DIGITUS®

Layer 2 Industrial Switch

Web configuration manual

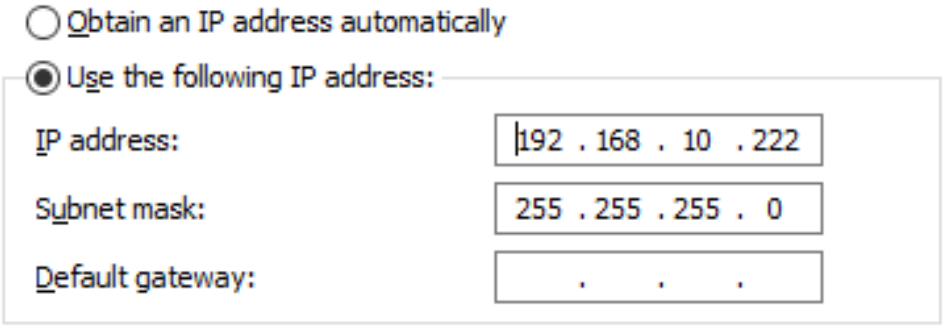
DN-651154, DN-651155
DN-651156, DN-651157
DN-651158, DN-651159

Table of content

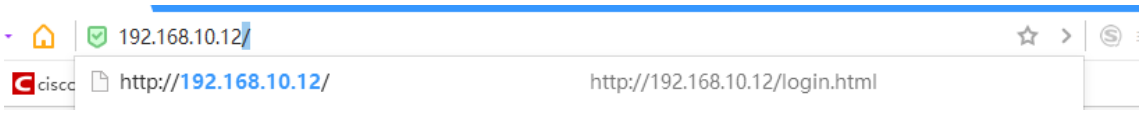
1. Log into the Switch Web Interface 3
2. Switch Information 4
2.1 Global Information 4
2.2 Statistical Information 5
2.3 Log Information 6
2.4 Alarm List 6
3. Port Management 7
3.1 Port Configuration 7
3.2 Port Isolation 7
3.3 Mirroring Port 8
3.4 Rate Limited 8
3.5 Storm Control 9
3.6 Port Energy Saving 9
4. PoE 10
4.1 PoE Port Configuration 10
4.2 Devices Power Supply 10
4.3 Timing Power Supply Configuration 11
4.4 Intelligent Power Supply Configuration 12
5. L2 Management 13
5.1 MAC address table 13
5.2 VLAN Configuration 13
5.3 GVRP 16
5.4 Link Aggregation 16
5.5 MSTP Configuration 19
5.6 Loop Protection 20
5.7 DHCP-snooping 22
5.8 IGMP Snooping 23
5.8 802.1x authentication 24
6. Senior Management 26
6.1 QOS Configuration 26
6.2 ACL Configuration 27
6.3 SNMP Configuration 29
6.4 RMON 30
6.5 LLDP Configuration 32
6.6 NTP Configuration 33
6.7 Anti Attack 33
7. System Management 34
7.1 User Settings 34
7.2 Network Settings 34
7.3 Alarm Configuration 35
7.4 Service Configuration 35
7.5 Configuration Management 35
7.6 Firmware Update 36
7.8 Diagnostic Testing 36
7.9 Reboot Device 37

1. Log into the Switch Web Interface

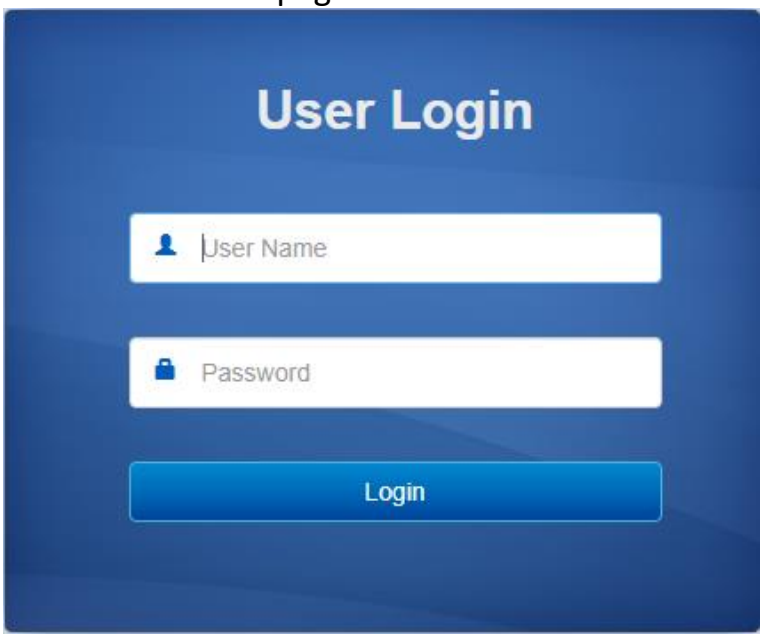
The default management address of the switch is 192.168.10.12/24, when logging into the web management page of the switch, you need to set the IP address of the local network card and the IP address of the switch are in the same segment, as shown in the following screen: the IP address of the local network card is set to 192.168.10.222/24.



Enter the management address of the switch in the search bar of the browser, screen as below:



Confirm to enter the web verification page of the switch.



User Name: admin
Password: admin.
Click login to login to the web interface of the switch.

2. Switch Information

This module is used to view the internal data of the switch when it is running, including the flow rate of the port, the working mode, and the log information of the switch.

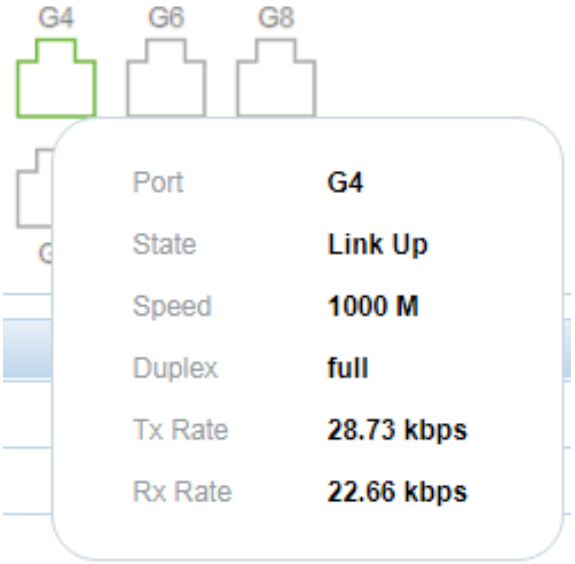
2.1 Global Information

The following functions are in included:

①View the current port status, port working mode and port speed of the switch.

Move the mouse to the 

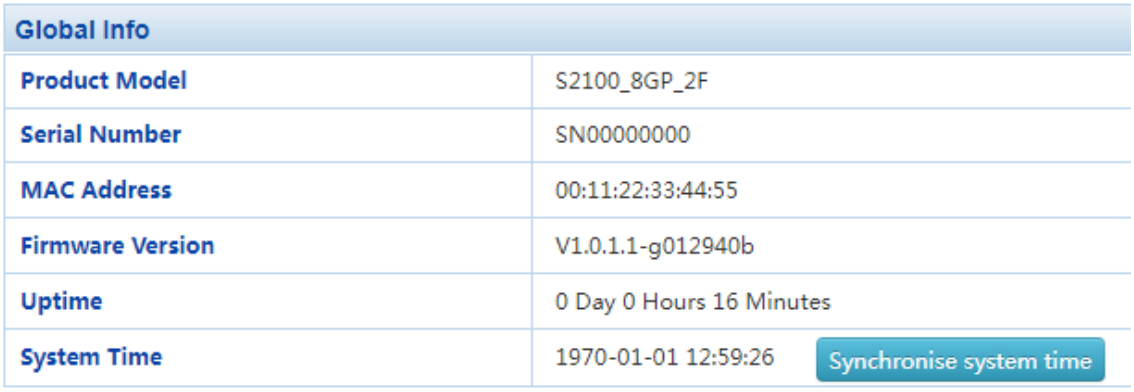
icon and he port name, status, bandwidth, duplex mode, and rate will be displayed.



Indicates that the port has been enabled and the connection has been established,  indicates that the port is not enabled, and  indicates the optical port.

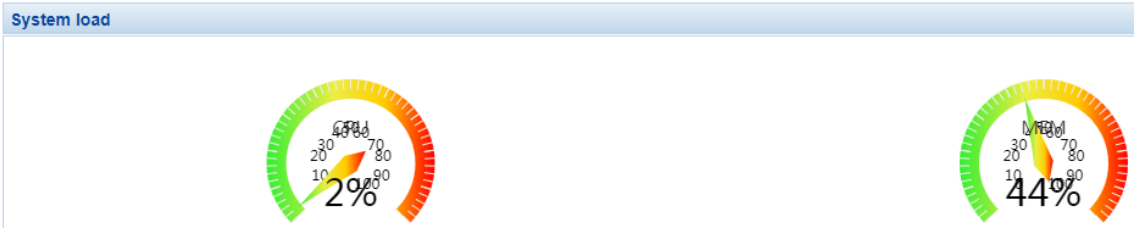
②View the switch property information, click 

in the page to synchronize the local computer time with the system time of the switch.



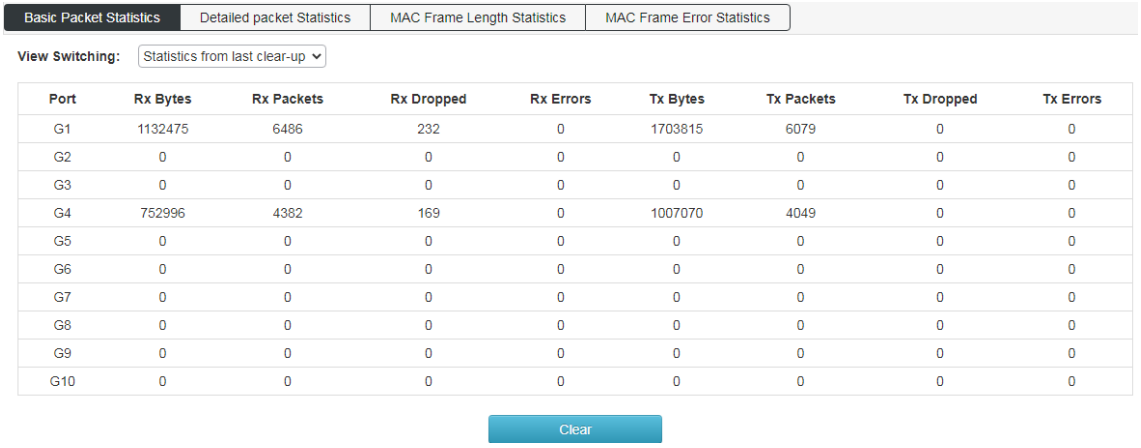
Global Info	
Product Model	S2100_8GP_2F
Serial Number	SN00000000
MAC Address	00:11:22:33:44:55
Firmware Version	V1.0.1.1-g012940b
Uptime	0 Day 0 Hours 16 Minutes
System Time	1970-01-01 12:59:26 Synchronise system time

③To check the CPU and memory usage of the switch.



2.2 Statistical Information

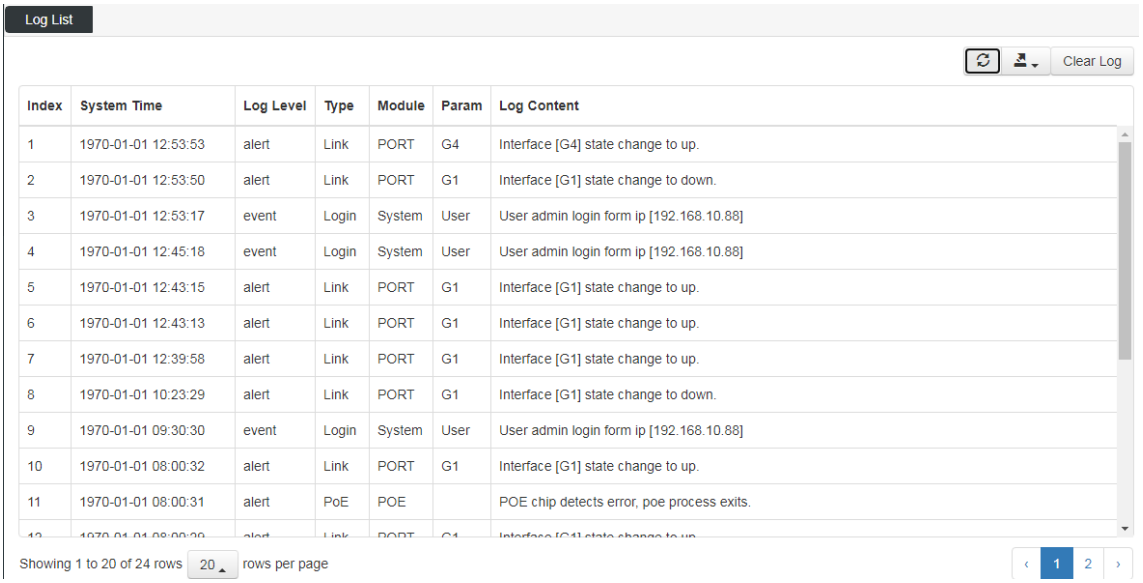
To check the message data received and sent by various ports, including Basic Packet Statistics, Detailed Packet Statistics, MAC Frame Length Statistics and MAC Frame Error Statistics.



Port	Rx Bytes	Rx Packets	Rx Dropped	Rx Errors	Tx Bytes	Tx Packets	Tx Dropped	Tx Errors
G1	1132475	6486	232	0	1703815	6079	0	0
G2	0	0	0	0	0	0	0	0
G3	0	0	0	0	0	0	0	0
G4	752996	4382	169	0	1007070	4049	0	0
G5	0	0	0	0	0	0	0	0
G6	0	0	0	0	0	0	0	0
G7	0	0	0	0	0	0	0	0
G8	0	0	0	0	0	0	0	0
G9	0	0	0	0	0	0	0	0
G10	0	0	0	0	0	0	0	0

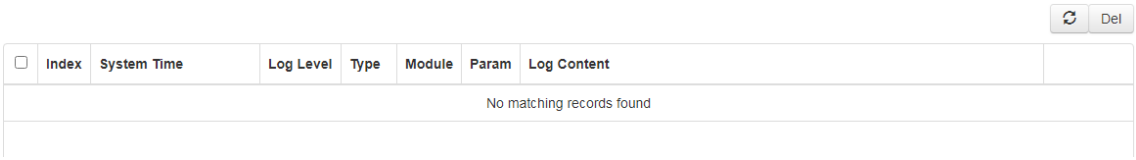
2.3 Log Information

Log is used to view simple switch log, and can view switch startup and port startup data, screen as blew:



2.4 Alarm List

This page is used to view the alarm information of the switch;



3. Port Management

3.1 Port Configuration

In this page, you can set the port rate, duplex mode, the max frame length (the value range is 1518-10240), flow control and switch port.

In the link status,  indicates that the port is not connected, or the port has been manually down. When the link status is  or , it indicates that the port is working normally, the color is the port working mode (green is Gigabit, yellow is 100MB).

On this page, you can not only view the port link status and port working mode, but also set the port working mode, such as "100MB full / half duplex", "Gigabit full / half duplex" and "adaptive". You can also close the specified port through this page, which is the same as the command “shut down”.
For the frame size setting, the default is basic frame 1522, which can be modified to super long frame 9600. The value range of this item is 1518-10240.

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

Apply

3.2 Port Isolation

This page is used to configure the port isolated. The isolated ports cannot communicate with each other, and the isolated ports can communicate with other non-isolated ports.

