Four-Faith

Xiamen Four-Faith Communication Technology Co.,Ltd

FNS420-Series Industrial Switch

Web configuration manual

Index

1. Log in to the switch web

1.1 System requirements for WEB access

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

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

1.2 Log in to the WEB configuration interface

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

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

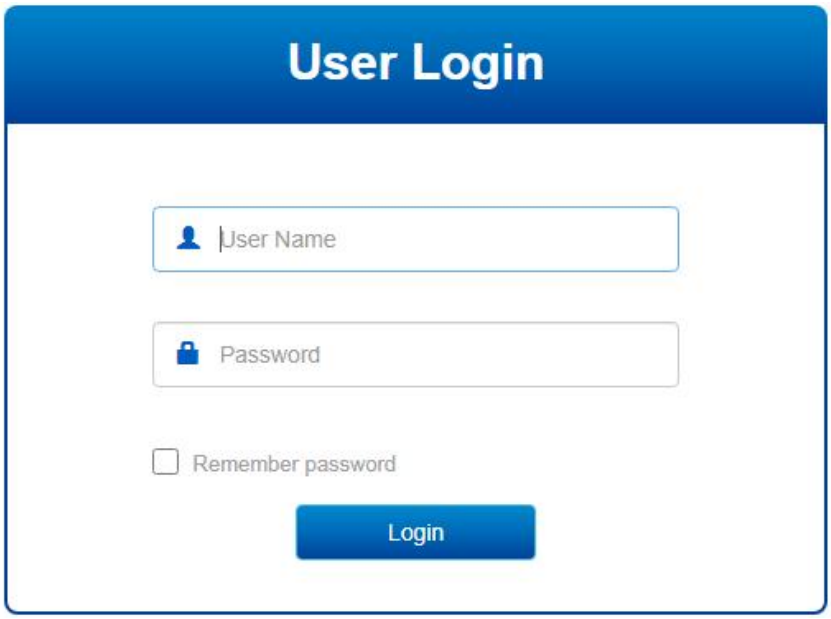
The steps to log in to the WEB configuration interface are as follows：

Step 1 Run the computer browser;

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

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

Figure 1-1 WEB interface login window



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

2. System Information

2.1 Global Information

【Function Description】

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

【Operation path】

Information > Global

【Interface description】

Figure 2-1 System Information Interface

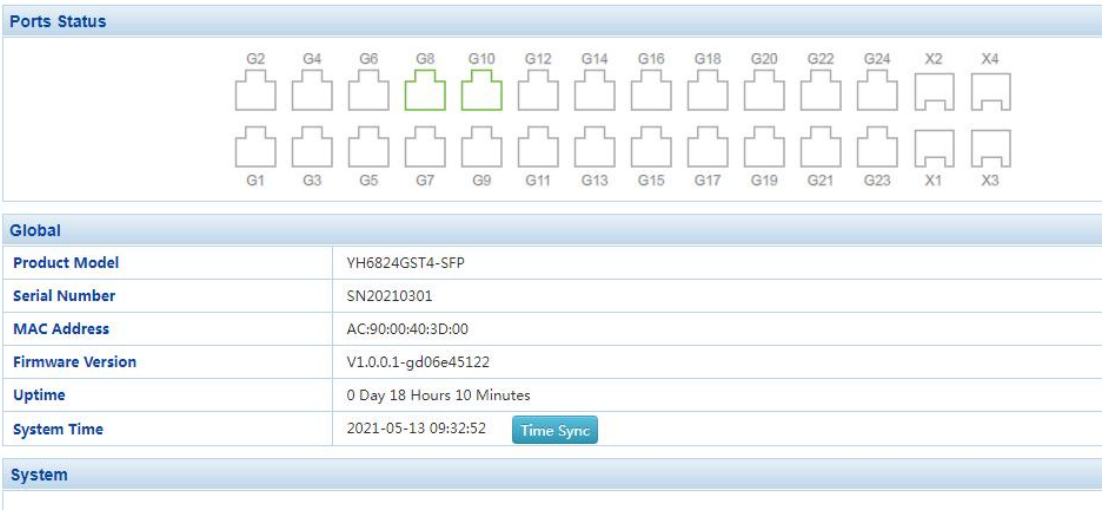


Table 2-1 Main elements of the system information interface

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

2.2 Statistics

【Function Description】

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

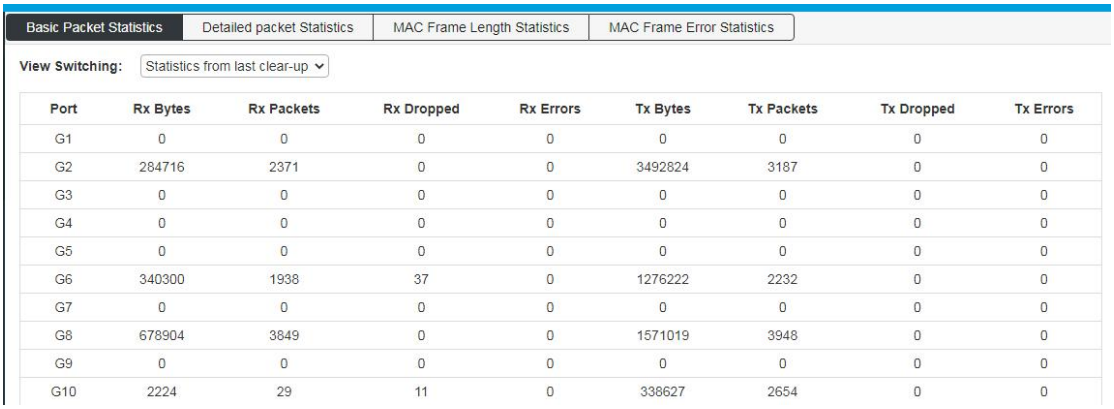
【Operation path】

Information > Statistics

【Interface description】

Figure 2-2 Port data

statistics



Port	Rx Bytes	Rx Packets	Rx Dropped	Rx Errors	Tx Bytes	Tx Packets	Tx Dropped	Tx Errors
G1	0	0	0	0	0	0	0	0
G2	284716	2371	0	0	3492824	3187	0	0
G3	0	0	0	0	0	0	0	0
G4	0	0	0	0	0	0	0	0
G5	0	0	0	0	0	0	0	0
G6	340300	1938	37	0	1276222	2232	0	0
G7	0	0	0	0	0	0	0	0
G8	678904	3849	0	0	1571019	3948	0	0
G9	0	0	0	0	0	0	0	0
G10	2224	29	11	0	338627	2654	0	0

2.3 Log

【Function Description】

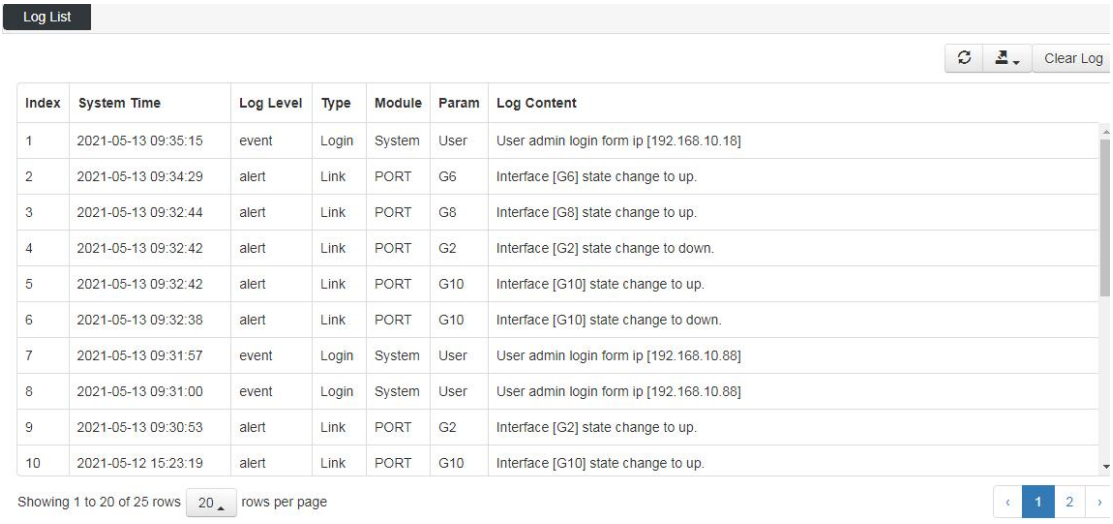
On the "Log" page, you can view and download the system log.

【Operation path】

Information > Log

【Interface description】

Figure 2-3-1 Log interface



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

3. Port Management

3.1 Port Config

【Function Description】

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

【Operation path】

Port > Port Config

【Interface description】

Figure 3-1 Port configuration

interface

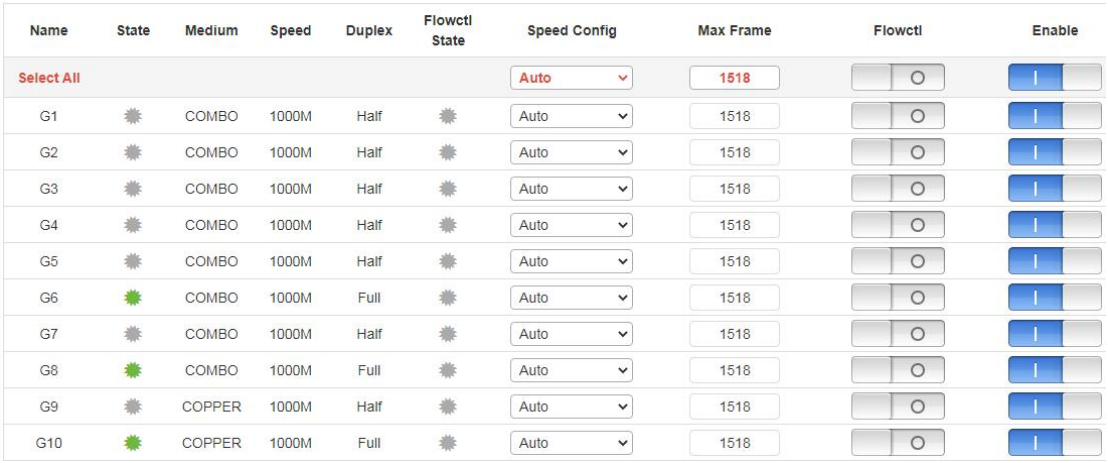


Table 3-1 Main elements of the port configuration interface

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

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

3.2 Port Isolate

【Function Description】

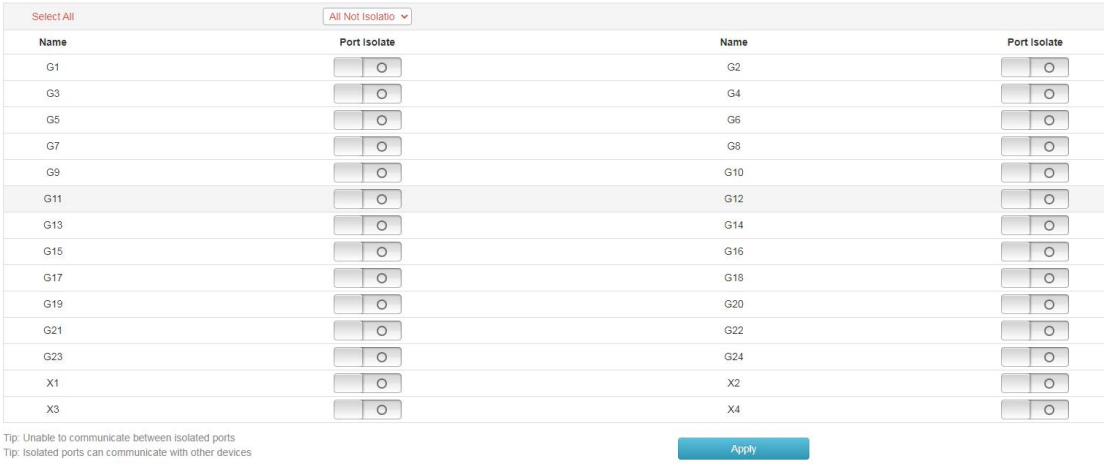
On the "Port Isolation" page, you can configure the port isolation.

【Operation path】

Port > Port Isolate

【Interface description】

Figure 3-2 Port Isolate interface



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

3.3 Port Mirror

【Function Description】

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

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

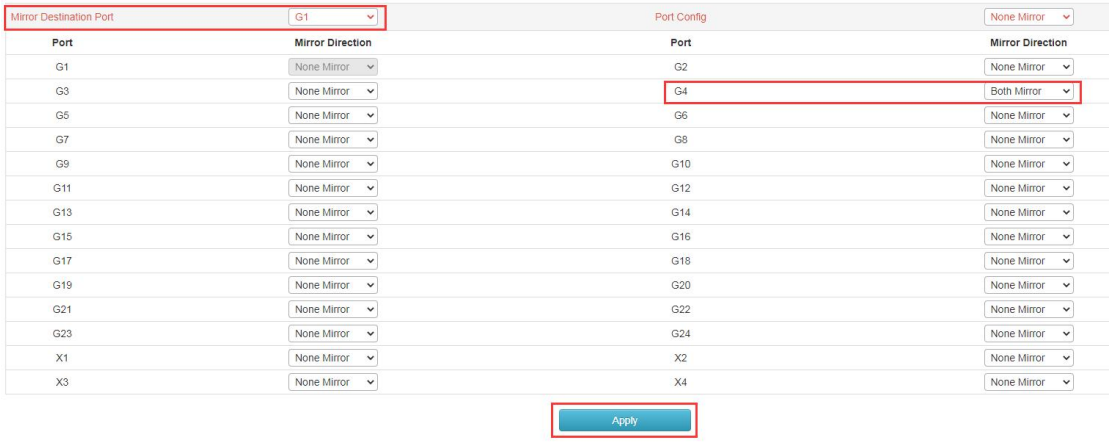
【Operation path】

Port > Port Mirror

【Interface description】

Figure 3-3 Port mirror interface

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



3.4 Port Limit

【Function Description】

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

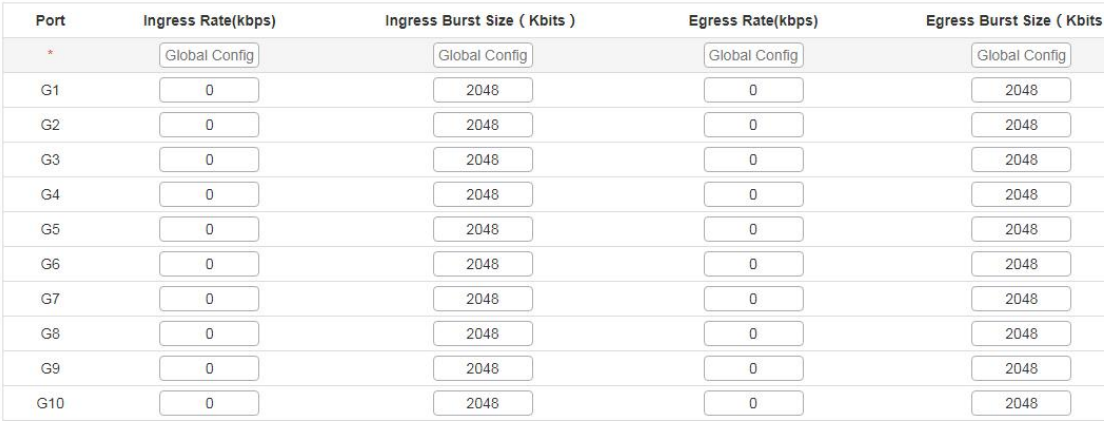
【Operation path】

Port > Port Limit

【Interface description】

Figure 3-4 Port rate limit

interface



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

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

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

3.5 Storm Control

【Function Description】

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

【Operation path】

Port> Storm Control

【Interface description】

Figure 3-5 Storm control interface

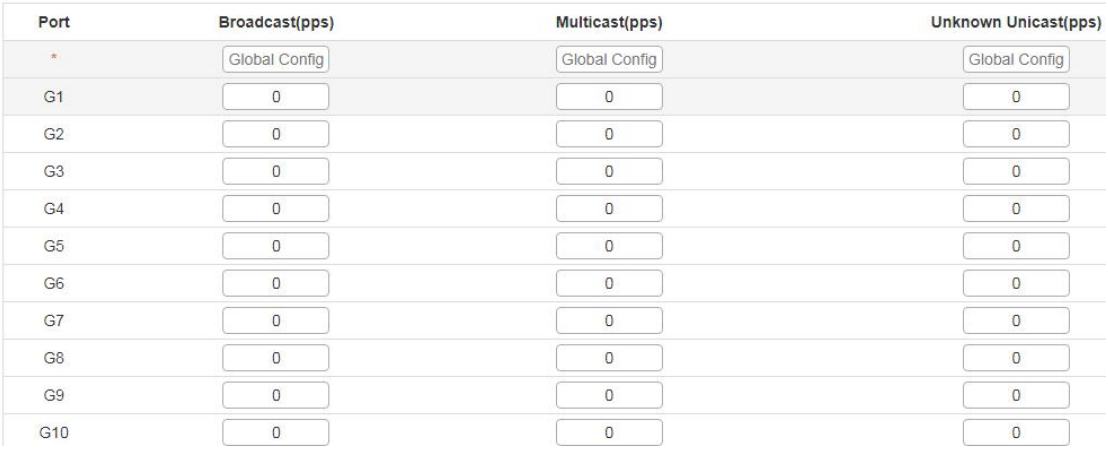


Table 3-5 Main elements of storm Control interface

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

3.6 EEE(Enery-Efficient-Ethernet)

【Function Description】

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

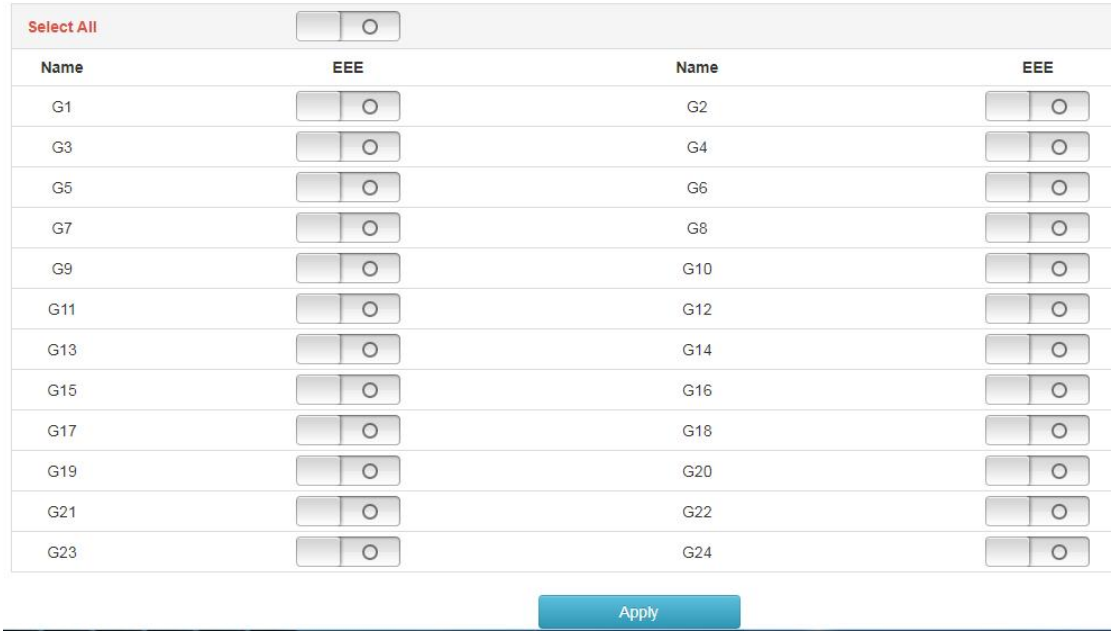
【Operation path】

Port> EEE

【Interface description】

Figure 3-6 EEE

Interface



4. Basic(Layer 2 Management)

4.1 MAC Table

【Function Description】

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

【Operation path】

Basic > mac

【Interface description】

Figure 4-1 MAC Table

interface

4.2 VLAN

【Function Description】

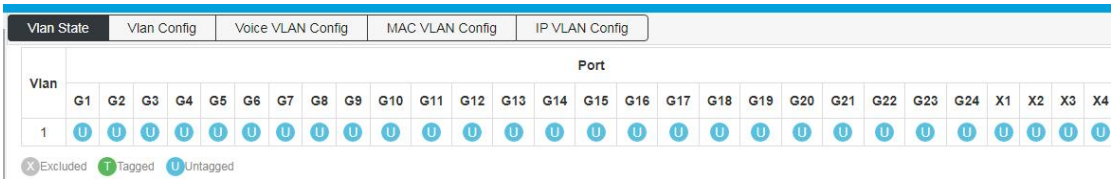
On the "VLAN" page, you can view VLAN status, set port VLAN, voice VLAN, and configure MAC-based VLAN and IP-based VLAN.

