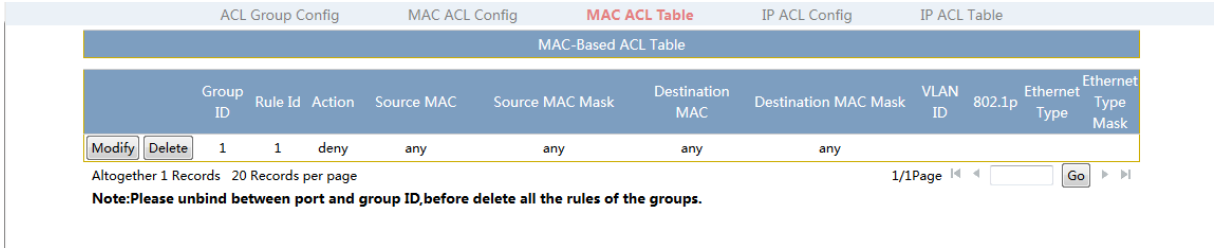


Figure7-4-4 IP ACL Config interface

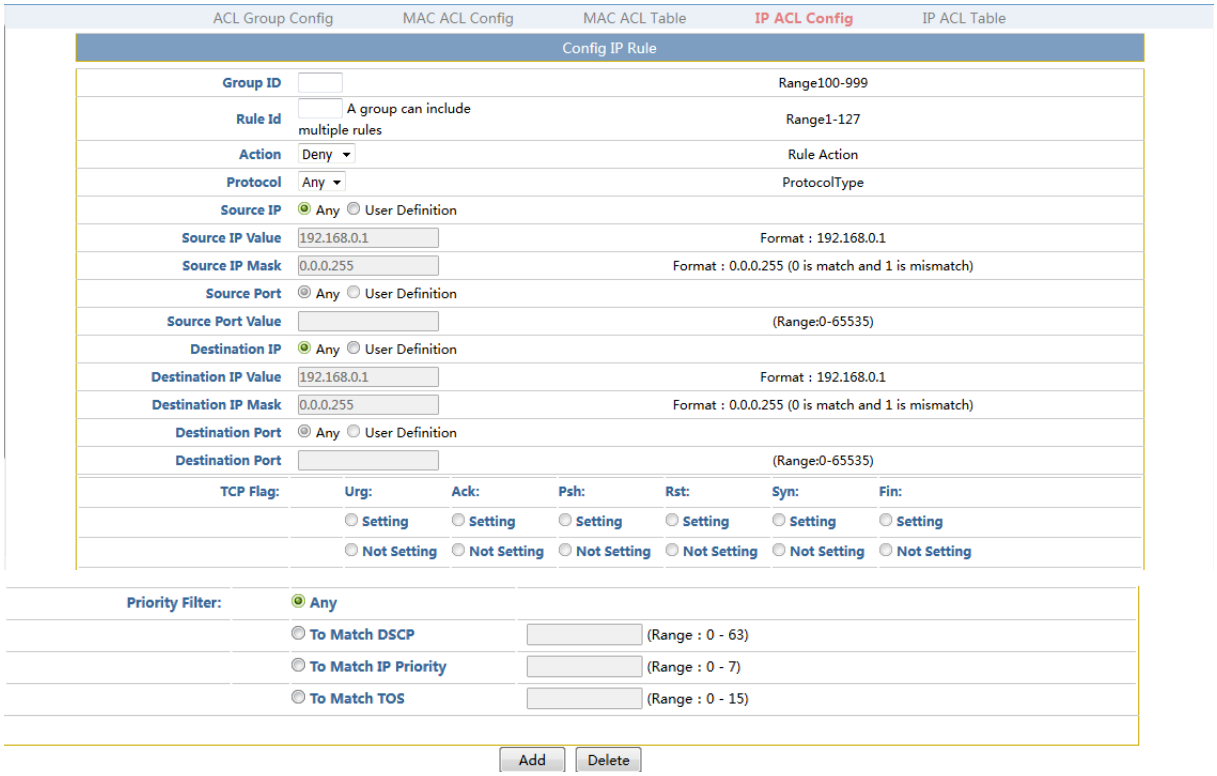
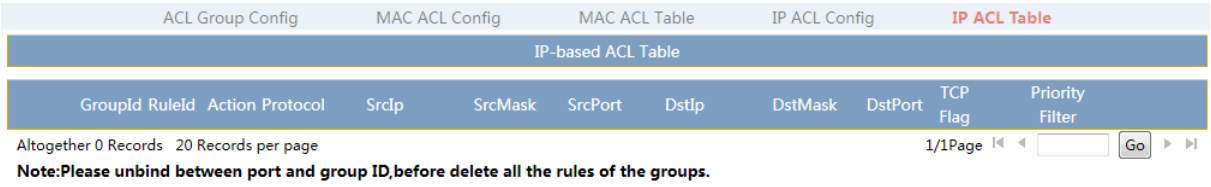


Table7-4-4 Main elements

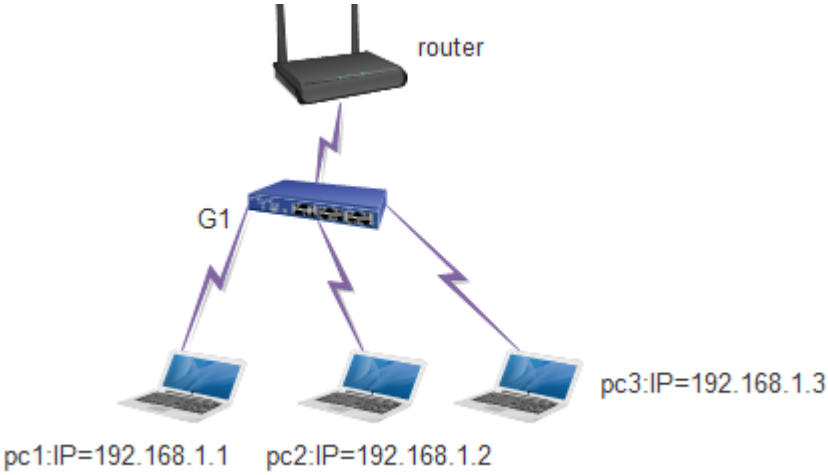
Interface element	Description
Group ID	Configure ACL group id.Range of values is 100-999.
Rule ID	Configure rule id.Range of values is 1-127.
Action	Select rules of the data packet processing ,deny or permit.
Protocol	Selection protocol type.
Source IP Value	Configuration source IP address.

Source IP Mask	Configuration source MAC address mask.The mask set 1 indicates a tight match.
Source Port	Configure TCP/UDP source port number.
Destination IP Value	Configure destination ip address.
Destination IP Mask	Configure destination ip address mask,The mask set 1 indicates a tight match.
Destination Port	Configure TCP/UDP destination port number.
TCP Flag	Select "TCP flag" when protocol select tcp.
Priority Filter	Select the priority of filtering.

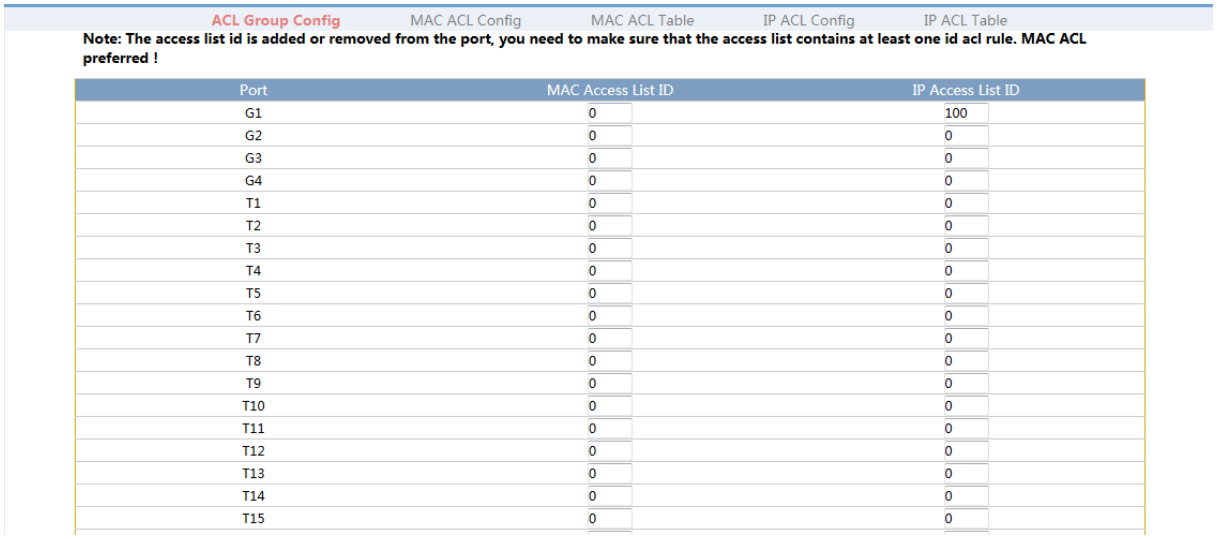
Figure7-4-5 IP ACL table interface



【Example】



1.Set the group ID is 100,Rule ID is 1,Action is deny,Source ip is 192.168.1.1 and destination ip is 192.168.1.3



2.Set IP access list id is 100 on port G1 and click"add"button,you can see

192.168.1.1 can communicate with 192.168.1.2 but can not communicate with 192.168.1.3.