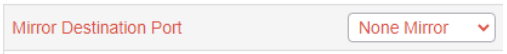
Select All | All Not Isolatio

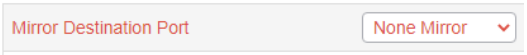
Name	Port Isolate	Name	Port Isolate
G1		G2	
G3		G4	
G5		G6	
G7		G8	
G9		G10	

Tip: Unable to communicate between isolated ports
Tip: Isolated ports can communicate with other devices

Apply

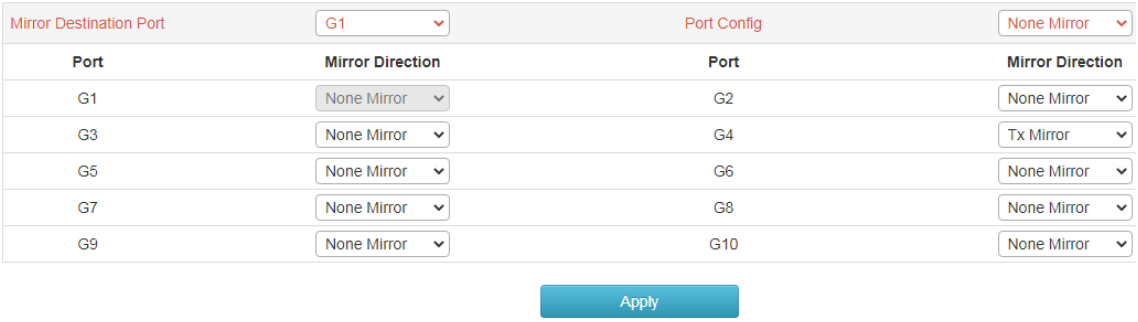
3.3 Mirroring Port

This page is used to configure the mirror port, 

is used to configure to accept mirror data； 

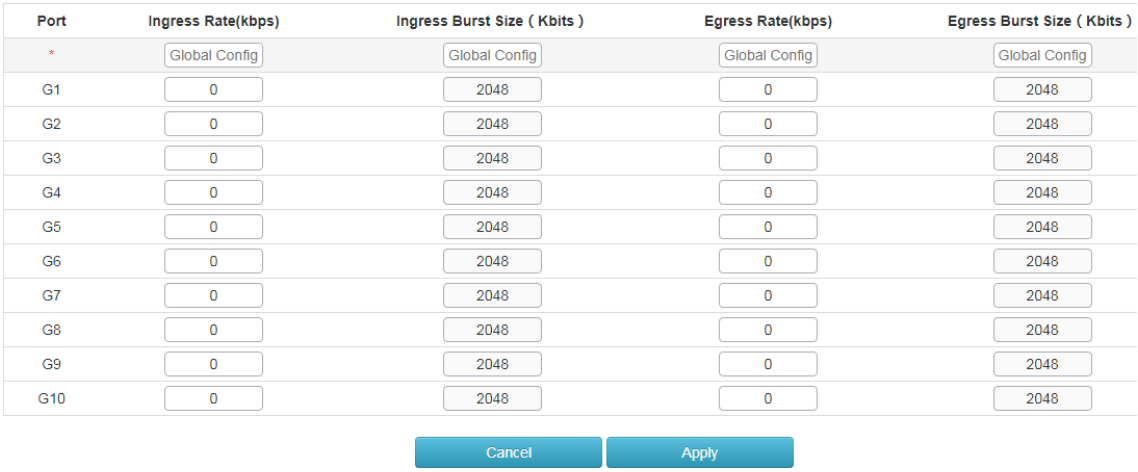
is used to configure all port mirroring properties in one step.

The configuration representative in the following page mirrors the sent message data of port 4 to port 1, screen as blew:



3.4 Rate Limited

This page is used to limit the upper limit of port rate;



3.5 Storm Control

This page is used to limit the packet rate of port broadcast, multicast and unicast,

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

Cancel Apply

3.6 Port Energy Saving

This function is used to open the energy saving mode of switch port, screen as blew:

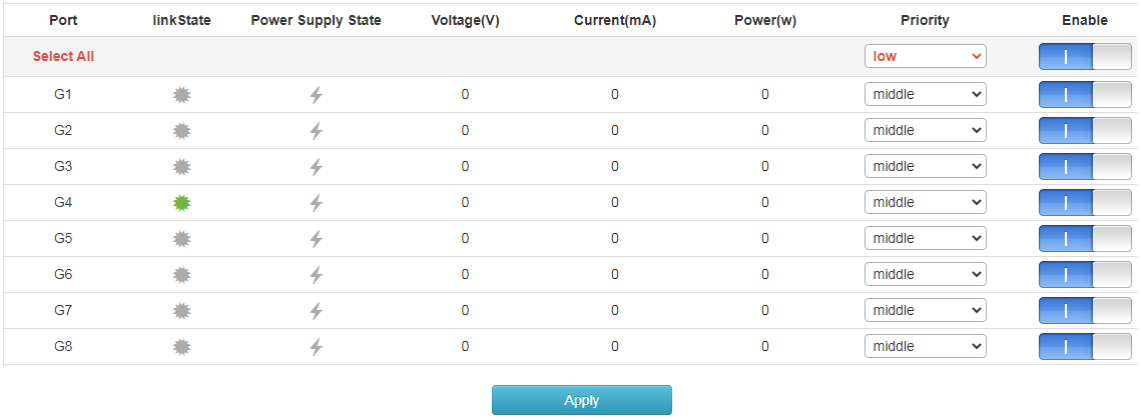
Select All			
Name	EEE	Name	EEE
G1		G2	
G3		G4	
G5		G6	
G7		G8	

Apply

4. PoE

4.1 PoE Port Configuration

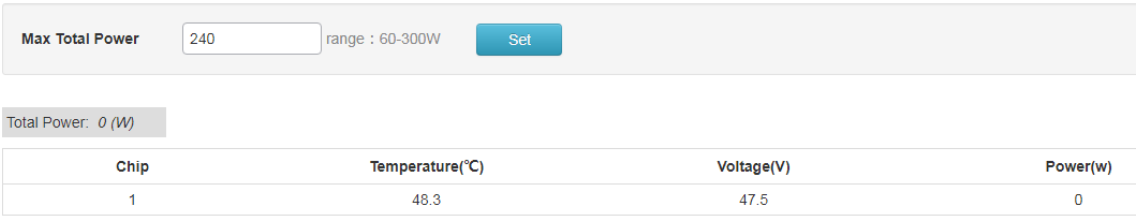
You can view the working status of the port PoE and the current voltage and current data provided, screen as blew:



In the link column of the page, indicates that the port has no data transmission, indicates that the port is in forwarding state, in the power supply status column indicates that the port is not PoE powered, and indicates that the port is in PoE power supply state. The voltage, current, and power columns respectively display the voltage, current and power provided by the POE power supply port. The priority column is used to change the PoE power supply priority of the switch port. When the overall power is insufficient, the port with higher priority will give priority to power supply. The startup bar is used to enable the port PoE function.

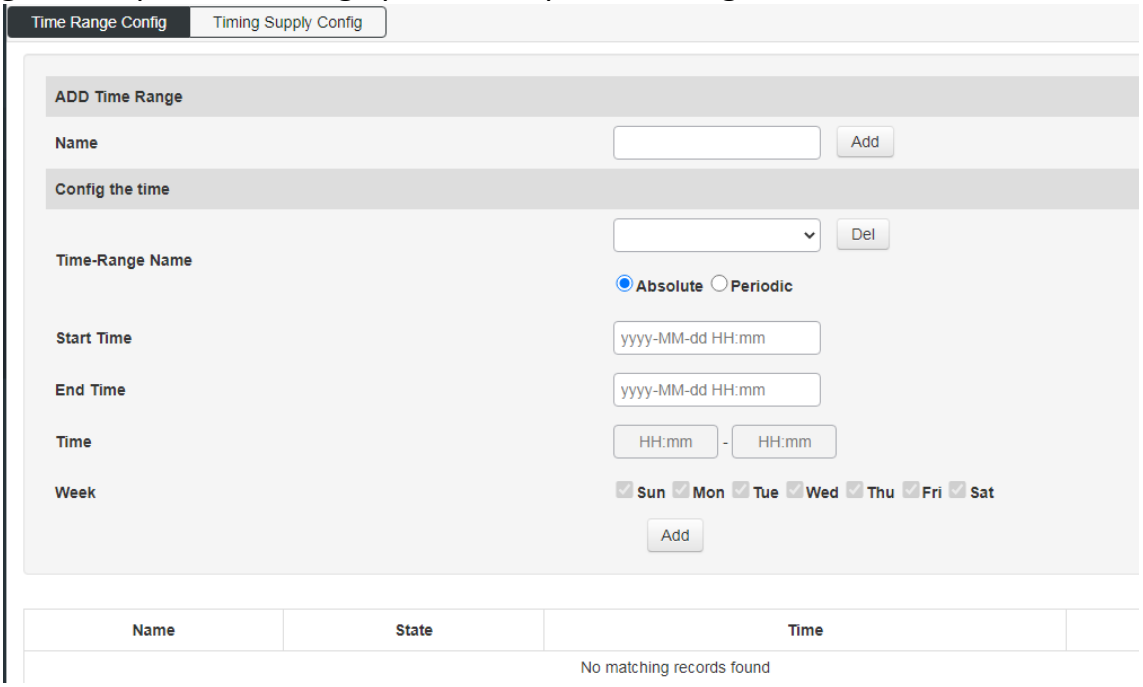
4.2 Devices Power Supply

This page is used to set the total output power of the switch, with a value range of 60 ~ 300W. It can also be used to view the total output power and chip temperature of the current switch.

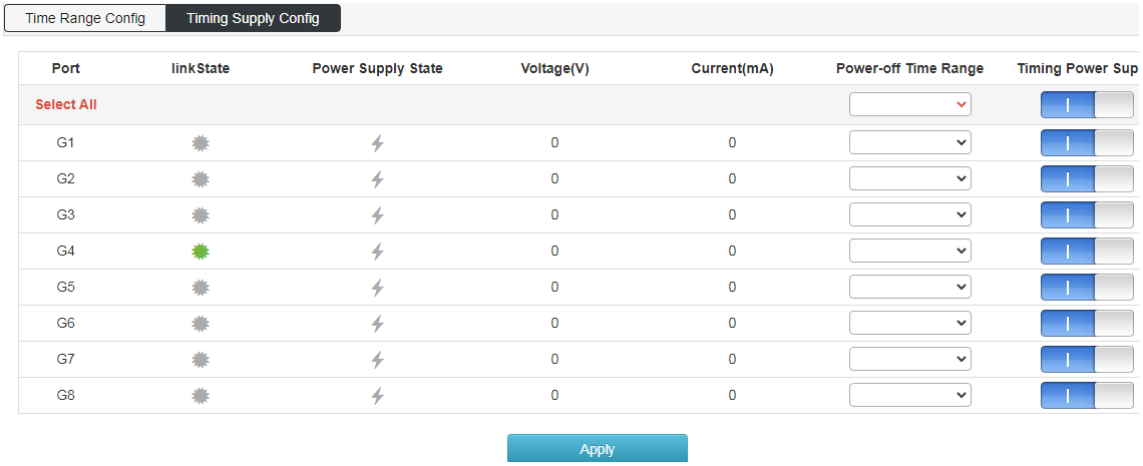


4.3 Timing Power Supply Configuration

Configure the periodic outage period or specific outage time of the switch.

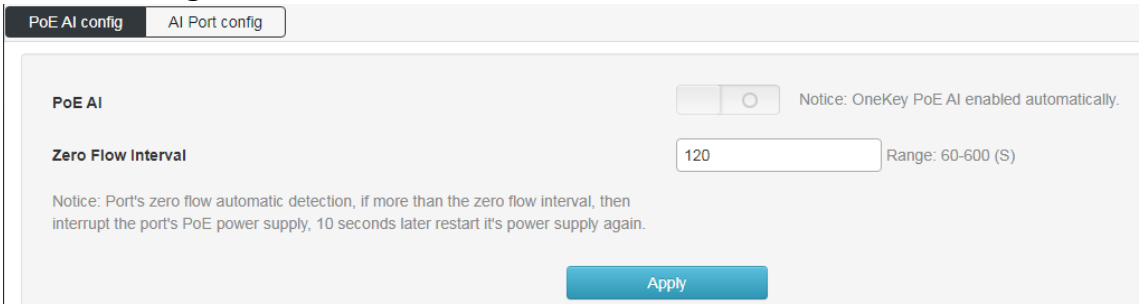


Apply the set power-off time to the port, and turn on this function by default for all ports.

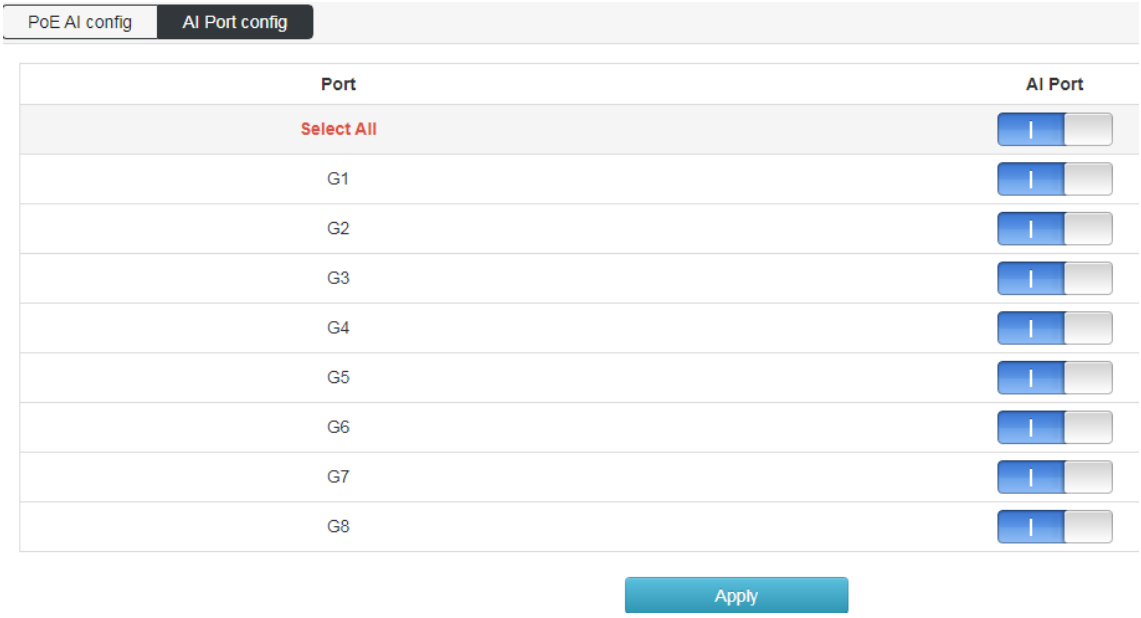


4.4 Intelligent Power Supply Configuration

Set PoE port to automatically disconnect power supply when there is no data transmission within a certain period of time. The default value is that when there is no data transmission in 120 seconds, the POE port will disconnect the power supply, and the value range is 60 ~ 600 seconds.



Open the port intelligent power supply function, which is all on by default.



5. L2 Management

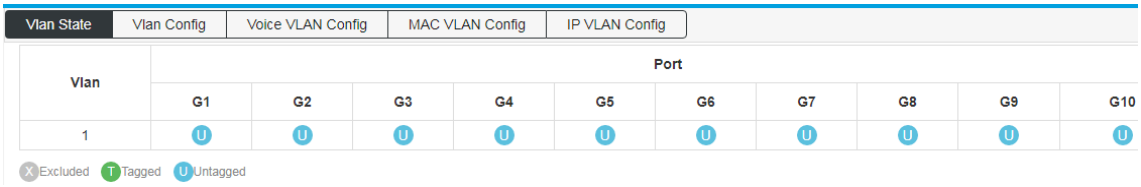
5.1 MAC address table

Check the MAC address of the device mounted on the switch

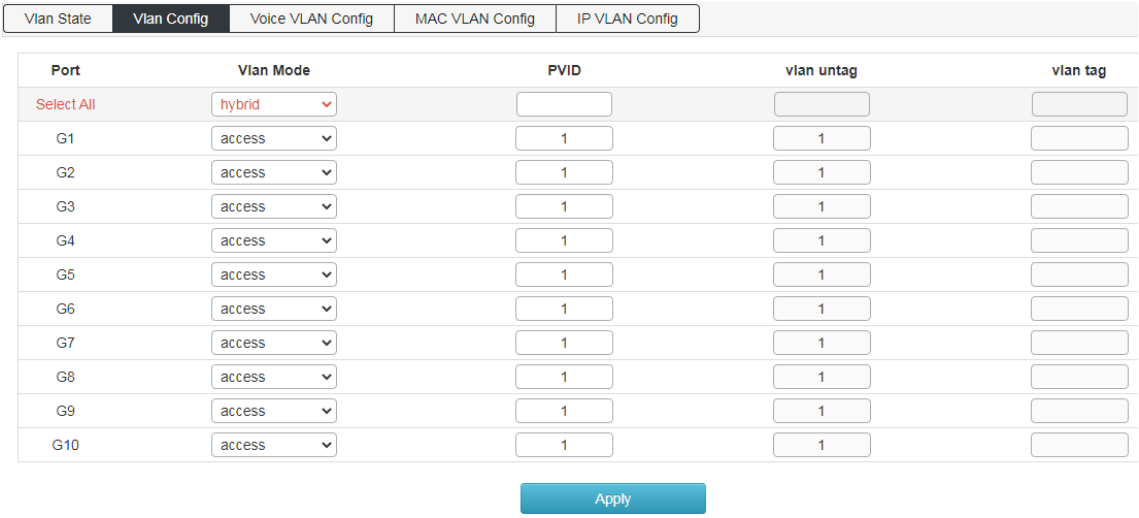
5.2 VLAN Configuration

This page includes viewing VLAN State, VLAN Configuration, Voice VLAN Configuration, MAC VLAN configuration and IP VLAN configuration.

Screen as blew:



The screen below shows the configuration of port VLAN;



Port properties that can be set:

Access：

Access ports are normally used to connect to end stations. Dynamic features like voice VLAN may add the port to more VLANs behind the scenes. Access ports have the following characteristics:

- Member of exactly one VLAN, the Port VLAN (Access VLAN), which by default is 1.
- Accepts untagged and C-tagged frames.
- Discards all frames that are not classified to the Access VLAN
- On egress all frames classified to the Access VLAN are transmitted untagged.
- The access port is usually used to connect to the terminal station. For example,

the dynamic characteristics of voice VLAN can add ports to multiple VLANs behind the scenes. 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 unlabeled frames and C-labeled frames,
- Drop all frames in unclassified access VLAN,
- All frames to the exit are sent unmarked.