【Operation path】

Basic > VLAN

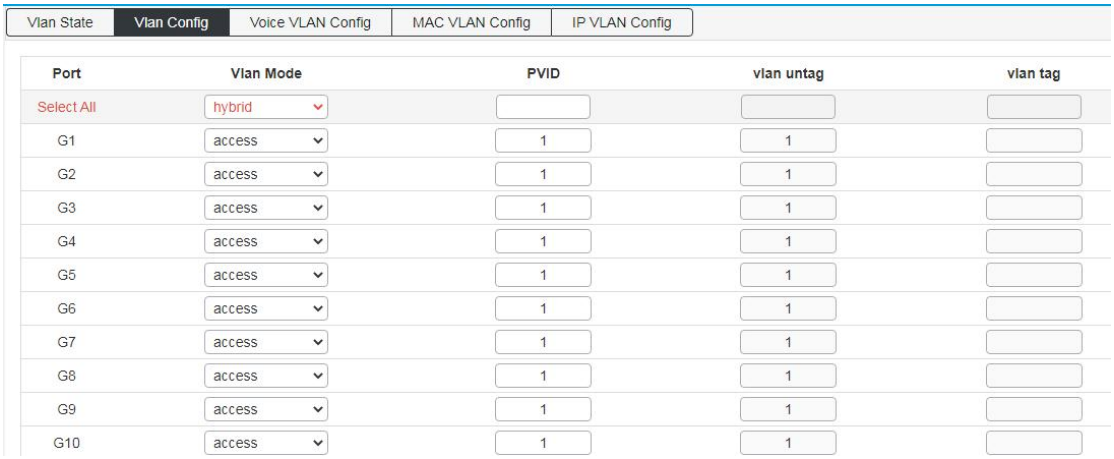
【Interface description】

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



The following figure shows the configuration of port

VLAN,



Port properties that can be set:

Access：

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

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

Trunk：

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

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

Hybrid：

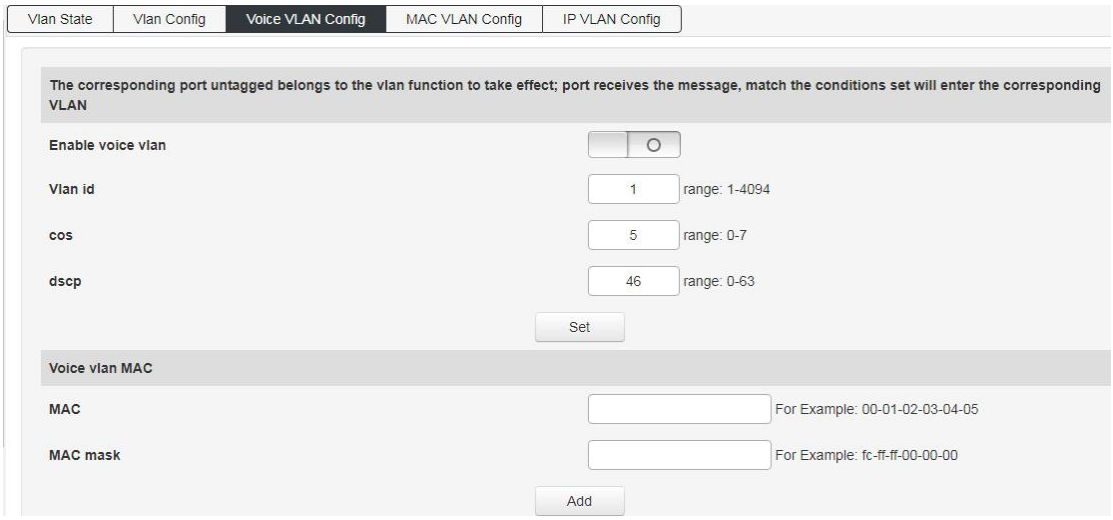
Hybrid ports are similar to Trunk ports in many ways, but with additional port configuration capabilities. In addition to the features described for trunk ports, Hybrid ports have these capabilities:

- Can be configured as VLAN tag or unknown, C-tag all, S tag all, or S-custom tag all,
- Inlet filtering can be controlled,
- Enter the acceptance frame, the exit label and configuration can be configured independently.

Port VLAN:

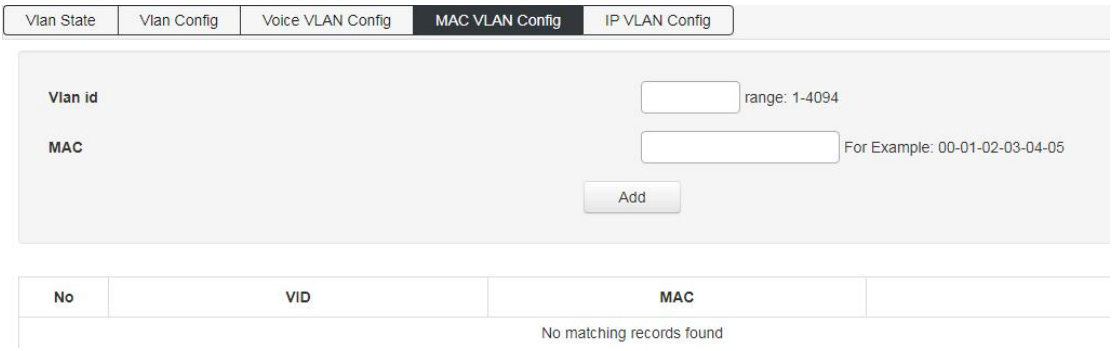
The VLAN ID of the port (also called PVID). The allowed VLAN range is 1 to 4095, and the default is 1。

The following page is the voice VLAN config interface；

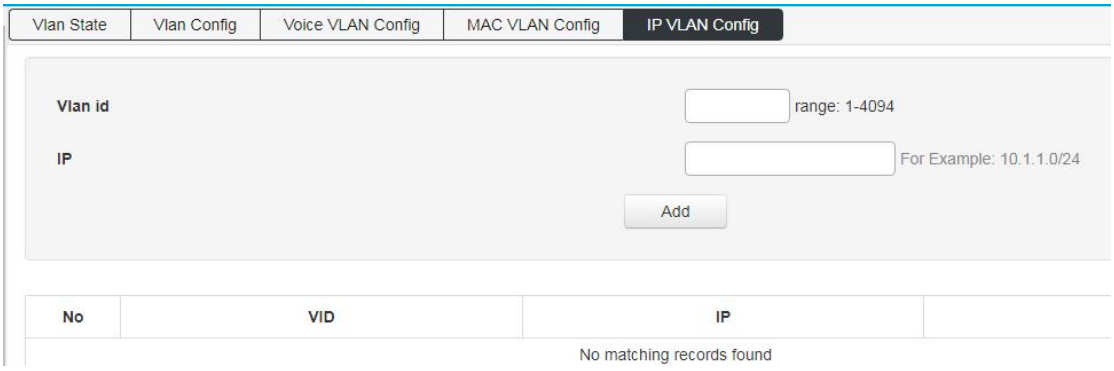


When the voice VLAN feature is enabled, the Access port can carry IP voice traffic from IP phones. When the switch is connected to a Cisco IP phone (such as a Cisco 7960 IP phone), the voice traffic sent by the IP phone has three layers of IP priority. And the CoS value of the second layer, both of these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

Configure MAC address-based VLAN，



Configure IP-based VLAN,



4.3 **GVRP**

【Function Description】

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

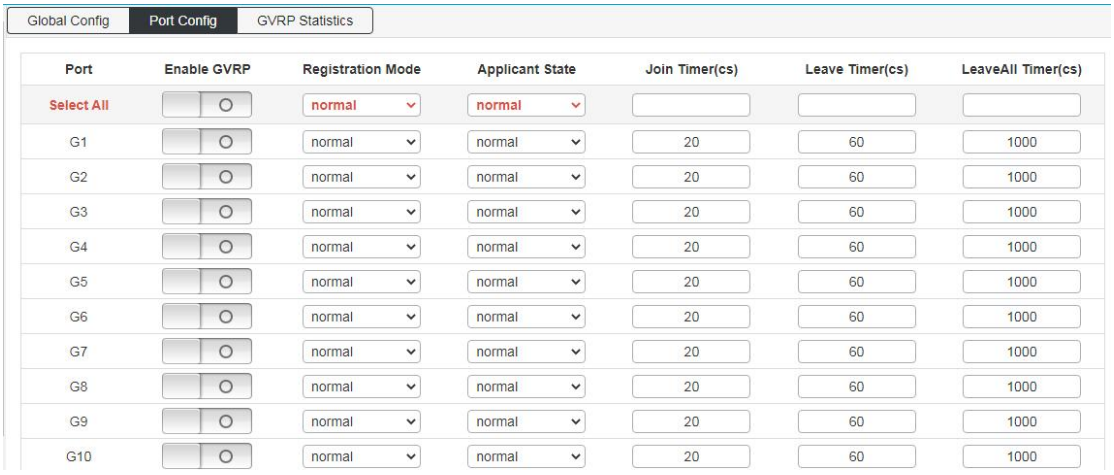
【Operation path】

Basic > GVRP

【Interface description】

Enable or disable GVRP function;

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



View the operating information of

GVRP;

4.4 Link aggregation

【Function Description】

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

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

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

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

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

4.4.1 Static aggregarion config

【Function Description】

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

【Operation path】

Basic >Link Aggr

【Interface description】

Figure 4-4-1 Static aggregation

interface

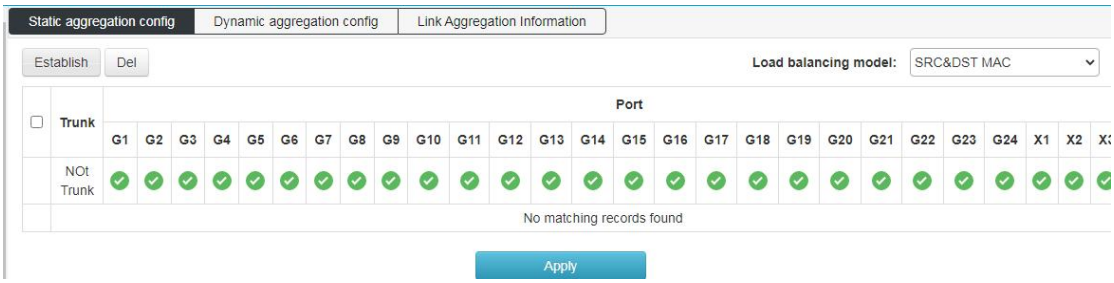


Table 4-4-1 Main elements of static aggregation interface

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

Special Note:

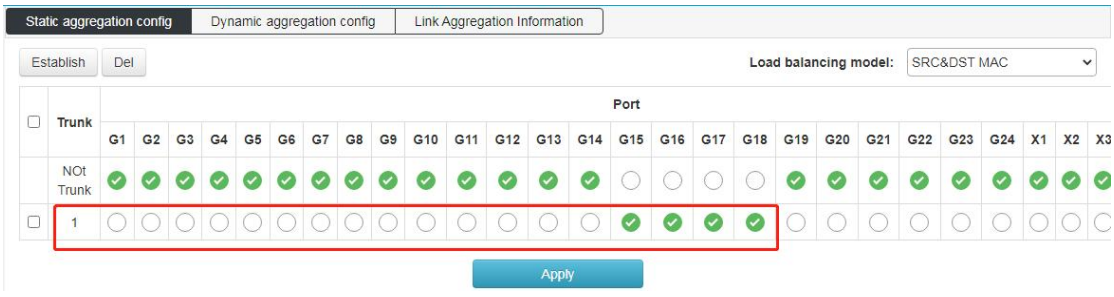
(1) The static aggregation of the same port cannot be configured at the same time as the dynamic LACP aggregation;

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

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

【Example】

Select SMAC&DMAC for load balancing mode, and add ports 15, 16, 17, 18 to aggregation group 1, as shown in the figure below:



4.4.2 Dynamic aggregation config

【Function Description】

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

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

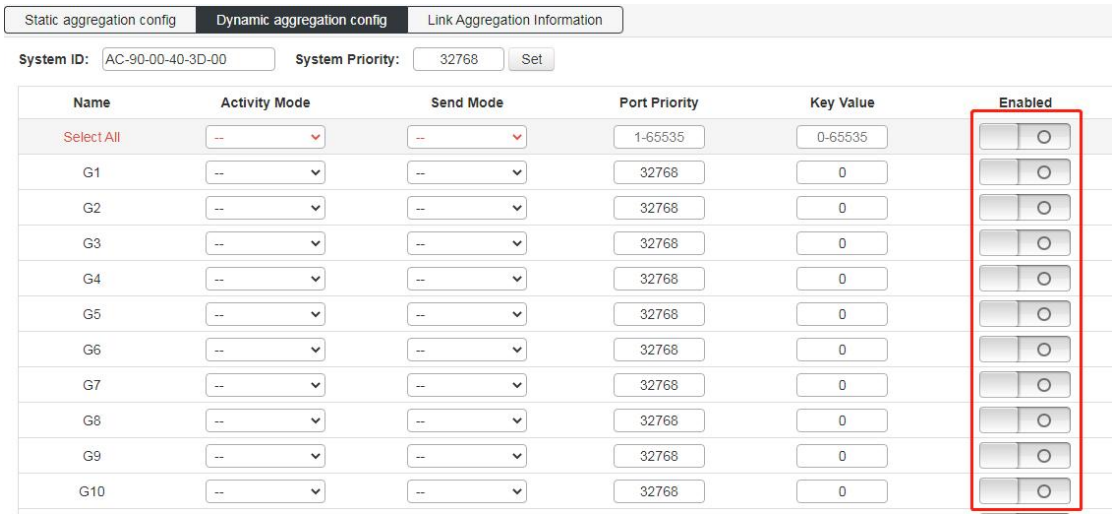
Only the ports with the LACP protocol enabled will carry out LACP negotiation, which may form an aggregation link. The key is the basis of negotiation, and only ports with the same key can negotiate to form an aggregation link. The negotiation mode is "active/passive". When "active" is selected, the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

【Operation path】

Basic > Link Aggr > Dynamic aggregarion config

【Interface description】

Figure 4-4-2 LACP configuration interface



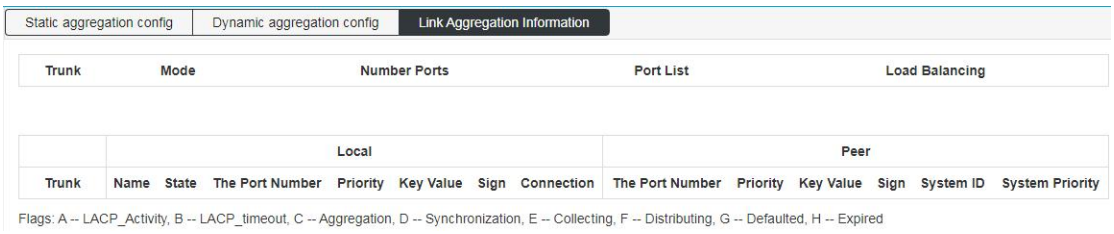
Link aggregation information: view switch aggregation port information;

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

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

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

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



4.5 MSTP Configration

【Function Description】

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

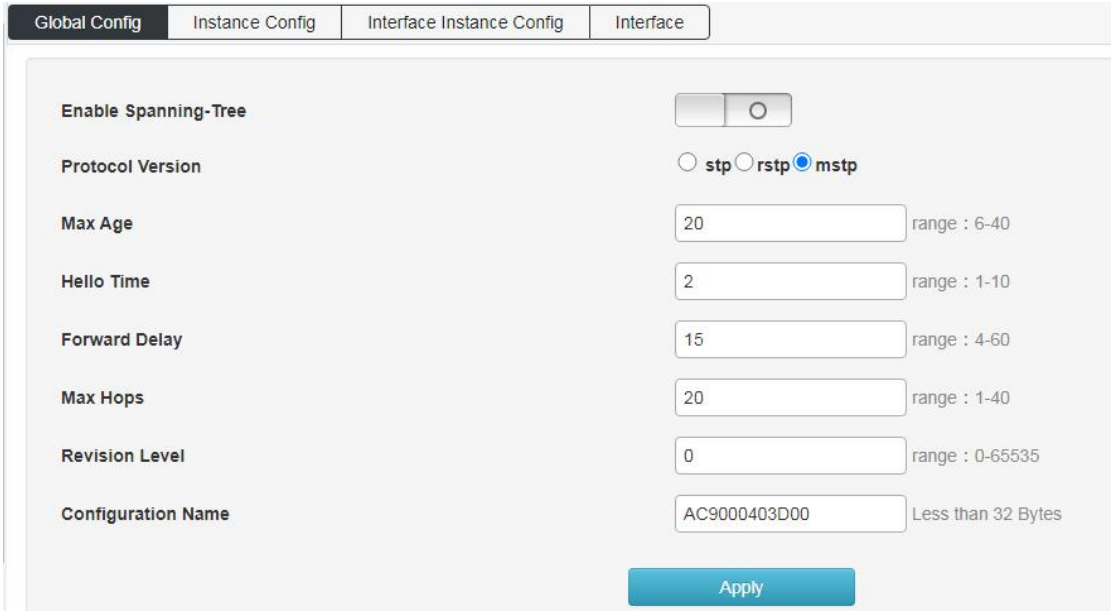
infinite loop in the road network avoids the problem of reduced message processing capacity caused by the repeated reception of the same message.

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

Basic > mstp

【Interface description】

Figure 4-5-1 Global configuration interface



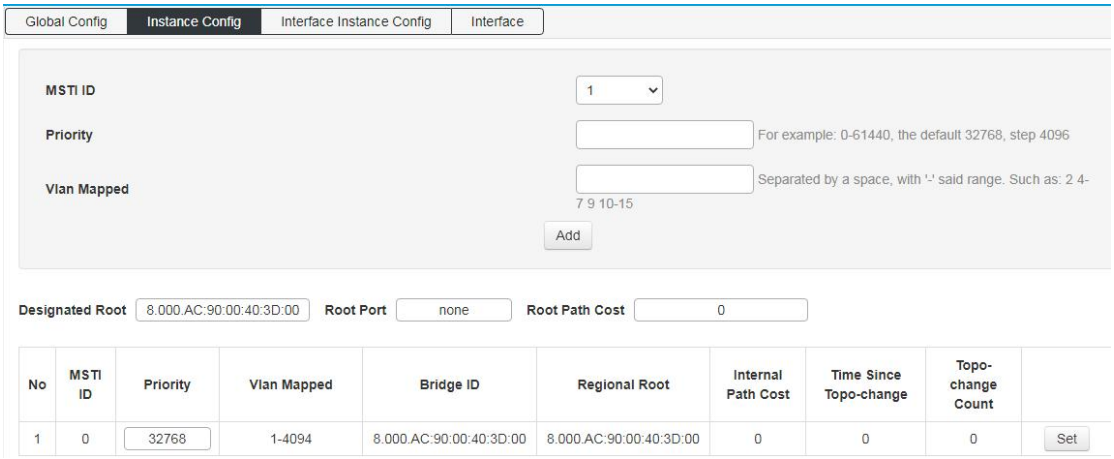
Instance configuration: configure MSTP instance,

Set the mapping Vlan for multiple spanning trees

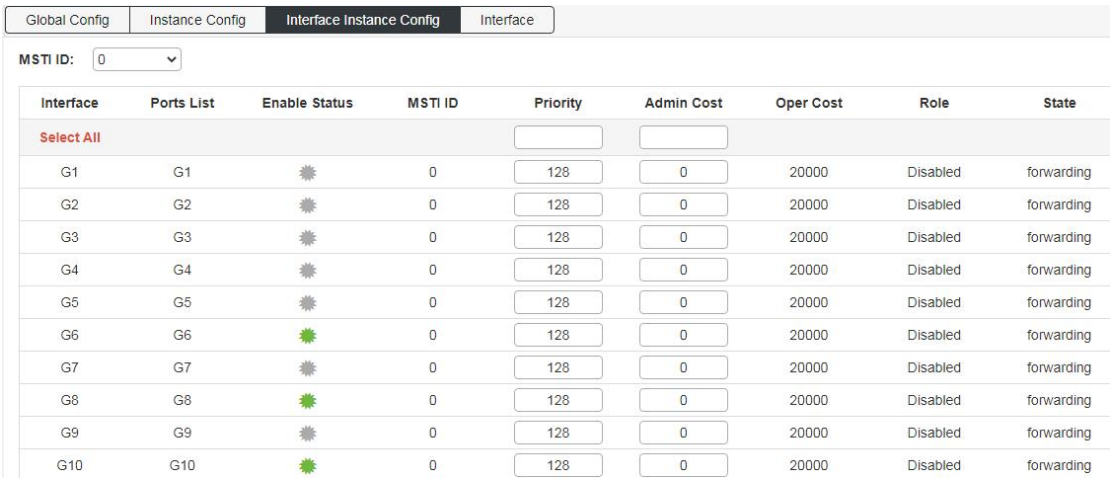
Configuration name: Identifies the name of the VLAN to MSTI mapping, the bridge must share the name and revision (see below), and the VLAN-to-MSTI mapping configuration in order to share the MSTI spanning tree. (In the area) The name can be up to 32 characters.