7.5 802.1X config

【Function description】

802.1x was proposed by IEEE802 LAN/WAN Standards Committee to resolve the security issues of the WLAN. Later this protocol is used on the Ethernet as a common access control mechanism of LAN ports. 802.1x is mainly used to resolve the authentication and

security issues on the Ethernet. It implements authentication and control on devices connected to ports of the LAN access devices.

【Operating path】

Network Security > 802.1X config

【Interface description】

You can enable or disable the 802.1x authentication function related parameters on the "Config Global" page.

Figure7-5-1 Global Config innterface

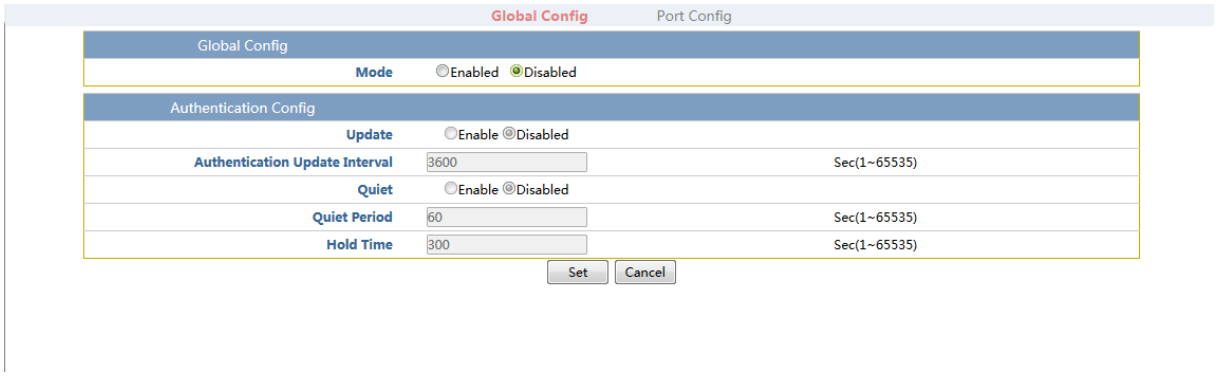
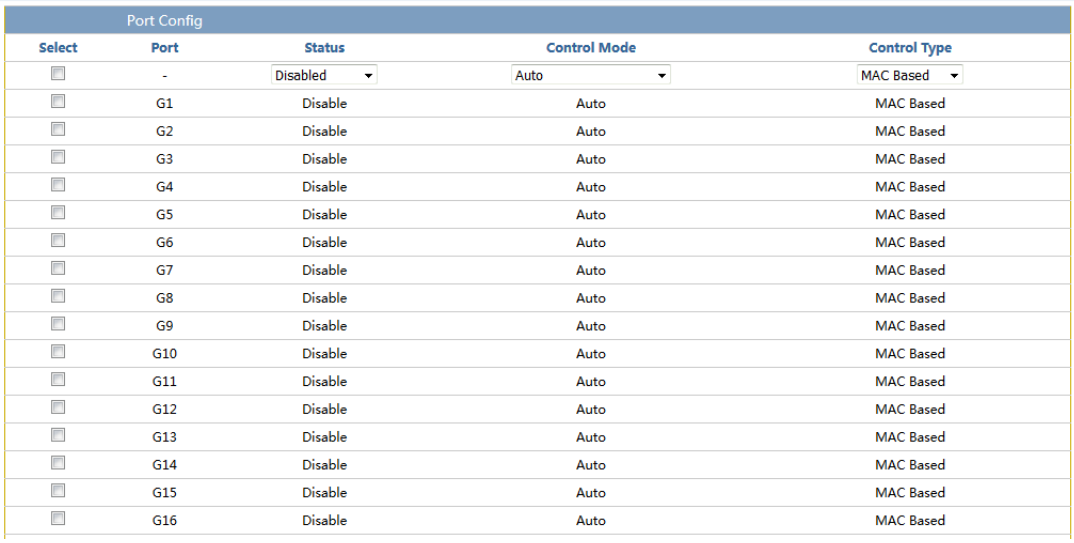


Table7-5-1 Main elements

Interface element	Description
Mode	Enable/disable 802.1X.
Update	Enable/disable authentication update.
Authentication update interval	Configure time intervals of authentication update .default time is 3600s.
Quiet	Enable/disable to silence the timer.
Quiet-period	Configure the quiet-period cycle time.Default time is 60s.
Hold time	Configure hold time.Default time is 300s.

Figure7-5-2 Port Config interface



Port Config

Select	Port	Status	Control Mode	Control Type
	-	Disabled	Auto	MAC Based
	G1	Disable	Auto	MAC Based
	G2	Disable	Auto	MAC Based
	G3	Disable	Auto	MAC Based
	G4	Disable	Auto	MAC Based
	G5	Disable	Auto	MAC Based
	G6	Disable	Auto	MAC Based
	G7	Disable	Auto	MAC Based
	G8	Disable	Auto	MAC Based
	G9	Disable	Auto	MAC Based
	G10	Disable	Auto	MAC Based
	G11	Disable	Auto	MAC Based
	G12	Disable	Auto	MAC Based
	G13	Disable	Auto	MAC Based
	G14	Disable	Auto	MAC Based
	G15	Disable	Auto	MAC Based
	G16	Disable	Auto	MAC Based

Table7-5-2 Main elements

Interface element	Description
Select	Select the port to configuration.
Port	Displays the name of the port on which the 802.1X is opened.
Status	Choose whether to enable 802.1X function in this port.
Control Mode	Select authentication mode.
Control Type	Select the type of authentication,port based or MAC based.

7.6 AAA

【Function description】

AAA is the abbreviation of authentication, authorization and accounting.It is a security management mechanism for access control in network security.Provide authentication, authorization and accounting for three kinds of security services.

【Operating path】

Network Security > AAA

【Interface description】

Figure7-6-1 Radius Config interface

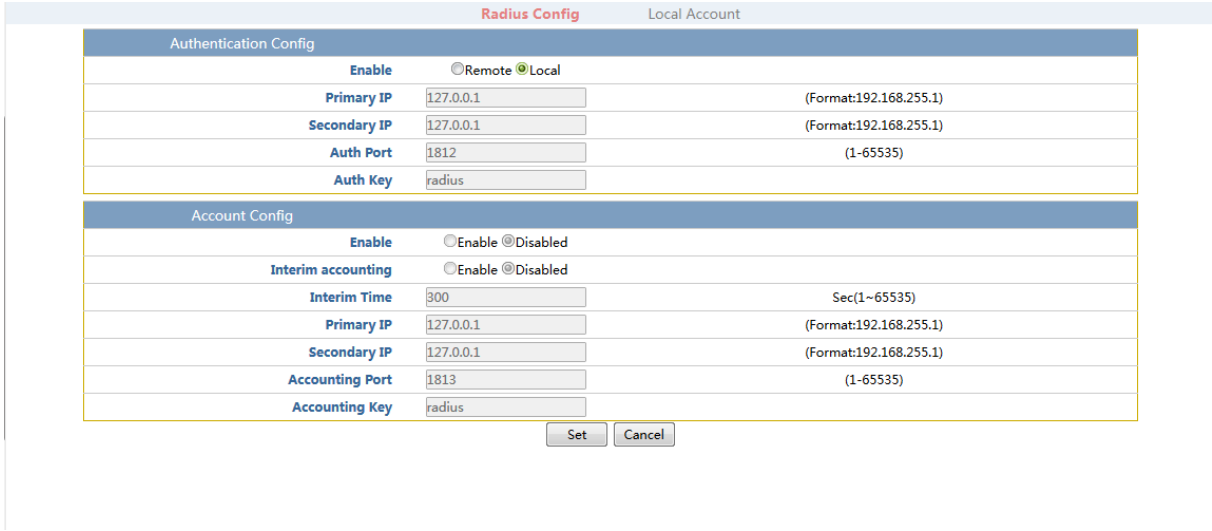


Table7-6-1 Main elements

Interface element	Description
Authentication Config	
Enable	Select local authentication or remote authentication.
Primary IP	Configure the address of the master radius server.
Secondary IP	Configure the address of the standby radius server.
Auth Port	Configure authentication port number.
Auth Key	Configure the key shared by the switch and the server.
Account Config	
Enable	Enable billing function.
Interim accounting	Enable real-time billing functions.
Interim Time	You can configure interim time,default time is 300s.
Primary IP	Configure the main billing server address.
Secondary IP	Configure alternate billing server addresses.
Accounting Port	Configure billing port number.
Accounting Key	Configure the switch to share the password with the server.