Trunk：

The trunk port can traffic multiple VLANs at the same time and is usually used to connect to other switches. The trunk port has the following features:

- By default, the trunk port is a member of all existing VLANs. This can be achieved by using a limited number of VLANs.
- Unless enabled on the port of VLAN relay, divided into different VLANs, and the frame of that the port is not a member will be discarded.
- By default, all frames, but VLAN (also known as local VLAN) frame tags classified into ports get about exits. The frames classified to the port VLAN do not get the exit of c-tag,
- The exit marker can change all frames of the marker, in which case only the entry of the marked frame is accepted,
- VLAN trunking may be enabled.

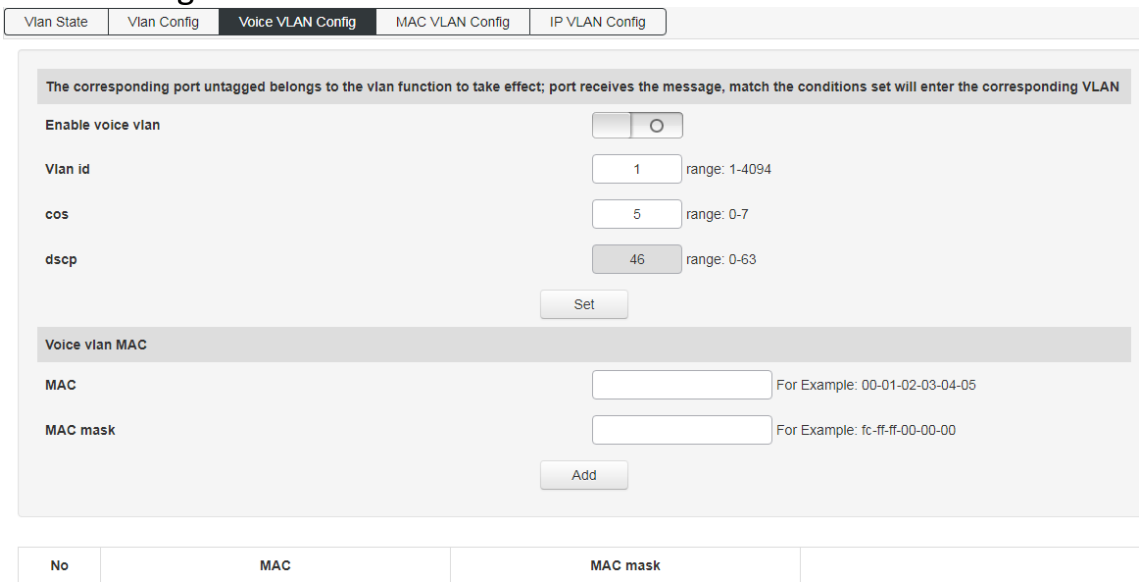
Hybrid：

The hybrid port is similar to the trunk port in many ways, but adds additional port configuration capabilities. In addition to the characteristics described for the relay port, the hybrid port also has the following capabilities:

- It can be configured as VLAN tag or unknown, C-tag all, S tag all, or S-custom tag all.
- The inlet filtration can be controlled.
- The exit annotation and configuration of the access frame can be configured independently.

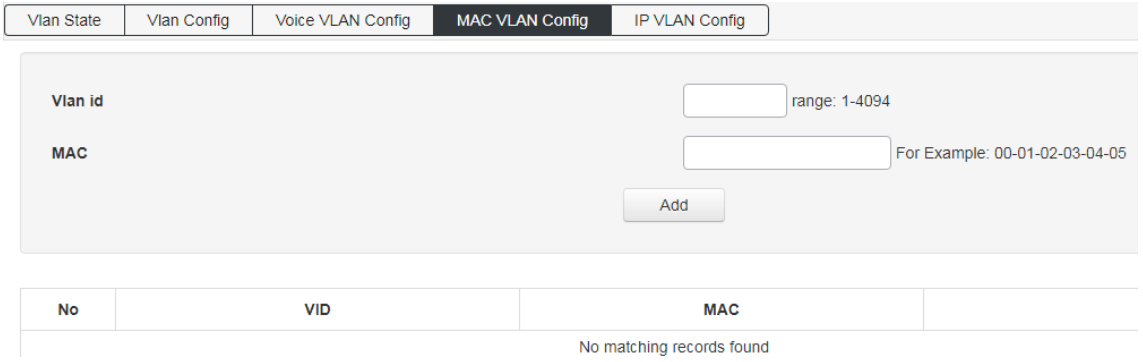
Port VLAN: Determine the VLAN ID (also known as PVID) of the port. The allowable VLAN range is 1 to 4095, and the default is 1.

Voice VLAN configuration's screen as blew:

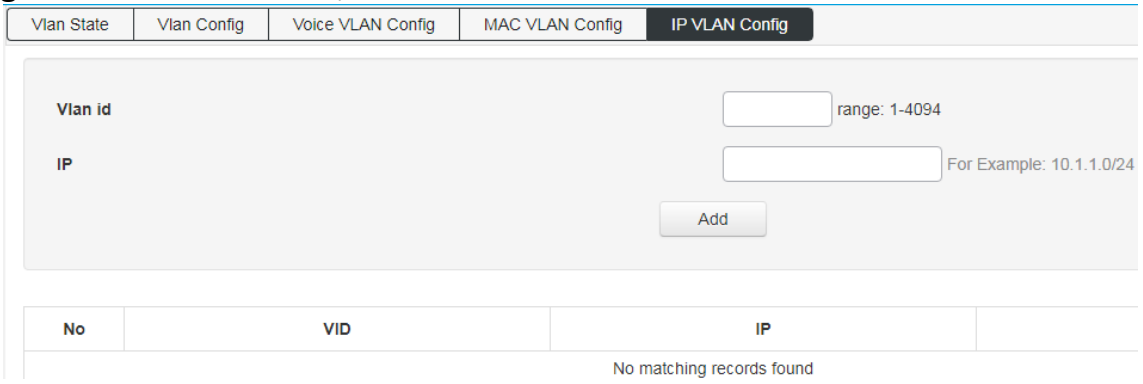


Enable Voice VLAN, the Access port will carry the IP voice traffic from the IP phone. When the switch is connected to Cisco IP phone (such as Cisco 7960 IP phone), the voice traffic sent by IP phone has three layers of IP priority and two layers of CoS value, which are set to 5 by default. For IEEE 802.1Q or IEEE 802.1p tagged traffic, the default cos value is untrusted.

Configure VLAN based on MAC address, screen as blew:



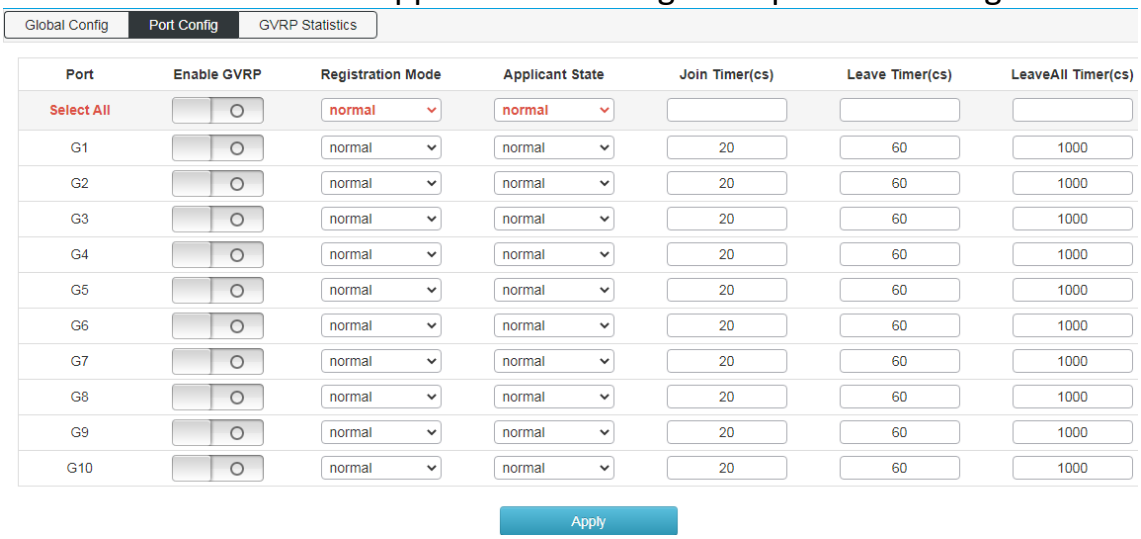
Configure VLAN based on IP, screen as blew:



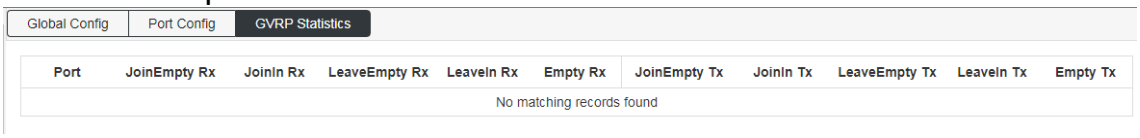
5.3 GVRP

Enable the GVRP function, screen as blew:

The enabled GVRP function is applied to the designated port and configure its timer.



Used to view the operation information of GVRP.



5.4 Link Aggregation

On this page, you can configure static aggregation groups, dynamic aggregation groups, and view link aggregation information;

Static aggregation configuration: click create static aggregation group TID value range is (1-4), that is, up to 4 static aggregation groups can be created.

Port Member: Port join aggregation must be the same speed and full duplex

This switch supports 32 groups of aggregation, each group supports up to 8 ports. To configure an aggregation group, just select the convergence port to the same line

group number, as shown in Figure 21: 1-2 ports converge in a group; 3-4 ports in a group. Please keep configuration consistency for the ports of aggregation group members, such as port rate mode, VLAN information, etc.

Link aggregation load balancing mode supports:

"Source MAC address" (load balancing calculation based on source MAC address of message)

"Destination MAC address" (load balancing calculation based on the destination MAC address of the message),”

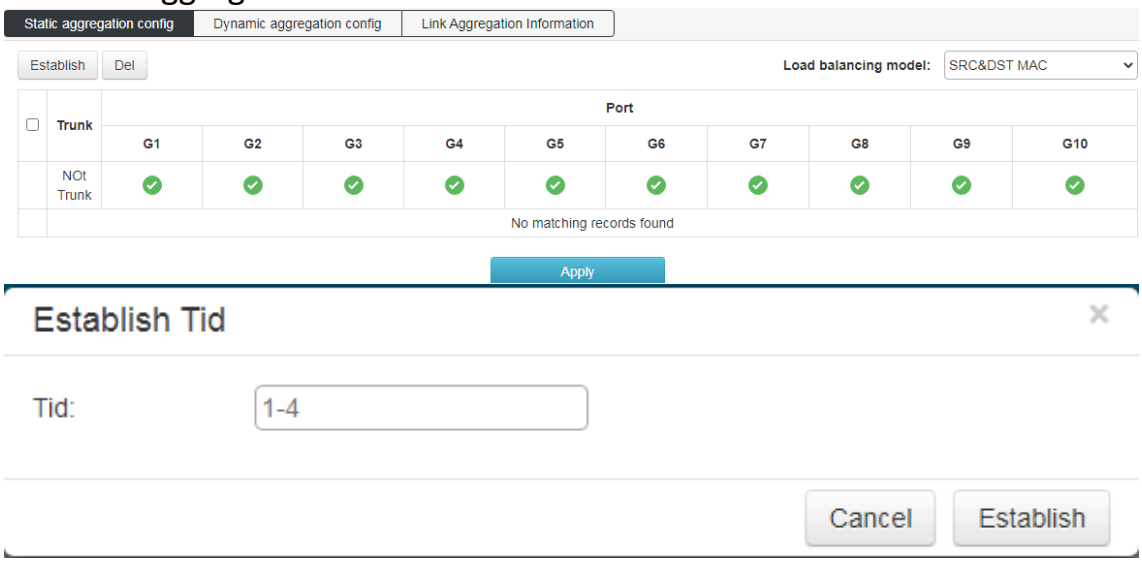
"IP address" (the source IP address and the destination IP address of the message are XOR, and then the load balancing calculation is performed)

"TCP / UDP port number" (load balancing calculation is based on the TCP / UDP port number of the message).

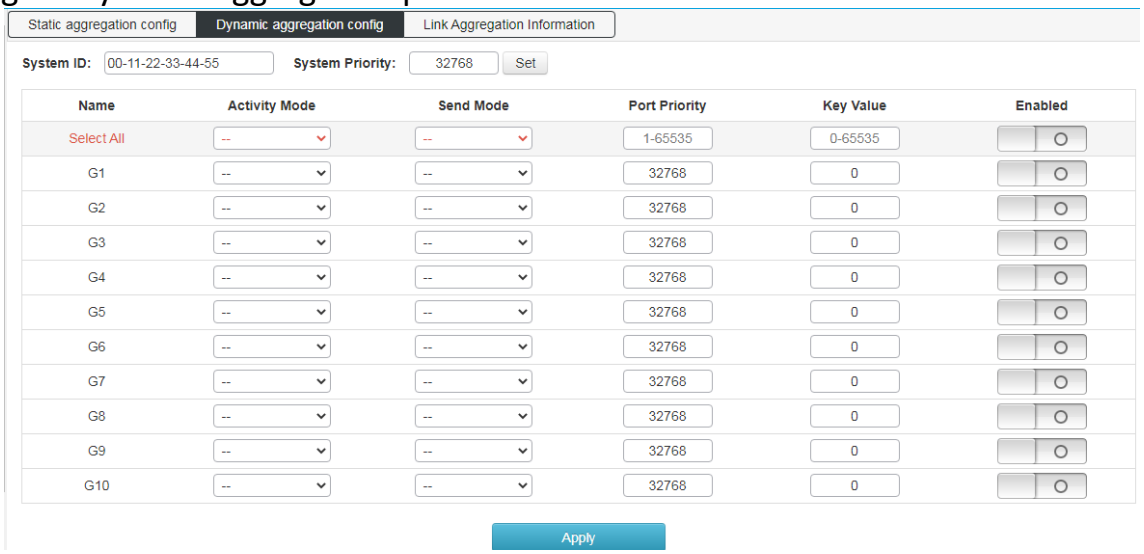
Four modes can be selected and combined. The assignment of equalization algorithm is global.

If LACP dynamic aggregation protocol is enabled on some ports, static aggregation cannot be configured manually.

Note:
Static aggregation on the same port cannot be configured simultaneously with dynamic LACP aggregation.



Configure dynamic aggregation port as blew:

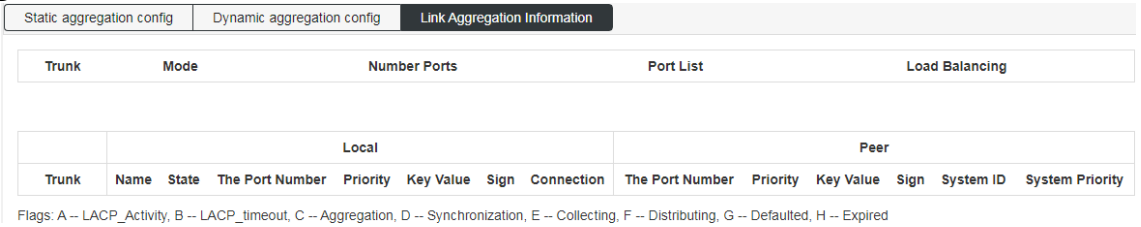


Link aggregation information: view switch aggregation port information.

The switch supports port dynamic aggregation. After enable the dynamic protocol of the port, the devices on both sides of the convergence exchange information through the protocol. According to the parameters and status of both sides, the matching links are automatically gathered together to send and receive data. After the convergence is formed, the switching equipment maintains the convergence link state, and automatically adjusts or disbands the aggregation link when the configuration of both sides changes.

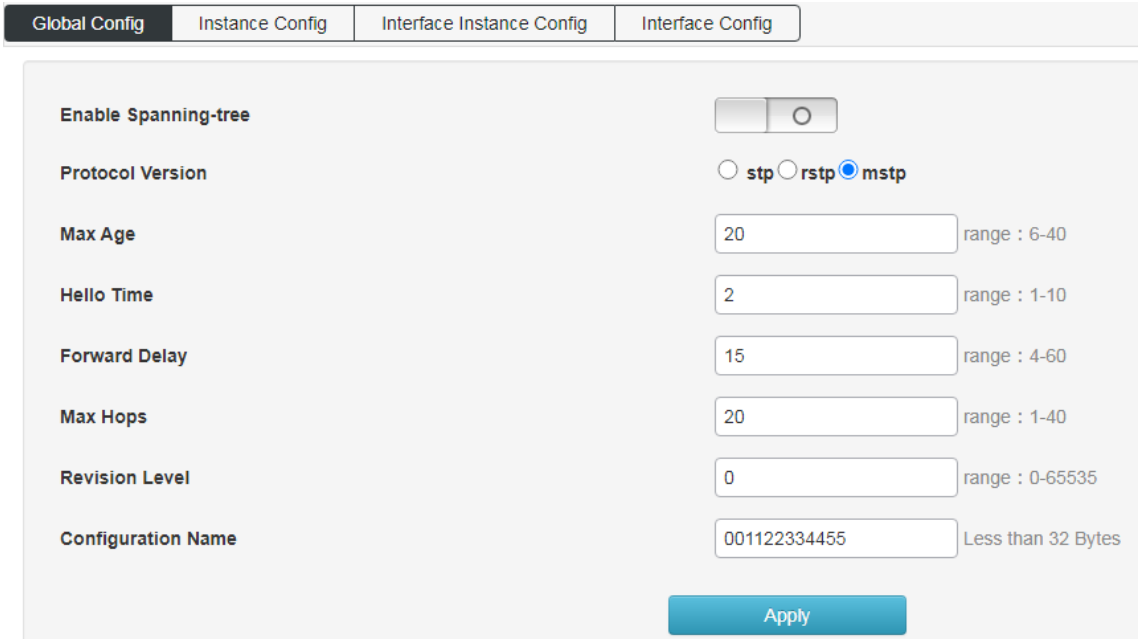
The configuration parameters of dynamic protocol include protocol switch state, key negotiation and active / passive mode selection. Only when the dynamic protocol is turned on can the dynamic negotiation be carried out, which may lead to the formation of aggregation links. The key is the basis of negotiation. Only the 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 aggregation negotiation; when "passive" is selected, the device will passively accept the aggregation negotiation initiated by other devices. If some ports have been converged statically, the dynamic convergence of LACP cannot be realized.

