Smart WEB Managed Switch

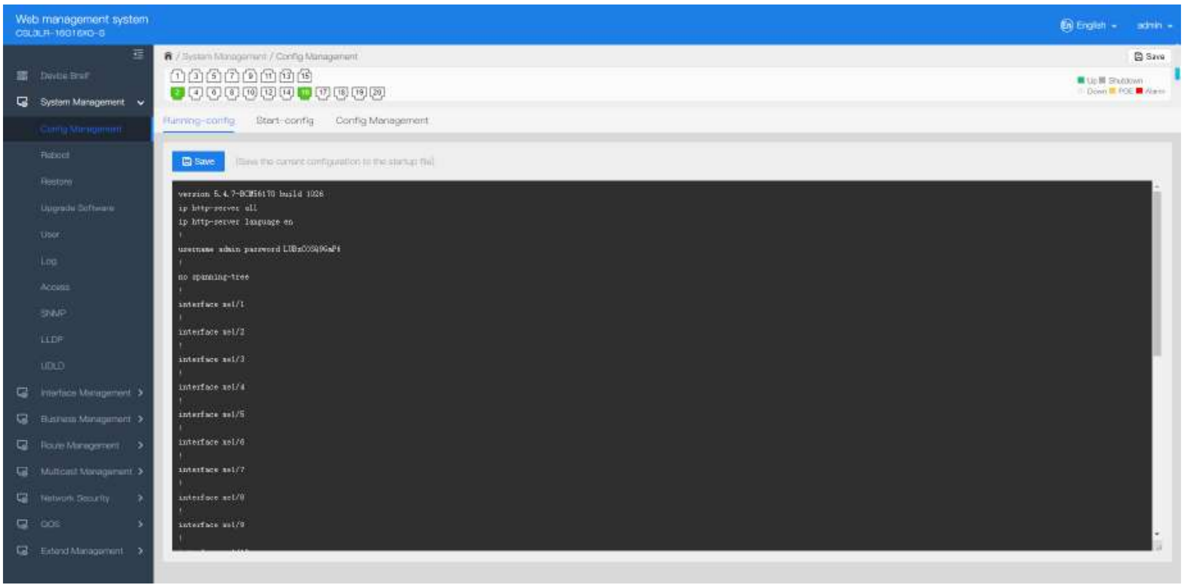
User manual

SIE-16G16XG-S

Web Configuration Guide

Notes: This software version after the configuration function is completed; You must go to System Administration - Configuration Administration - click Save; Otherwise, all configurations won't be saved after restarting the device; Or simply click the icon in the upper right corner 

of the WEB page to save;



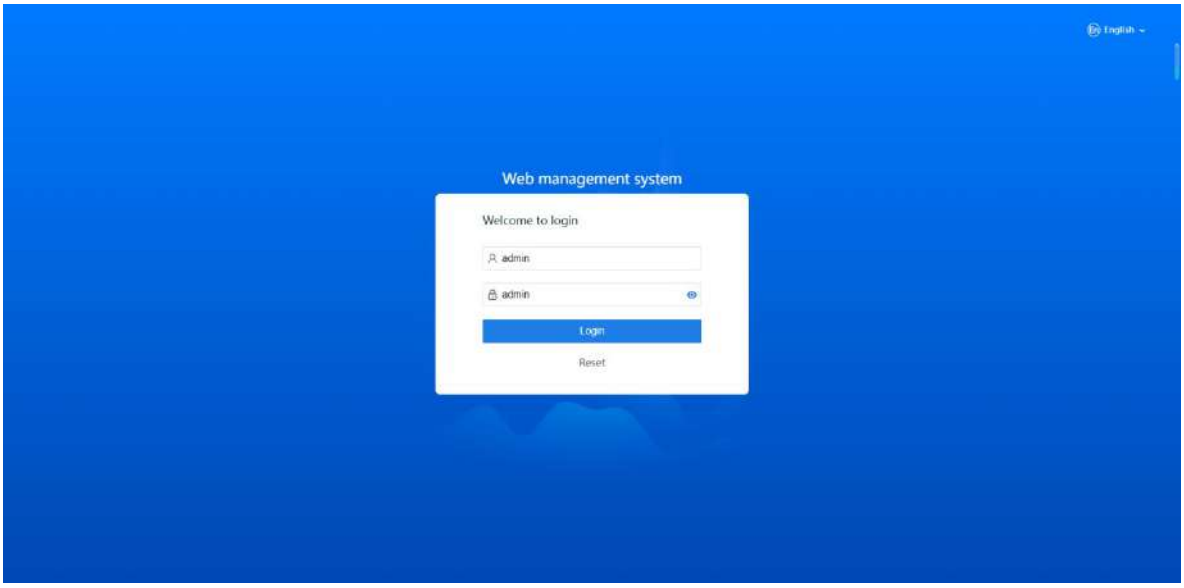
Contents

1. Log in to the WEB world

1. Open a browser;

2. Enter the default IP in OOB standalone Administration port: http://192.168.0.10 or in vlanif1 service port: http://192.168.1.168 Press Enter;