Figure7-6-2 Local Account interface

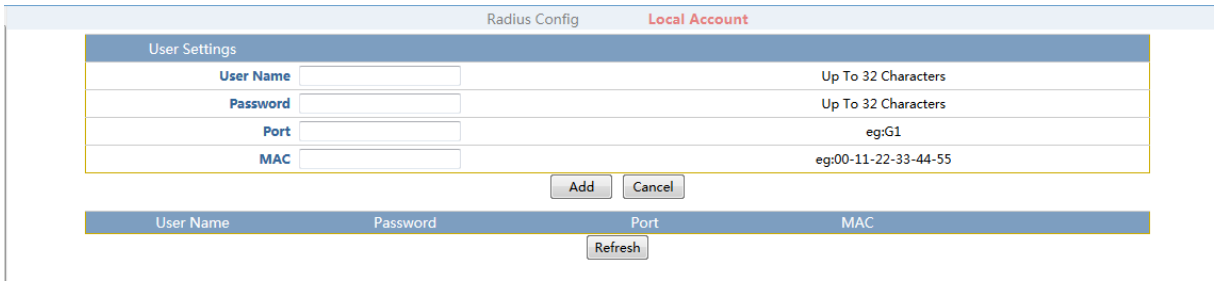
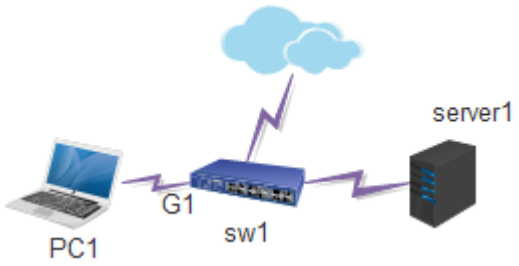


Table7-6-2 Main elements

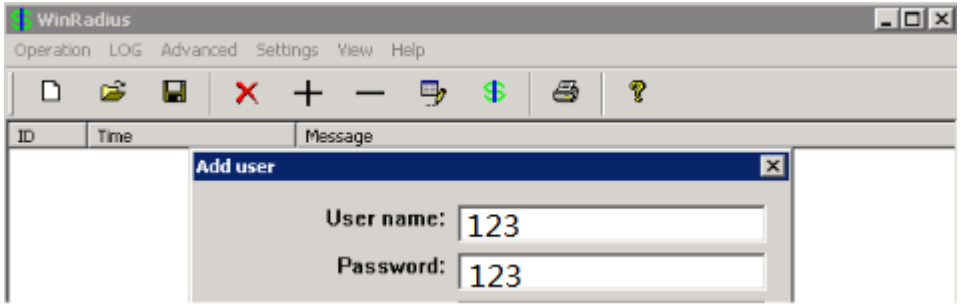
Interface element	Description
User Name	Configure the local authentication account.
Password	Configure local authentication password.
Port	Configure port for binding account.
MAC	Configure the MAC address for the binding account.

【Example】



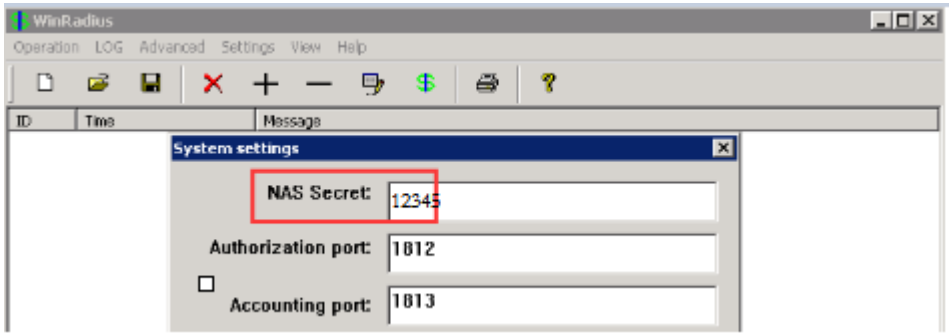
1.Configure ip is 192.168.2.96 in server1.

2.Start the WinRadius. Choose **Operation** > **Add Account** to add an account and password.

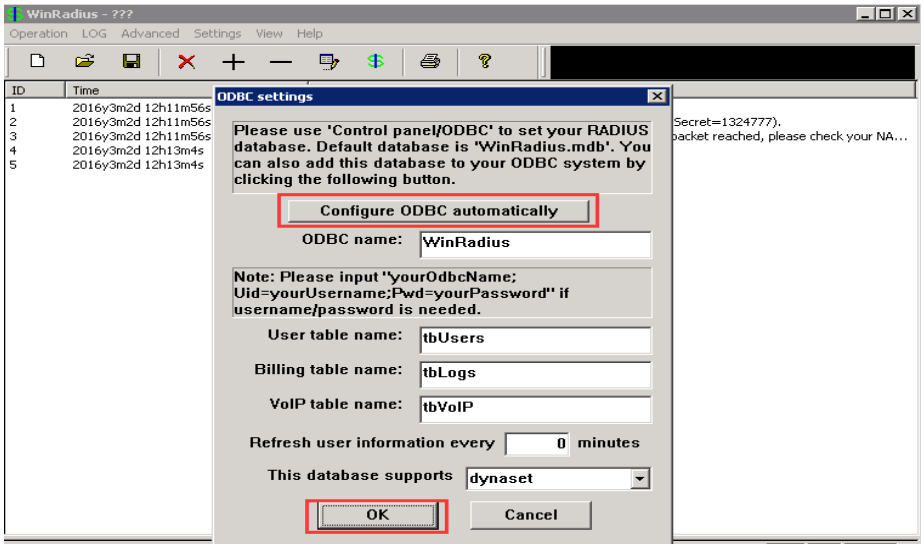


3.Choose **Advanced** > **Create RADIUS Table** to create a RADIUS table.

4.Choose **Settings** > **System Settings**. Modify the NAS key so that the NAS key is the same as the key configured on the web page of the switch.



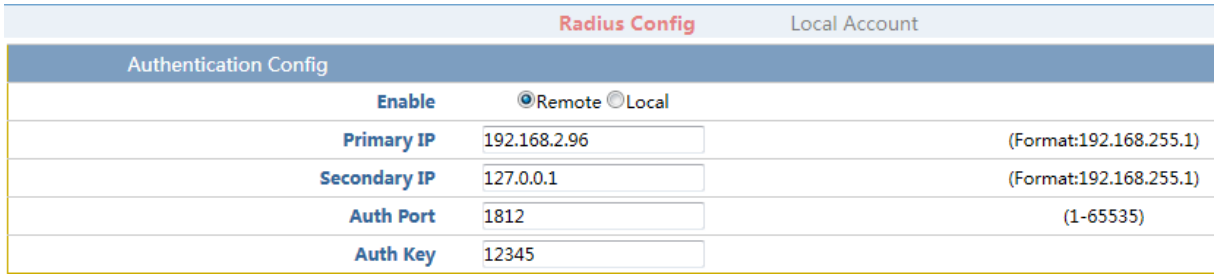
5.Choose **Settings** > **Data Settings**. Click **Configure ODBC automatically**, and then click **OK**.



6.Restart the WinRadius.

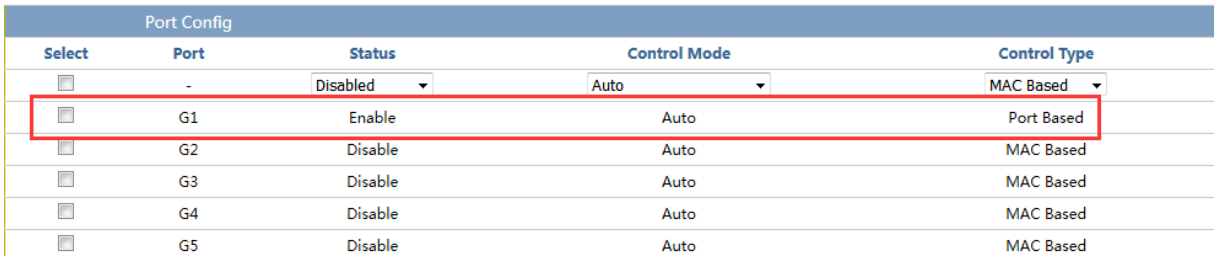
7.Remove and then insert the network cable that is connected to port 1 of the PC where the client is installed. An authentication login page is displayed on the client. Enter the user name and password. Then, the client can access the network normally.

8.Enable remote radius in"AAA" page,primary IP=192.168.2.96,Auth key=12345.other parameters default.



9.Enable 802.1X function in radius config page,and enable G1 in port config page,control

mode choose"auto",control type choose"port based".

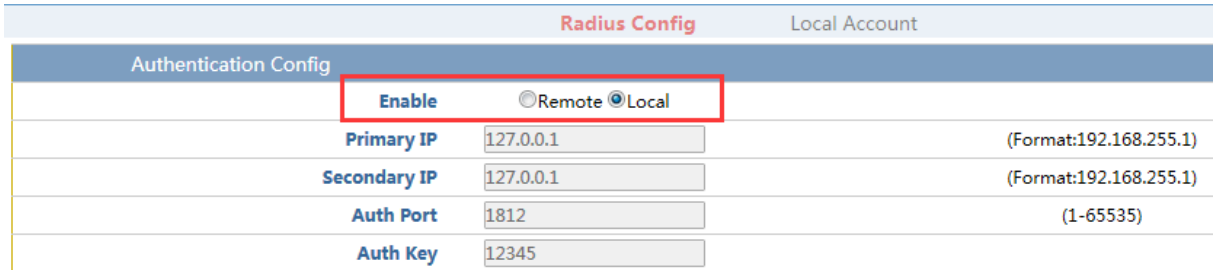


10.Enable 802.1X authentication function and choose MD5 authentication in pc1.

11.Enter user name and password in the login interface of the client.then you can access networks after authentication.