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

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

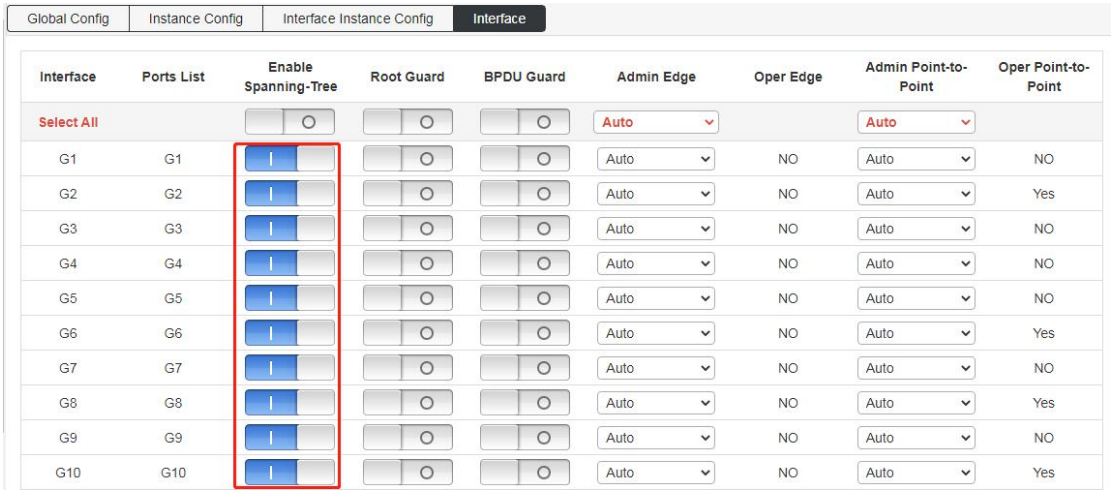


Interface instance configuration: configure the enablement of the instance on the port.



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

packets;



4.6 ERPS

【Function Description】

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

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

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

【Operation path】

Basic > ERPS

【Interface description】

Figure 4-6-1 ERPS Global Config interface

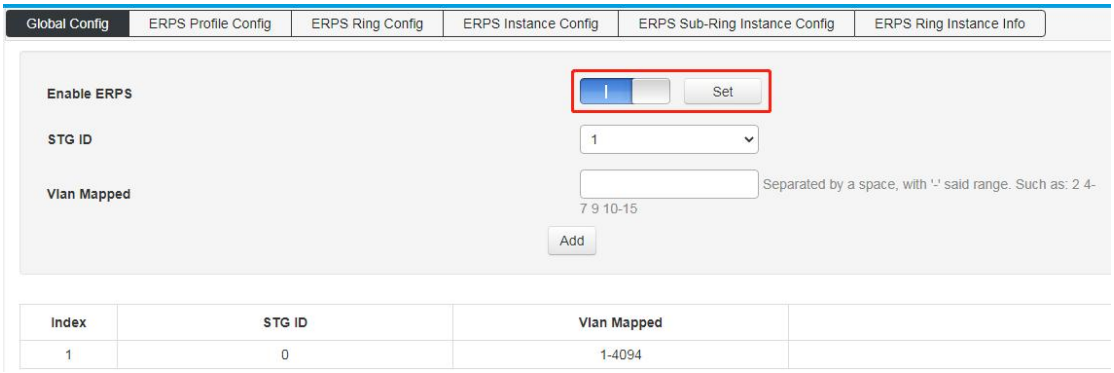


Figure 4-6-2 ERPS Profile Config interface

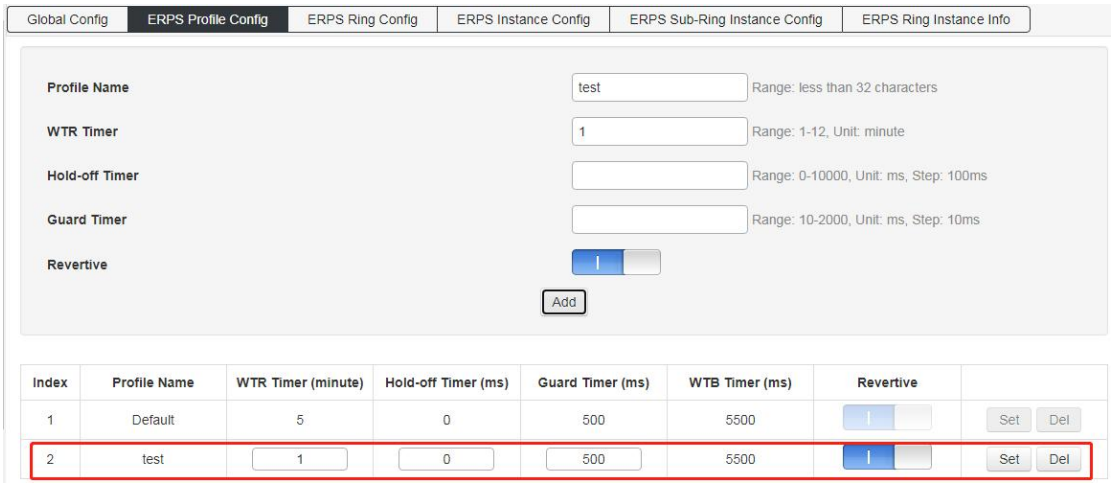


Figure 4-6-3 ERPS Ring Config interface

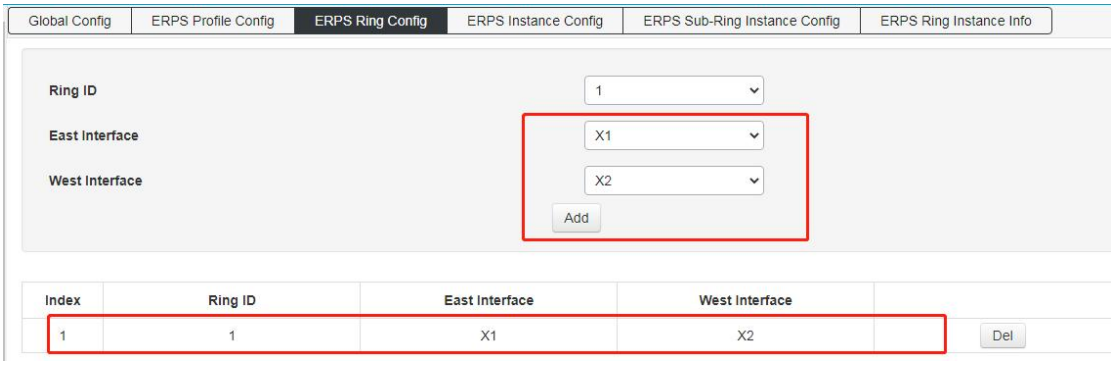


Figure 4-6-4 ERPS Instance Config interface

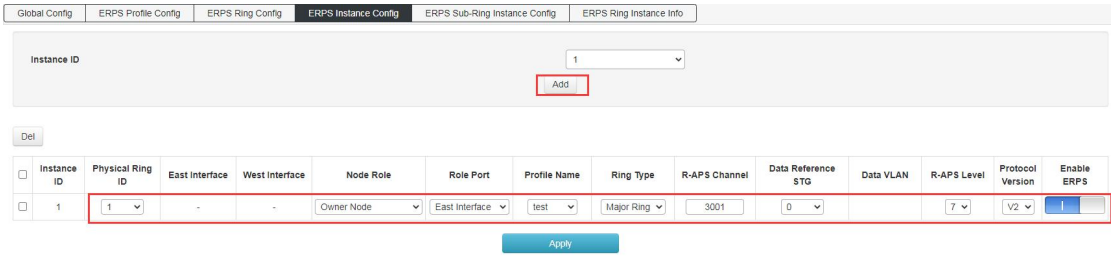
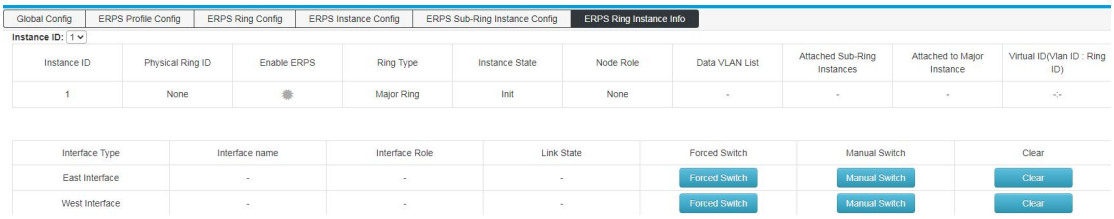


Figure 4-6-5 ERPS Ring Instance Info interface



4.7 Loop Protect

【Function Description】

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

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

【Operation path】

Basic > Loop Protect

【Interface description】

Figure 4-7-1 Loop protection Global Config

interface

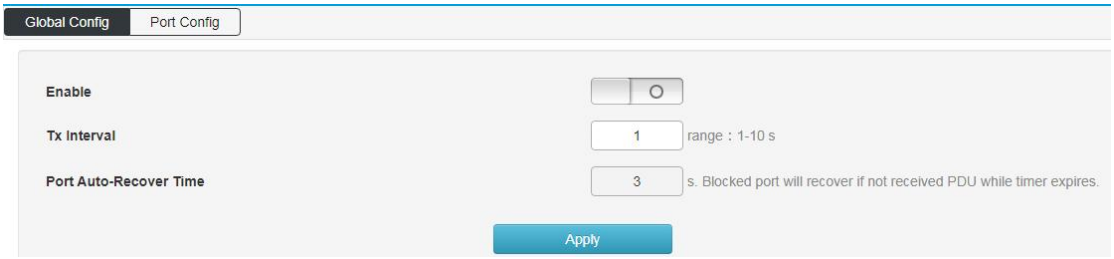
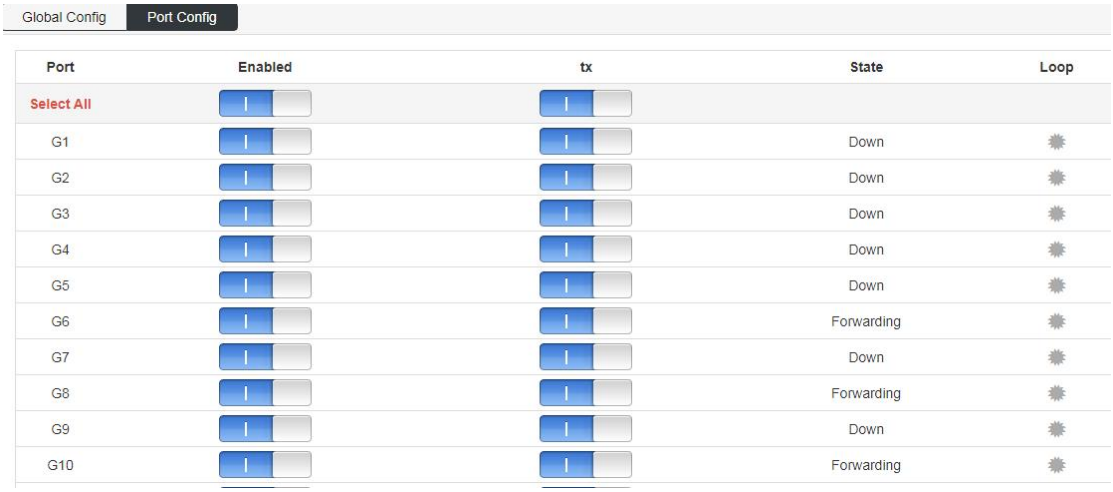


Figure 4-7-2 Loop protect port config

interface



4.8 PTP

PTP enable: enable PTP function globally;

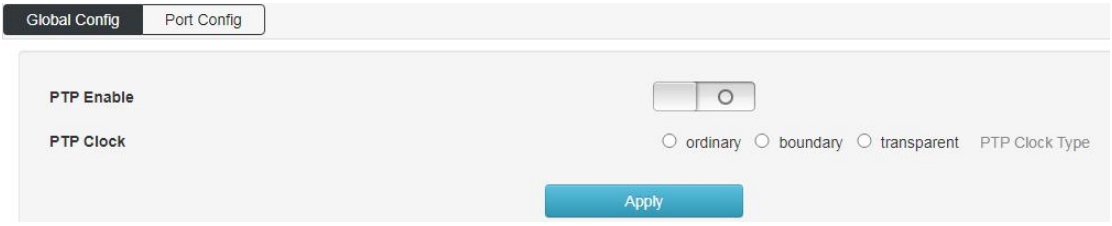
The PTP protocol defines the following three types of basic clock nodes:

OC (Ordinary Clock): Only one PTP communication port clock is an ordinary clock.

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

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

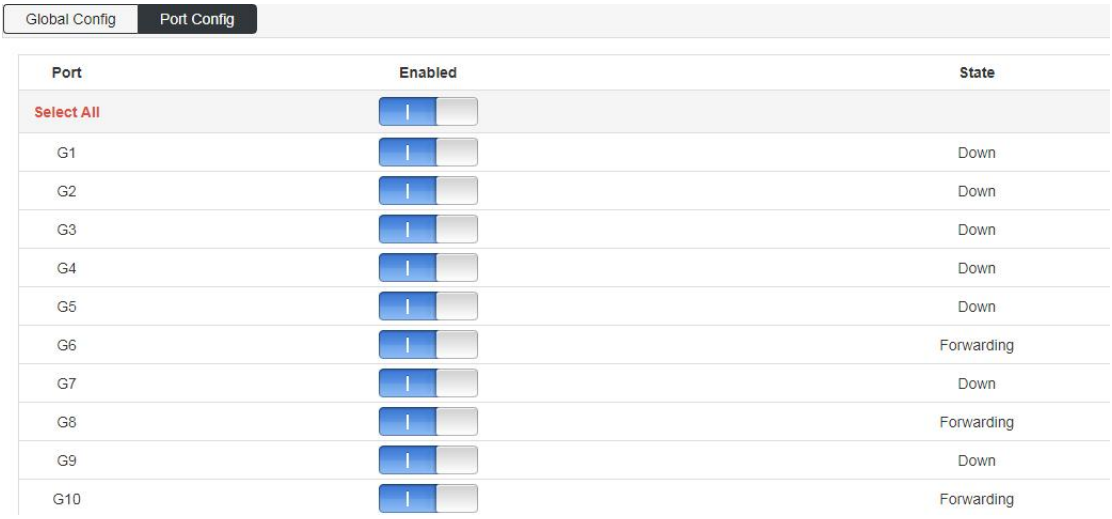
port.



Port configuration

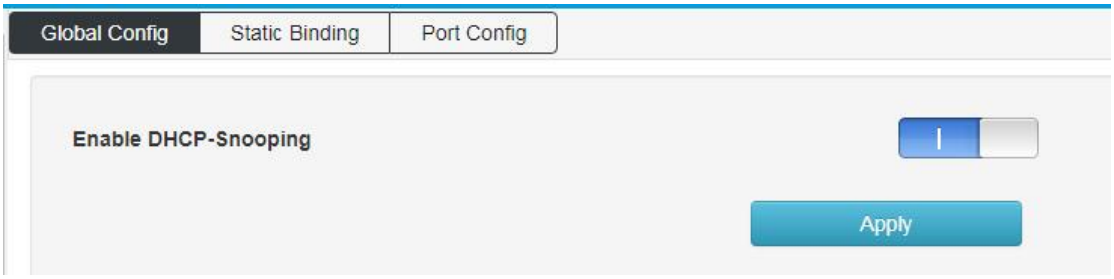
Enable the PTP function of the designated

port;

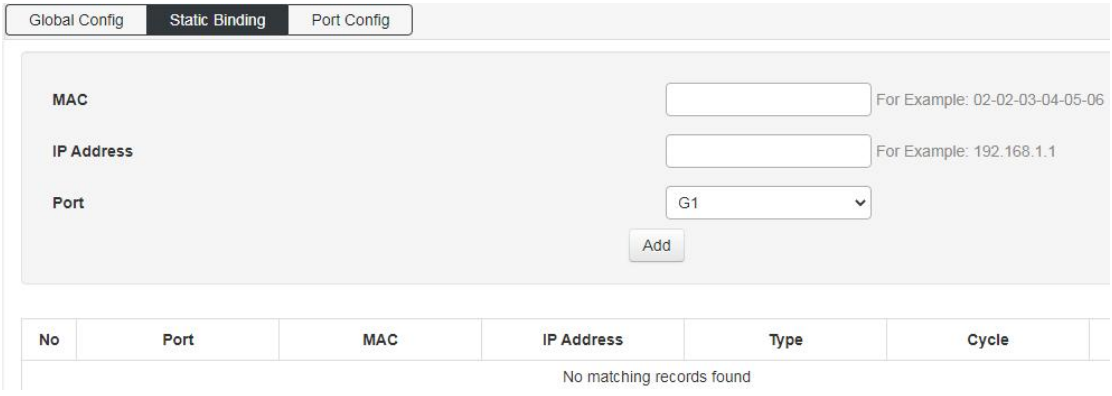


4.9 DHCP-snooping

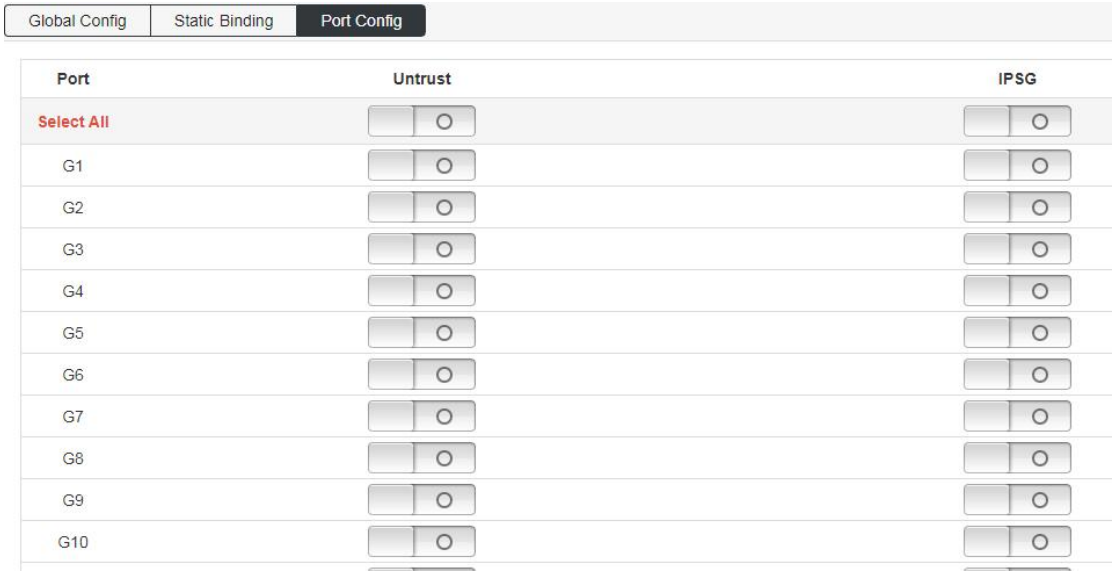
Global configuration: enable DHCP monitoring function;



Static Binding：configure static monitoring port



Port configuration: enable the DHCP monitoring function on the port;