Note: dynamic LACP aggregation and static convergence on the same port cannot be configured at the same time



5.5 MSTP Configuration

Global configuration: select the spanning tree protocol version (STP / RSTP / MSTP is optional), MSTP protocol is selected by default.



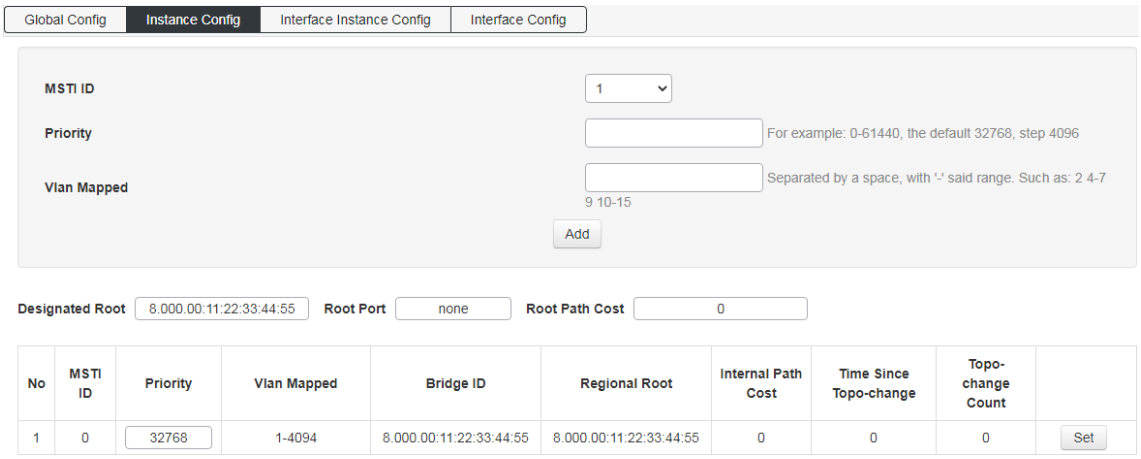
An example of configuring MSTP:

Set the mapping VLAN of multi spanning tree.

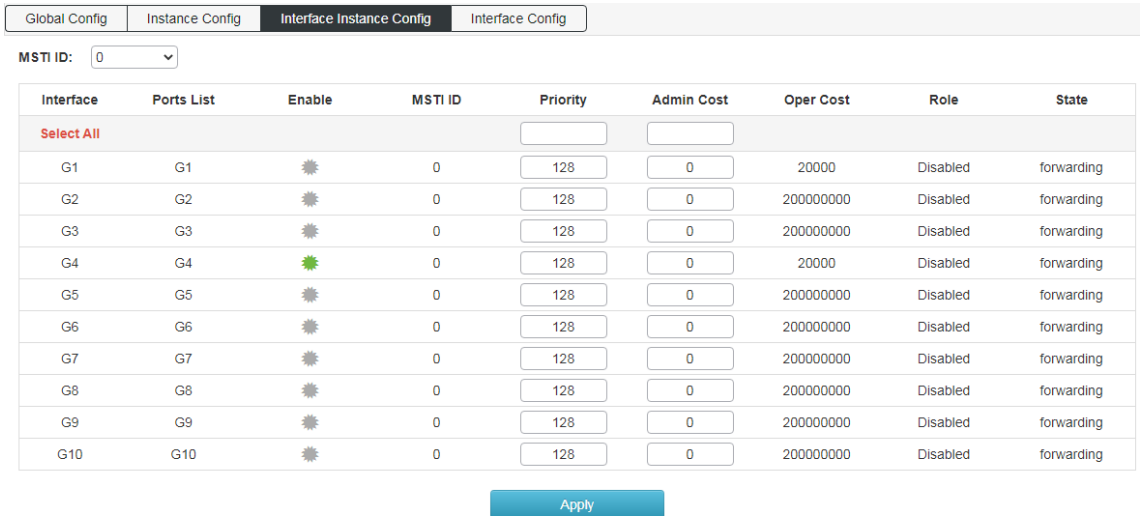
Configuration name: identifies the name of the VLAN to MSTI mapping, the bridge must share the name and revision (see below), and the VLAN-to-MSTI mapping configuration in order to share the MSTI spanning tree. (Within region) the name is up to 32 characters.

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

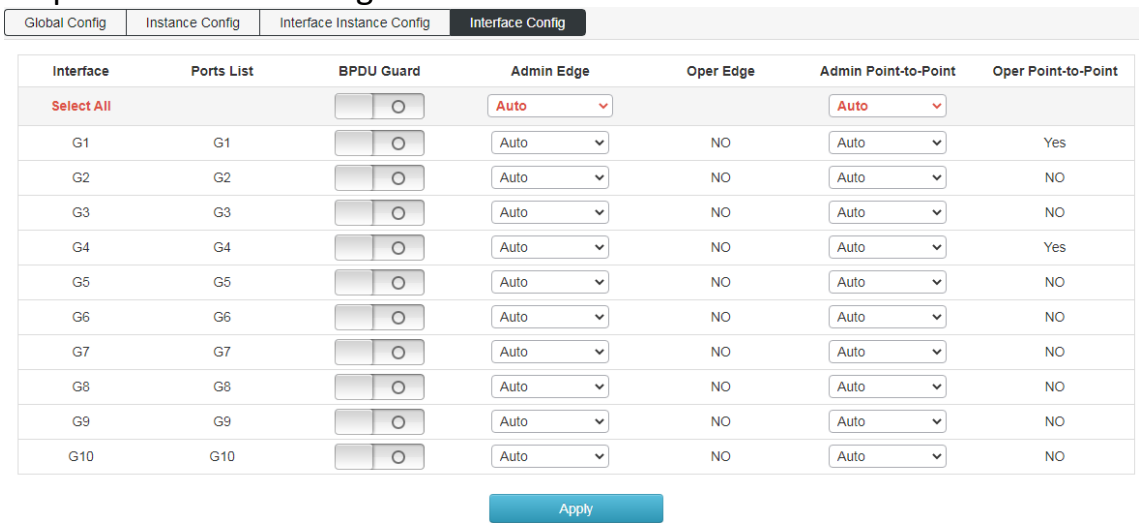
Mapped VLANs: a list of VLANs mapped to MSTI. VLANs must be separated by commas and / or spaces. VLAN can only be mapped to one MSTI. An unused MSTI should remain empty. (That is, no VLAN is mapped to it).



Interface instance configuration: configure the enable of the instance on the port.
Screen as blew:

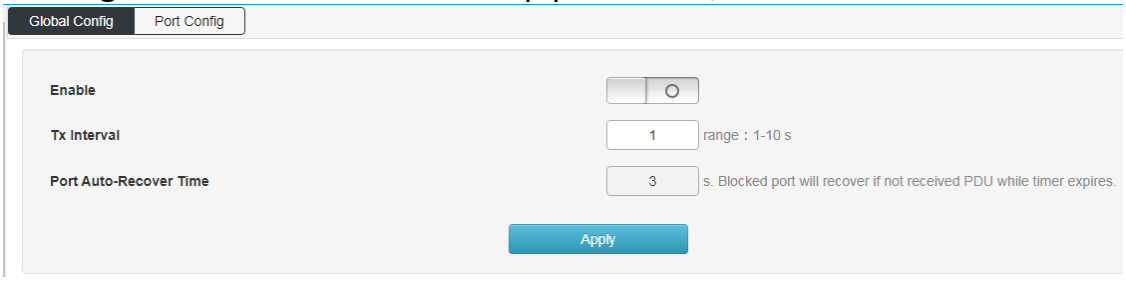


Interface configuration: configure the enabled port of spanning tree protocol and the enabled port of BPDU message. Screen as blew:



5.6 Loop Protection

Global Configuration: enable and set loop protection, screen as blew:

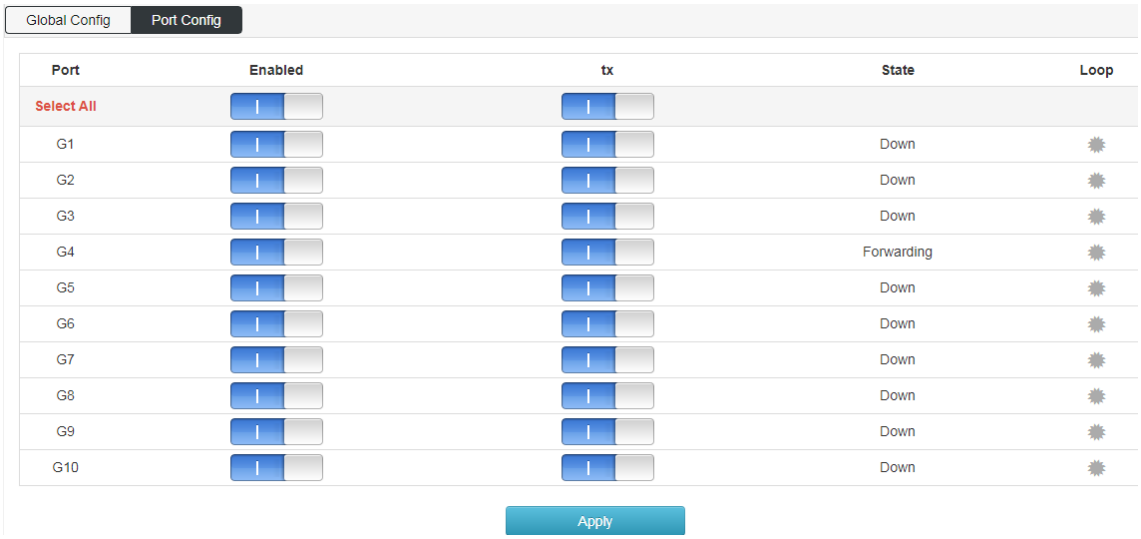


Port Configuration: enable the loop protection function on the port.
The loop protection includes double fiber ring protection and four fiber ring protection.

The unidirectional ring is usually composed of two optical fibers, one of which is the working fiber, represented by S; the other is the protective fiber, represented by P. Protection switching is accomplished by a reverse switch.

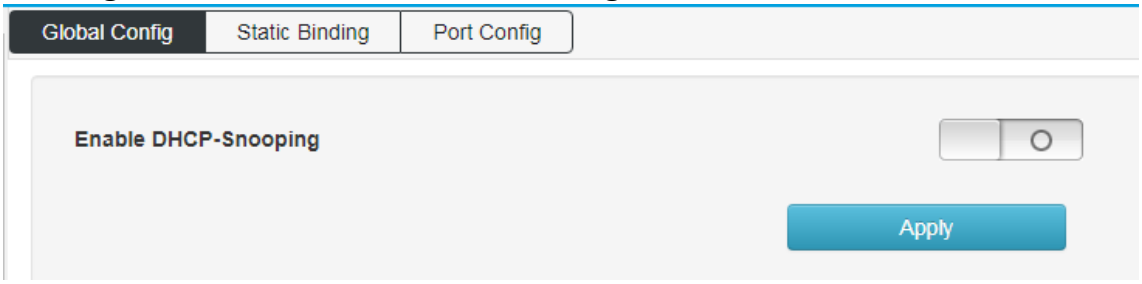
In addition to the unidirectional switching ring, there are also bidirectional multiplexer switching double fiber ring and bidirectional multiplexing segment switching four fiber ring. But the analysis shows that the unidirectional path switching double fiber ring is the best considering the node cost, system complexity and product compatibility.

The working mode is divided into recovery mode and non-recovery mode. In the recovery mode, when the working section has recovered from the failure state, the working path automatically switches back to the working section. In the non-recovery mode, even if the working section has been restored to normal, the working path is still unchanged in the protection section. Generally, 1 + 1 protection can work in both recovery mode and non-recovery mode, while 1: N protection can only work in recovery mode.

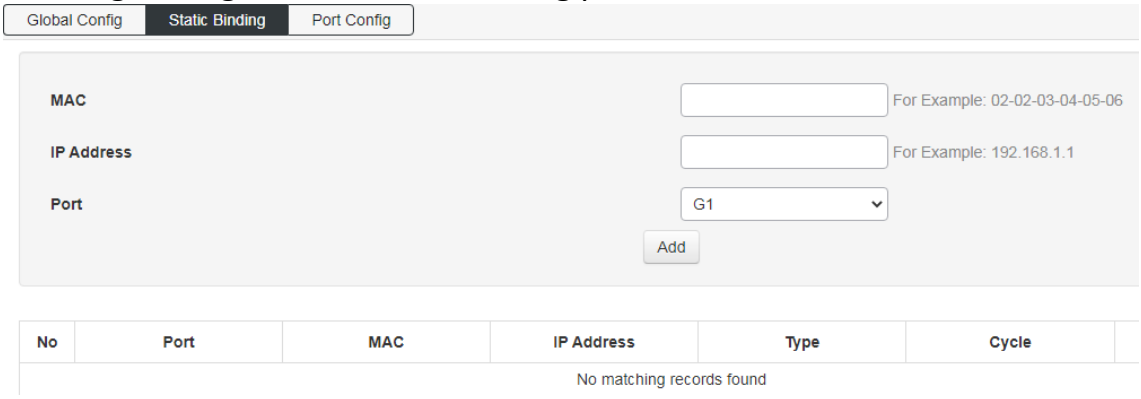


5.7 DHCP-snooping

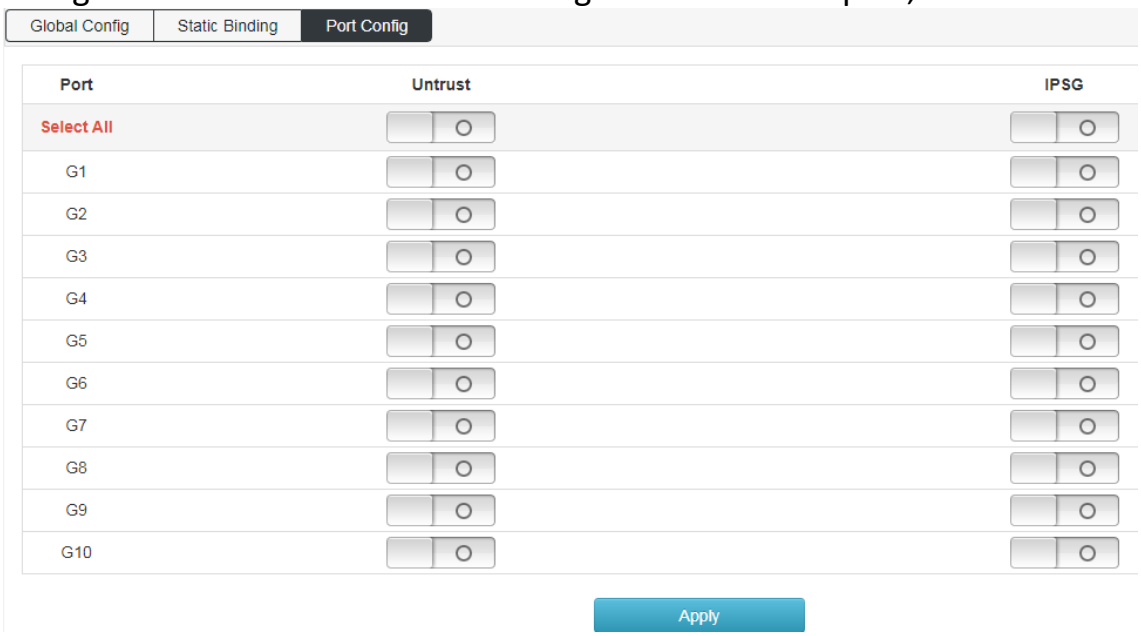
Global configuration: enable DHCP monitoring function, screen as blew:



Static Binding: configure the static listening port, screen as blew:

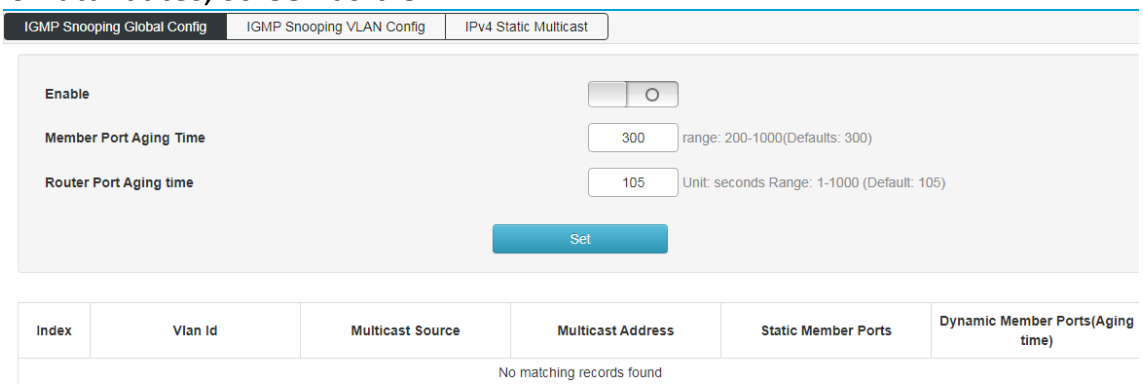


Port Configuration: enable DHCP monitoring function on the port, screen as blew:

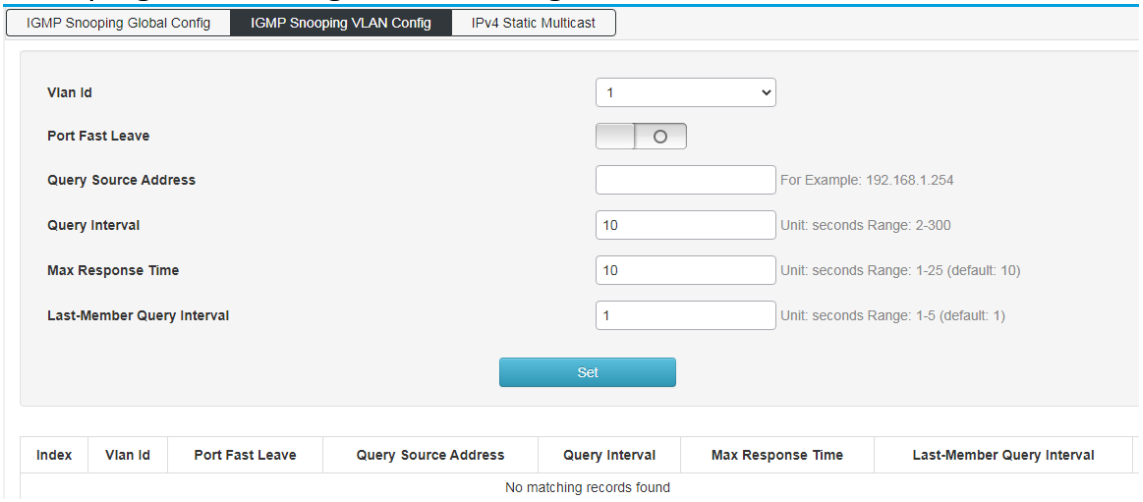


5.8 IGMP Snooping

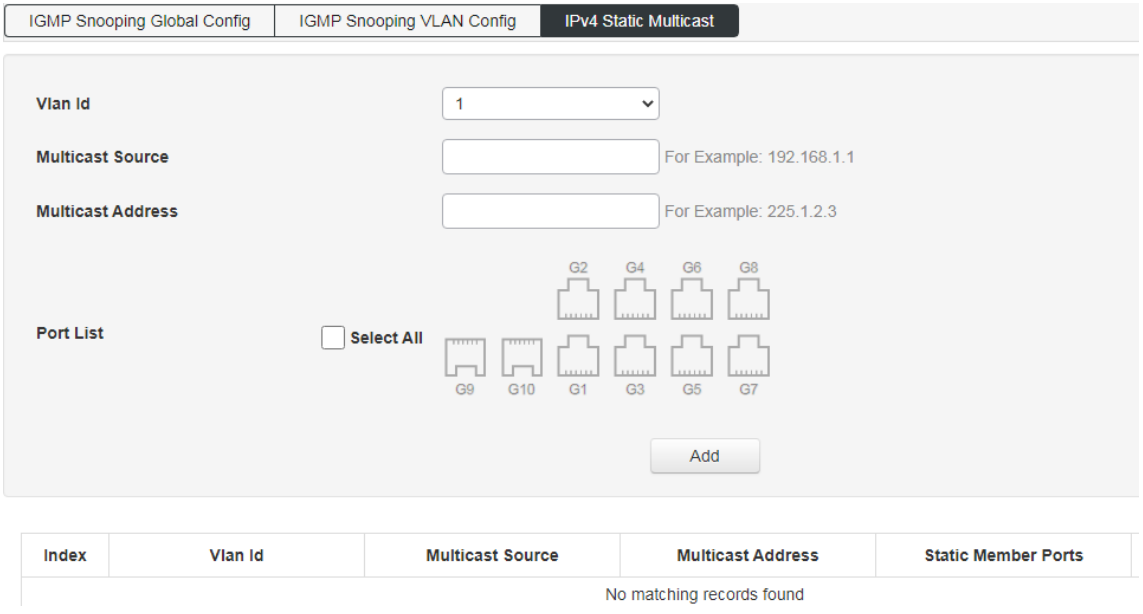
IGMP snooping global configuration: configure IGMP monitoring enable and IGMP function attributes, screen as blew:



IGMP snooping VLAN configuration: configure static multicast VLAN, screen as blew:



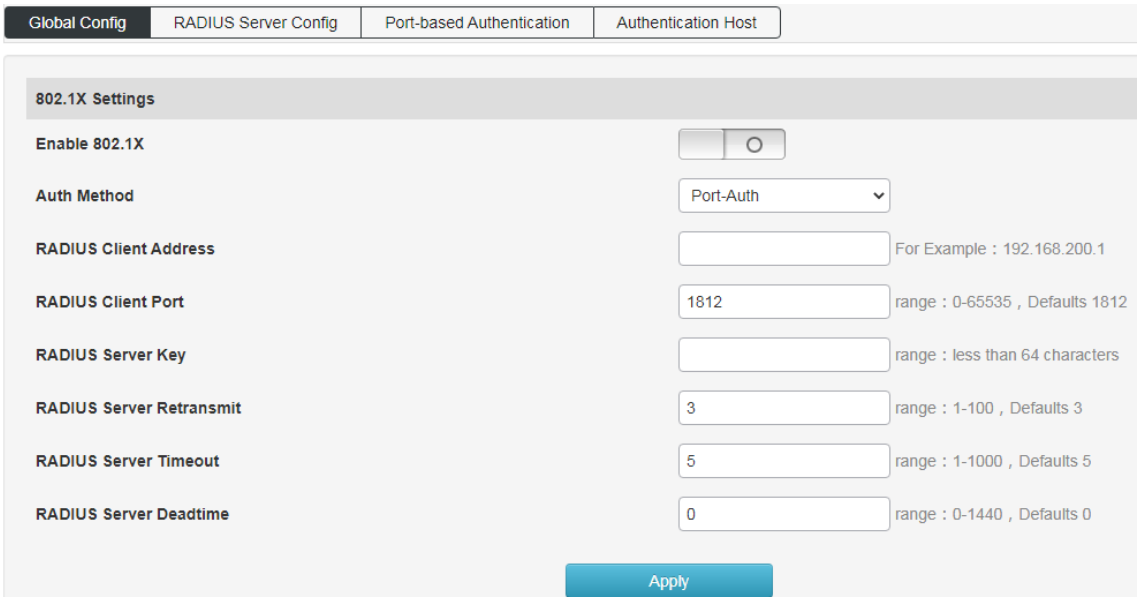
IPv4 Static Multicast: configure static multicast function and enable port static multicast function, screen as blew:



5.8 802.1x authentication

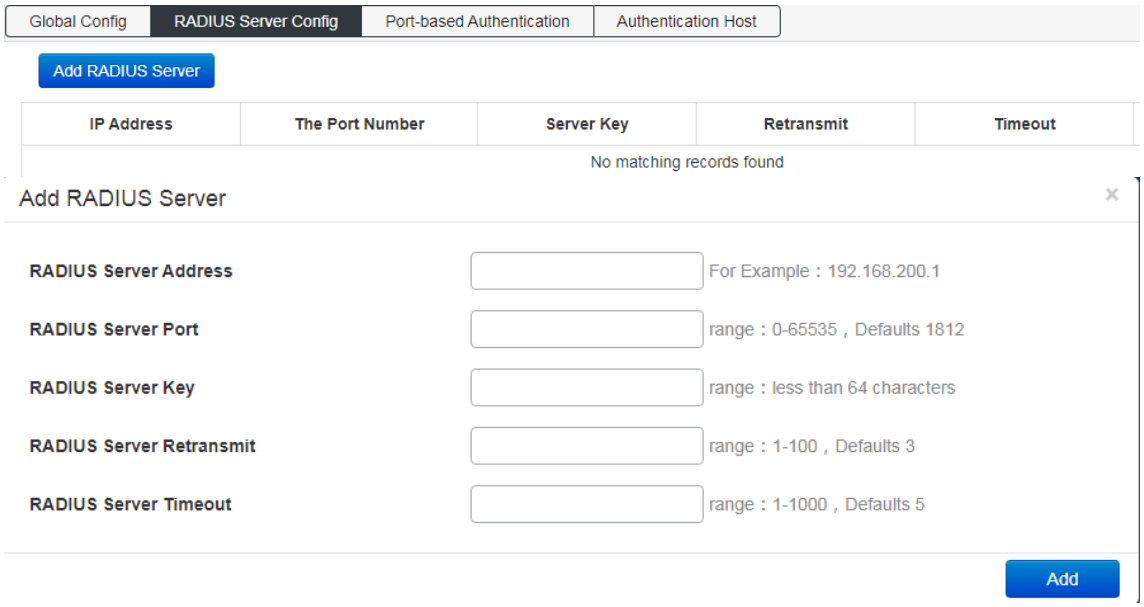
Global configuration: enable 802.1x authentication function.
Radius client address: configure radius authentication client address.
Radius server shared secret key: a secret of up to 29 characters is shared between the server and the switch.

Radius server timeout: (can be set to a number between 3 and 3600 seconds) It is the maximum time to wait for a response from the server. If the server does not respond within this time frame, we will consider it dead and continue to use the next enabled server (if any); the RADIUS server uses the UDP protocol, which is not reliable by design. In order to deal with the lost frames, the super interval is divided into three sub intervals, each of which has the same length. If no response is received within the subinterval, the request is transmitted again. This algorithm will cause radius server to be queried up to three times before it is considered as dead server.

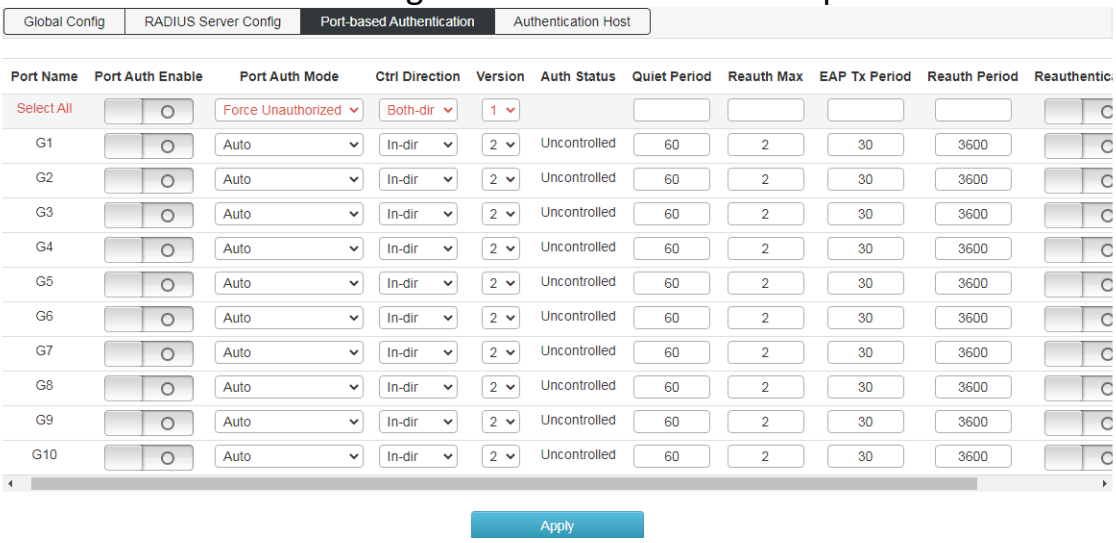


Radius server settings: set radius server attributes.
Radius server address: configure the radius server address.
Radius server port number: configure the radius server port number.
Radius server shared password: a secret of up to 29 characters is shared between the server and the switch.
Radius server retransmission times: configure the radius service death retransmission times.
Radius server timeout: (can be set to a number between 3 and 3600 seconds) is the maximum time to wait for a response from the server. If the server does not respond within this time frame, we will consider it dead and continue to use the next enabled server (if any). The RADIUS server uses the UDP protocol, which is not reliable by

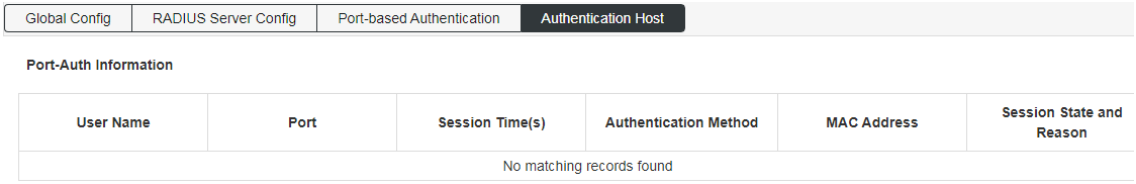
design. In order to deal with the lost frames, the super interval is divided into three sub intervals, each of which has the same length. If no response is received within the subinterval, the request is transmitted again. The server will be considered dead before the server is killed at most 3 times.



Port-based Authentication: Configure 802.1x authentication port.



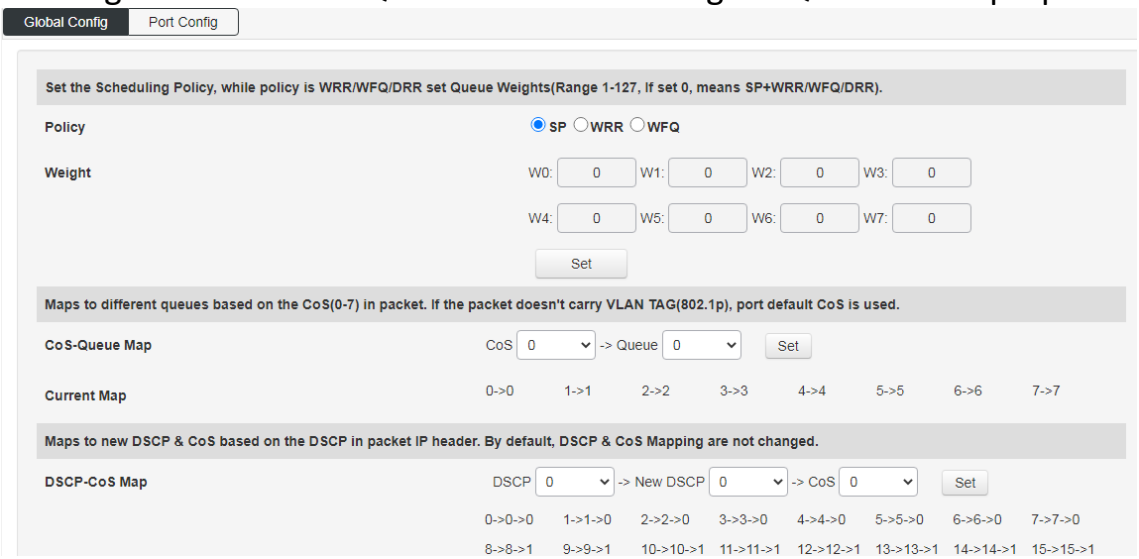
Authentication Host: View 802.1x authentication host properties.



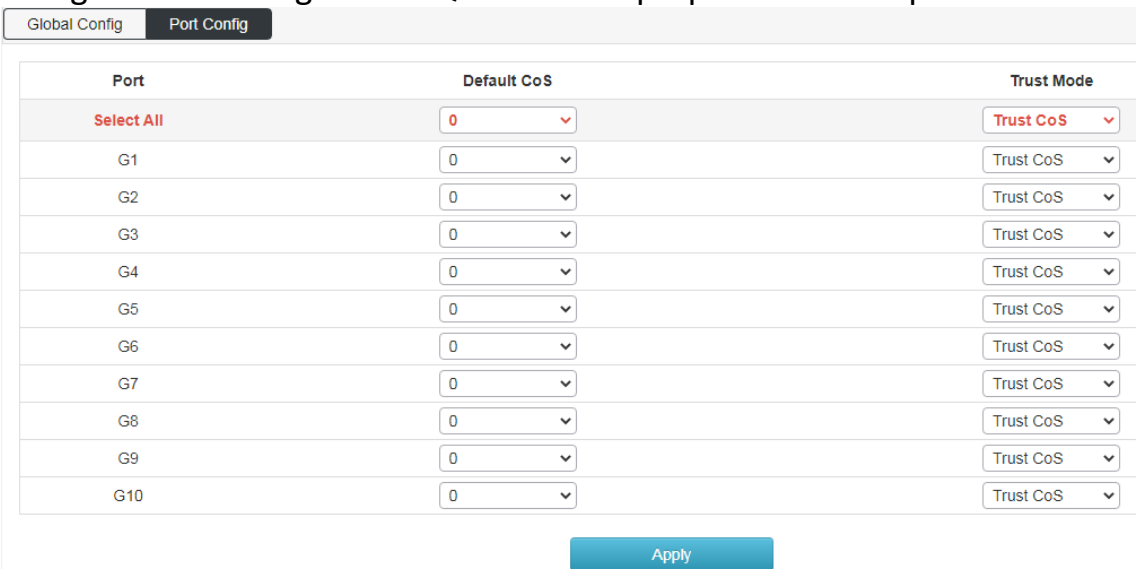
6. Senior Management

6.1 QOS Configuration

Global Configuration: Enable QoS function and configure QoS function properties.