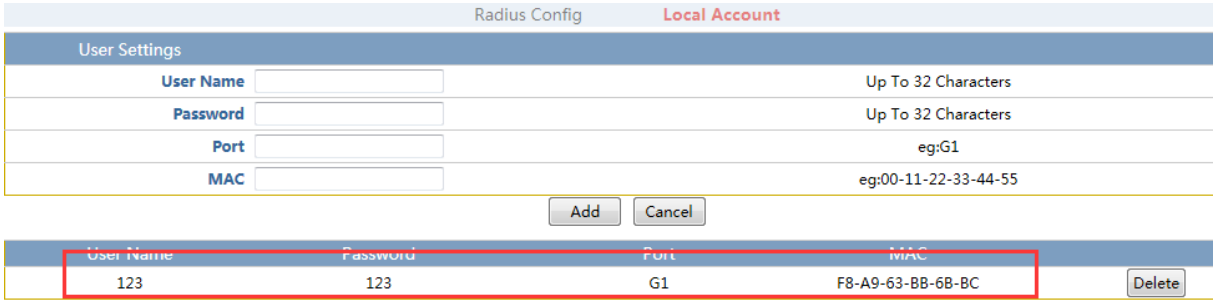
Local authentication:

a.Enable local authentication:

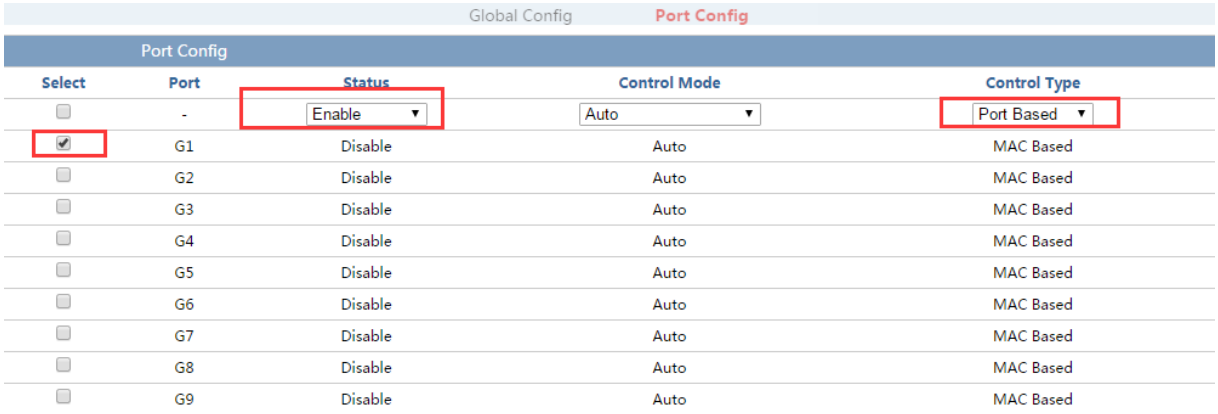


b.Set up the account in the"local authentication" page as follows:

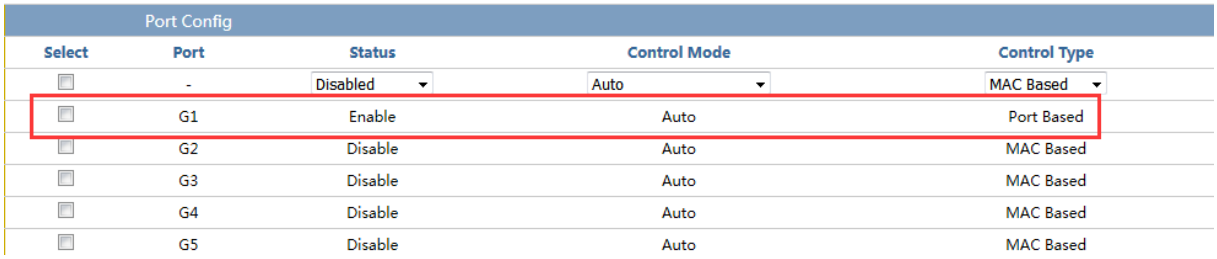
c.Username and password are 123,port G1 and MAC address be bound.(MAC address of PC1)



d.Enable 802.1X function in“802.1X" page.and select G1 port and status select"Enable" and control type select"Port Based"and then click"set"button in"Port config" page.



The following figure is the result:



e.Plug in cable again and login box will pop up,and then enter user name and password.

7.7 Port isolation

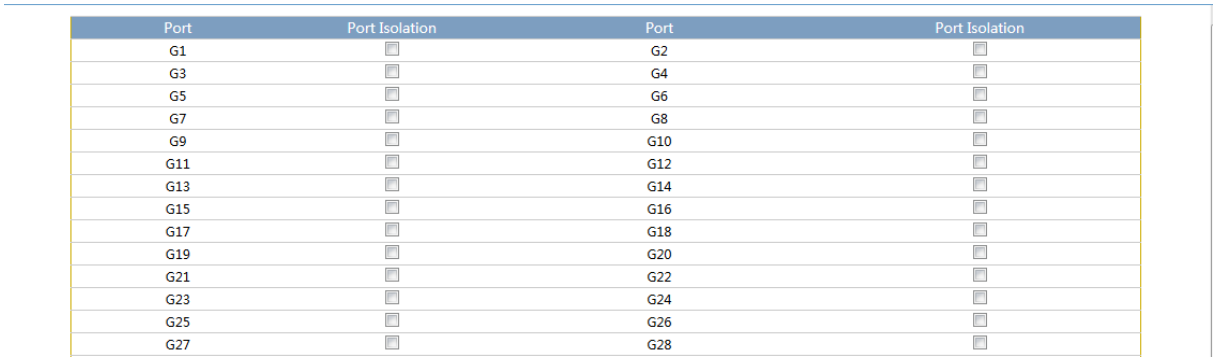
【Function description】

On the "Isolation Port" page, you can configure the ports to be isolated from each other.
【Operating path】

Network Security > port isolation

【Interface description】

Figure7-7 Port Isolation interface

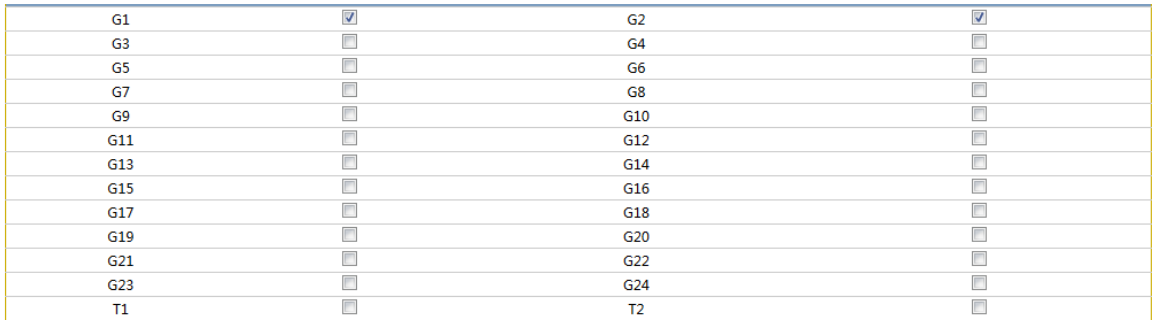


Port	Port Isolation	Port	Port Isolation
G1		G2	
G3		G4	
G5		G6	
G7		G8	
G9		G10	
G11		G12	
G13		G14	
G15		G16	
G17		G18	
G19		G20	
G21		G22	
G23		G24	
G25		G26	
G27		G28	

Table7-7 Main elements

Interface element	Description
Port	Display each port number.
Port isolation	Check the port's "Isolation Port" check box, indicating that the corresponding port will be isolated.

【Example】



G1	✓	G2	✓
G3		G4	
G5		G6	
G7		G8	
G9		G10	
G11		G12	
G13		G14	
G15		G16	
G17		G18	
G19		G20	
G21		G22	
G23		G24	
T1		T2	

If the two ports open the port isolation function, then they can not communicate .

Communication between the isolated port and the port without isolation is normal.

7.8 Storm control

【Function description】

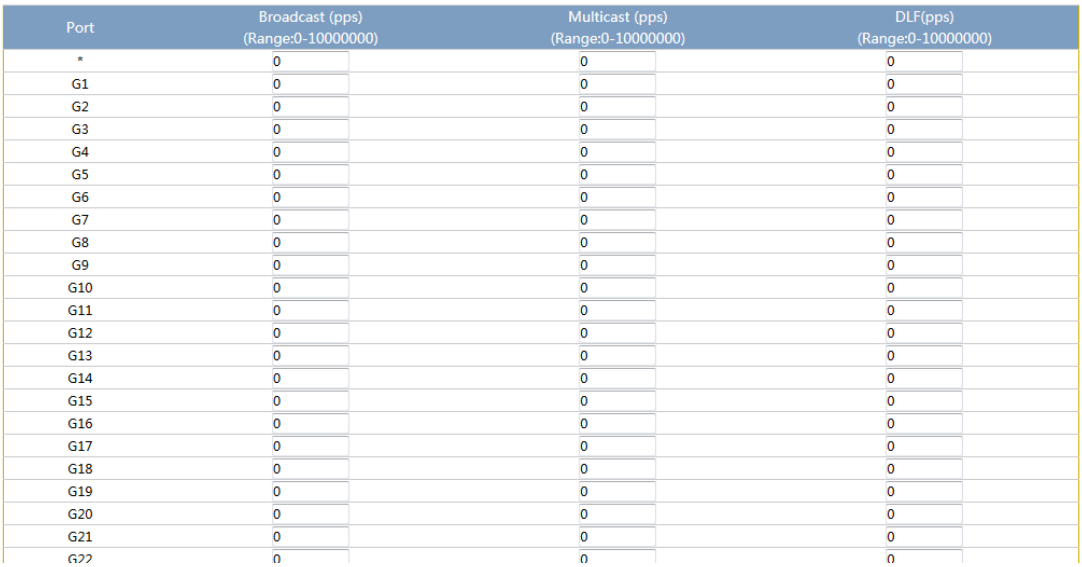
On the "Control Storm" page,You can configure the rate for each port with the broadcast packets ,the multicast packets and the unknown unicast packets,to achieve the function of storm control.