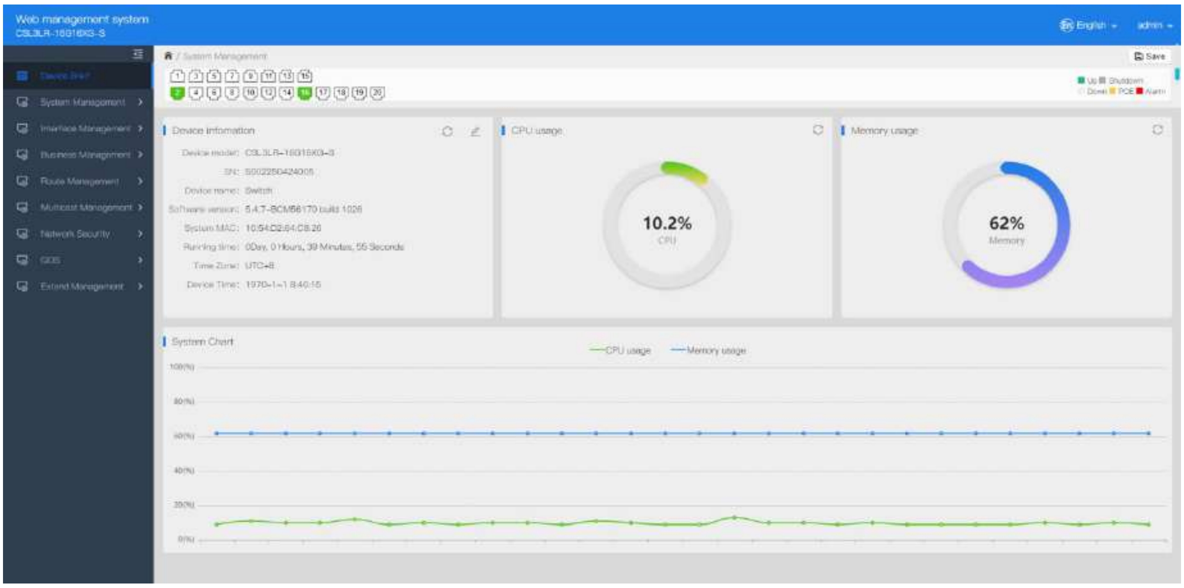
3. Appear the login page, default username admin, default password admin;



4 Click the "Login" button to enter the web configuration interface.

2. Web overall page layout

The following picture is the overall effect picture you see after entering the web configuration interface:



1 Go to "Device Overview" to view product information, CPU utilization, memory utilization, and system trend chart.

2 Click the menu tree on the left to expand the corresponding sub-menu link, click a certain sub-menu, swipe the card to

expand the configuration item under that sub-menu, and configure it.

3. Click the "" button in the upper right corner to save the 

device-to-device configuration for this login.

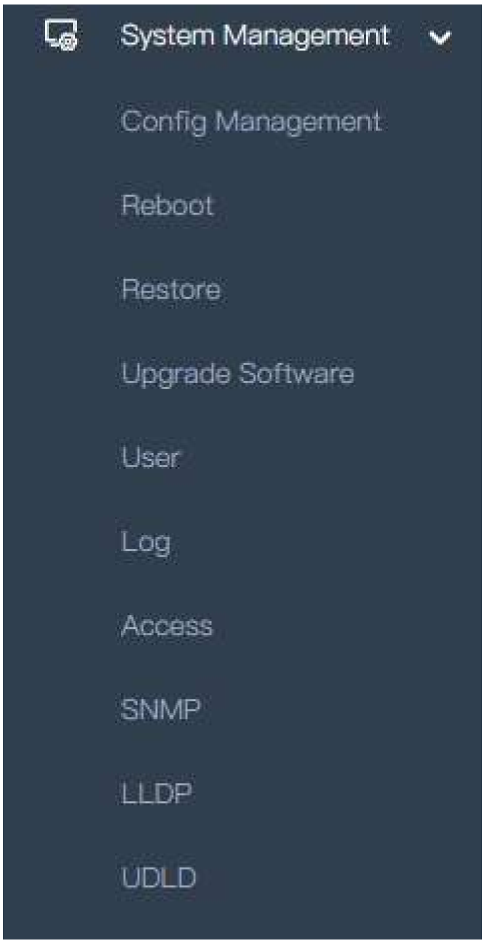
4 Click the "" icon to set 

the page language (Simplified Chinese, English).

3. WEB Configuration Guide

3.1 System Administration

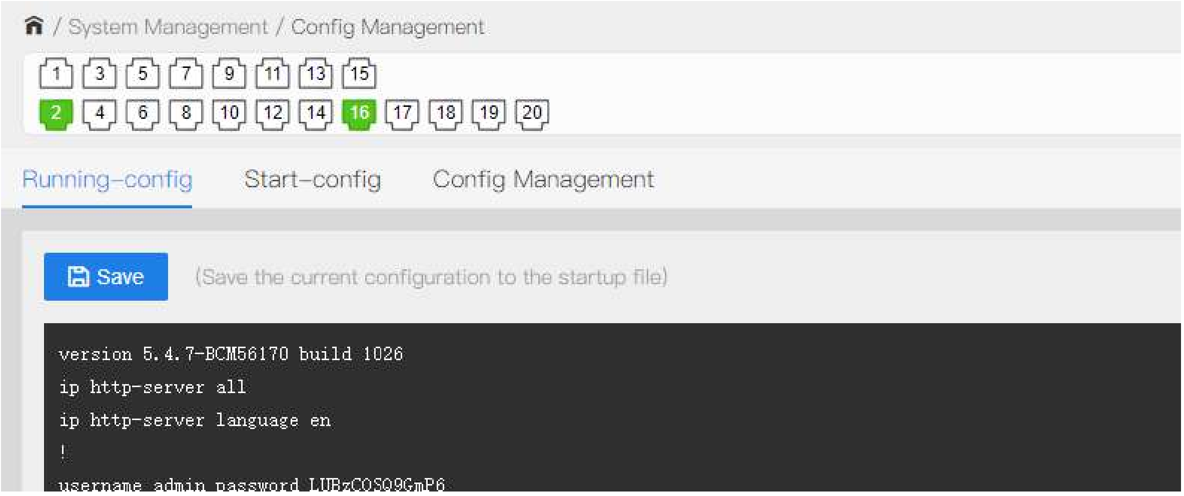
Expand this setup and you can manage configuration, restart devices, restore factory Settings, online upgrades, users, logs, access configuration, SNMP, LLDP, UDLD, etc.