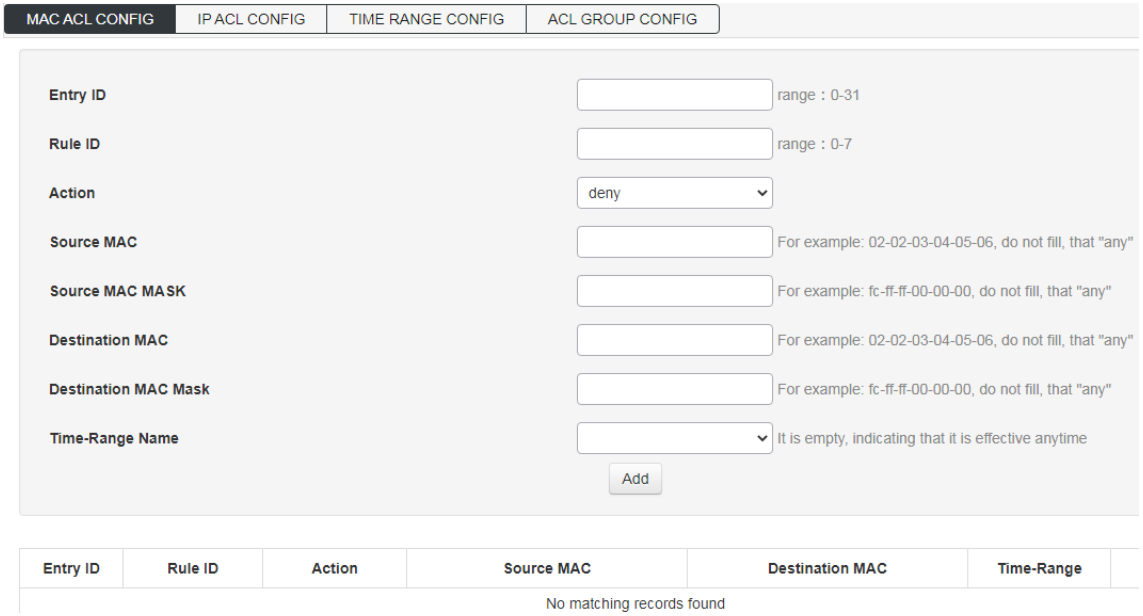


Port Configuration: Configure the QoS function properties on the port.

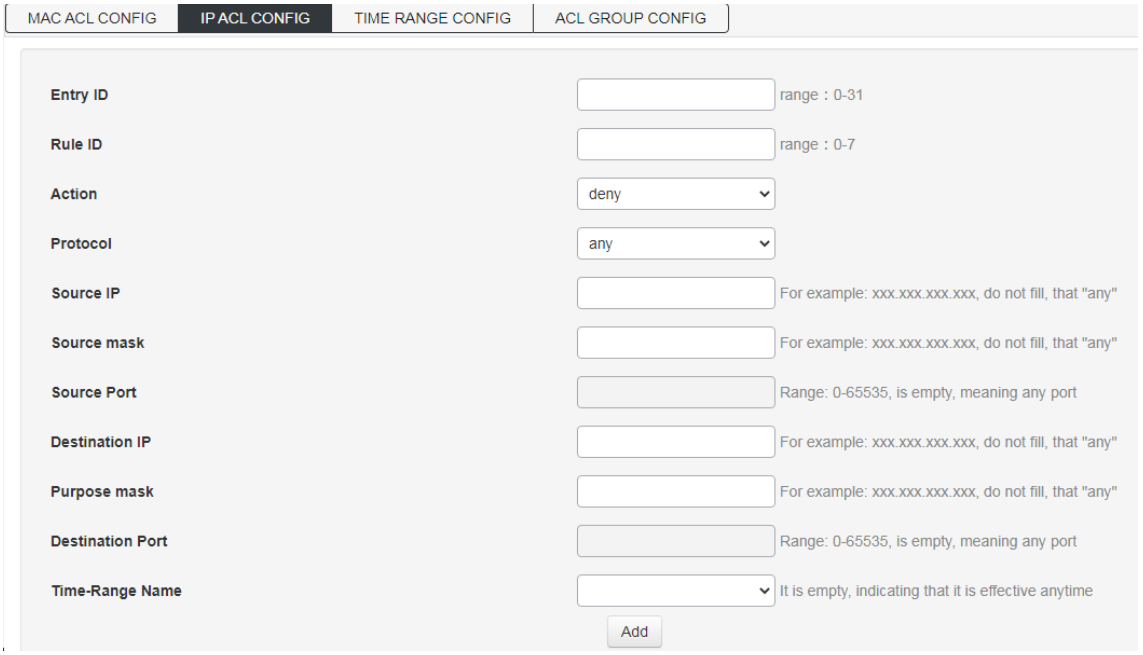


6.2 ACL Configuration

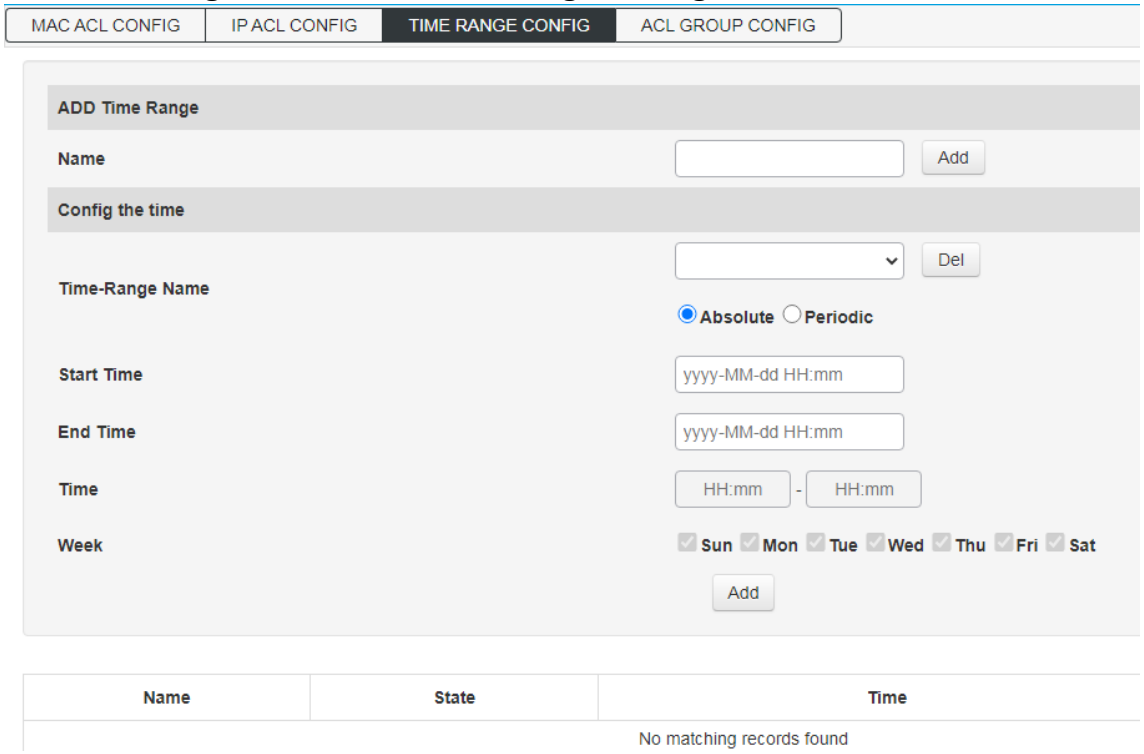
MAC ACL configuration： Configure MAC based ACL access list.



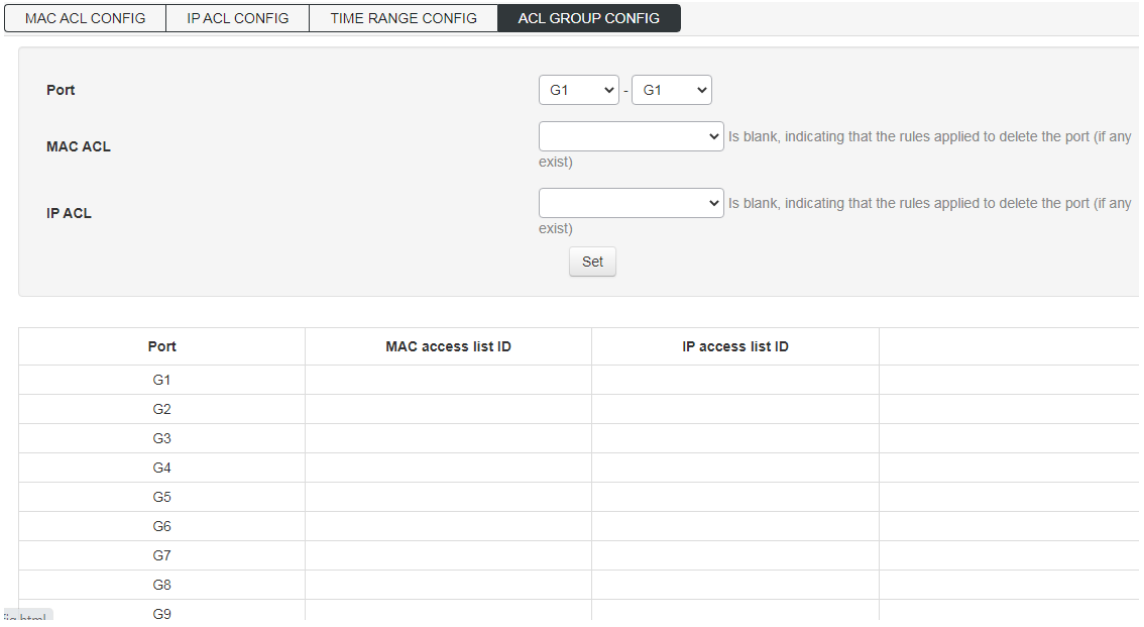
IP ACL Configuration： Configure IP based ACL access control list.



TIME RANGE Configuration： ACL time range setting.

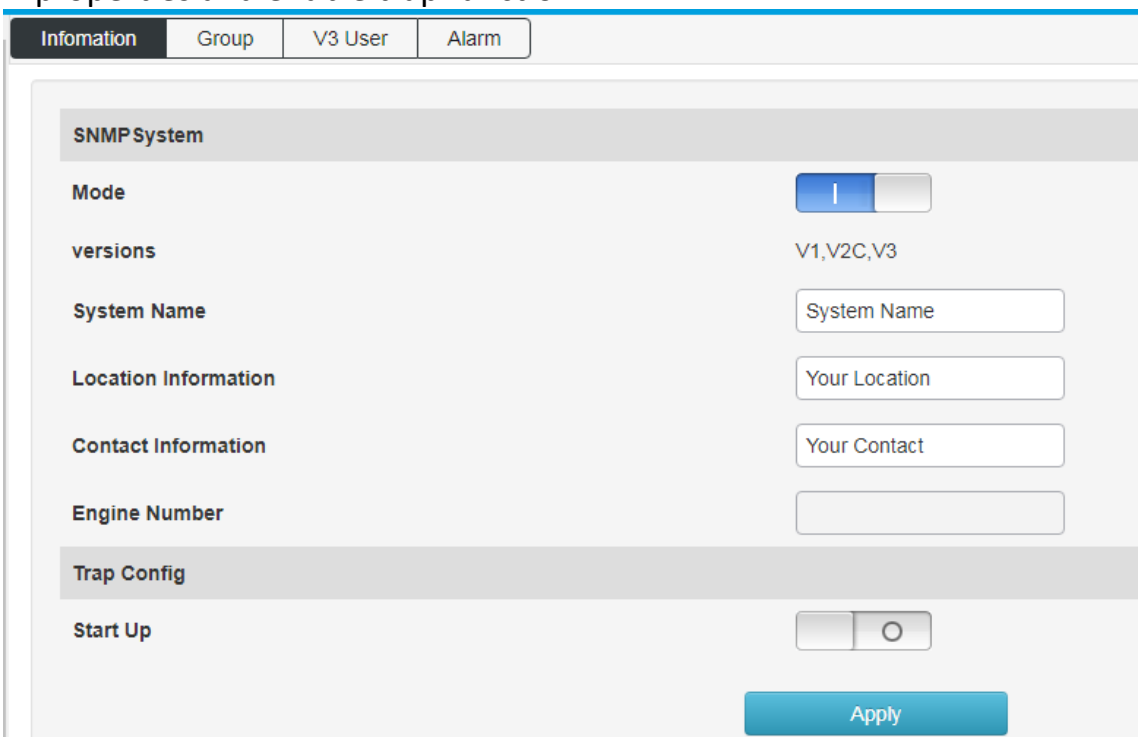


ACL GROUP Configuration： Configure ACL access control list port group.

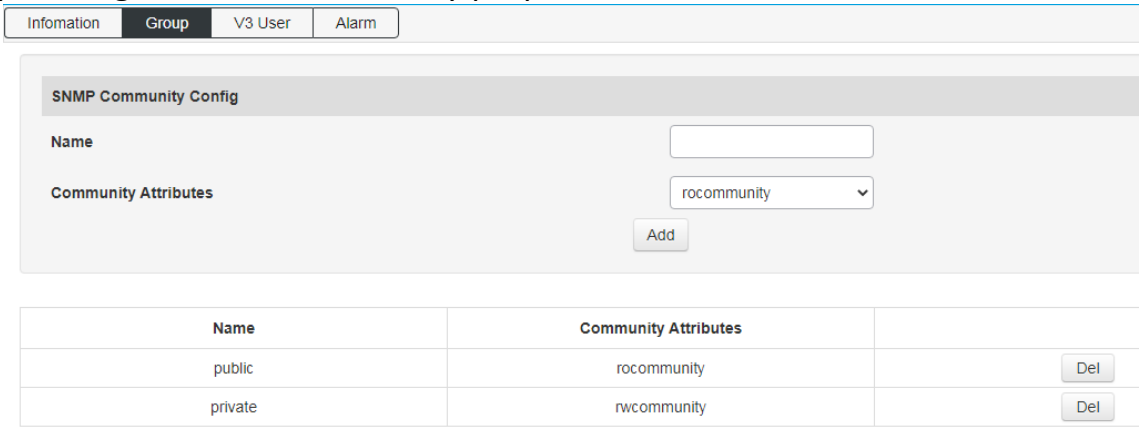


6.3 SNMP Configuration

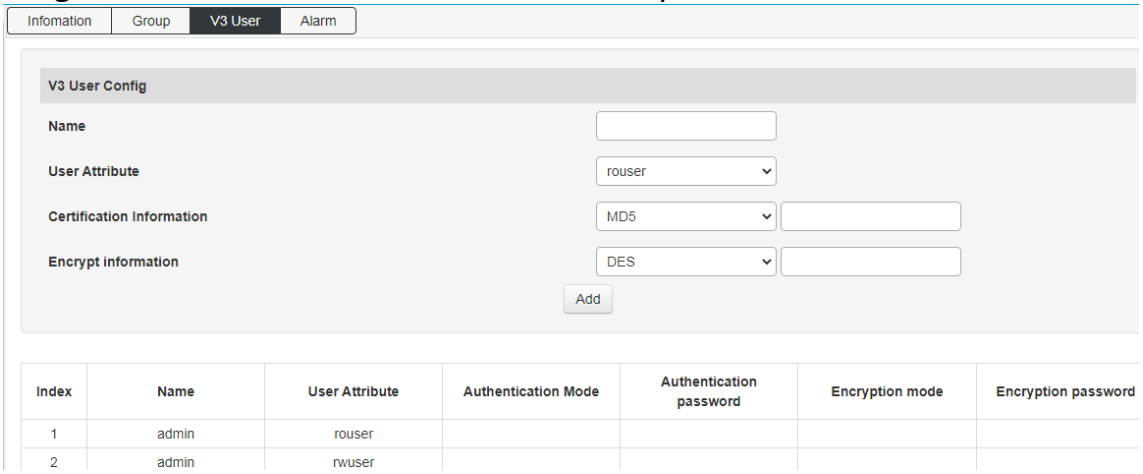
System Information： Enable all SNMP protocol versions, configure SNMP protocol system properties and enable trap function.