【Operating path】

Network Security > storm control

【Interface description】

Figure7-8 Storm Control interface



Port	Broadcast (pps) (Range:0-10000000)	Multicast (pps) (Range:0-10000000)	DLF(pps) (Range:0-10000000)
*	0	0	0
G1	0	0	0
G2	0	0	0
G3	0	0	0
G4	0	0	0
G5	0	0	0
G6	0	0	0
G7	0	0	0
G8	0	0	0
G9	0	0	0
G10	0	0	0
G11	0	0	0
G12	0	0	0
G13	0	0	0
G14	0	0	0
G15	0	0	0
G16	0	0	0
G17	0	0	0
G18	0	0	0
G19	0	0	0
G20	0	0	0
G21	0	0	0
G22	0	0	0

Table7-8 Main elements

Interface element	Description
Port	Display each port number.
Broadcast	Configure the broadcast suppression rate for the corresponding port. Unit: pps
Multicast	Configure multicast suppression rate for the corresponding port. Unit: pps
DLF	Configure unknown unicast suppression rate for the corresponding port. Unit: pps

7.9 ERPS-Ring config

【Function description】

Loop protection is similar to STP, but it lacks an IEEE standard and is a private protocol. Loop protection is easy to configure and use. It is suitable for a simple ring topology and common network services, and has obvious advantages in line backup.

And set the relevant parameters.Enable port loop protection function and set the relevant parameters.On the "Config ERPS-Ring" page, you can enable or disable the ERPS-Ring feature.

The loop protection function of the enable port and set the relevant parameters.

【Operating path】

Network Security > erps-ring config

【Interface description】

Figure7-9 ERPS-Ring Global Config interface

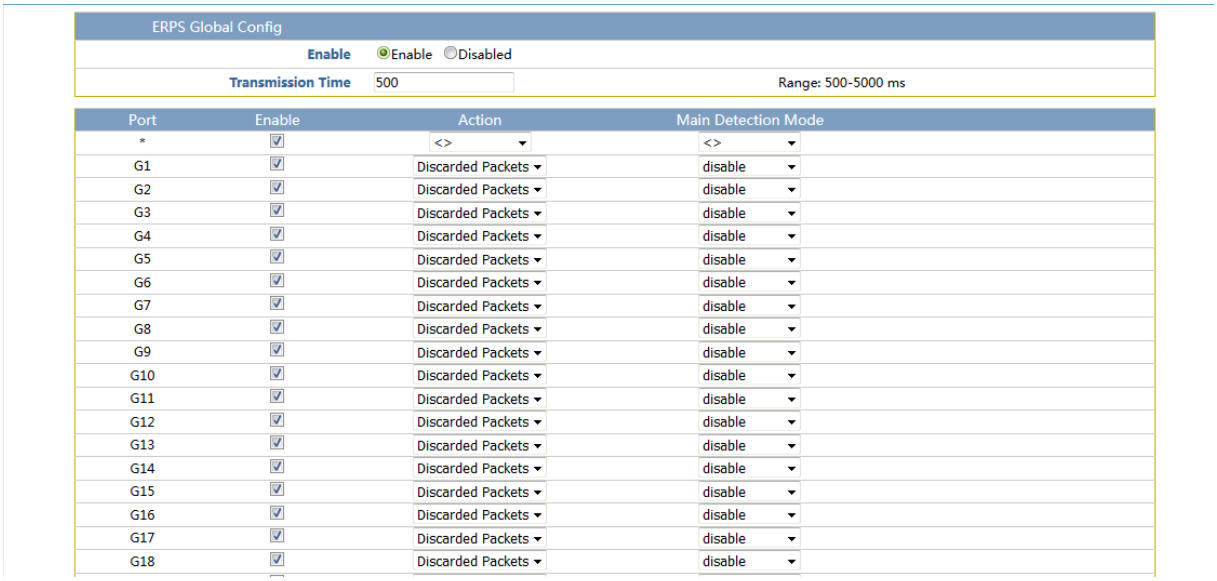


Table7-9 Main elements

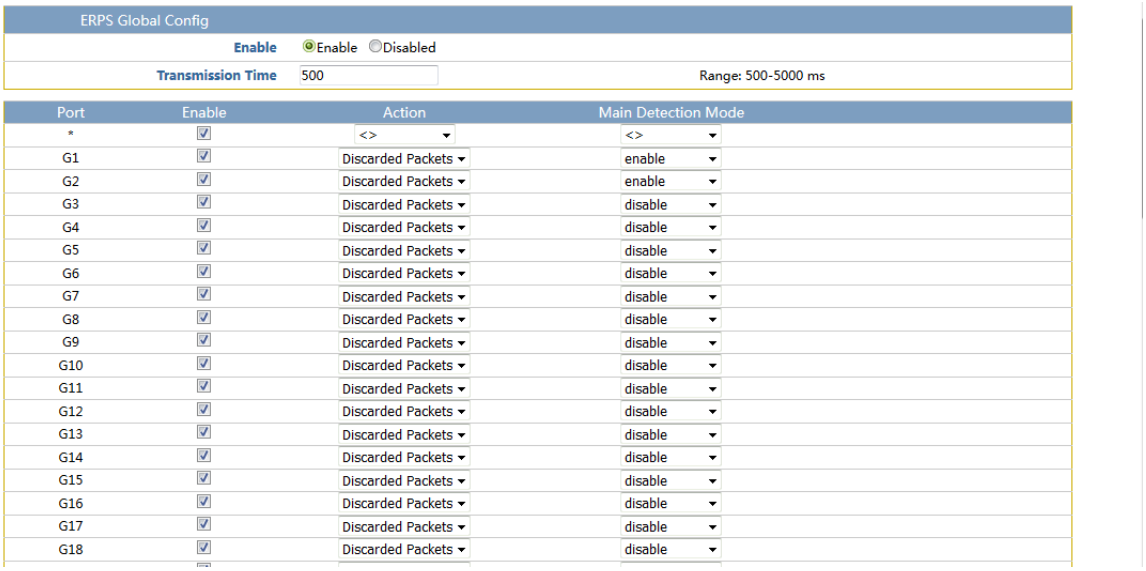
Interface element	Description
Enable	Enable or disable ERPS-Ring functionality.
Transmission Time	Configuring transmission time. The default time is

	500ms,the range is 500-5000ms
Port	Shows the switch port number.
Enable	Check the "enable" check box, Indicates the corresponding port is enabled
Action	Select the behavior of the corresponding port. The default state is to drop packets.
Main Detection Mode	Select the master detection mode of port. Disable: Close master detection mode; Enable:Open master detection mode.

【Example】

All switches turn on ERPS-Ring function.One of the main open detection mode,

Two ports are open.



ERPS Global Config

Enable: Enable / Disabled

Transmission Time: 500 (Range: 500-5000 ms)

Port	Enable	Action	Main Detection Mode
*	☑	<>	<>
G1	☑	Discarded Packets	enable
G2	☑	Discarded Packets	enable
G3	☑	Discarded Packets	disable
G4	☑	Discarded Packets	disable
G5	☑	Discarded Packets	disable
G6	☑	Discarded Packets	disable
G7	☑	Discarded Packets	disable
G8	☑	Discarded Packets	disable
G9	☑	Discarded Packets	disable
G10	☑	Discarded Packets	disable
G11	☑	Discarded Packets	disable
G12	☑	Discarded Packets	disable
G13	☑	Discarded Packets	disable
G14	☑	Discarded Packets	disable
G15	☑	Discarded Packets	disable
G16	☑	Discarded Packets	disable
G17	☑	Discarded Packets	disable
G18	☑	Discarded Packets	disable

one of the ports was blocked,In the following pages you can see.

ERPS Status

Port	Action	Transmission Packets	Port Status	Loop
G1	Discarded Packets	Allow	Up	-
G2	Discarded Packets	Allow	Disabled	Loop
G3	Discarded Packets	Disabled	Down	-
G4	Discarded Packets	Disabled	Down	-
G5	Discarded Packets	Disabled	Down	-
G6	Discarded Packets	Disabled	Down	-
G7	Discarded Packets	Disabled	Down	-
G8	Discarded Packets	Disabled	Down	-
G9	Discarded Packets	Disabled	Down	-
G10	Discarded Packets	Disabled	Down	-
G11	Discarded Packets	Disabled	Down	-
G12	Discarded Packets	Disabled	Down	-
G13	Discarded Packets	Disabled	Down	-
G14	Discarded Packets	Disabled	Down	-
G15	Discarded Packets	Disabled	Down	-
G16	Discarded Packets	Disabled	Down	-
G17	Discarded Packets	Disabled	Down	-
G18	Discarded Packets	Disabled	Down	

7.10 ERPS-E config

【Function description】

Ethernet Ring Protection Switching (ERPS) is an Ethernet multi-ring protection technology defined in ITU-TG.8032. Aiming to improve network performance and security, ERPS is an Ethernet ring technology that becomes an important redundancy protection measure on the L2 network.