3.1.1 Configuration Management

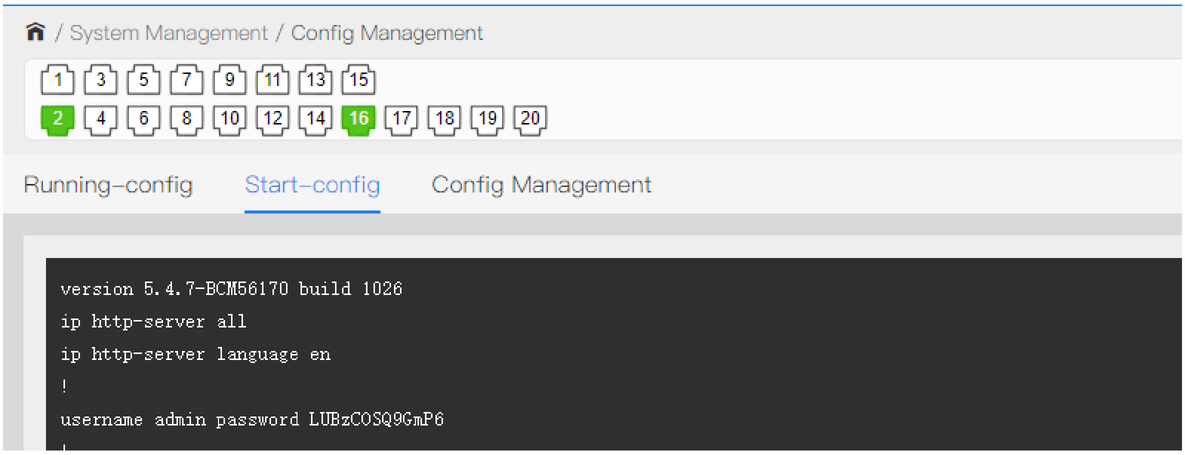
Configuration management: It consists of three parts: viewing running configuration, viewing startup configuration, and configuration file management.

3.1.1.1 View the running configuration



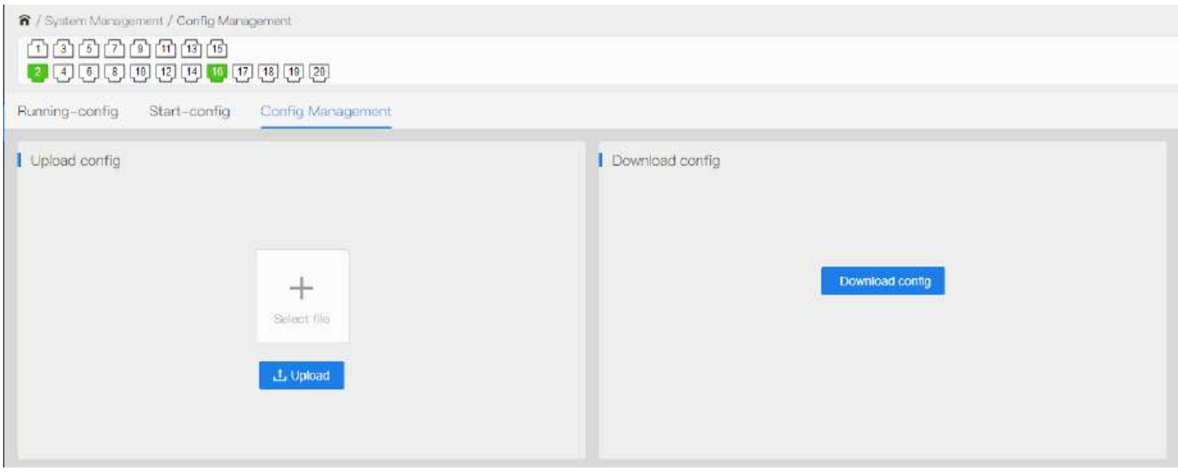
View running configuration: You can view all current configurations.

3.1.1.2 Check the startup configuration



View startup configuration: You can view the configuration information that is loaded and runs when the switch starts up.