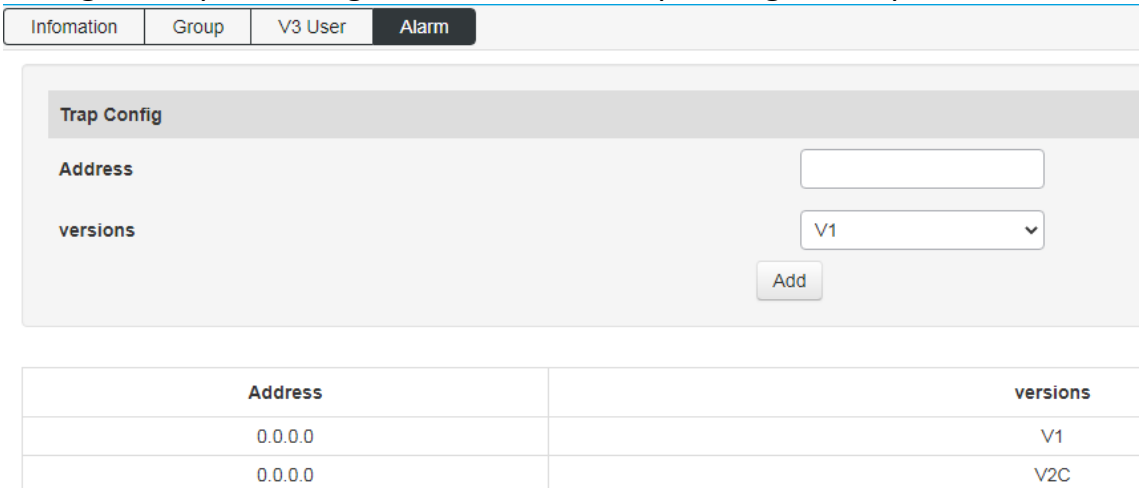
Group: Configure SNMP community properties.



V3: configure the member attribute of SNMP V3 protocol version.

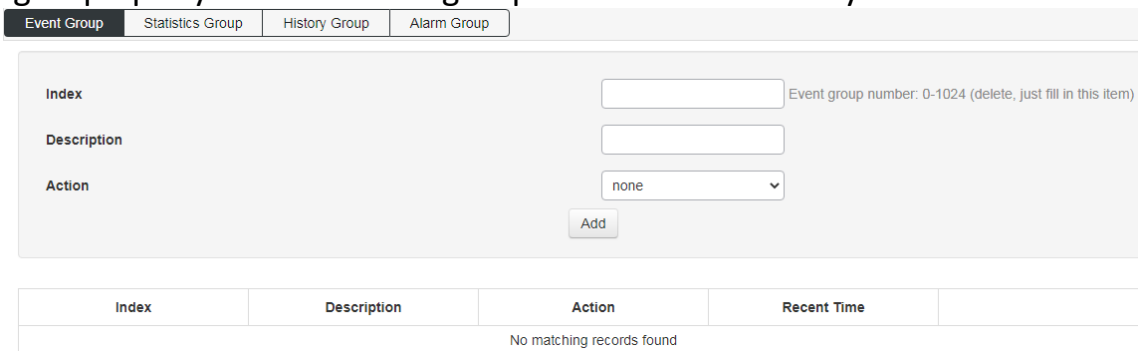


Trap: configure trap receiving address and corresponding SNMP protocol version.

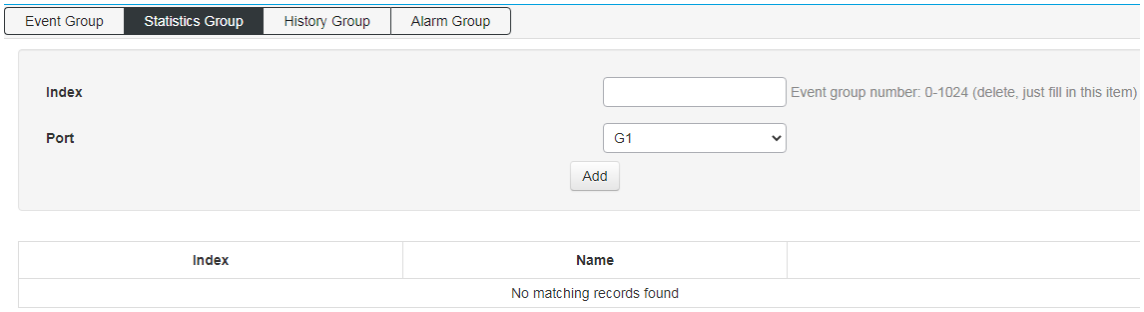


6.4 RMON

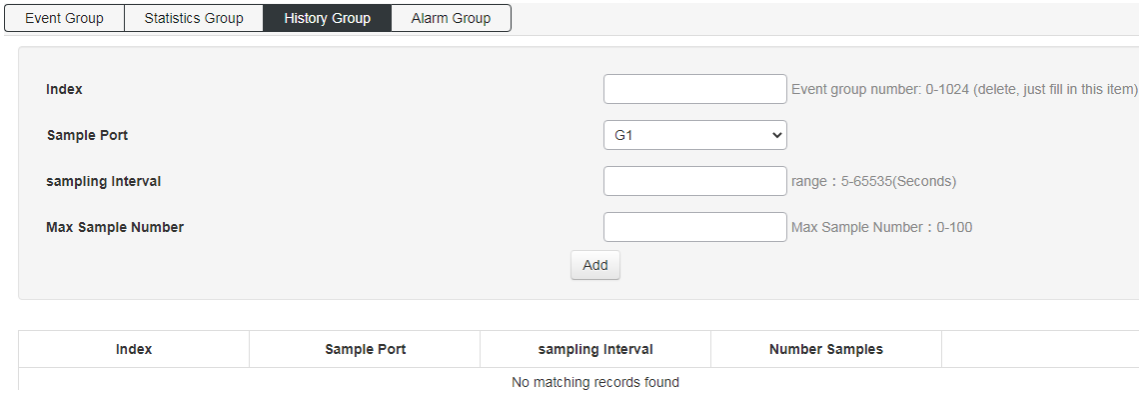
Event group: query and add event groups monitored remotely.



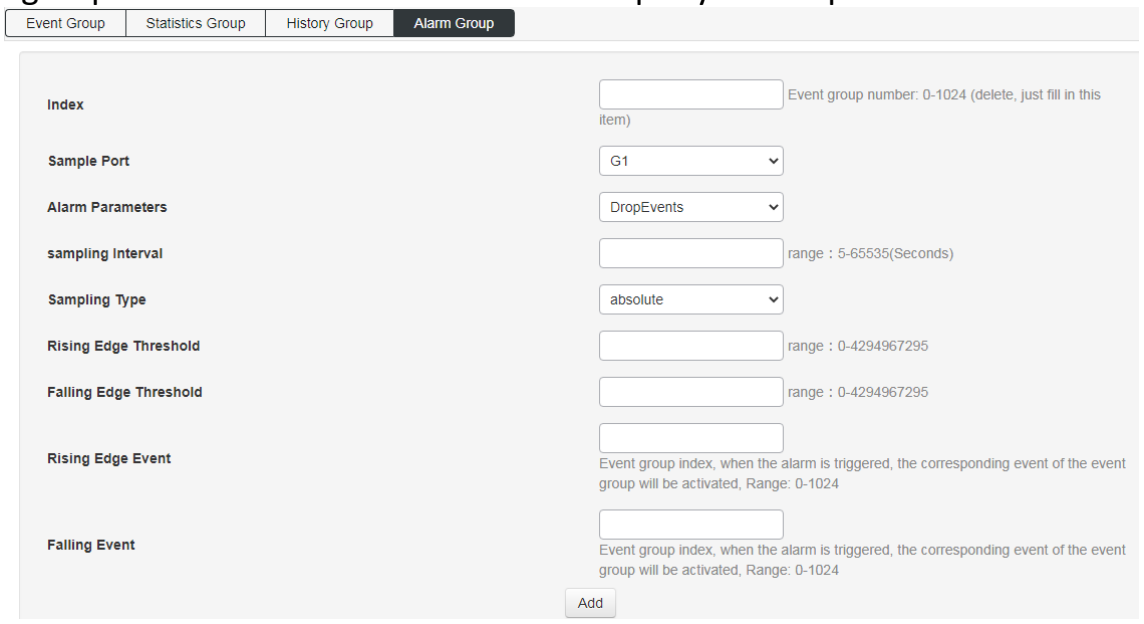
Statistics group: query the statistical information of specific events after the event is broken.



History group: add and query the history of a specific event at the port.

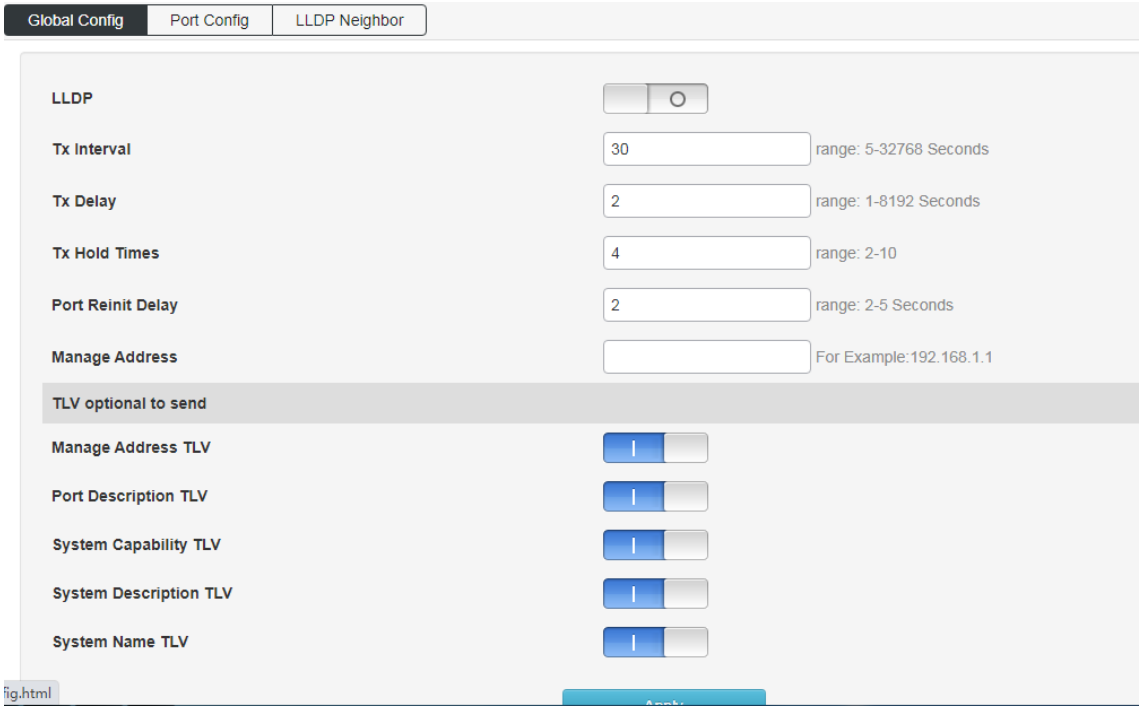


Alarm group: add the attribute of alarm event query on the port.

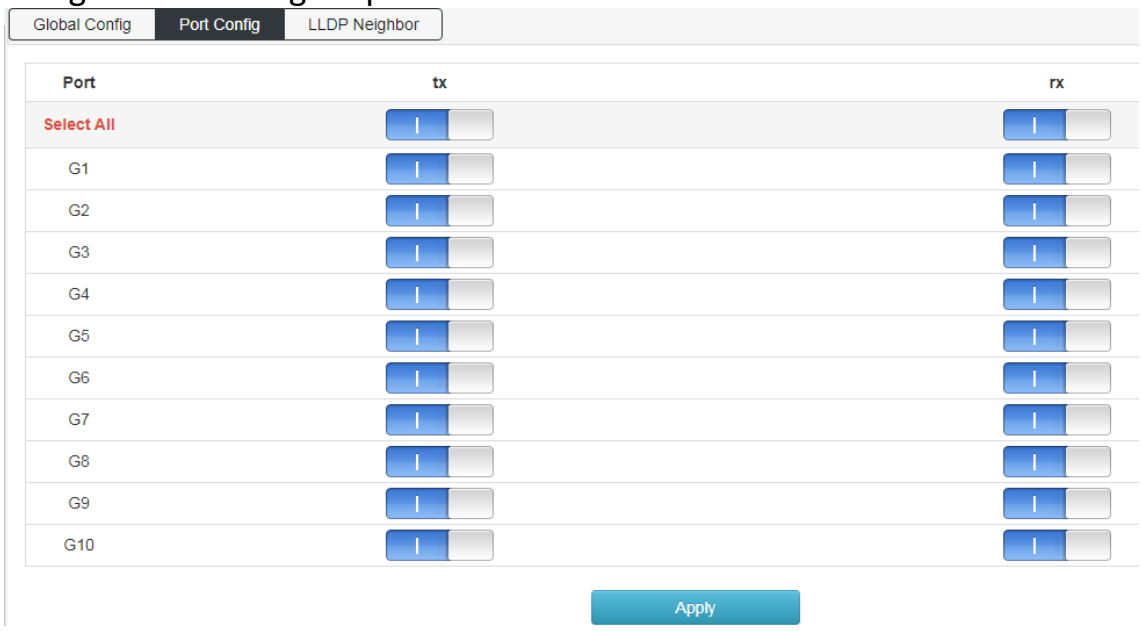


6.5 LLDP Configuration

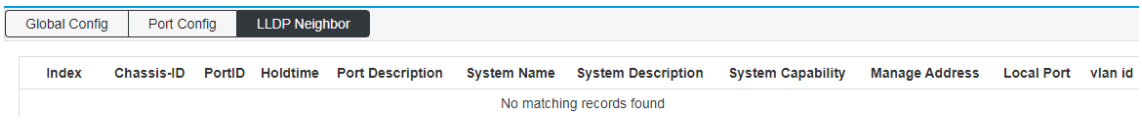
Global configuration: turn on and configure LLDP function attributes.



Port configuration: configure port LLDP function attributes.

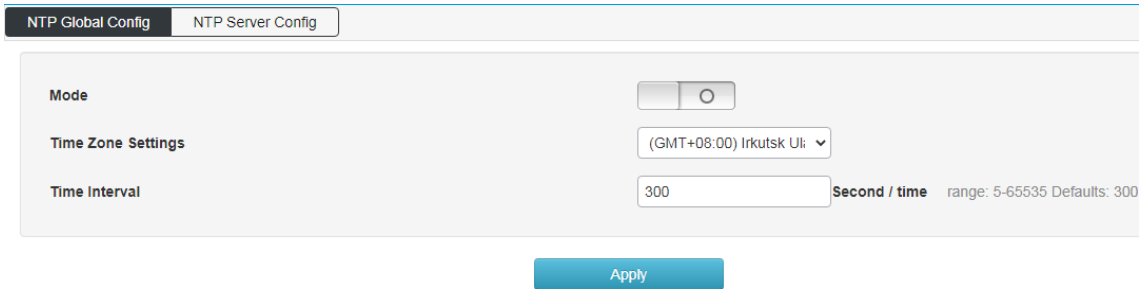


LLDP 邻居：查询 LLDP 邻居信息；

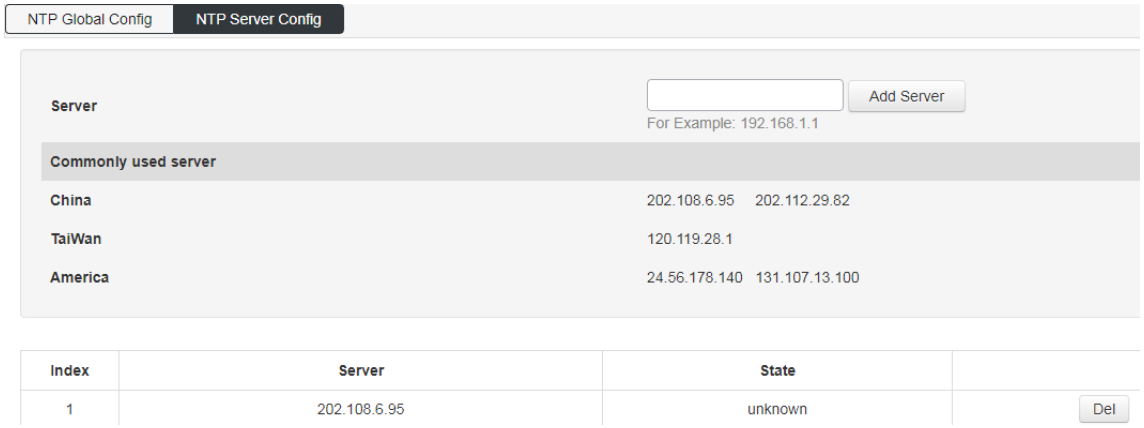


6.6 NTP Configuration

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

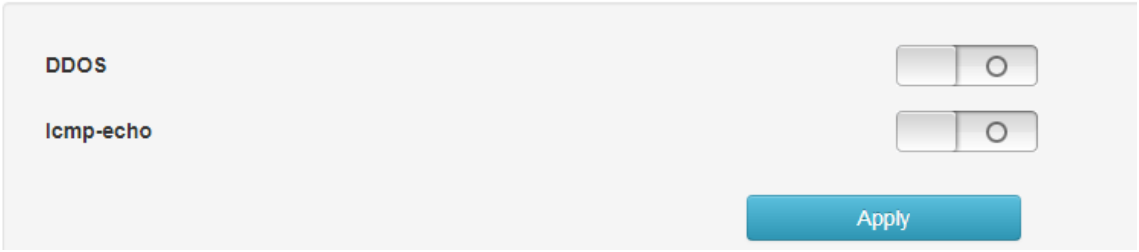


NTP server configuration: configure the NTP server address and view the NTP server status.