On the L2 network, STP is often used to ensure network reliability, and the loop protection protocol may also be used. STP is a standard ring protection protocol developed by IEEE, and has been widely used. In practice, application of STP is restricted by the network size, and the convergence time is affected by the network topology. The convergence time of STP is generally several seconds, or longer if the network diameter is large. The use of RSTP/MSTP can reduce the convergence time to several milliseconds, but still cannot meet the requirements of services (such as 3G and NGN voice services) that require a high Quality of Service (QoS). ERPS emerges to further reduce the convergence time and eliminate the impact caused by the network size.

ERPS is a link layer protocol dedicated for the Ethernet ring. It can prevent broadcast storms caused by data loops in an Ethernet ring. When a link on the Ethernet ring is disconnected, the backup link can be quickly enabled to recover communication between nodes on the ring network. Compared with STP, ERPS features a fast topology convergence speed (less than 20 ms) and the convergence time that is independent of the number of nodes on the ring network. Loop protection is similar to STP and ERPS, but it lacks an IEEE standard and is a private protocol. Loop protection is easy to configure and use. It is suitable for a simple ring topology and common network services, and has obvious advantages in line

backup.

【Operating path】

Network Security >erps-e config

【Interface description】

Figure7-10-1 ERPS-E settings interface

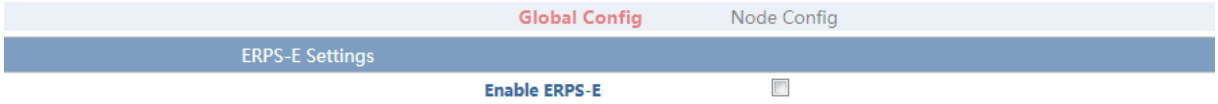


Table7-10-1 Main elements

Interface element	Description
Enable ERPS-E	Enable or disable ERPS-E functionality.

Figure7-10-2 Node settings interface

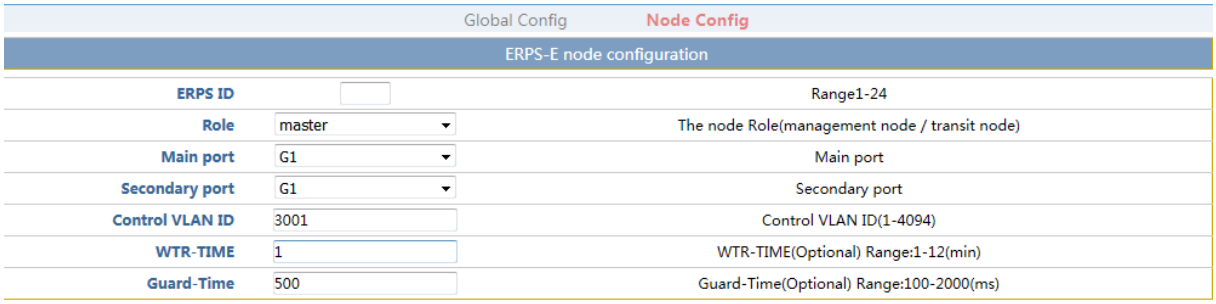
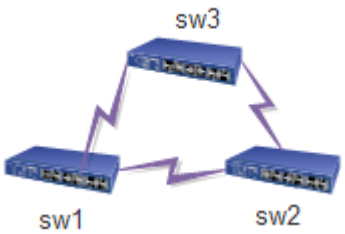


Table7-10-2 Main elements

Interface element	Description
ERPS ID	ERPS domain identity, with an integer, the range is 1-24.
Role	Select node role.1.master,2.transit.
Main port	Select the main port.
Secondary port	Select from port.
Control vlan id	Configure the control VLAN ID,the range is 1-4094, default is 3001

Wtr-time	Configure the time of the wtr-time timer,the range is 1-12m. default time is 1m.
Guard time	Configure the time of Guard timer , the range is 100-2000ms, default time is 500ms.

【Example】



Enable ERPS-E function;

To configure ERPS ID=1,Role=master,main port=G19,secondary port=G20,Other values to select the default value .

ERPS ID	Role	Main port	Secondary port	master state	slave state	Control VLAN ID	WTR-TIME	WTR-remaining	state	
1	Master	G19	G20	block	forward	3001	1	22900	PENDING	Delete

7.11 IP source guard

【Function description】

Through the IP source protection function,port forwarding packets can be filtered control,prevent illegal message passing port,thus restricting the illegal use of network resources (Such as illegal host counterfeiting legitimate users IP access network,Improve the port security.)

On the IP source protection configuration page, you can enable or disable the IP source protection feature.

【Operating path】

Network Security >IP Source Guard

【Interface description】

Figure7-11-1 Source Guard interface

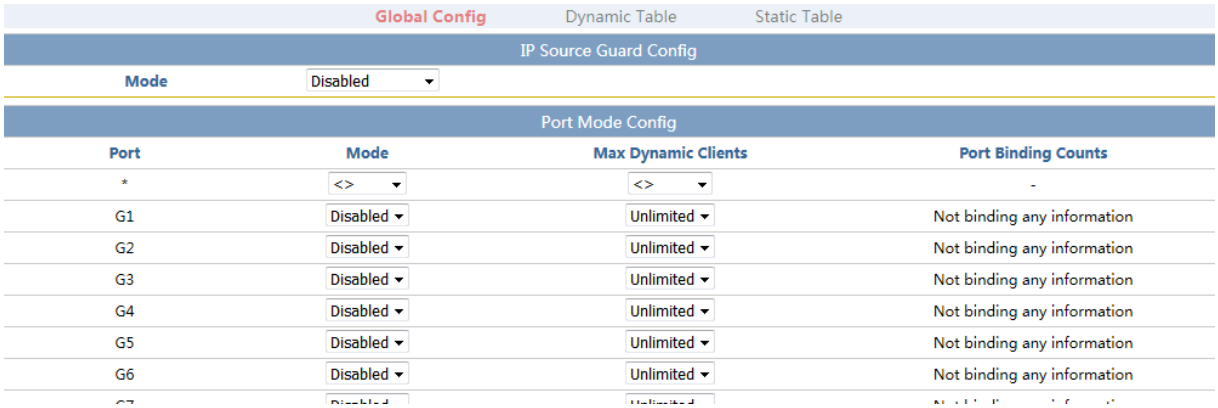
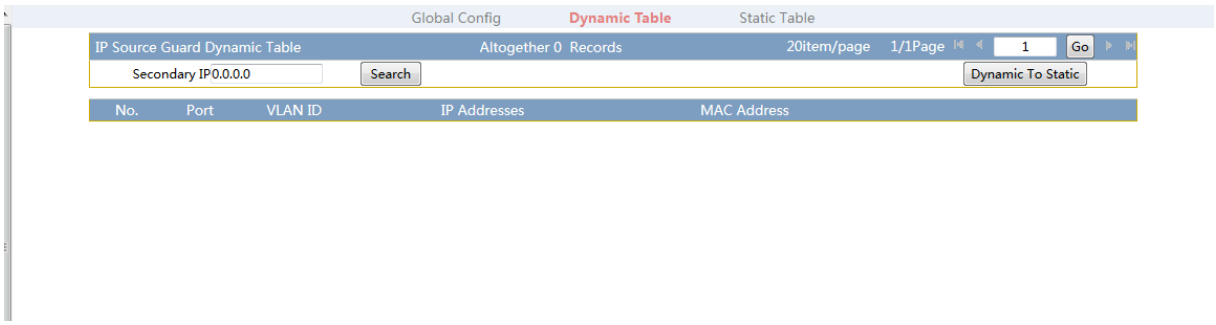


Table7-11-1 Main elements

Interface element	Description
Mode	Enables or disables global IP source protection.
Port	Display port number.
Mode	Enable or disable port IP source protection.
Max Dynamic Clients	Allows the maximum number of dynamic clients, optional 0,1,2, unlimited.
Port Bangding Counts	Displays the number of ports that are currently bound.

Figure7-11-2 Dynamic Table interface



Note: this feature can only be implemented in web, the command line can not be achieved.

Table7-11-2 Main elements

Interface element	Description
Search	Search the corresponding dynamic table entry.
Dynamic To Static	The dynamic table entry is converted to a static table entry.