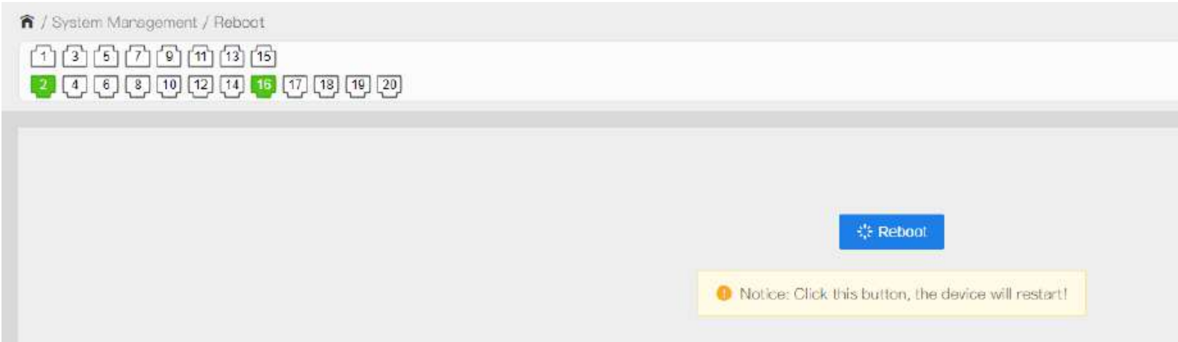
3.1.1.3 Profile management



Profile management:

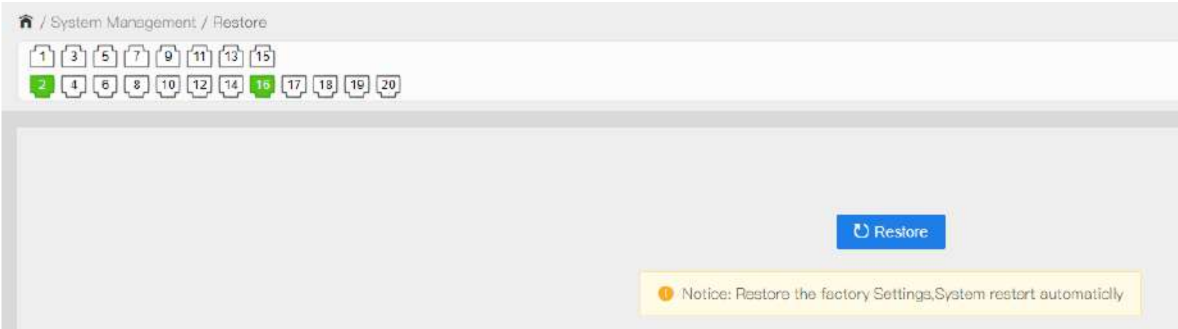
(1) Upload configuration files: Configuration files can be uploaded to the switch and run. (2) Download configuration file: You can download the current configuration file to your desktop to save.

3.1.2 Restart the device



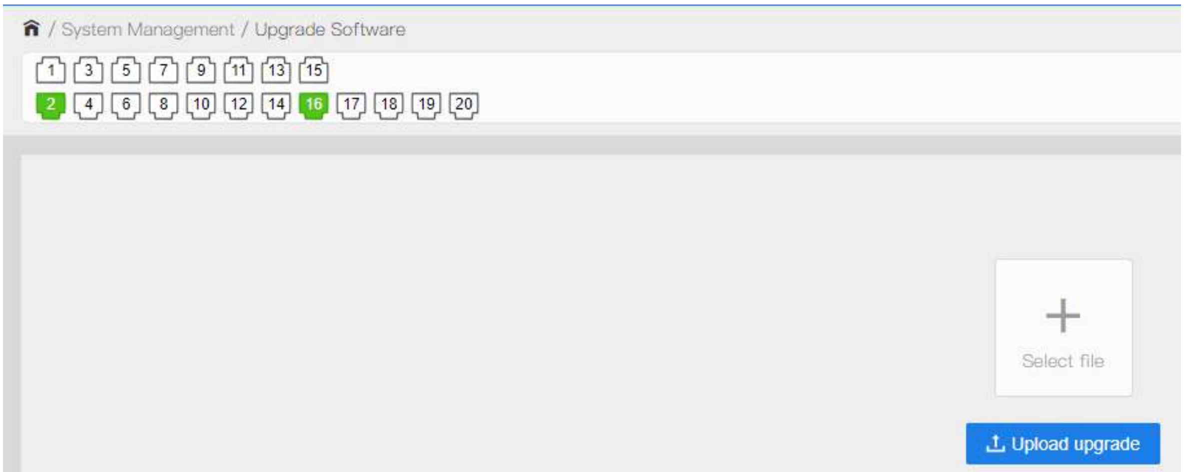
Restart the device: Restart the switch to run.

3.1.3 Restore to factory Settings



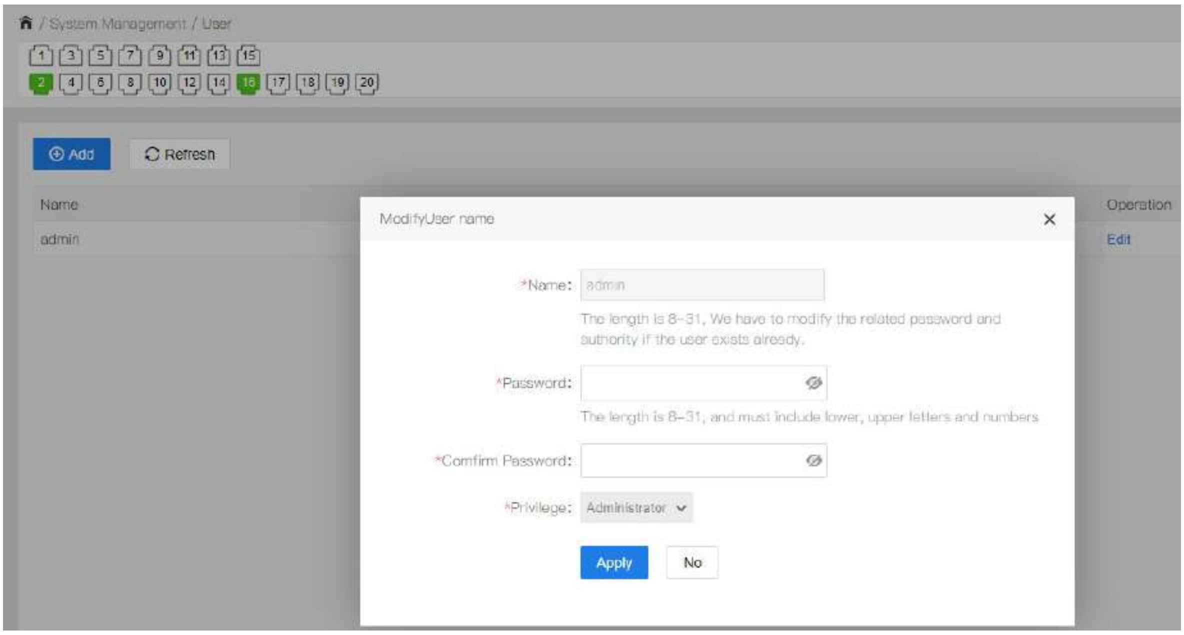
Restore to factory Settings: Clear the current configuration and restore to factory default Settings.