4.10 **802.1X**

【Function Description】

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

【Operation path】

Basic > 802.1X

【Interface description】

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

Figure 4-1-1 Global configuration

interface

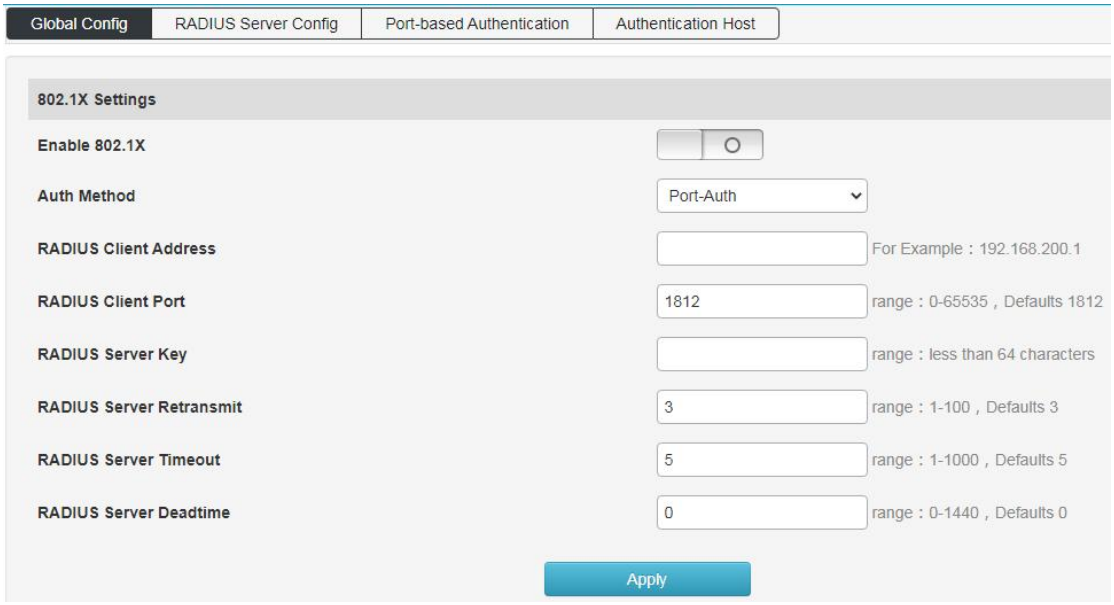


Figure 4-10-2 RADIUS Server Config interface

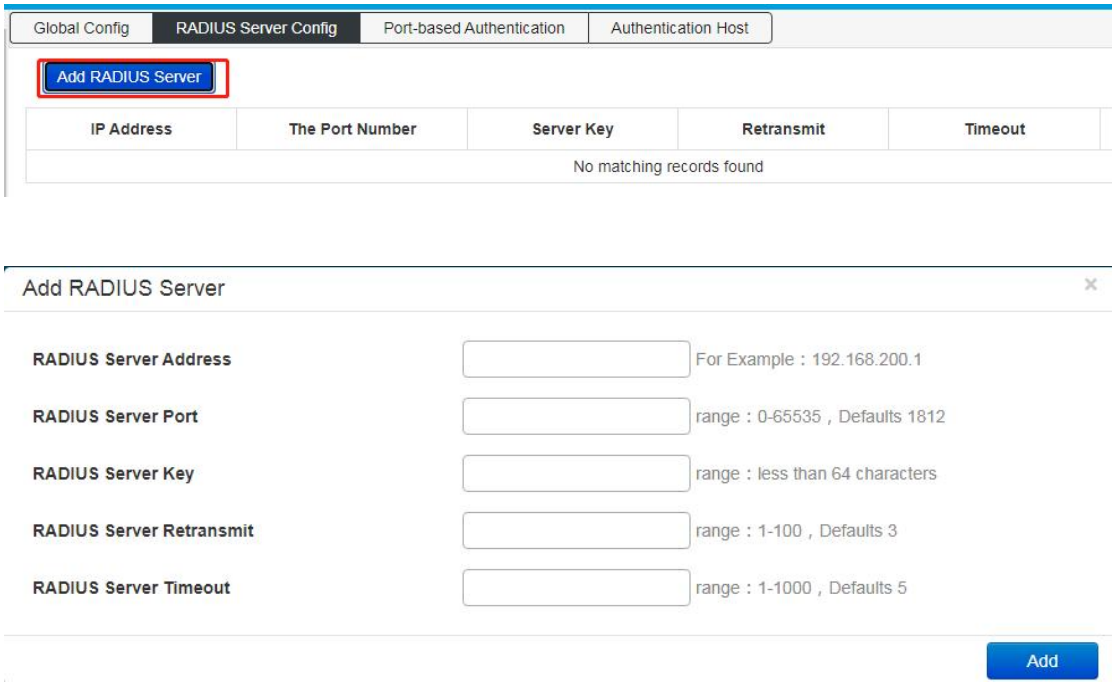


Figure 4-10-3 Port-based Authentication Interface

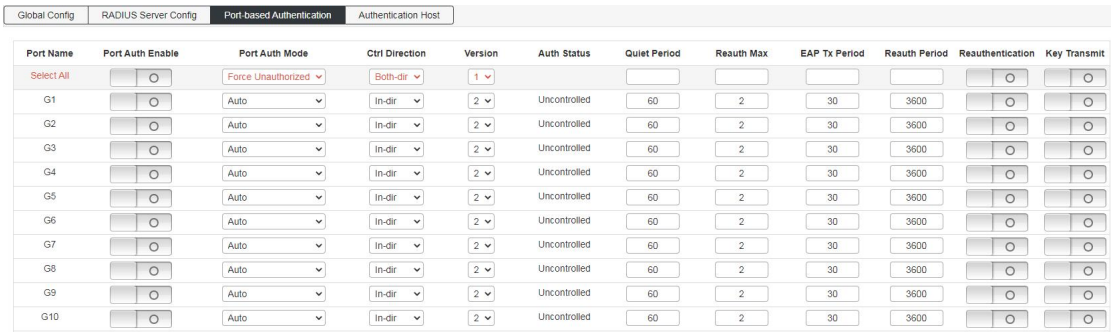


Figure 4-10-4 Authtication Host Interface

5. Layer 3 Config

5.1 Interface Config

【Function Description】

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

【Operation path】

Layer3 > Interface

【Interface description】

Figure 5-1 Interface Config Interface

【Example】

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

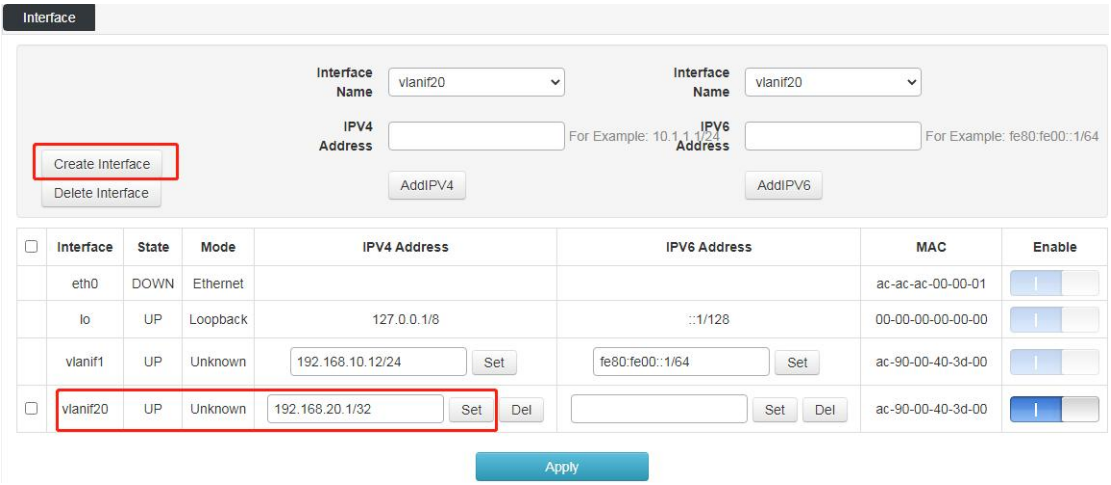


Table 5-1 Main elements of the interface configuration interface

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

5.2 Route Config

【Function Description】

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

【Operation path】

Layer3 > Route

【Interface description】

Figure 5-2-1 View IPv4 Route interface

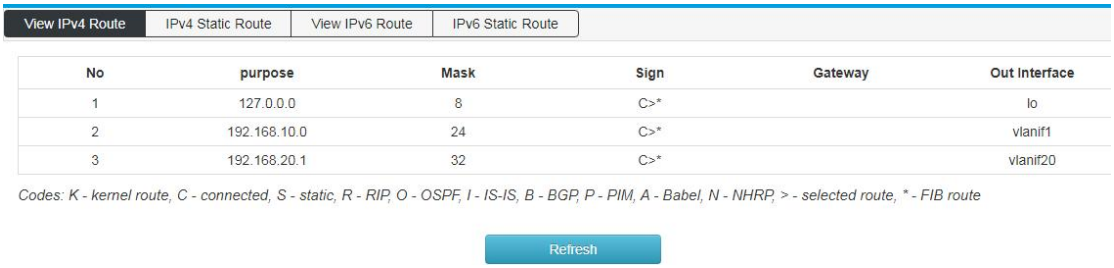


Figure 5.2.2 IPv4 Static Route Config interface

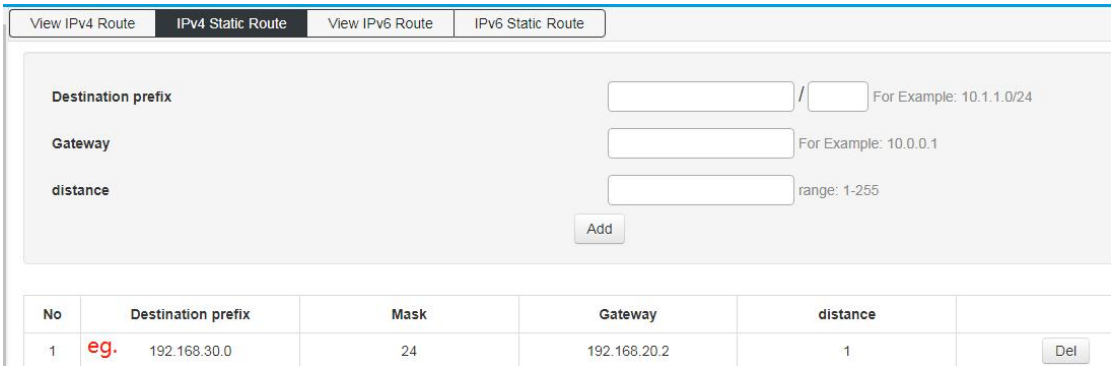


Table 5-2-2 Main elements of static routing interface

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

Figure 5-2-3 View IPv6 Route Interface

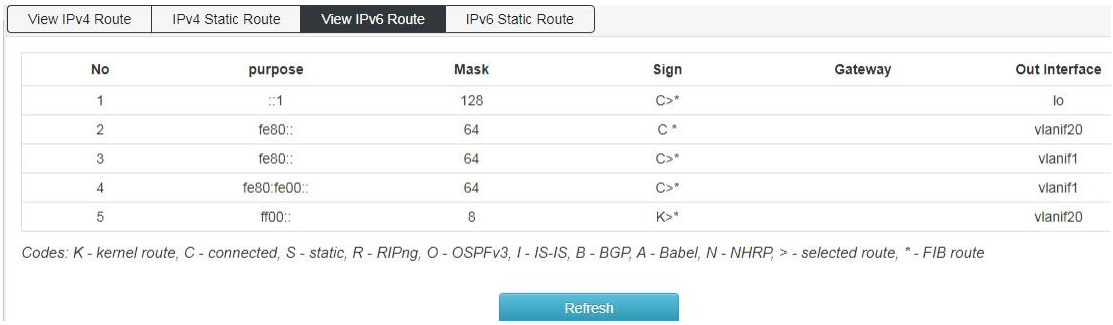
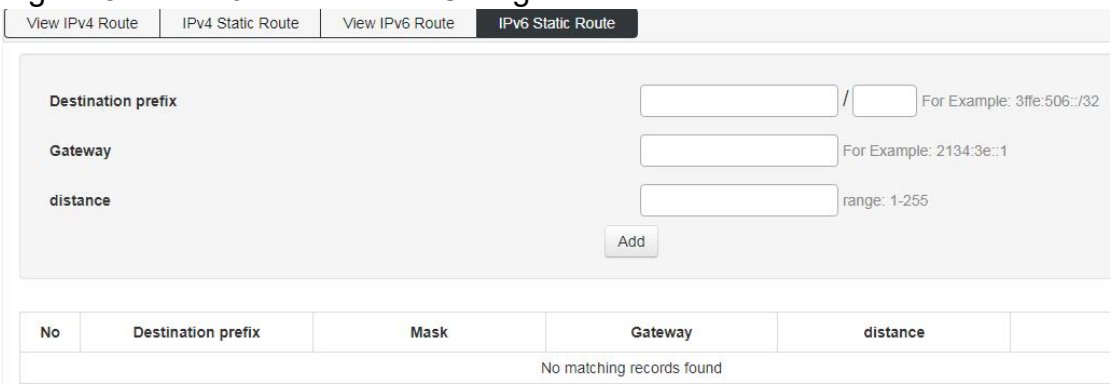


Figure 5.2.4 IPv6 Static Route Config Interface



5.3 ARP

【Function Description】

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

【Operation path】

Layer3 > arp

【Interface description】

Figure 5-3-1 View ARP

interface

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

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

Figure 5-3-2 Static ARP Config interface

Set the IP address and MAC address to be

bound;

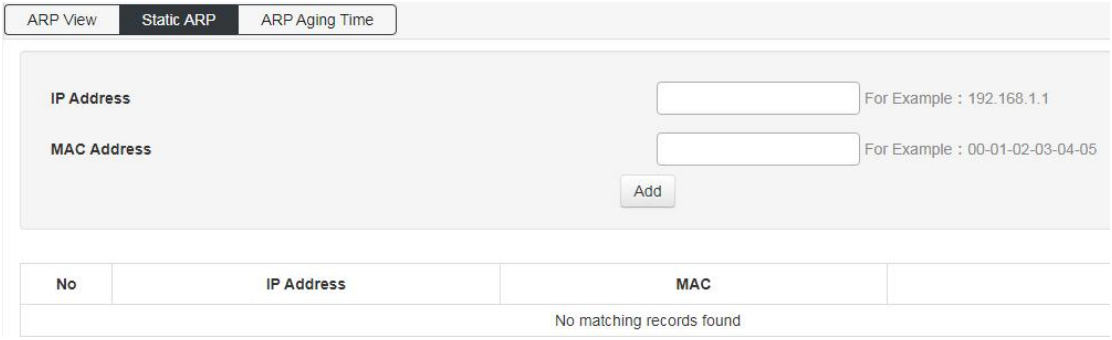
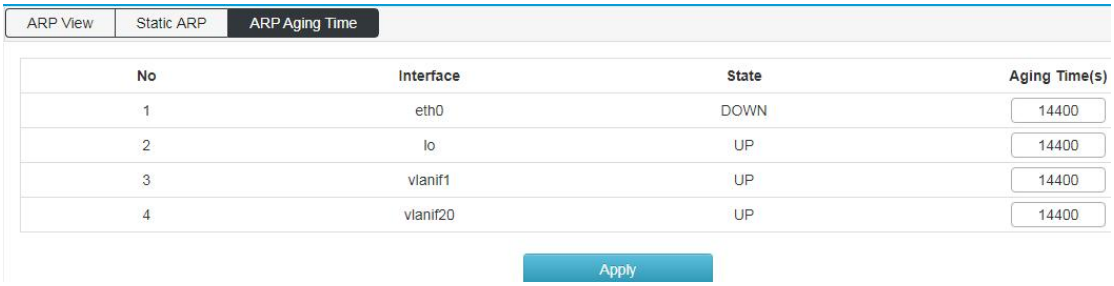


Figure 5-3-3 ARP Aging Time Config interface



5.4 ND Config

【Function Description】

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

【Operation path】

Layer3 > ND

【Interface description】

Figure 5-4-1 View ND interface

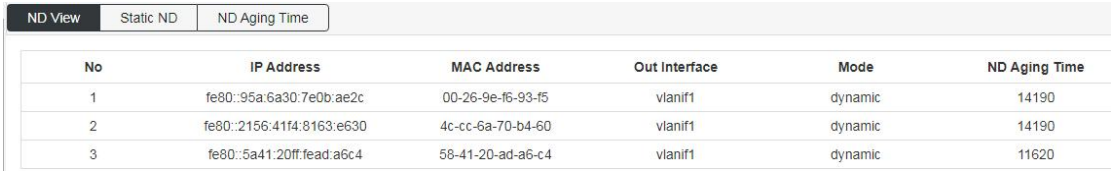


Figure 5-4-2 Static ND interface

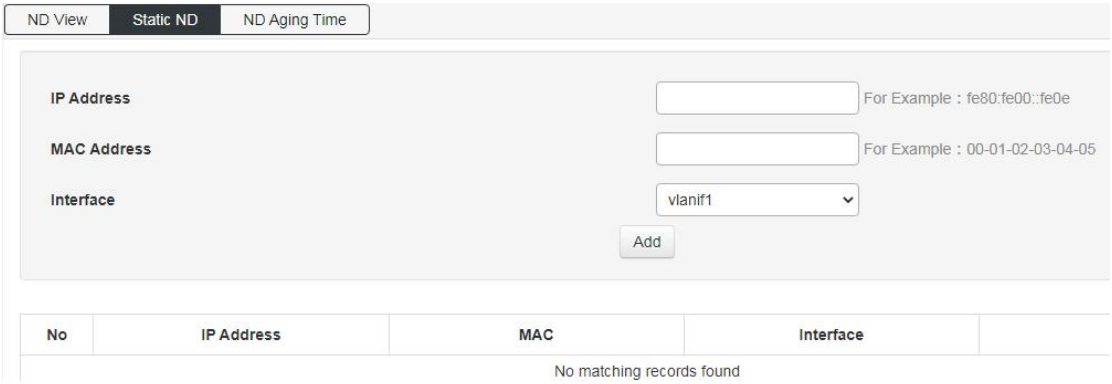
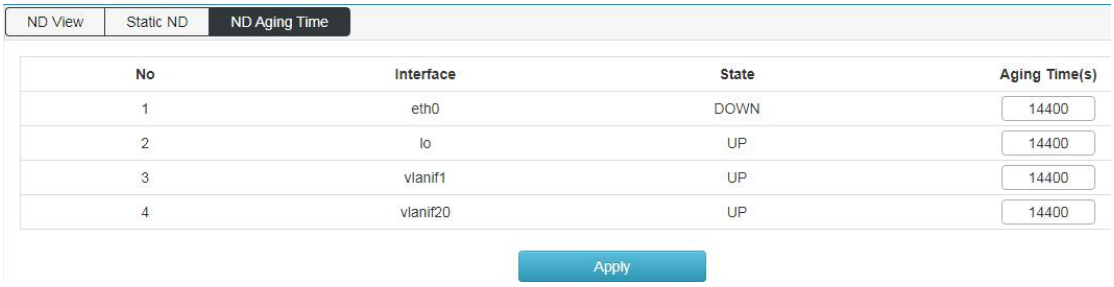


Figure 5-4-3 ND Aging Time Config interface



5.5 DHCP Server

【Function Description】

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

【Operation path】

Layer3 > DHCP Server

【Interface description】

Figure 5-5-1 Global configuration interface

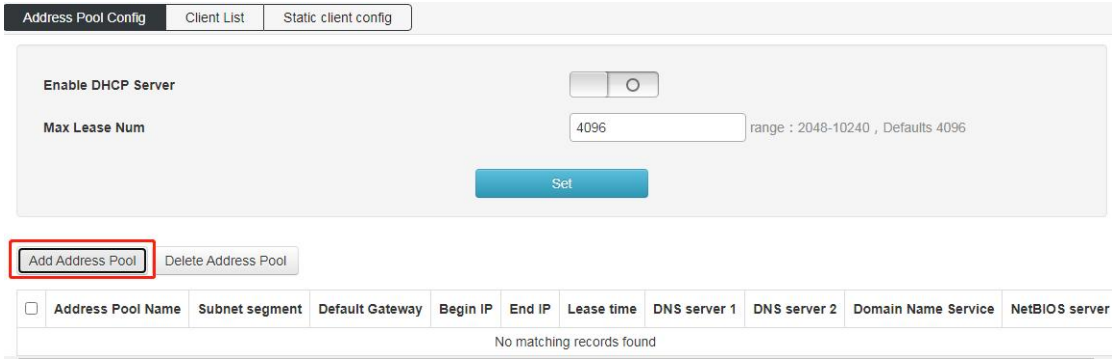


Figure 5-5-2 Address Pool Setting

Interface

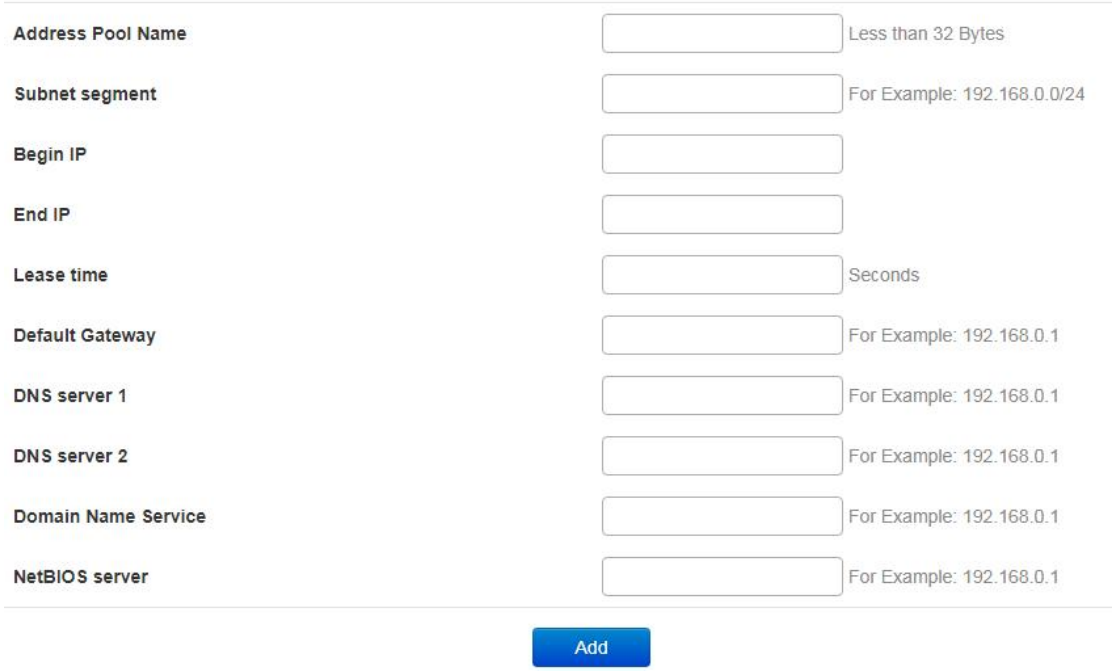


Table 5-5-2 Main elements of the address pool configuration interface

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

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

Figure 5-5-3 Client List interface;