Figure7-11-3 Static Table interface

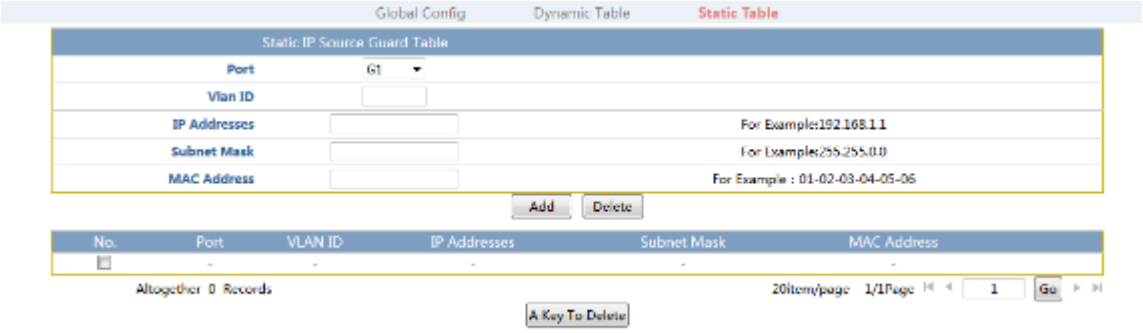


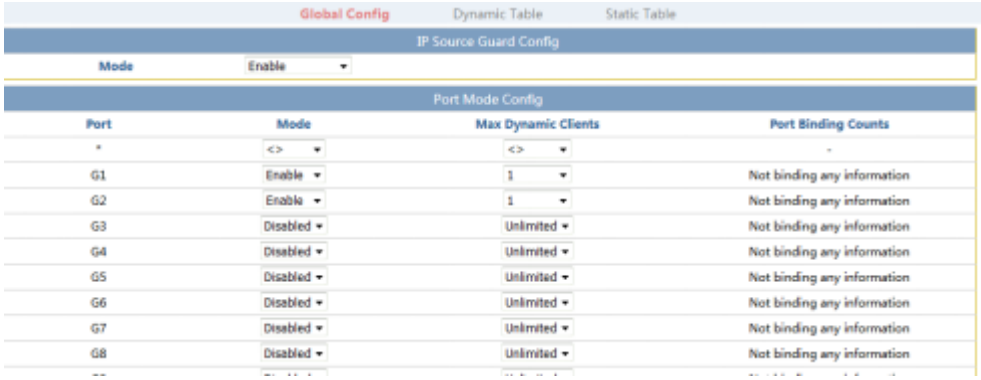
Table7-11-3 Main elements

Interface element	Description
Port	Select the port you want to bind.
Vlan ID	Fill port of the Vlan.
IP Address	Fill in the terminal IP address to be bound.
Subnet mask	Fill in the terminal subnet mask to be bound.
MAC Address	Fill in the terminal MAC address to be bound.

【Example】

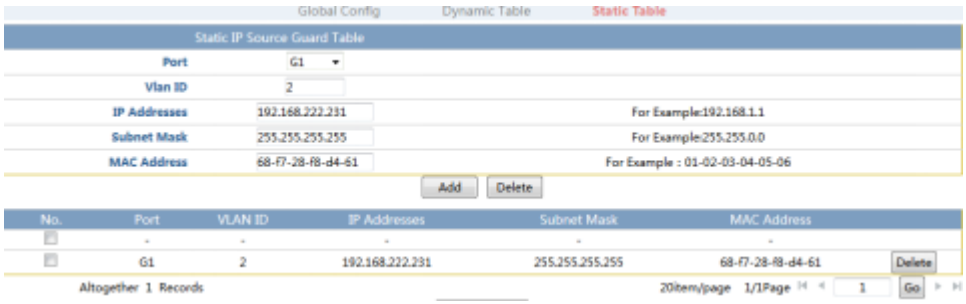
Open IP source protection function,Select the port to open source protection,

And select the number of bindings.



Bind VLAN2 on G1 port,IP address is 192.168.222.231,MAC is PC's 68-f7-28-d4-61.

This PC can only be in the G1 port to communicate,not in the G1 port can not communicate,other PC in this port can not be normal communication.



8 Network management

8.1 HTTP config

【Function description】

You can turn on or off the HTTP and HTTPS features on the "HTTP" page.

【Operating path】

Network management > HTTP config

【Interface description】

Figure8-1 HTTP config interface

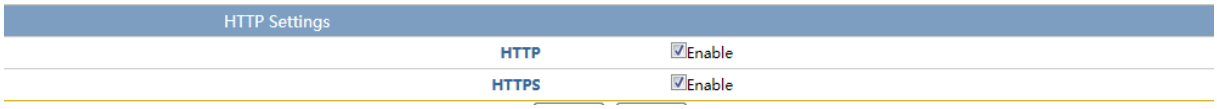


Table8-1 Main elements

Interface element	Description
HTTP	Check the "enable" , then open the HTTP function. You can log on the switch WEB page through the "http://192.168.255.1".
HTTPS	Check the "enable" , then open the HTTPS function. You can log on the switch WEB page through the "https://192.168.255.1".

8.2 SNMP config

【Function description】

SNMP is a network management protocol that is most popular on the UDP/IP network. It provides a management framework to monitor and maintain Internet devices.

SNMP network elements (NEs) are classified into two types: network management station (NMS) and agent.

- The NMS is a workstation on which the SNMP client runs. It provides a user-friendly human-computer interaction interface, with which network administrators can conveniently complete the majority of network management work.
- The agent is a process that resides on a device. It collects and processes requests sent from the NMS. In case of an emergency, for example, when the interface status changes, the agent will notify the NMS of the change.

The NMS is the manager of the SNMP network, whereas the agent is the managed object of the SNMP network. The NMS and the agent exchange management information over SNMP.

SNMP provides four basic operations:

- Get: The NMS uses this operation to query one or more object values of the agent.
- Set: The NMS uses this operation to reconfigure one or more objects in the MIB of the agent.
- Trap: The agent uses this operation to send alarms to the NMS.
- Inform: The agent uses this operation to send warning information to the NMS.

SNMP protocol versions:

Currently, the SNMP agent of the device supports SNMP v2, and is compatible with SNMP v1 .

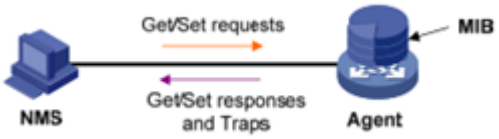
SNMP v1 uses the community name for authentication. The community name defines the relationship between the SNMP NMS and the SNMP agent. If the community name carried by an SNMP packet is not recognized by the device, the packet is dropped. The community name plays a role similar to the password, and is used to restrict the access of the SNMP NMS to the SNMP agent.

SNMP v2c also uses the community name for authentication. It is compatible with SNMP v1, and expands functions of SNMP v1. SNMP v2c provides more operation types (including GetBulk and InformRequest), supports more data types (such as Counter64), and

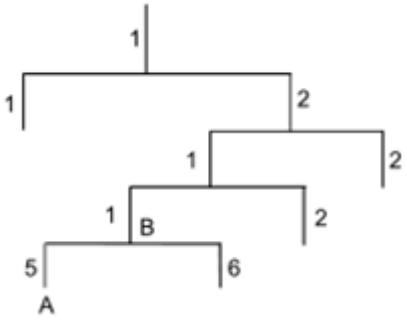
provides more error codes to distinguish errors in a more accurate manner.

Introduction to the MIB:

Any managed resource is represented as an object, which is also called a managed object. The MIB is a collection of managed objects. It defines a series of attributes for each managed object, including the name, access permission, and data type of the object. Each agent has its own MIB. The NMS can perform read/write operations on objects in the MIB based on the configured permissions. The following figure shows the relationship between the NMS, agent, and MIB.



Data is stored in the MIB using a tree structure. A node on the tree represents a managed object, which can be uniquely identified by a path starting from the root. As shown in the following figure, managed object B can be uniquely identified by a number string {1.2.1.1}. This number string is called object identifier (OID) of the managed object.



【Operating path】

Network management > SNMP config

【Interface description】

Figure8-2 SNMP Config interface

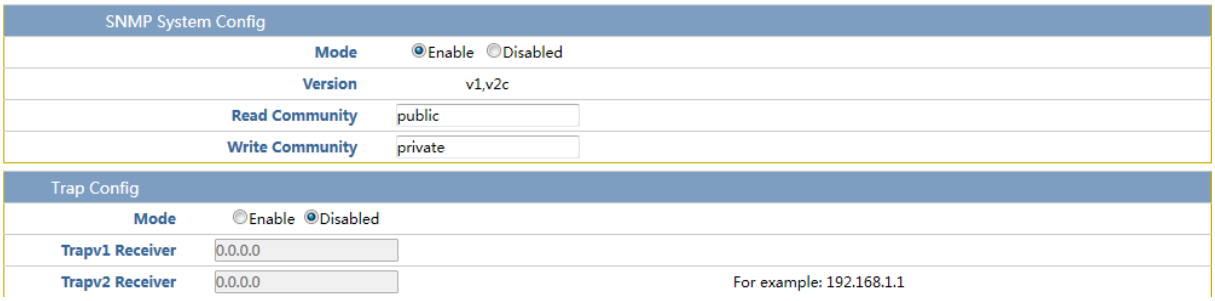


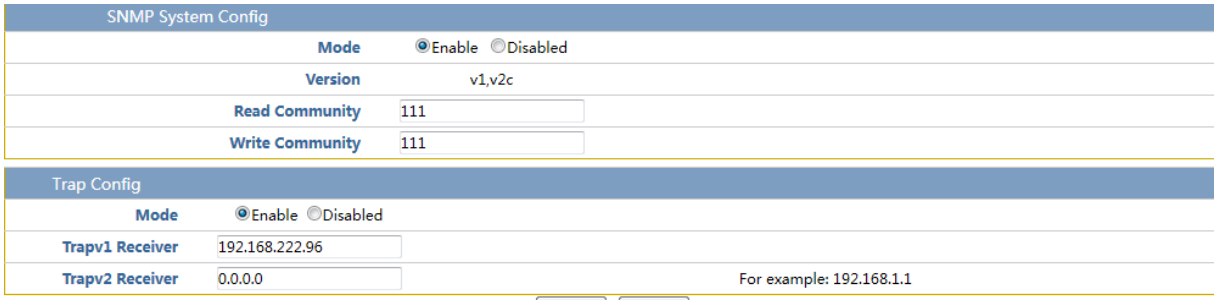
Table8-2 Main elements

Interface element	Description
Snmp system config	
Mode	SNMP Enable / disable.
Version	SNMP supported versions of V1, V2C.
Read community	Access the common name of the network management, permissions to read, the default is public.
Write community	Access the common name of the network management, permissions for the write, the default is private.
Trap config	
Mode	Trap Enable / disable.
Trapv1 Receiver	Fill in the SNMPV1 version of the trap to receive the address.
Trapv2 Receiver	Fill in the SNMPV2 version of the trap to receive the address.