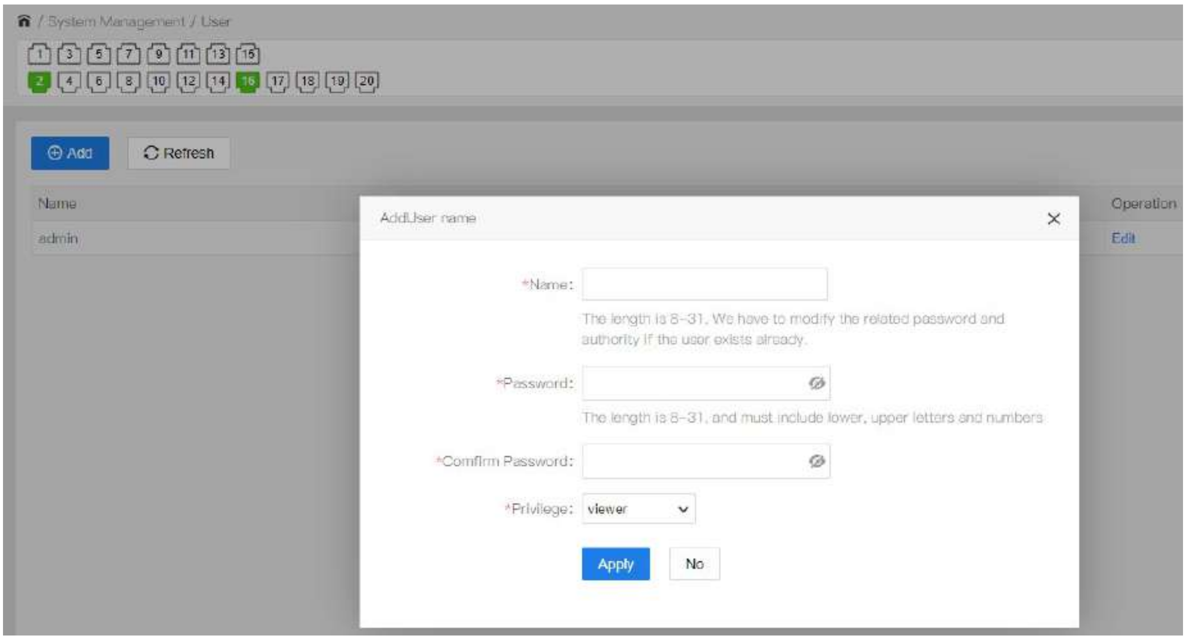
3.1.4 Online Upgrade



Online upgrade: Use the file menu to pass runtime code or configuration Settings, or configure the auto-upgrade feature.

3.1.5 Users



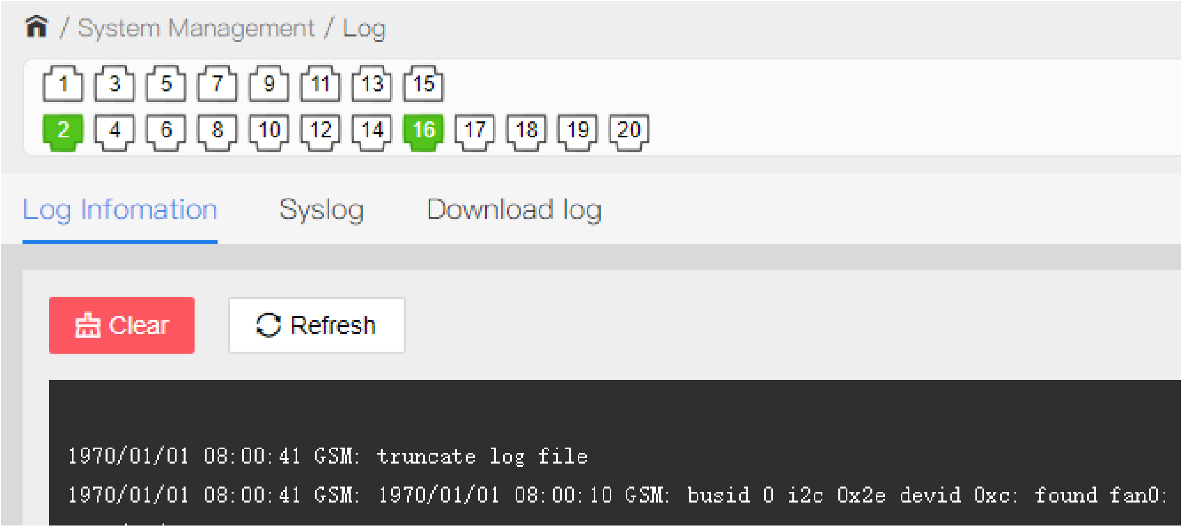


User: The login password of the switch can be modified and new users can be added.