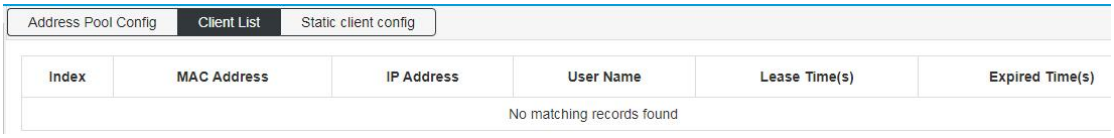


Figure 5-5-4 Static Client Config interface;

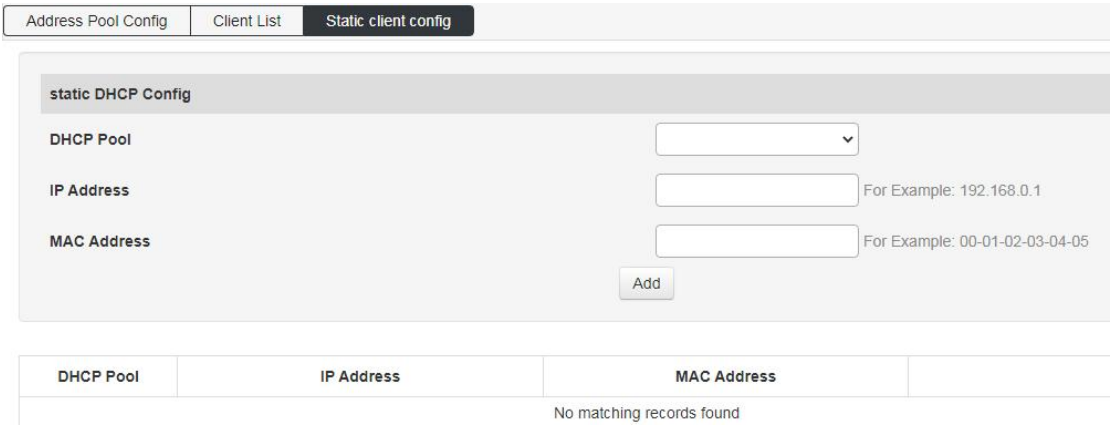


Table 5-5-4 Main elements of Static Client Config interface

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

5.6 DHCP Relay

【Function Description】

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

【Operation path】

Layer3 > dhcp relay

【Interface description】

Figure 5-6 DHCP relay interface

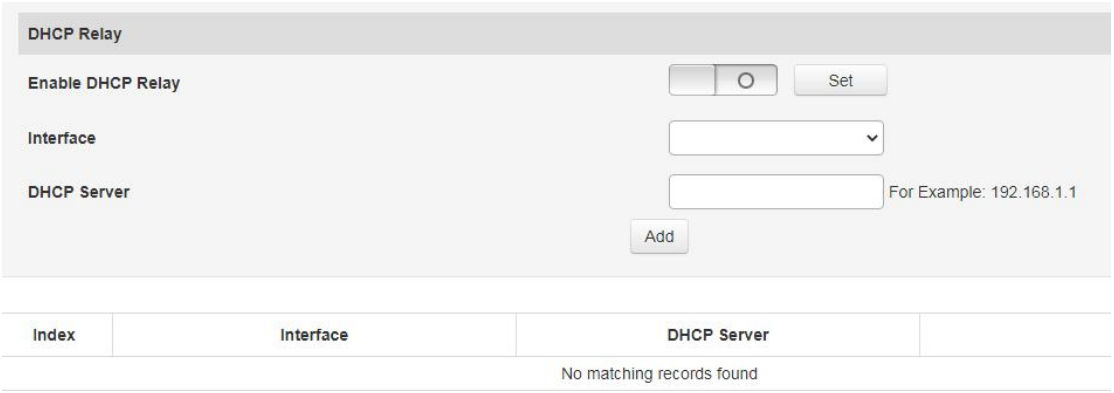


Table 5-6 Main elements of the DHCP relay interface

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

5.7 RIP

【Function Description】

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

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

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

【Operation path】

Layer3 > RIP

【Interface description】

Figure 5-7-1 RIP Global Config interface

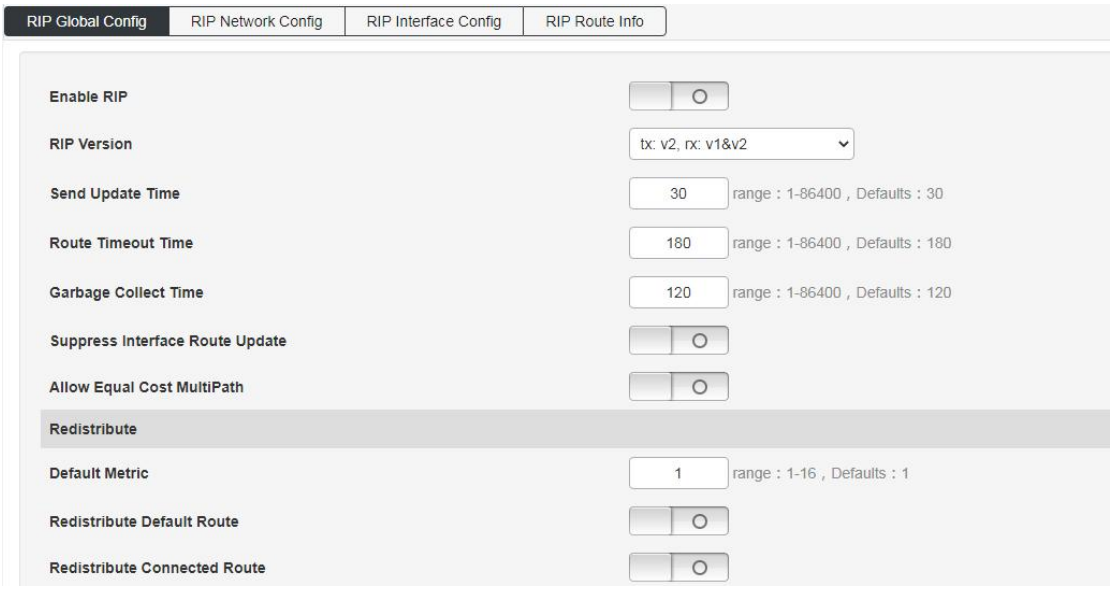


Figure 5-7-2 RIP Network Config interface

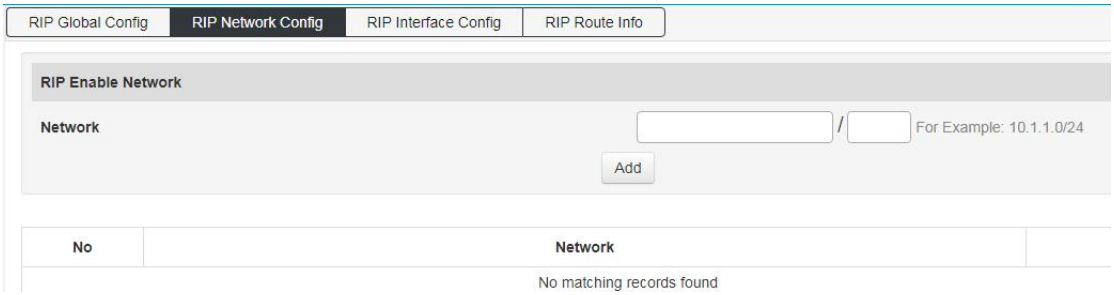
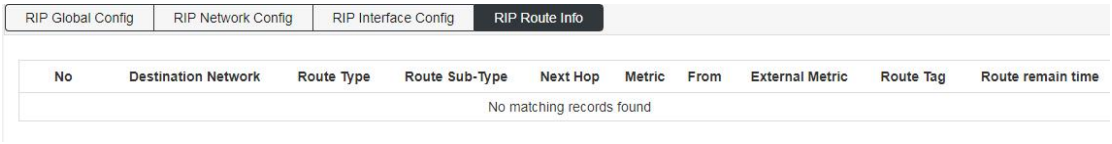


Figure 5-7-3 RIP Interface Config interface

Figure 5-7-4 RIP Route Info interface



5.8 OSPF

【Function Description】

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

【Operation path】

Layer3 > OSPF

【Interface description】

Figure 5-8-1 OSPF Global Config interface

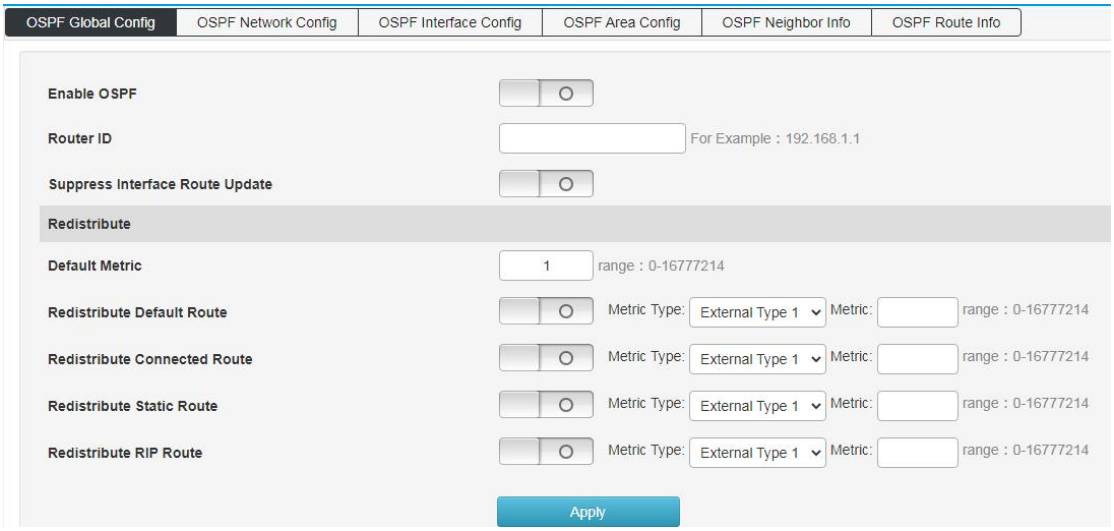


Table 5-8-1 Main elements of OSPF Global Config interface

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

Figure 5-8-2 OSPF Network Config interface

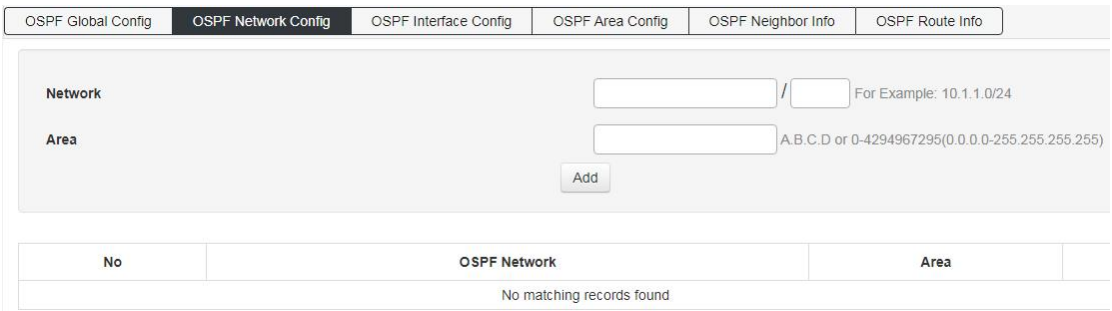


Table 5-8-2 Main elements of OSPF Network Config interface

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

Figure 5-8-3 OSPF Interface Config interface

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

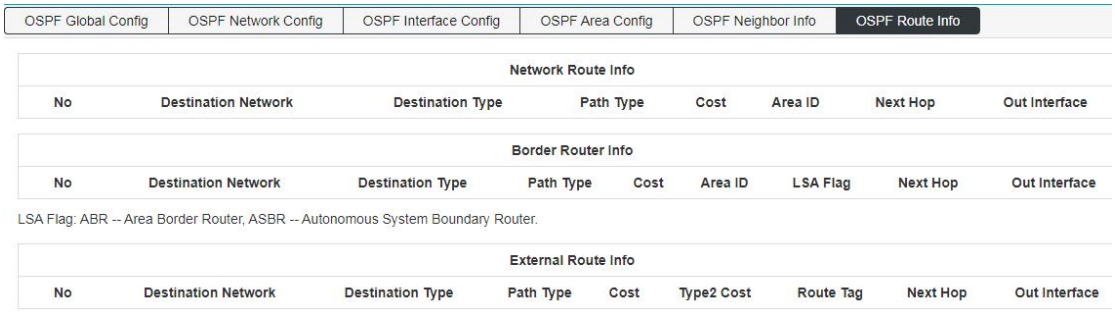
Interface elements	Description
interface	Display the interface name.
Network Type	Select the type of OSFP: P2P: Hello packets are sent to the multicast address 224.0.0.5, neighbors can be discovered automatically, DR/BDR is not elected, the default Hello timer is 10 seconds, and the Dead timer is 40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

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

Figure 5-8-4 OSPF Area Config interface

Figure 5-8-5 OSPF Neighbor Info interface

Figure 5-8-6 OSPF Route Info interface



5.9 RIPng

Figure 5-9-1 RIPng Global Config interface

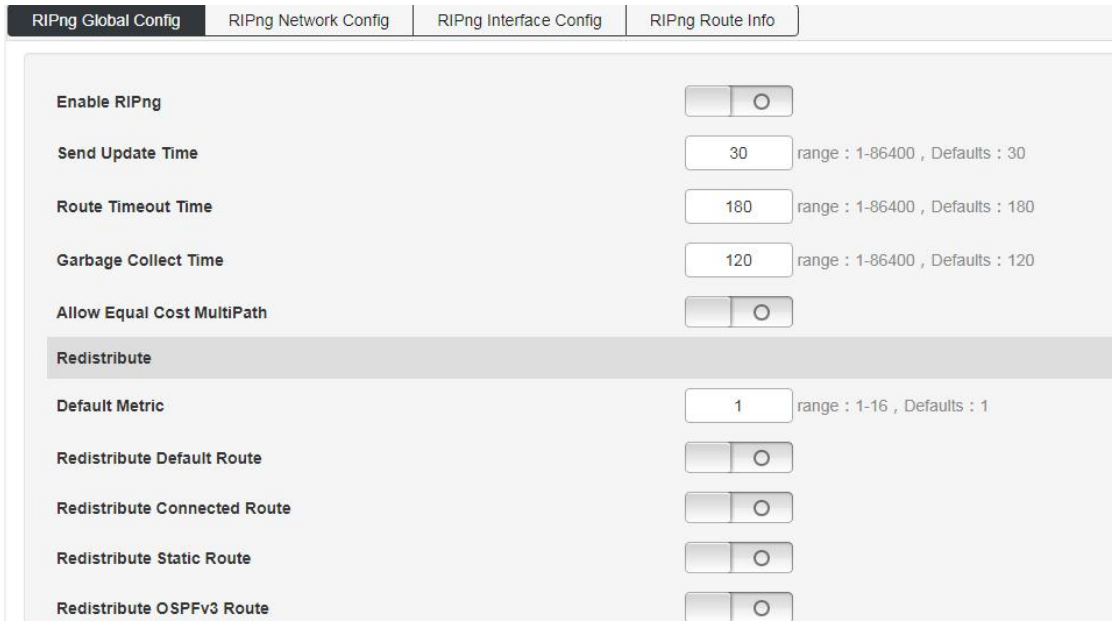


Figure 5-9-2 RIPng Network Config interface

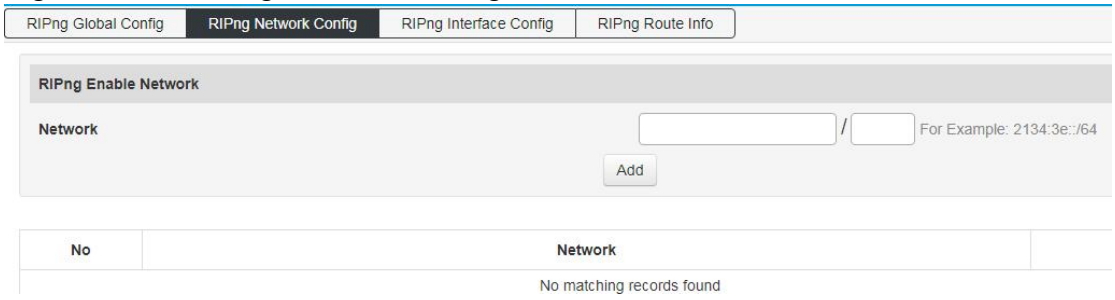


Figure 5-9-3 RIPng Interface Config interface

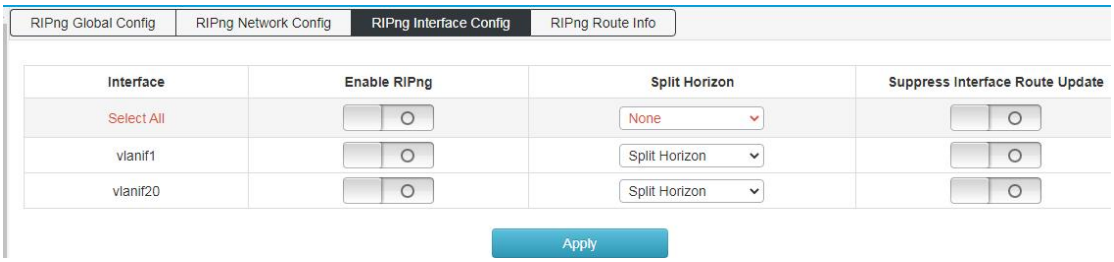


Figure 5-9-4 RIPng Route Info interfaceRIPng Route Info

5.10 OSPFv3

Figure 5-10-1 OSPFv3 Global Config interface

Figure 5-10-2 OSPFv3 Interface Config interface

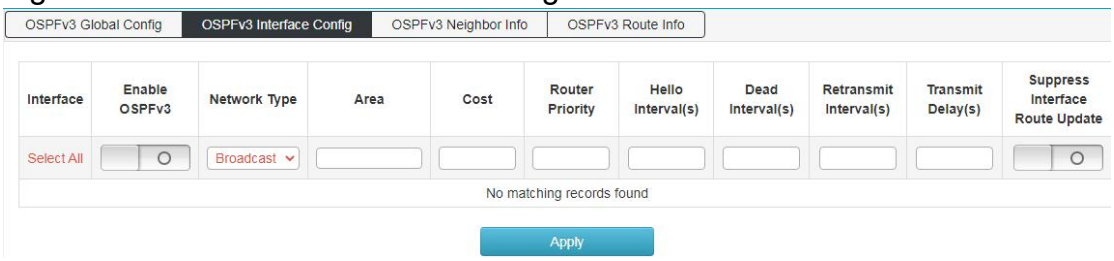
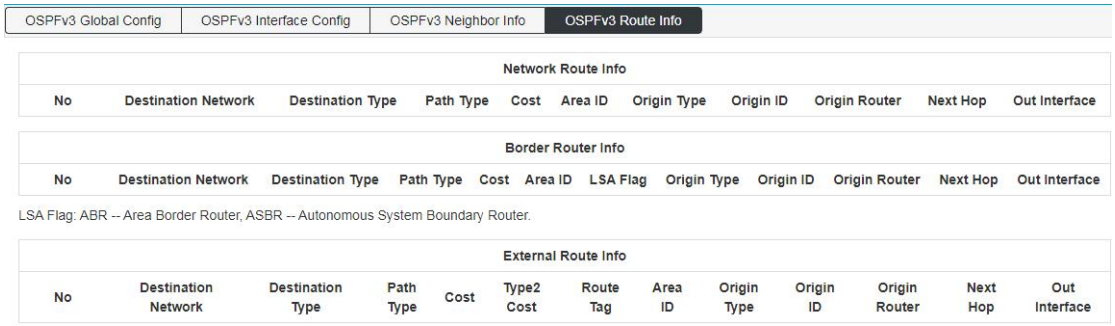