6.7 Anti Attack

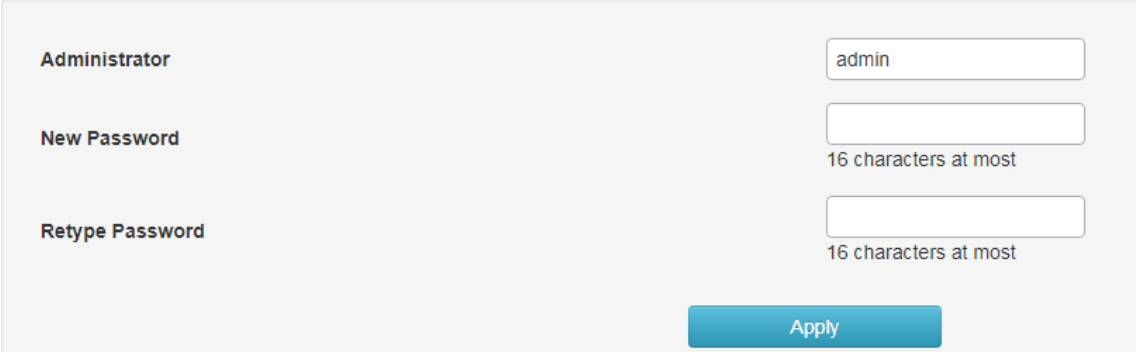
It can open DDoS and ICMP echo;



7. System Management

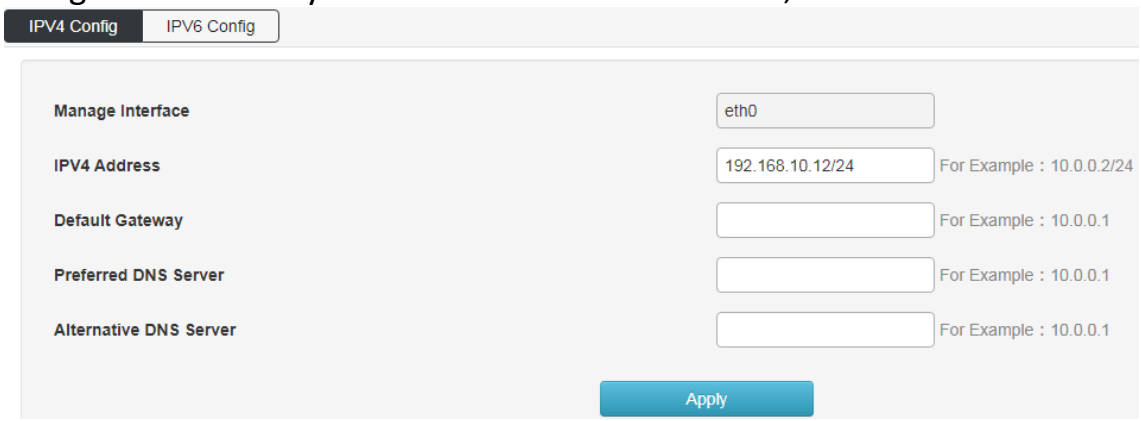
7.1 User Settings

Modify the user login password, the account name cannot be changed or added users.

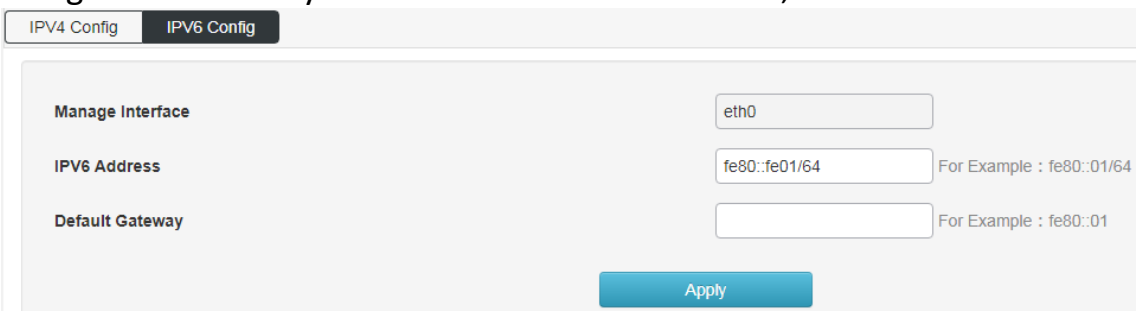


7.2 Network Settings

IPv4 configuration: modify the IPv4 address of the switch, cannot add IP address.

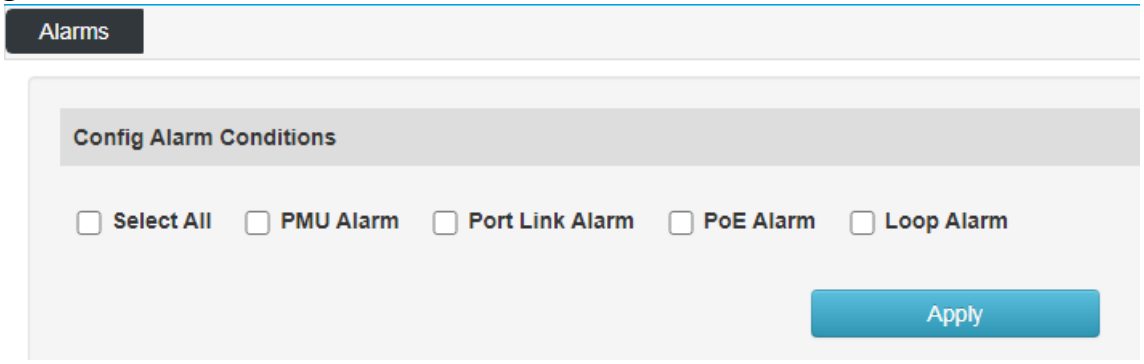


IPv6 configuration: modify the IPv6 address of the switch, cannot add IP address.



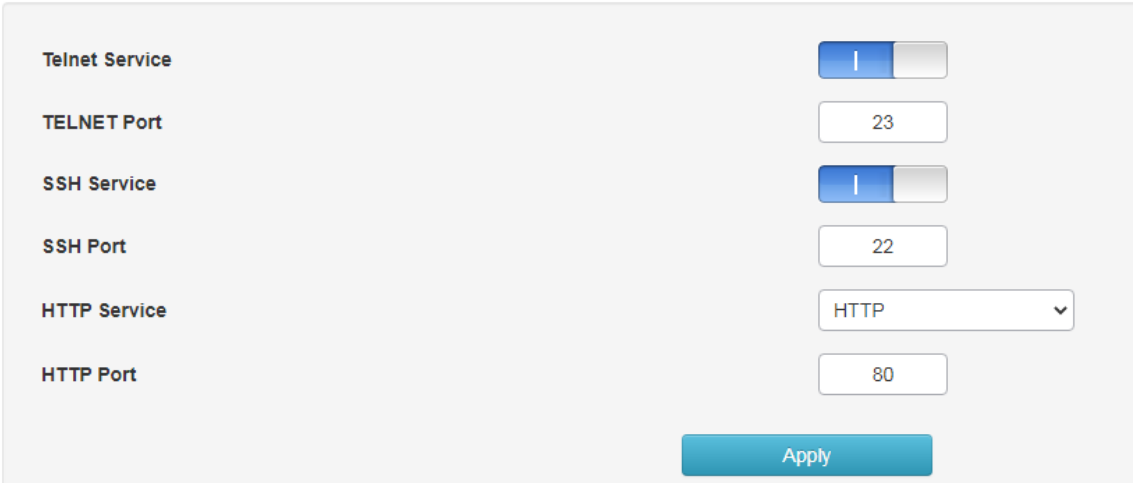
7.3 Alarm Configuration

Configure switch alarm function to enable.



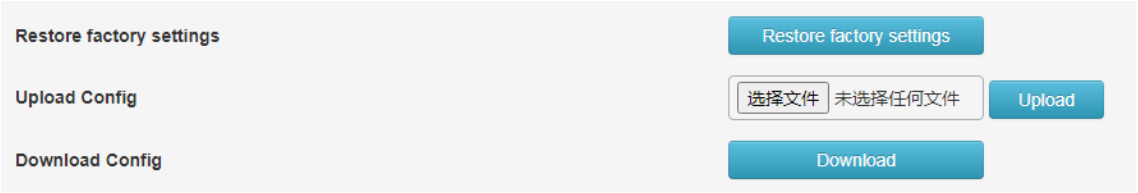
7.4 Service Configuration

Configure switch Telnet, SSH, HTTP version protocol and service port.



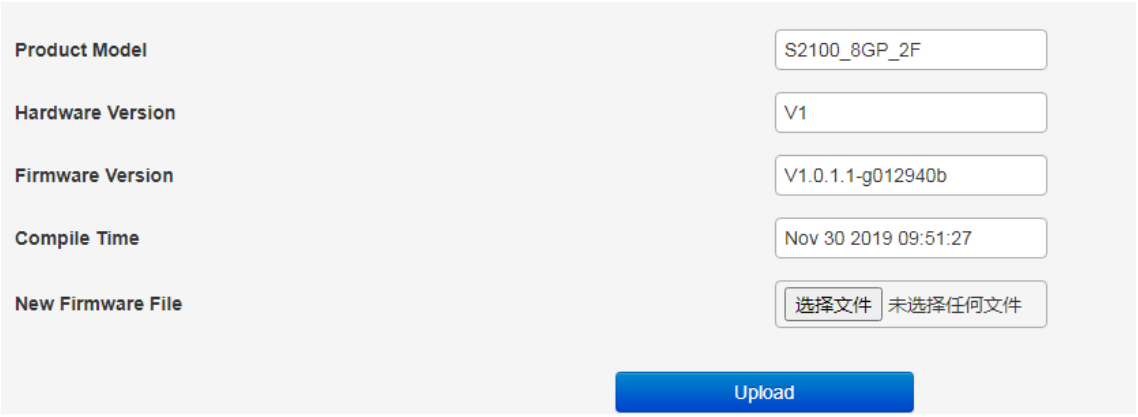
7.5 Configuration Management

For reset, upload and download switch configuration.



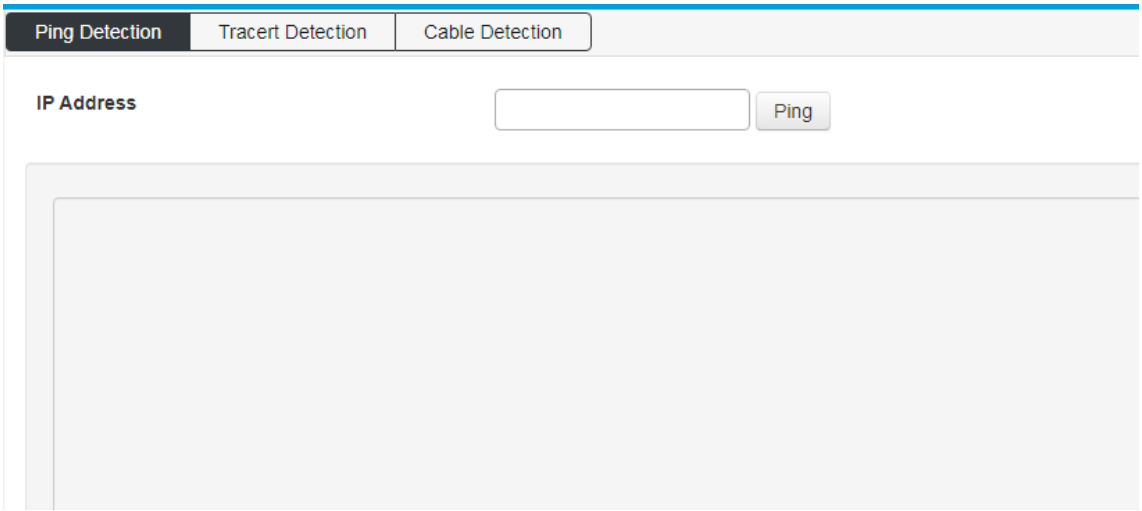
7.6 Firmware Update

It is used to upgrade the software version of the switch.

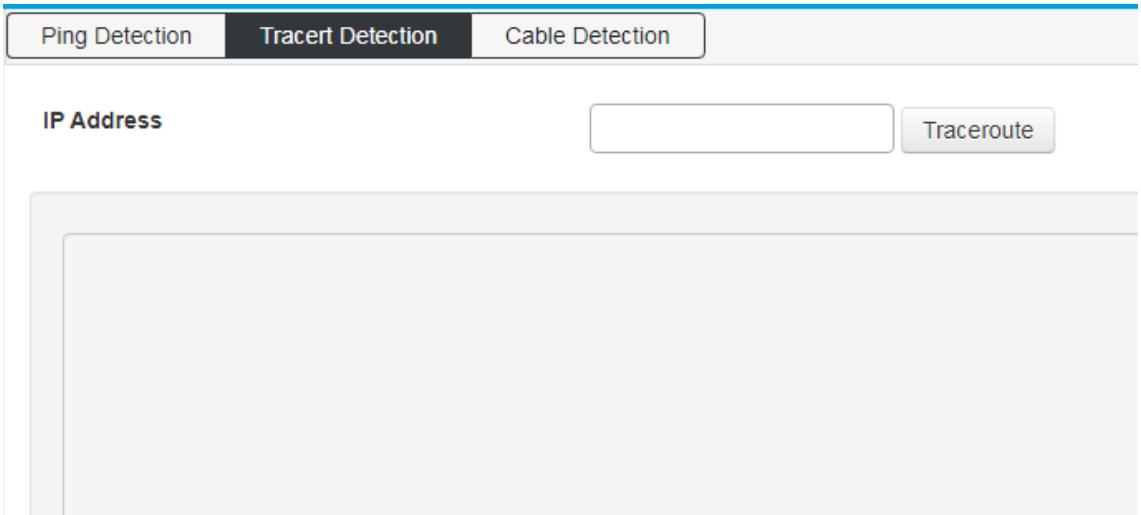


7.8 Diagnostic Testing

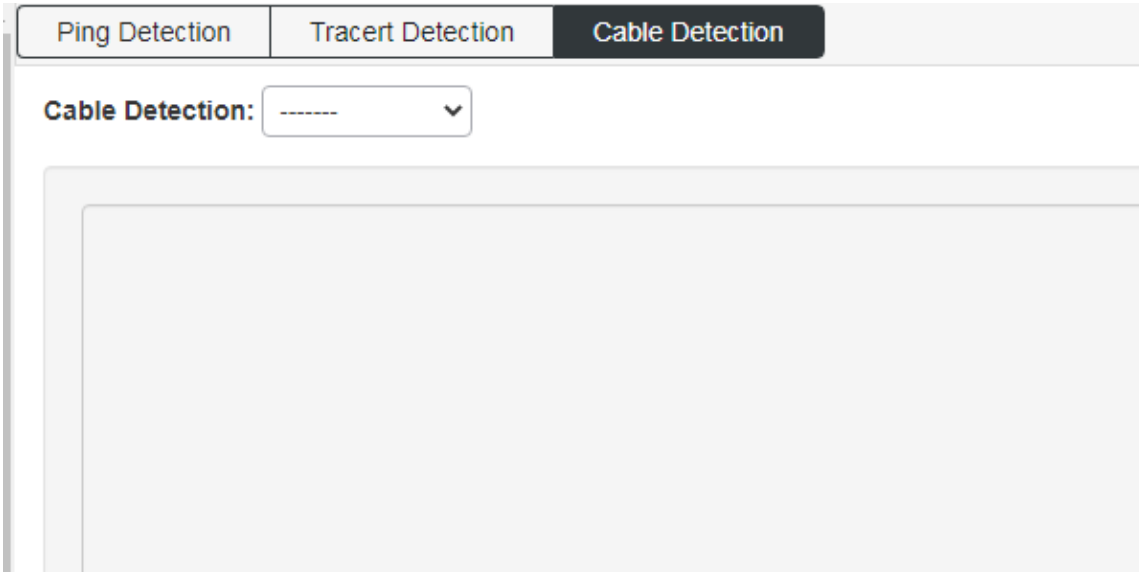
Ping detection: use the ping function of the switch to detect whether the link between the switch itself and other IP devices is smooth.



Tracert detection: Traceroute.

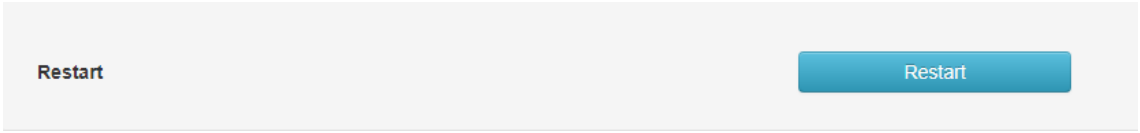


Network line detection: detect the network line attribute of all network ports of the switch.



7.9 Reboot Device

Restart the switch.



This is a Class A product. In home environment, this product may cause radio interference. In this case, the user may be required to take appropriate measures.

Hereby Assmann Electronic GmbH, declares that the Declaration of Conformity is part of the shipping content. If the Declaration of Conformity is missing, you can request it by post under the below mentioned manufacturer address

www.assmann.com
ASSMANN Electronic GmbH
Auf dem Schüffel 3
58513 Lüdenscheid, Germany