3.1.6 Logs

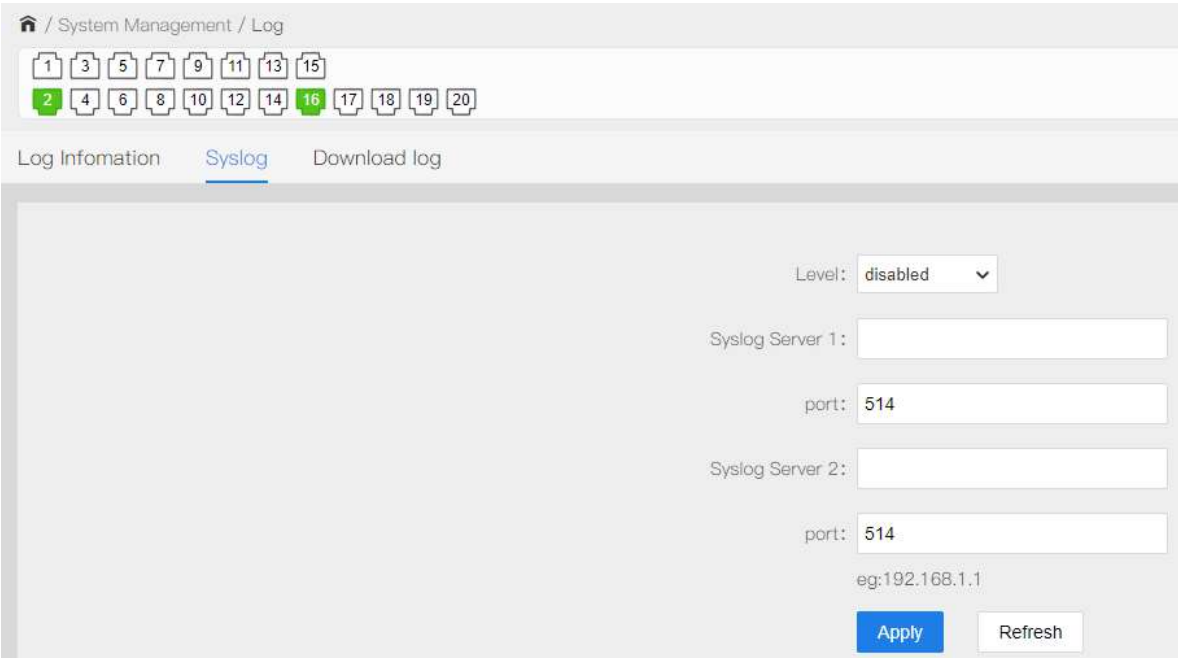
log: Consists of three parts: log information, Syslog, and download log.

3.1.6.1 Log information



Log information: The log function and the corresponding module can be enabled globally, and the log server address and log level can be set.

3.1.6.2 Syslog



Syslog: System logs.

Level: The following six levels are available:

①Debugging: Debug the level of daily patterns to facilitate problem diagnosis and record detailed information.

②Informational: Primarily used to record information about meaningful events in a system or application.

③Notifications: mainly to view some critical state changes or important operation results in the system.

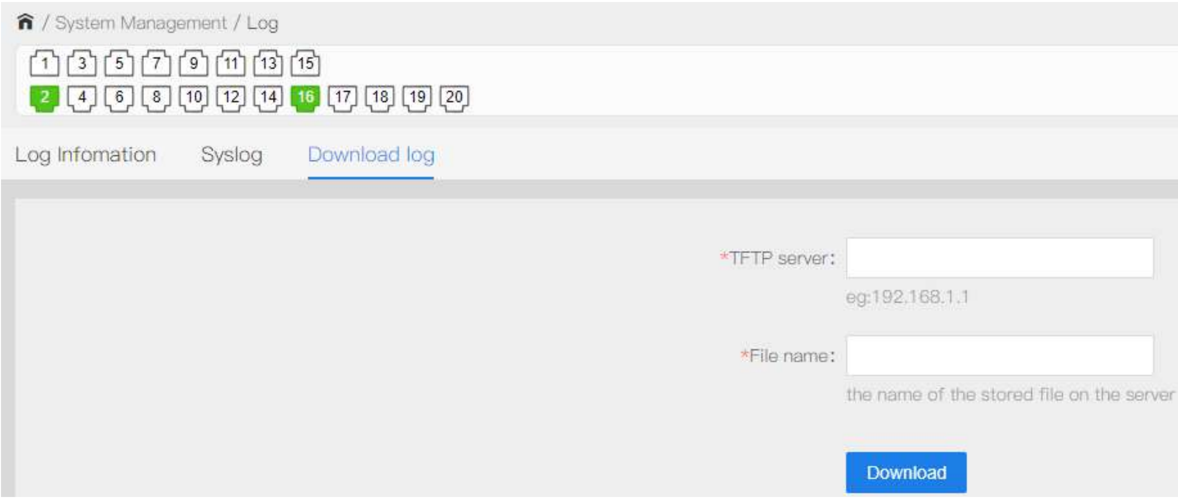
④Warnings: Check the warning messages sent by system programs.