Figure 5-10-2 OSPFv3 Neighbor Info interface

Figure 5-10-3 OSPFv3 Route Info interface



6. Multicast Management

6.1 IGMP Snooping

【Function Description】

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

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

【Operation path】

Multicast > IGMP Snooping

【Interface description】

Figure 6-1-1 IGMP Snooping Global Config

interface

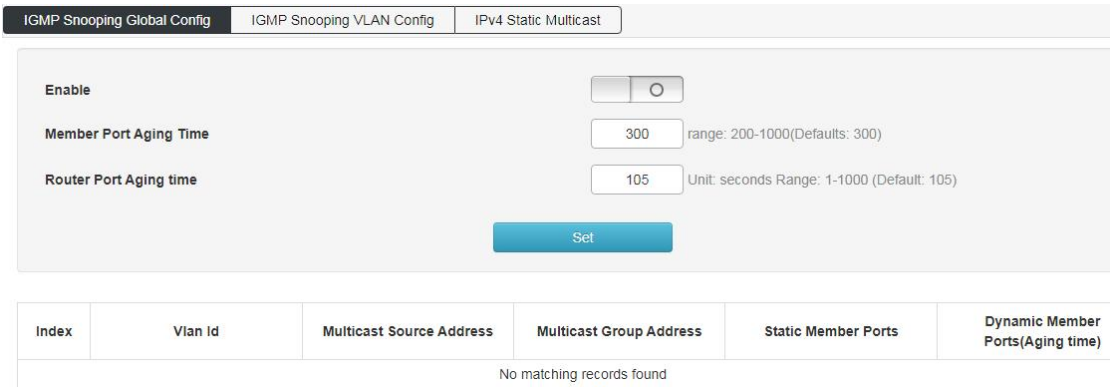


Figure 6-1-2 IGMP Snooping VLAN Config interface

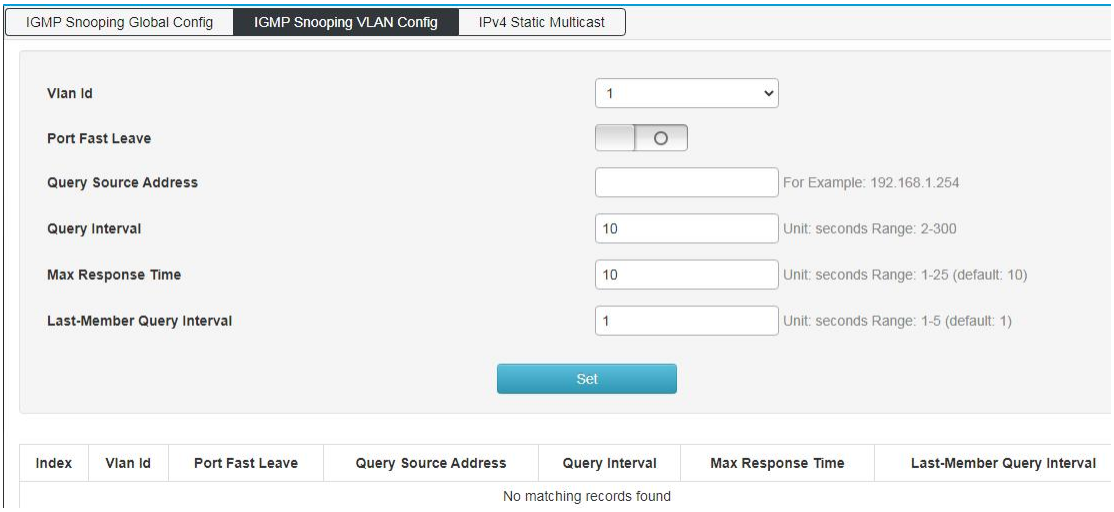
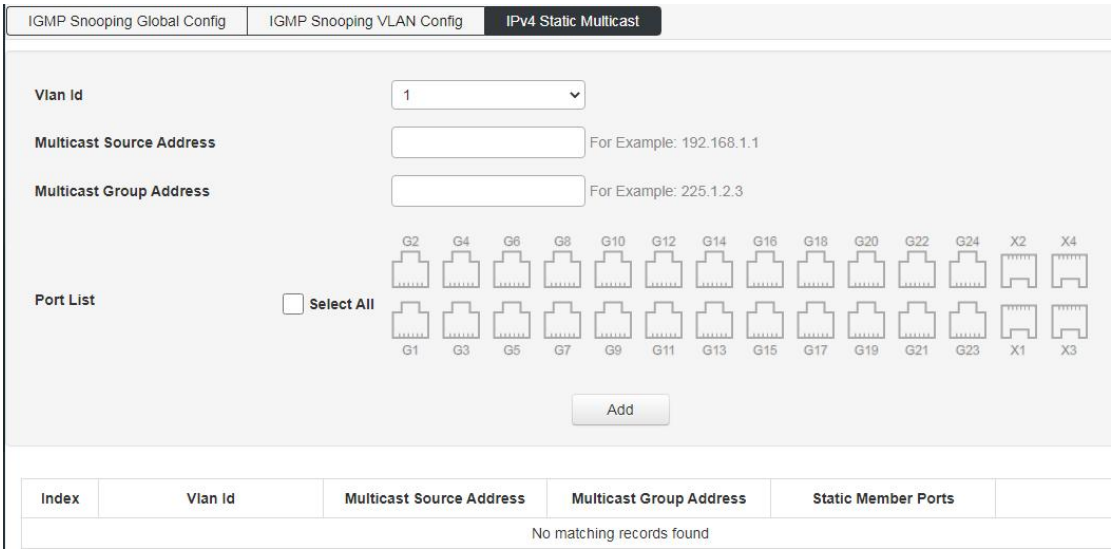


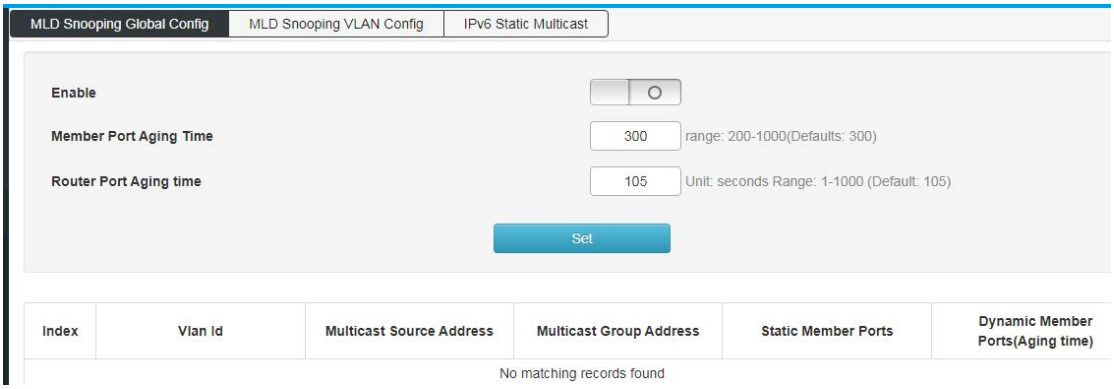
Figure 6-1-3 IPv4 Static Multicast Config interface



6.2 MLD Snooping

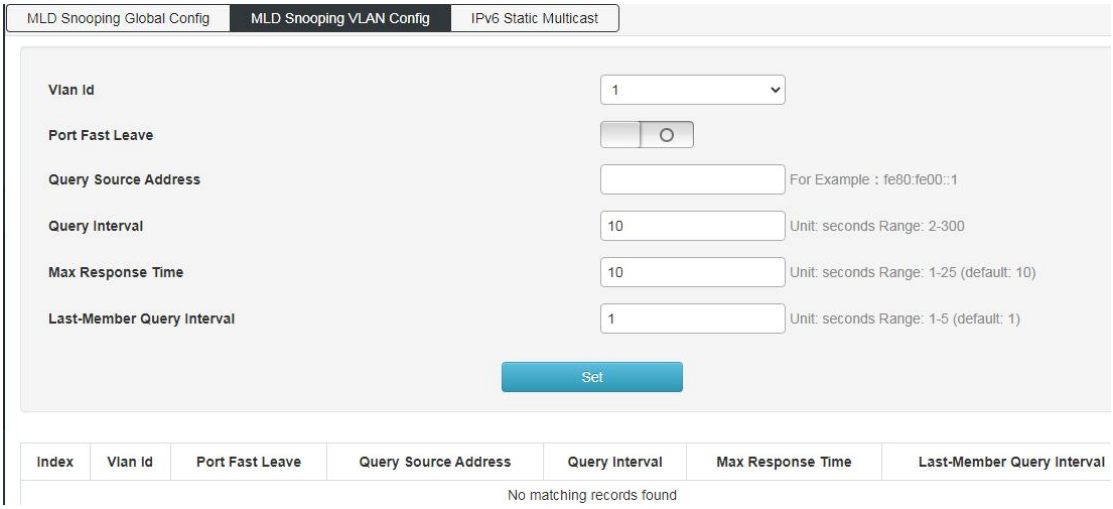
MLD Snooping global configuration: configure MLD monitoring enable and set MLD function

attributes;



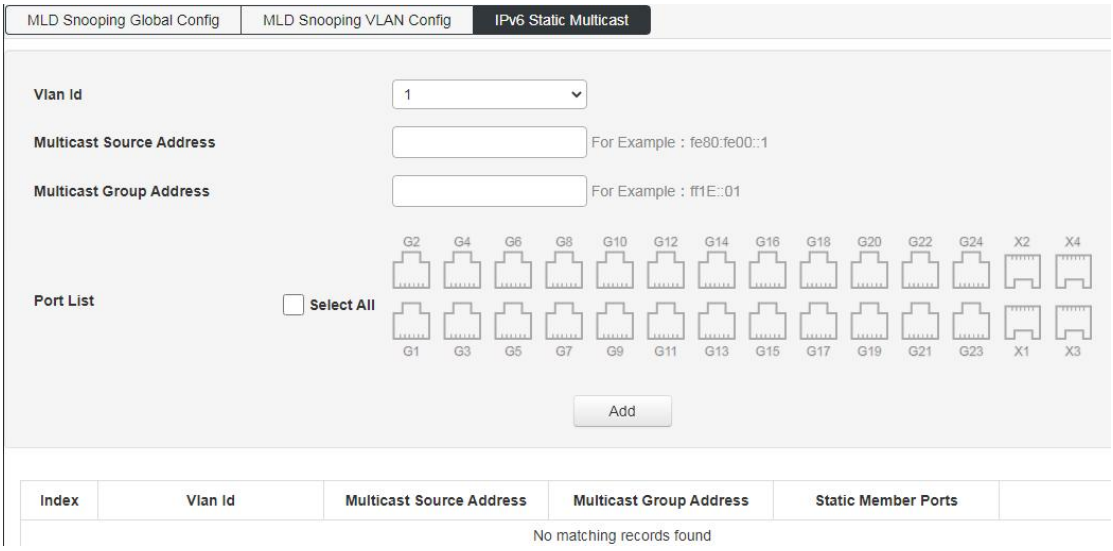
MLD Snooping VLAN configuration: Configure static multicast

VLAN;



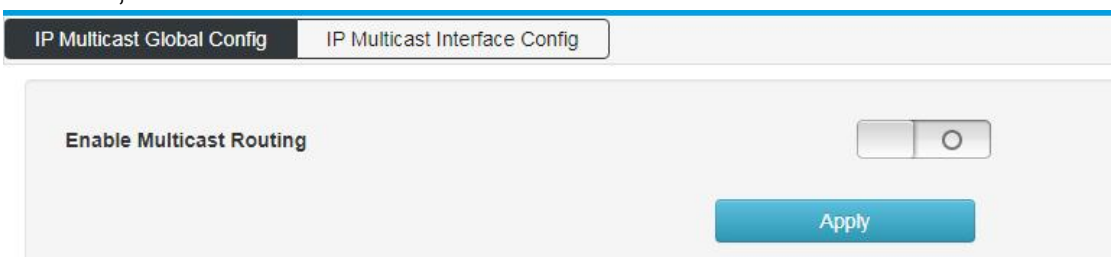
IPv6 static multicast: configure static multicast function, and enable port static multicast

function;

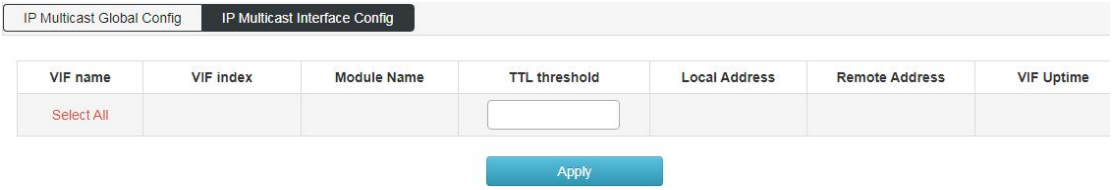


6.3 IP Multicast

IP multicast global configuration: multicast routing is enabled;



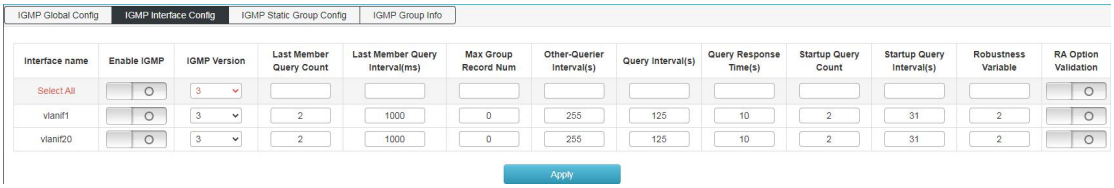
IP multicast interface configuration:



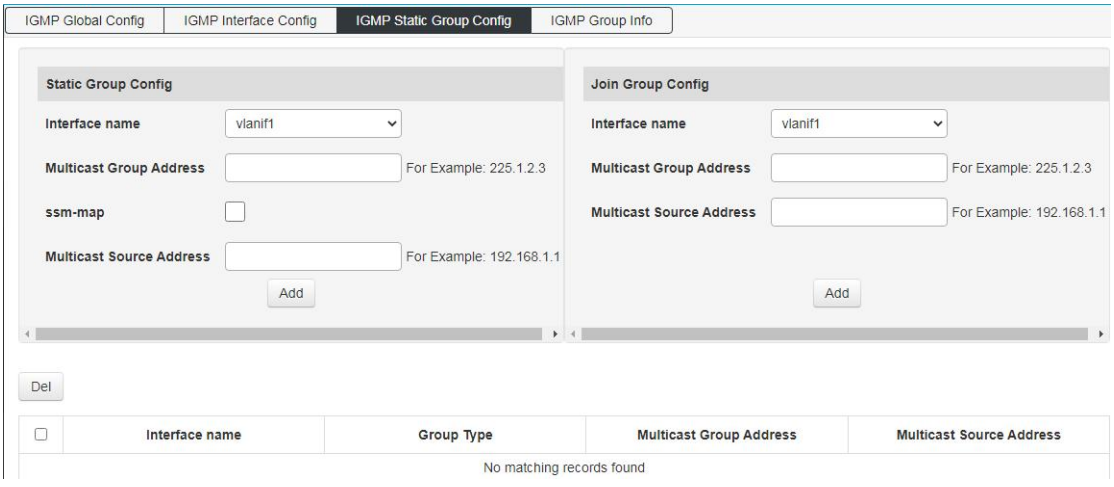
6.4 IGMP

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

IGMP interface configuration:



IGMP static group configuration,



IGMP group information:

7. Advance

7.1 QOS

【Function Description】

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

【Operation path】

Advance > QOS

【Interface description】

Figure 7-1-1 Global Config interface

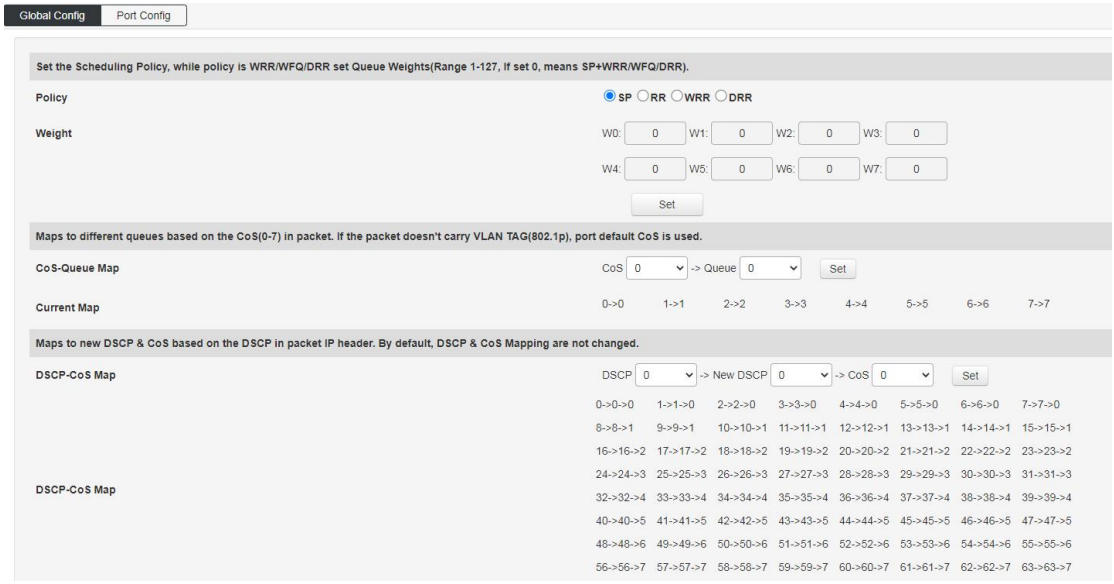


Figure 7-1-2 Port Config

interface

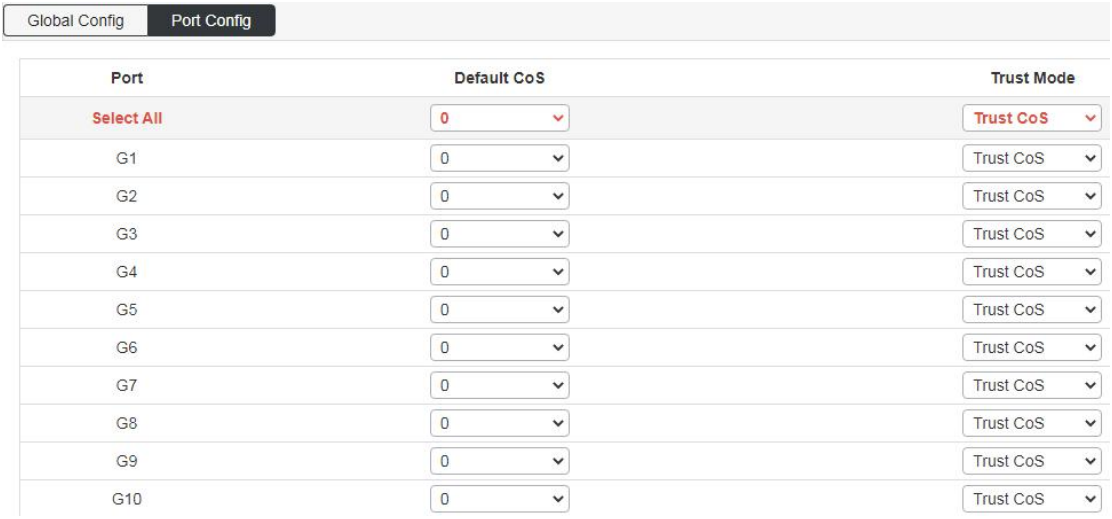


Table 7-1-2 Main elements of Port Config interface

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

7.2 ACL

【Function Description】

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

【Operation path】

Advance > ACL

【Interface description】

Figure 7-2-1 MAC ACL Config

interface

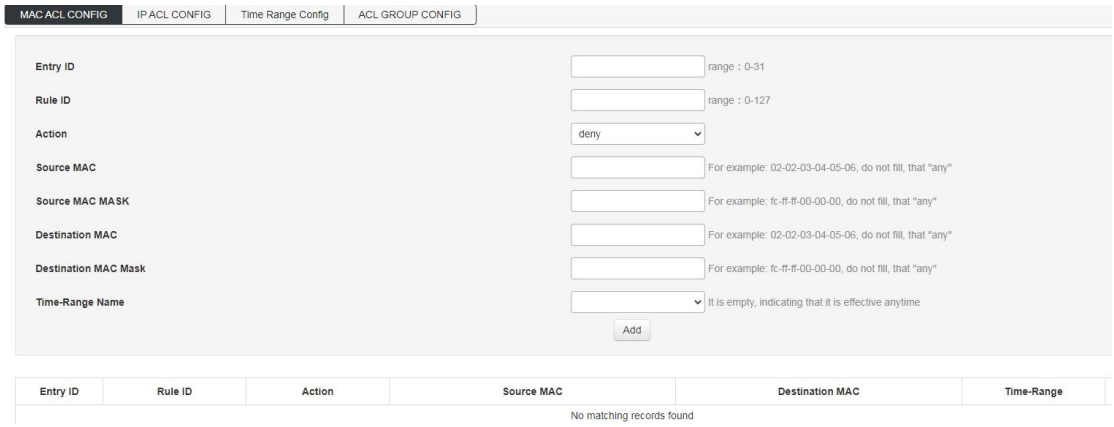


Table 7-2-1 Main elements of MAC ACL Config interface

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

Figure 7-2-2 IP ACL Config

interface

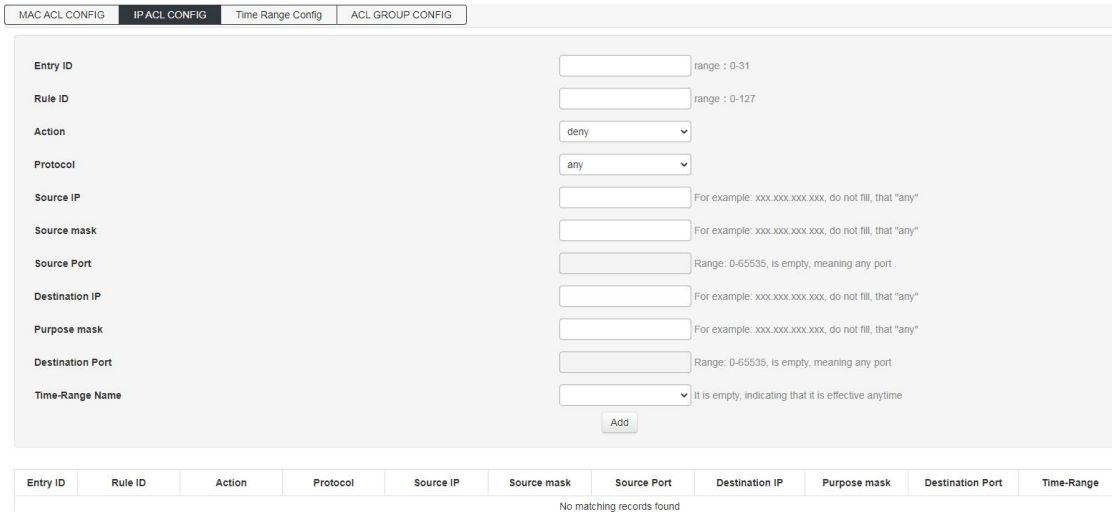


Table 7-2-2 Main elements of IP ACL Config interface

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

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

Figure 7-2-3 Time Range Config interface

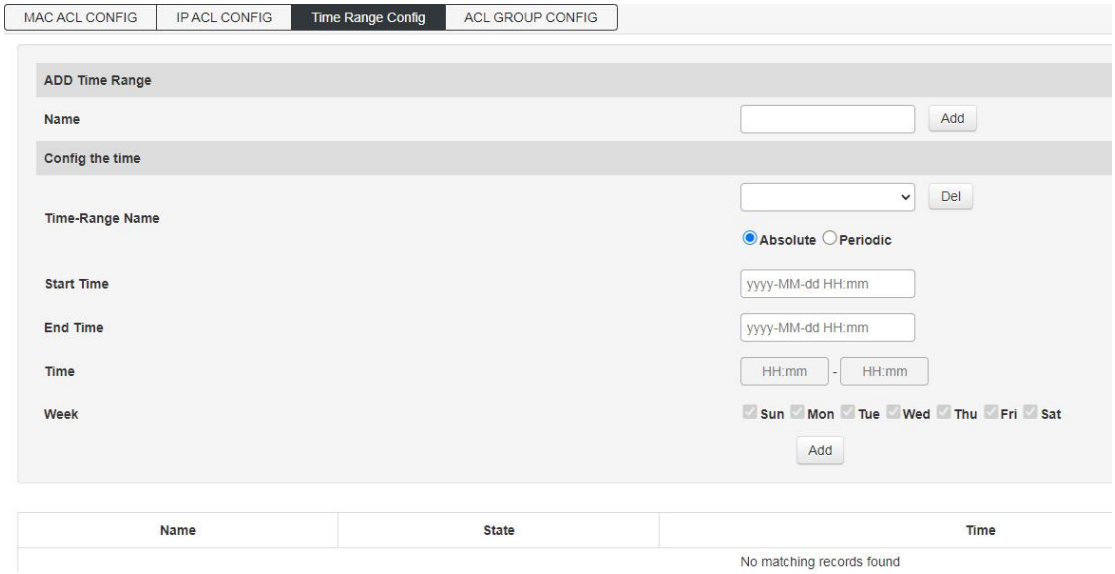
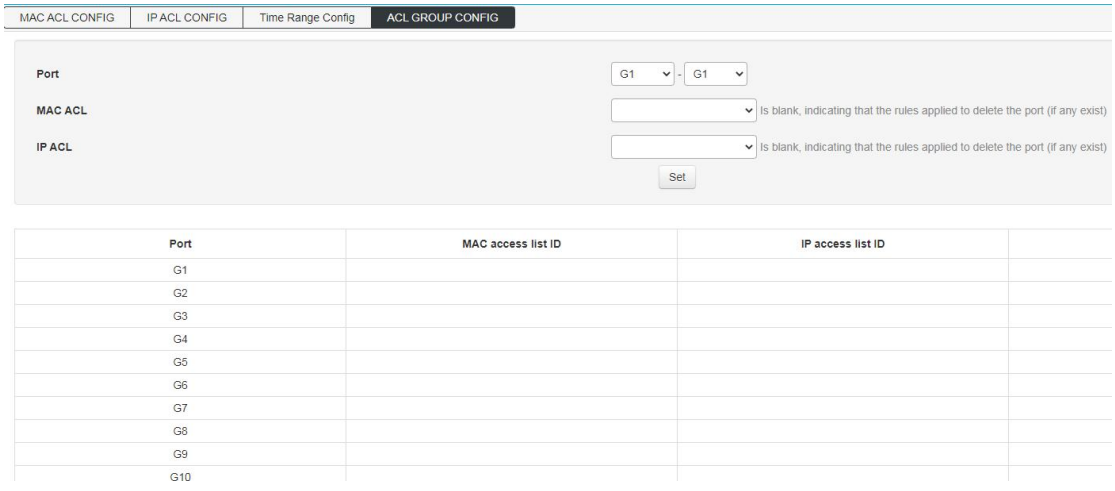


Figure 7-2-4 ACL GROUP CONFIG interface



7.3 SNMP

【Function Description】

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

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

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

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

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

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

SNMP provides four basic operations:

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

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

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

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

SNMP protocol version:

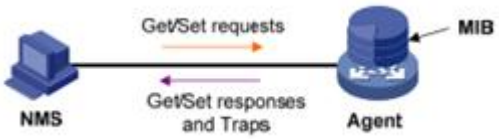
Currently, the SNMP Agent of the device supports SNMP v2c version and is compatible with SNMP v1 version.

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

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

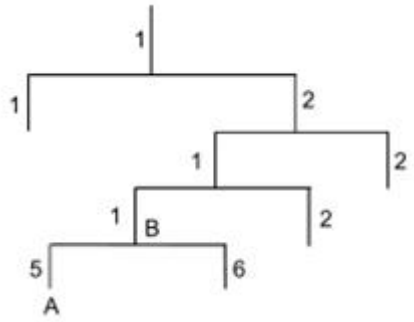
Introduction to MIB:

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



below:

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



【Operation path】

Advance > SNMP

【Interface description】

Figure 7-3-1 SNMP Global Config

interface

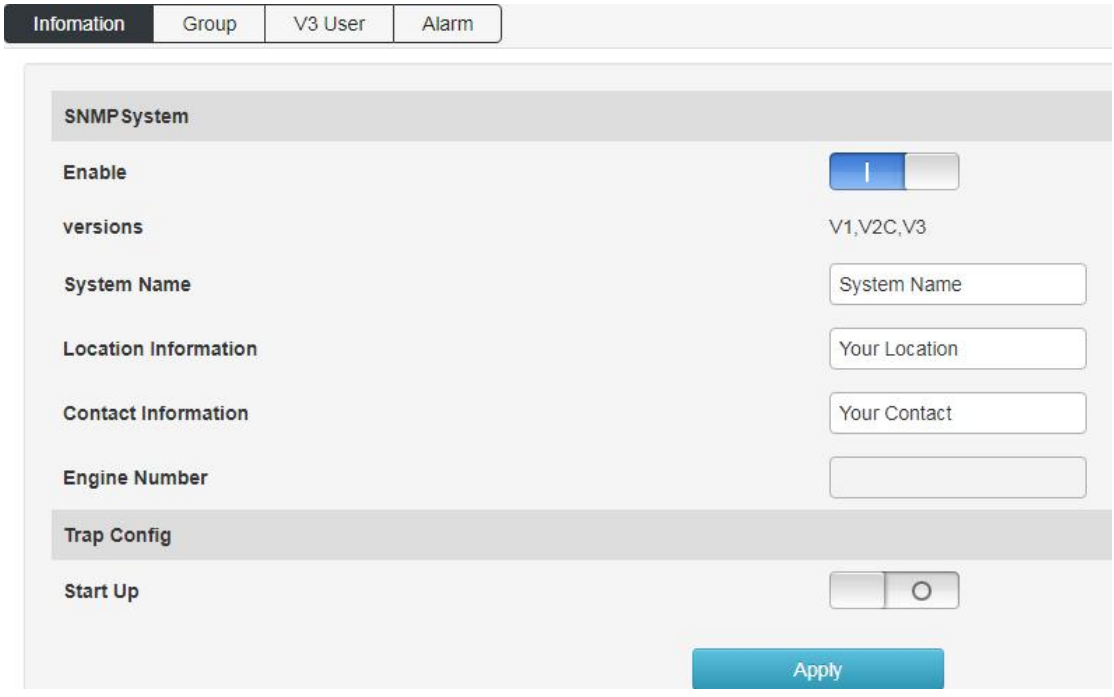


Figure 7-3-2 SNMP Group Config

interface

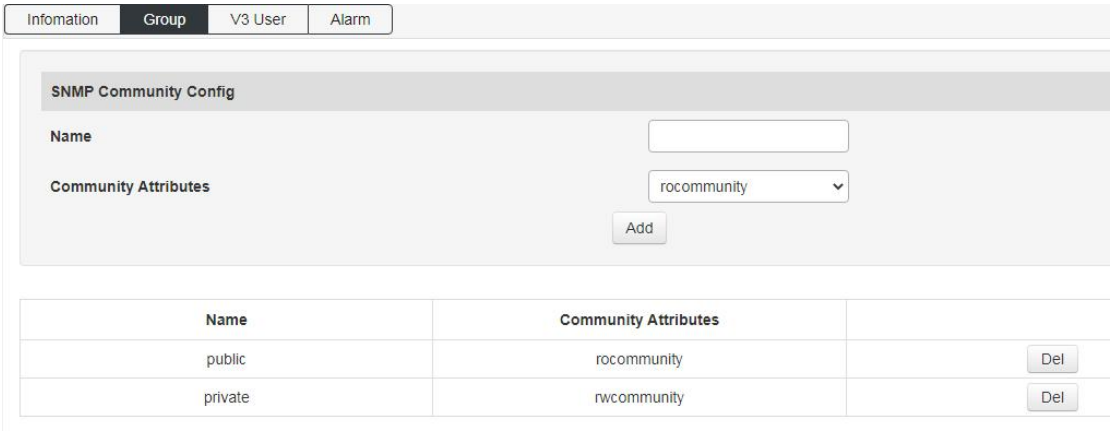


Figure 7-3-3 SNMP v3 User

Config

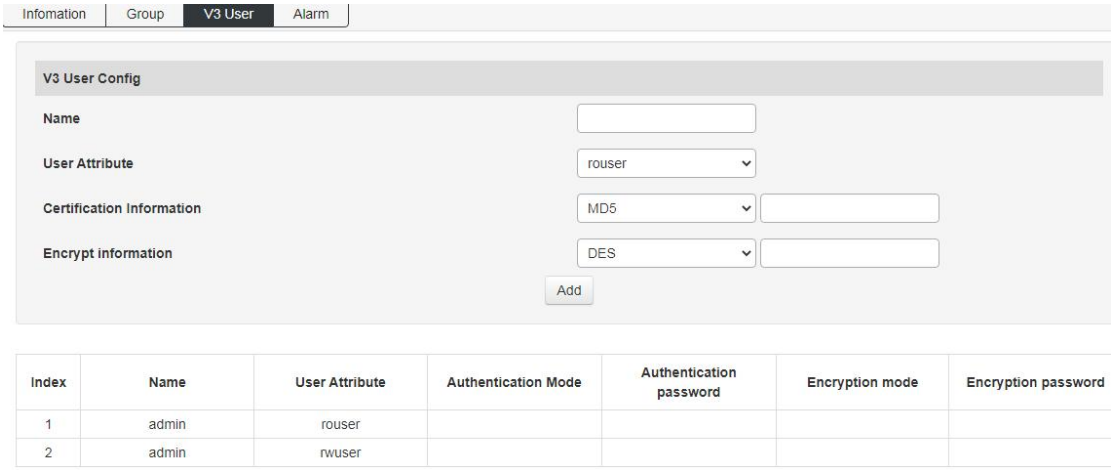
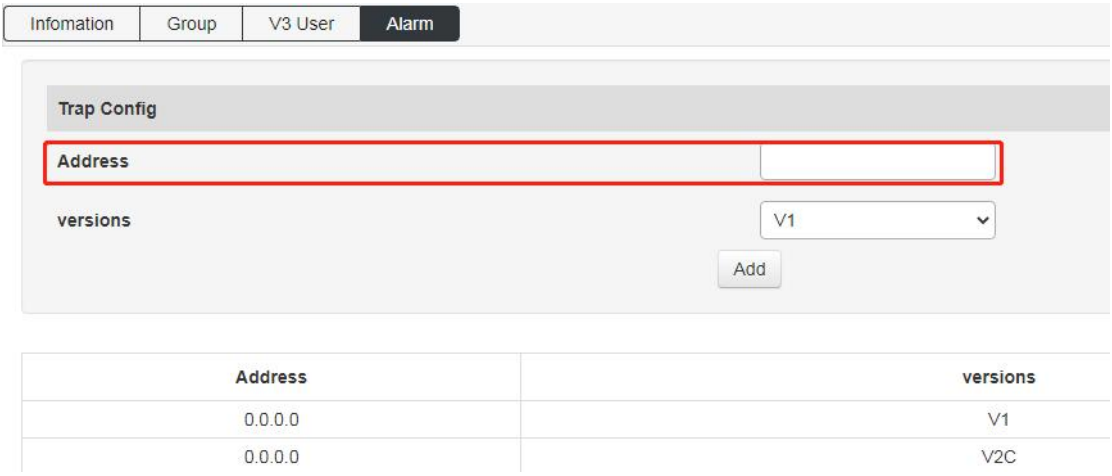


Figure 7-3-4 SNMP Alarm Config interface

Configure the TRAP trap receiving address and the corresponding SNMP protocol

version;



7.4 RMON

Figure 7-4-1 Event Group Config interface

Event group: query and add event groups monitored

remotely;

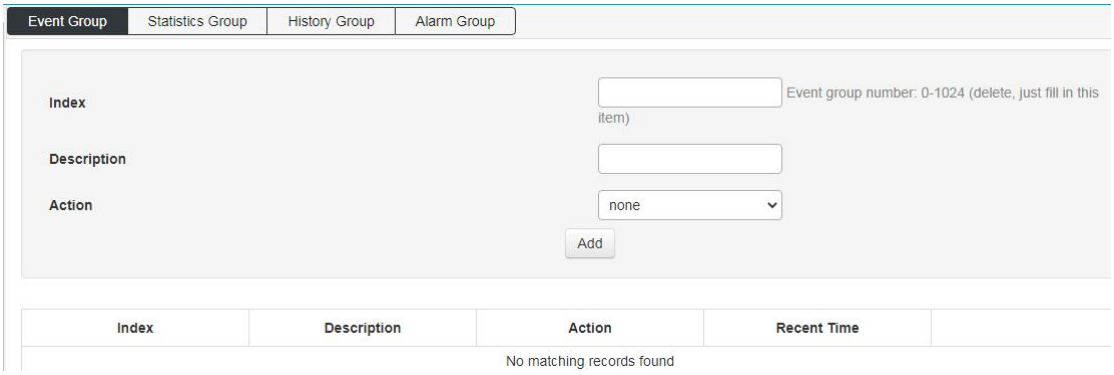


Figure 7-4-2 Statistics Group Config interface

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

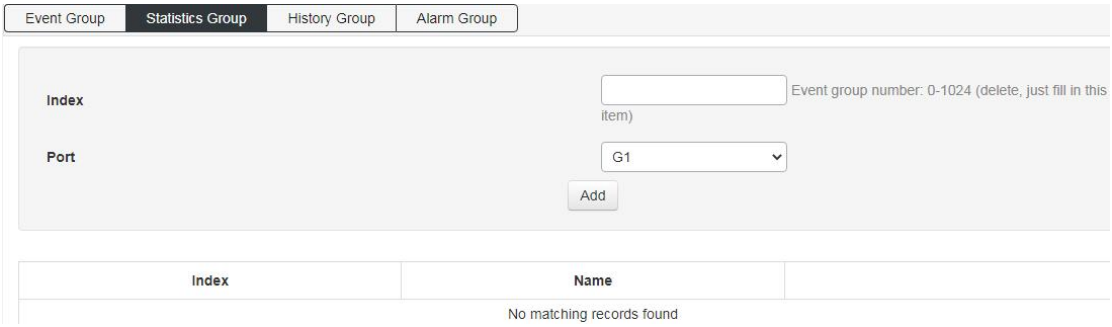


Figure 7-4-3 History Group Config interface

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

port;

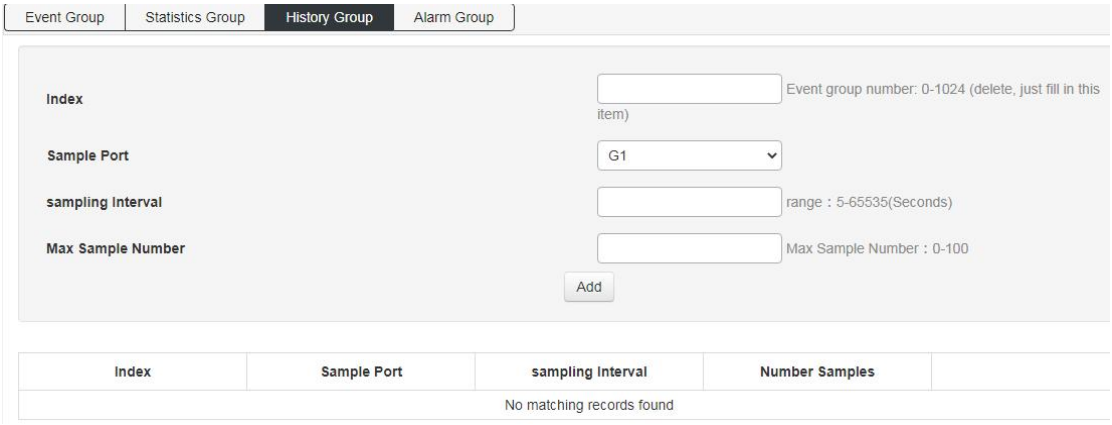
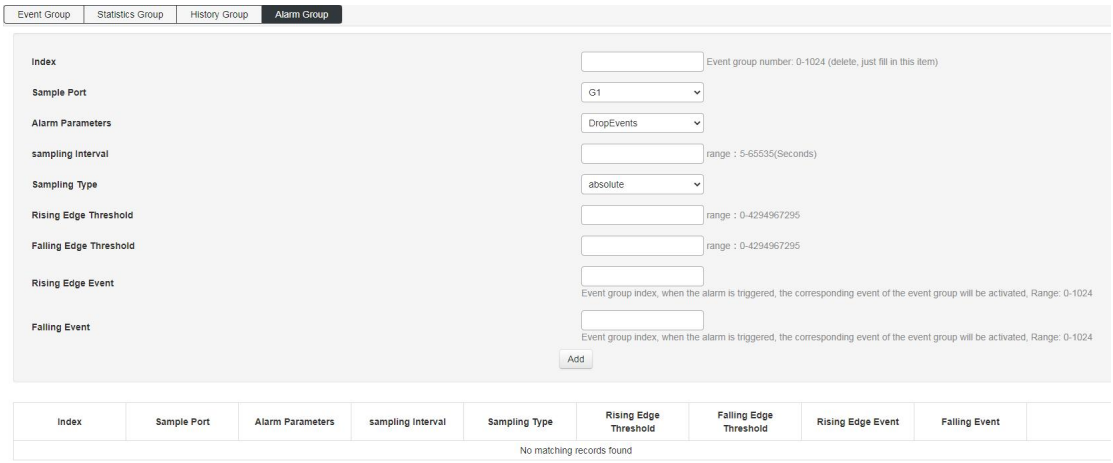