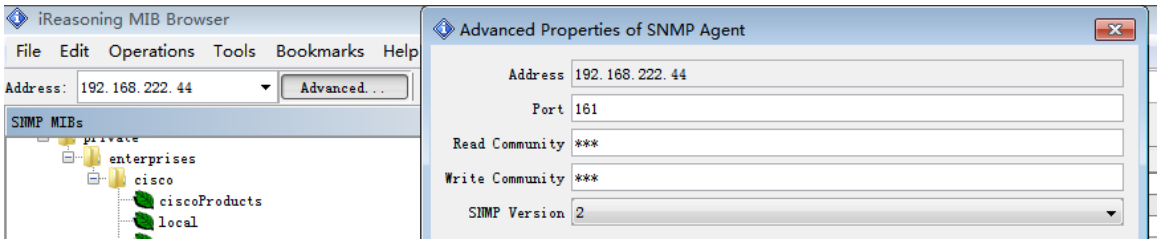
【Example】

1. Enable SNMP, and set the version to SNMP V1,V2c, Read Community to 111, and Write Community to 111.

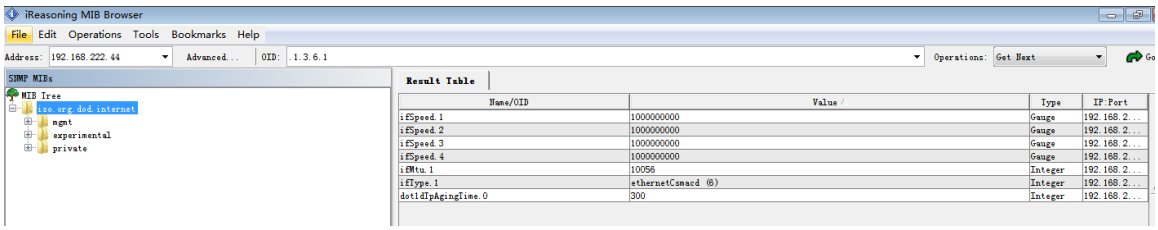
Enable trap, input 192.168.222.96 in trapV1 (management system side of the IP, our trap is currently only coldstart,linkup,linkdown,just configure the trapv1), click ‘save’.
The following figure shows the configuration results.



3. Use the MIB browser, load the corresponding MIB, fill in the IP address of the managed device,and set Read Community, Write Community, and SNMP Version, as shown in the following figure.



4 the following chart, right click iso.org.dod.internet, click 'work', in the information display page will display relevant information.



9 System maintenance

9.1 Reboot

【Function description】

You can restart the switch on the "reboot" page.

【Operating path】

System maintenance > reboot

【Interface description】

Figure9-1 restart device interface

Table9-1 Main elements

Interface element	Description
Restart	you can restart the switch if you click restart button.

9.2 Restore factory

【Function description】

You can restore the switch to the factory configuration on the "factory restore" page.

【Operating path】

System maintenance >restore factory

【Interface description】

Figure9-2 Factory restore interface

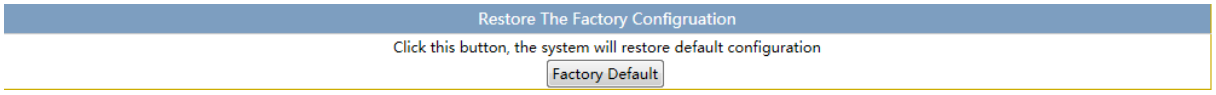


Table9-2 Main elements

Interface element	Description
Factory default	You can restore the switch to the factory configuration if you click"default factory".

In addition to the IP address, the other can restore the factory configuration.
DH-PFS6428-24T switch front panel has the RESET key, you only need to use the needle to be 5 seconds to restore the factory configuration.

9.3 Online upgrade

【Function description】

You can achieve the switch software online upgrade function on the "upgrade online" page.

【Operating path】

System maintenance >online upgrade

【Interface description】

Figure9-3 Upgrade Online interface

Table9-3 Main elements

Interface element	Description
File path	Click "file select", select the software you are ready to upgrade the file, click "Upload", you can realize the switch software online upgrade.

Note:

Please do not click or configure the switch to other WEB pages, and not to restart the switch in the software upgrade process; otherwise it will lead to the failure of the software upgrade, and resulting in the failure of the switch system and other phenomena.

And last,Due to compatibility issues,we suggest the use of chrome or Firefox to upgrade.

9.4 Config management

【Function description】

You can download the current profile from the switch, and you can also upload the existing configuration to the switch on the "configuration management" page.

【Operating path】

System maintenance > config management

【Interface description】

Figure9-4-1 Management config interface

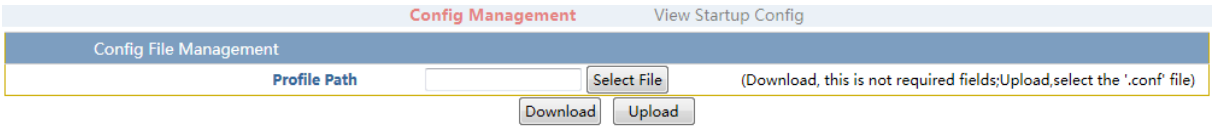


Table9-4-1 Main elements

Interface element	Description
Profile path	Click "download" to download the current profile of the switch. Click "select file", select the configuration file you are ready, and click "Upload", you can upload the existing configuration to the switch.

Please do not click or configure the switch to other WEB pages, and not to restart the switch if in the configuration file upload process; otherwise it will lead to the configuration file upload failed, and resulting in a breakdown of the switch system or other phenomena.

Figure9-4-2 Startup config view page

Table9-4-2 Main elements

Interface element	Description
Current startup config	Displays the current boot configuration information for the switch.

9.5 Ping test

【Function description】

Like the **ping** command on a common PC, the PING diagnose function is used to test connectivity between two nodes on the network. The difference between the **ping** command and PING diagnose is as follows: The **ping** command executed between two common PCs is used to check whether the physical connection between the two PCs is normal. The PING diagnose function of the switch helps the network administrator test whether a network device is disconnected on a LAN and locate network faults based on the test result.

【Operating path】

System maintenance > ping test

【Interface description】

Figure9-5 Test Ping interface

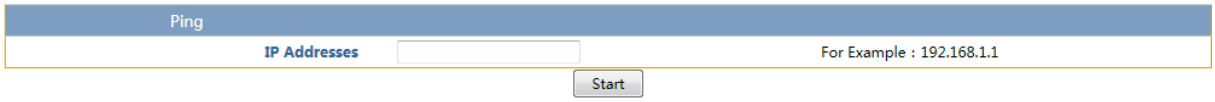


Table9-5 Main elements

Interface element	Description
Ip addresses	you can enter the IP address.

10 Diagnosis

Table 10-1 List of common fault diagnosis

Failure phenomena	Cause of failure	Solution
All the lights are not bright after power on.	Power connection error or power supply is not normal.	Check power cable and socket
LINK indicator light is not bright.	1.Cable damage or connection is not strong. 2.Cable type errors or network cable is too long,beyond the allowable range.	Replace cable.
Network communication is normal, but the transmission speed slowed and packet loss.	The switch port is not matched with the Ethernet port of the network terminal.	Set operation mode of the port to match or set it to an adaptive mode.
A certain port communication is normal, but the communication is not normal when the network cable to other ports.	If no data is sent when the network cable is changed to the other network port, the port will not be blocked because the switch will not be sent to the new address.	This phenomenon will disappear when the address of the switch will be automatically updated after 120 seconds ; or if you send data from the network port ,the address table will update immediately.
All ACT indicator light flashes and network speed becomes slow.	Broadcast storm	1.check whether the network connection into the loop and the reasonable configuration of the network.

		2.check if a large number of broadcast packets are send from a site.
A period of time to stop working after normal work.	1 power is not normal. 2 switch overheating.	1 check whether the power supply has a bad contact, or the voltage is too low or too high.. 2 check the surrounding environment, ventilation holes is free, and switch fan is working properly.