⑤Errors: Check for errors in system programs, such as software crashes, hardware failures, etc.

⑥Disabled: Check if a feature or service is disabled or disabled.

- Syslog Server 1: System log message Format Transport Protocol.
- Port: Port number, which is usually associated with the syslog protocol.
- Syslog Server 2: System Log Message Format Transport Protocol.
- Port: Port number, which is usually associated with the syslog protocol.

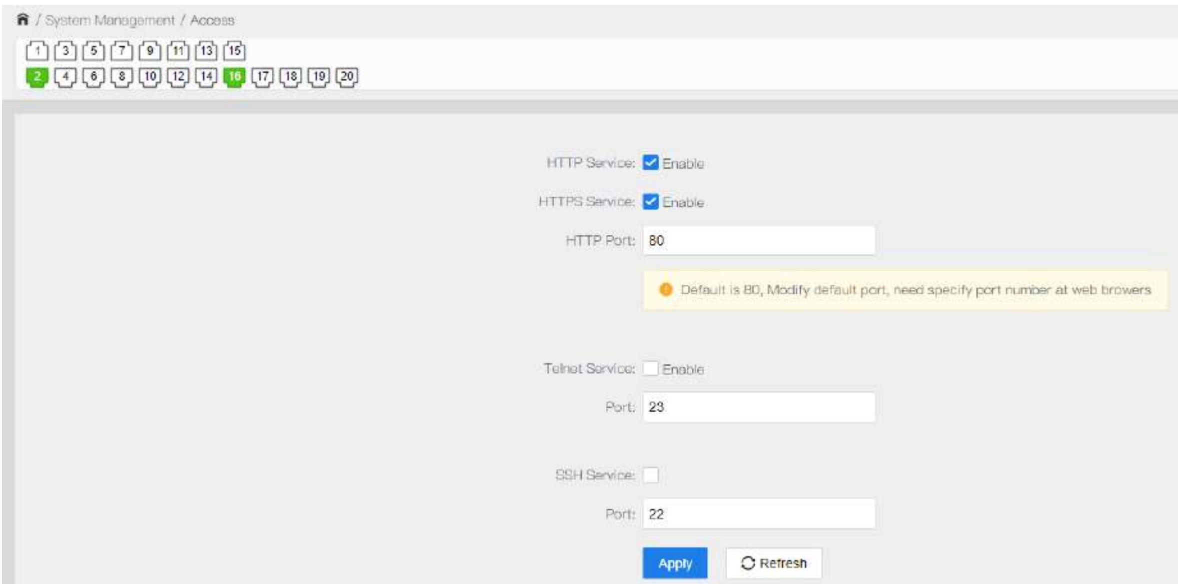
3.1.6.3 Download the log



Download log: Download log.

- TFTP server: File Transfer protocol.
- File name: The name where the file is saved on the server.

3.1.7 Access configuration



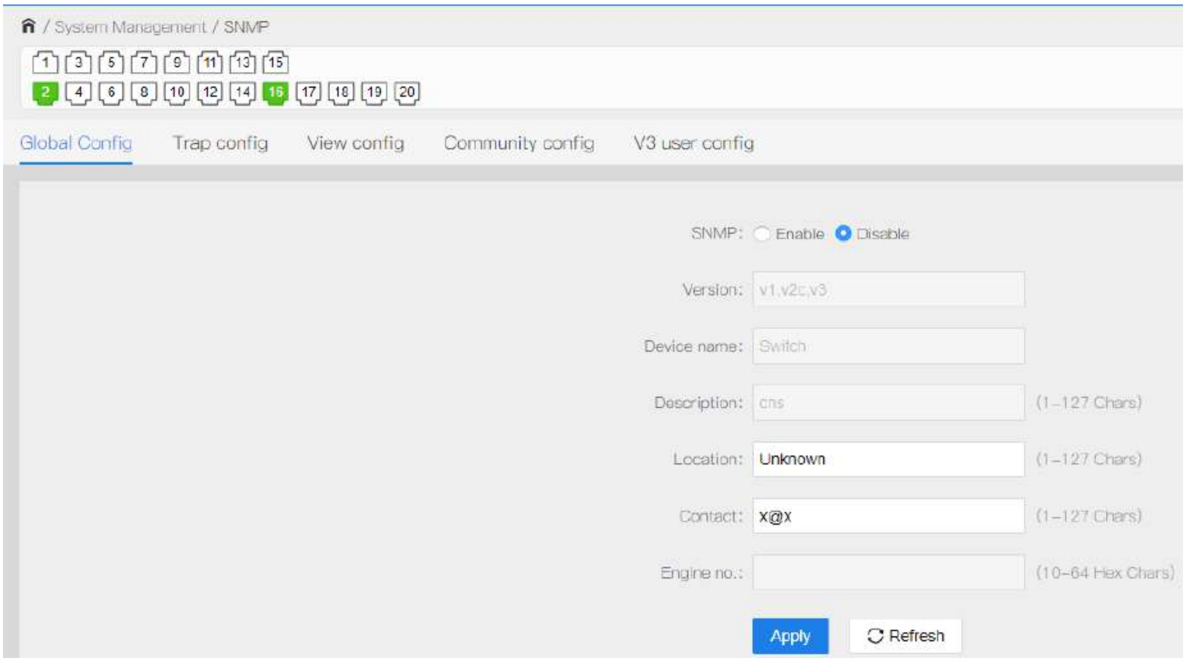
Access Settings:

- HTTPS service: It is a hypertext protocol used for network transmission.
- HTTPS service: It is a protocol that adds SSL/TLS protocol to encrypted transmission on top of HTTP.
- HTTP port: It is a port that manages the network and accesses the switch via the HTTP protocol.
- Telnet service: It is a protocol used for remote management and configuration of switches.
- Port: It is a port that manages the network and accesses the switch via the Telnet protocol.
- SSH service: A secure remote access protocol.
- Port: SSH Remote Access Protocol port.