Figure 7-4-4 Alarm Group Config interface

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



7.5 LLDP

Figure 7-5-1 LLDP Global Config interface

Global configuration: enable and configure the LLDP function;

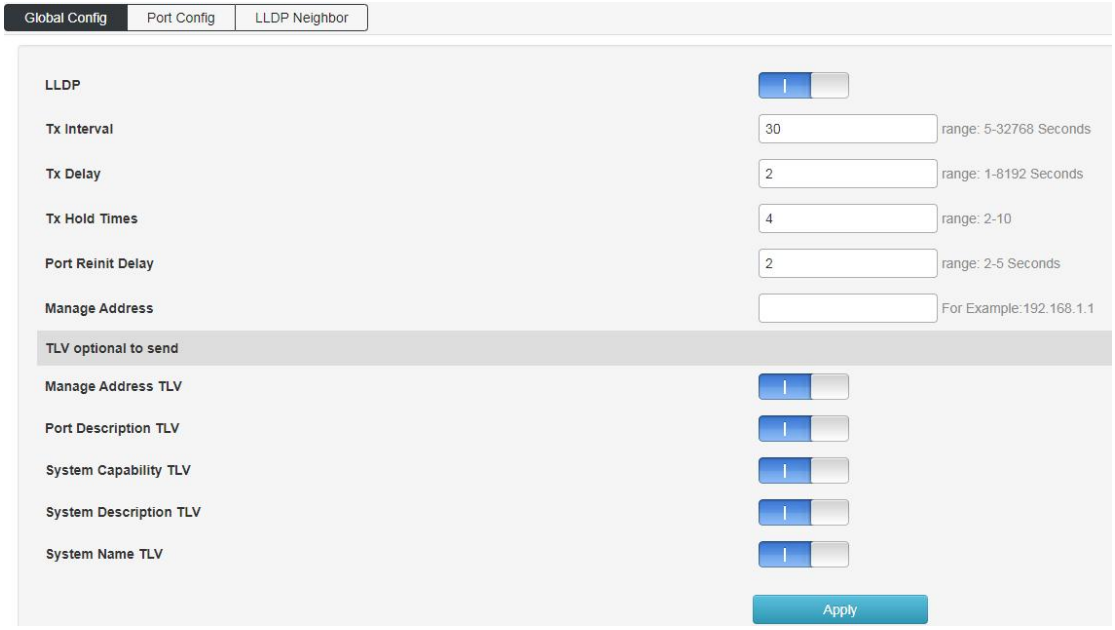


Figure 7-5-2 Port Config interface

Port configuration: configure port LLDP function attributes;

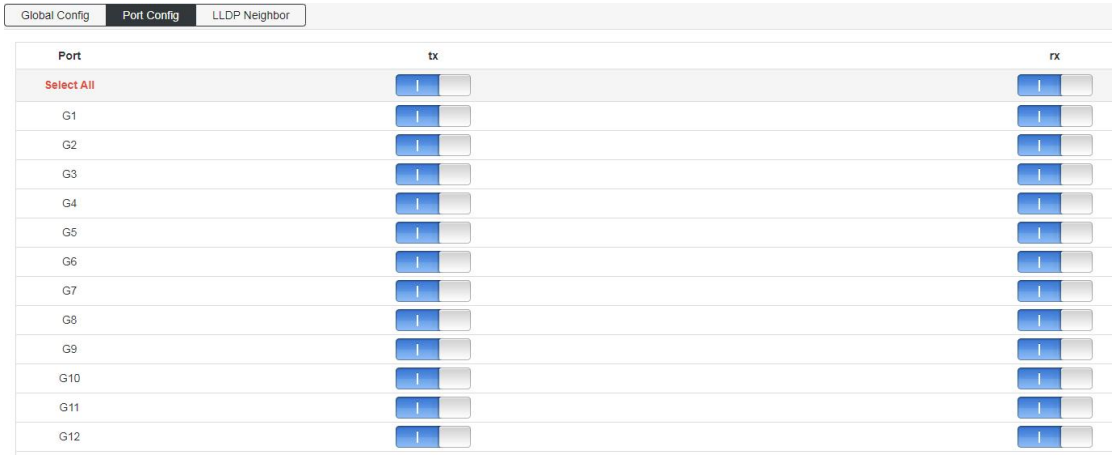
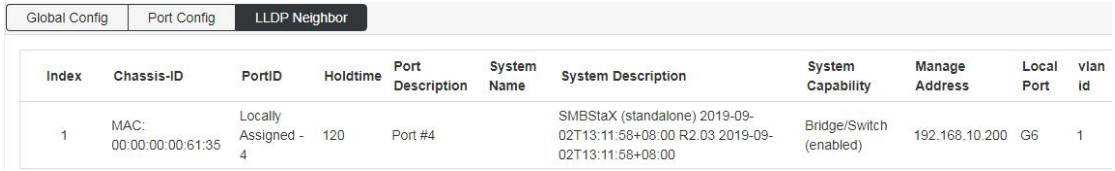


Figure 7-5-3 LLDP Neighbor Information Interface

LLDP neighbor: query LLDP neighbor information;



7.6 NTP

【Function Description】

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

【Operation path】

Advance > NTP

【Interface description】

Figure 7-6-1 NTP Global Config interface

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

interval;

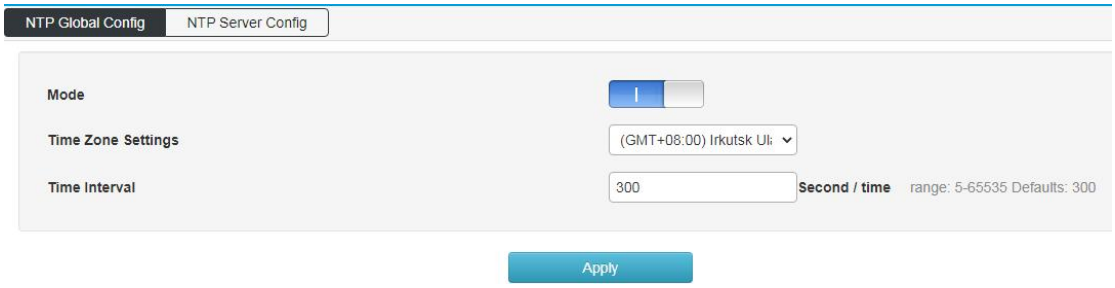
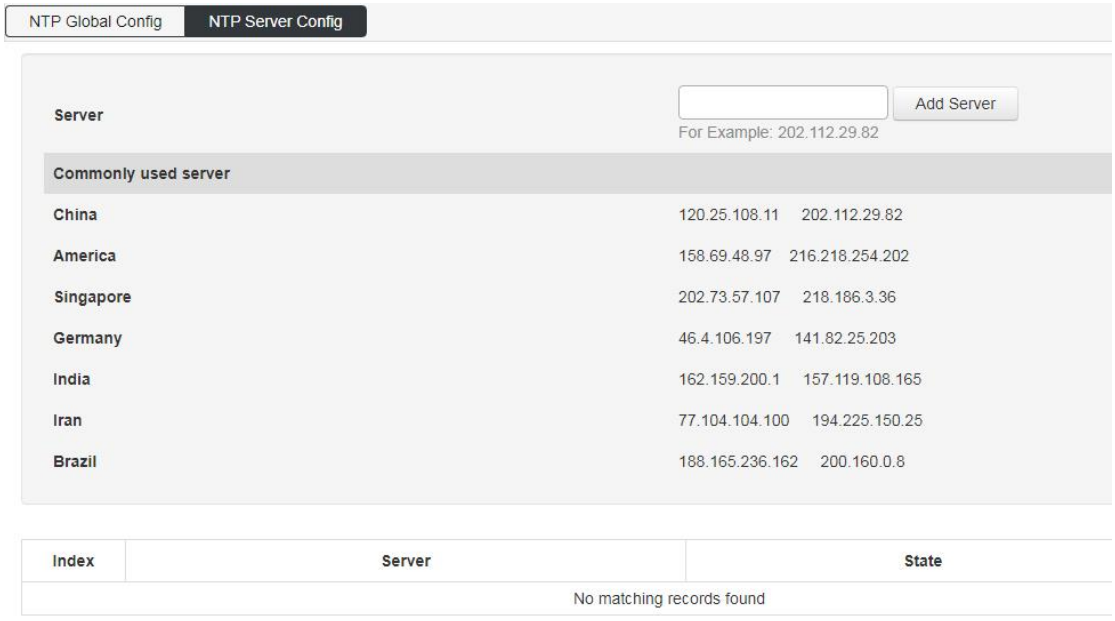


Figure 7-6-2 NTP Server Config interface

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

status;

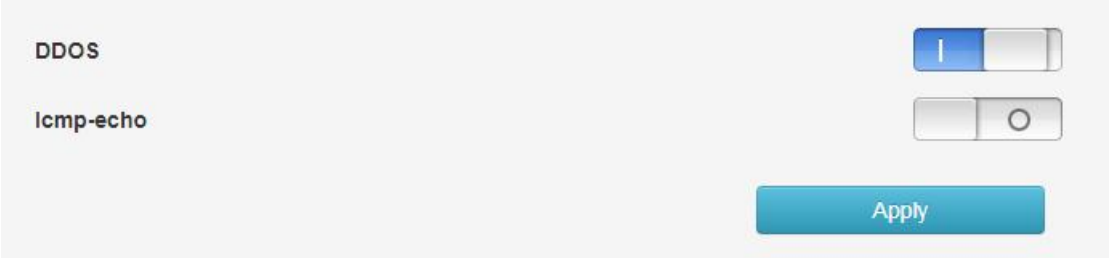


7.7 Secure

Figure 7-7-1 Scure configuration interface

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

on;



8. System Management

8.1 User Config

【Function Description】

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

【Operation path】

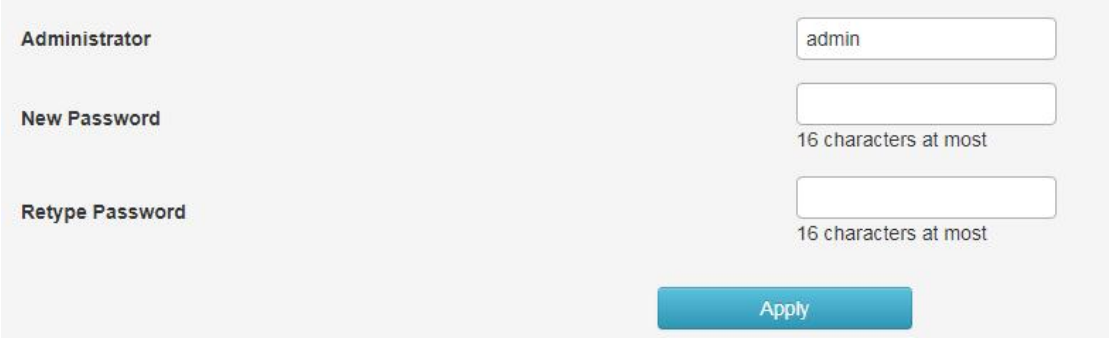
System > User

【Interface description】

Figure 8-1 User Config interface

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

added;



8.2 Network

【Function Description】

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

【Operation path】

System > Network

【Interface description】

Figure 8-2-1 IPv4 Config interface

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

address;

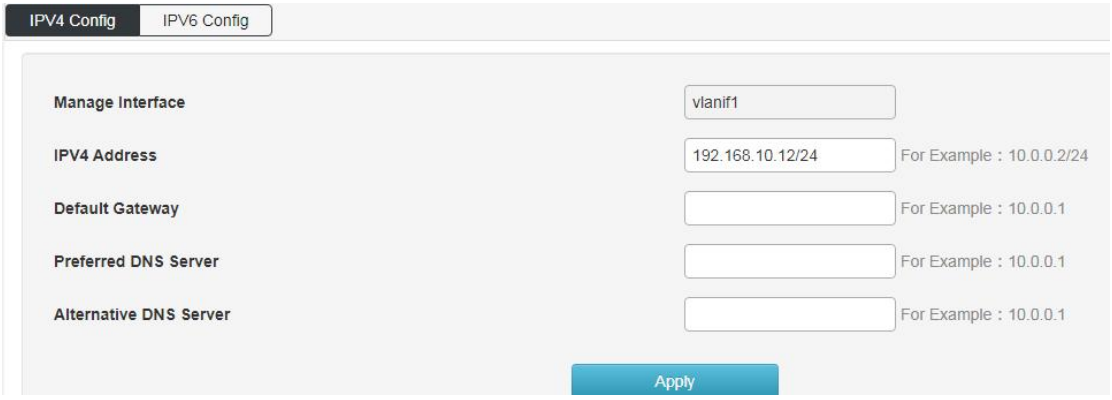
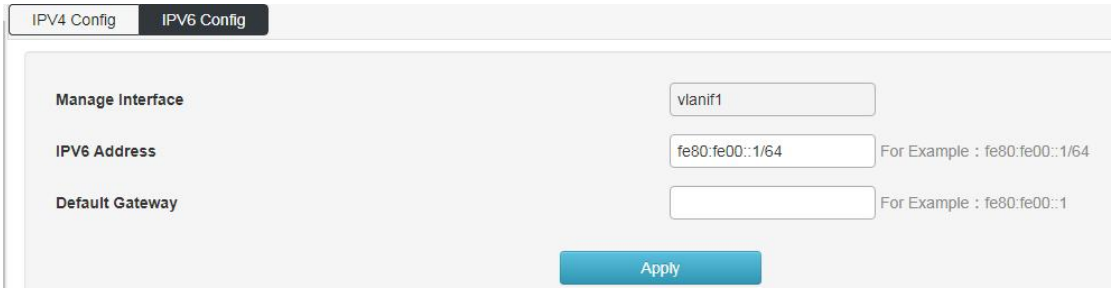


Figure 8-2-2 IPv6 Config interface

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

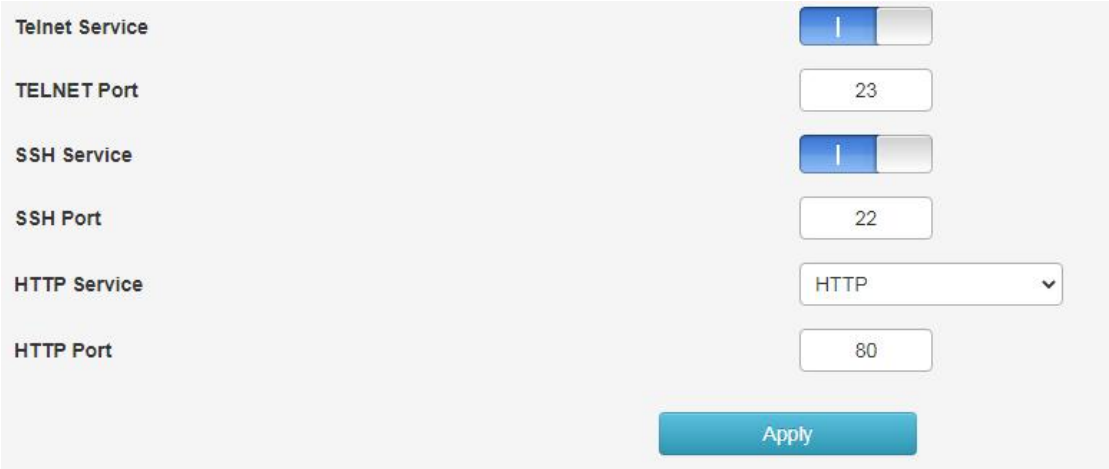
address;



8.3 Service Config

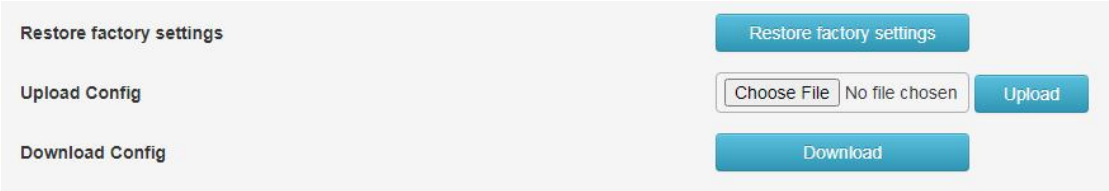
Figure 8-3-1 Service Config interface

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



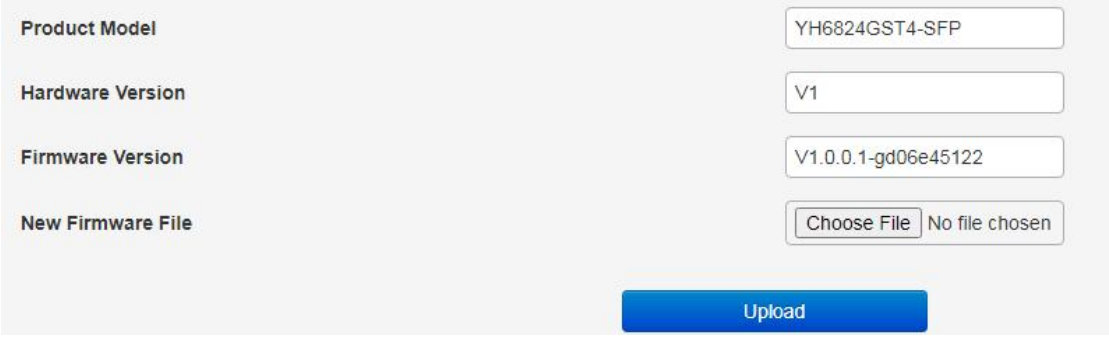
8.4 Configration management

Used to reset, upload and download switch configuration;



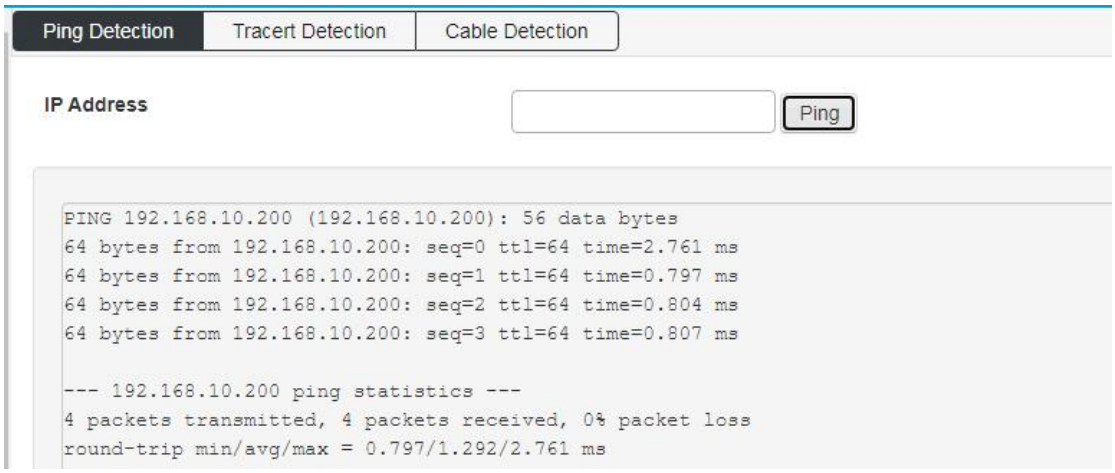
8.5 Firmware Upgrade

Used to upgrade the firmware version currently used by the switch;



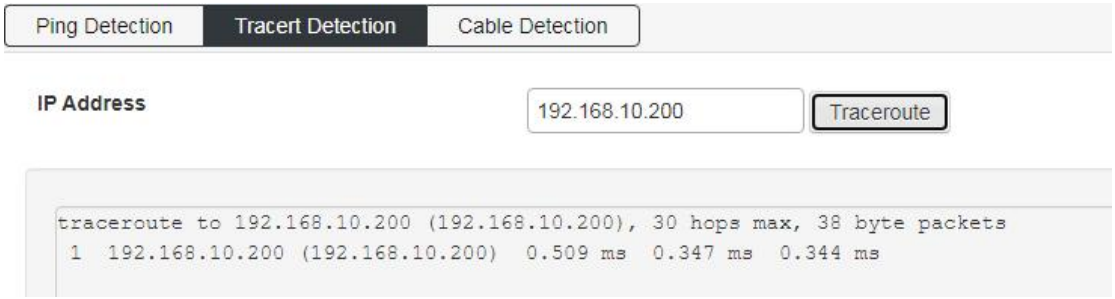
8.6 Diagnostic

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



Tracert detection:

Traceroute;



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

8.7 Restart

reboot the switch

Restart	Restart