3.1.8 SNMP

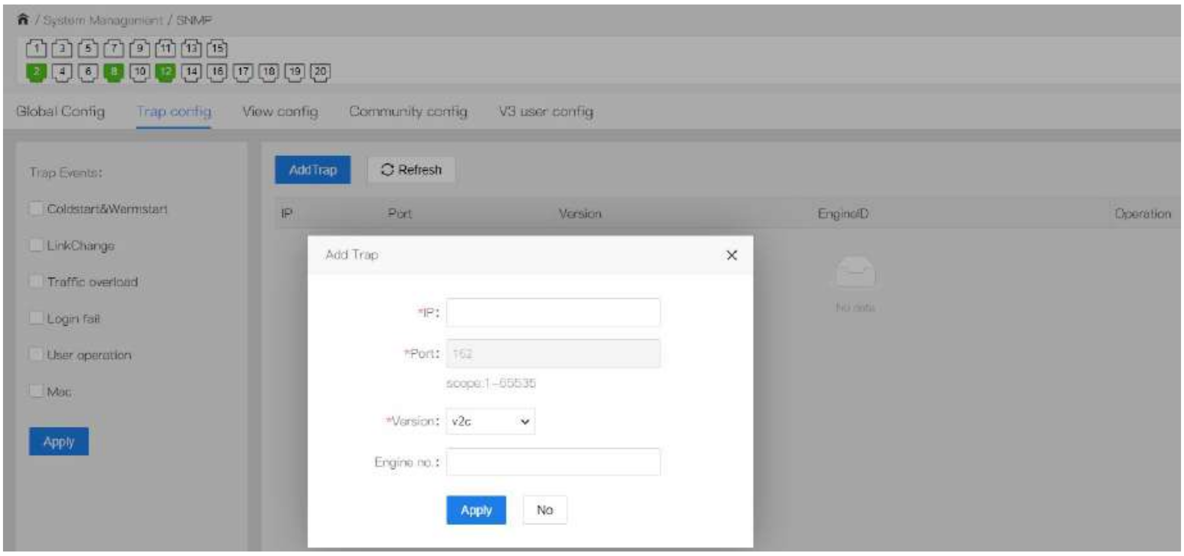
SNMP: Consists of five parts: global configuration, Trap configuration, view configuration, group configuration, and V3 user configuration.

3.1.8.1 SNMP Global Configuration



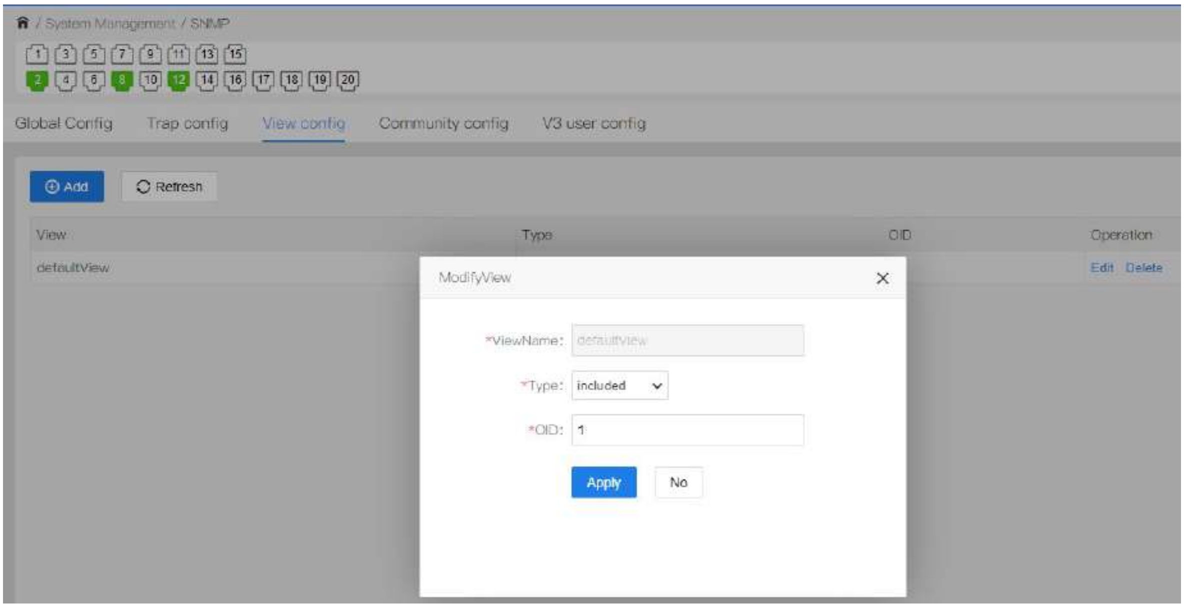
SNMP global configuration: Set up the SNMP functionality of the switch as a whole to enable network management and monitoring of the switch.

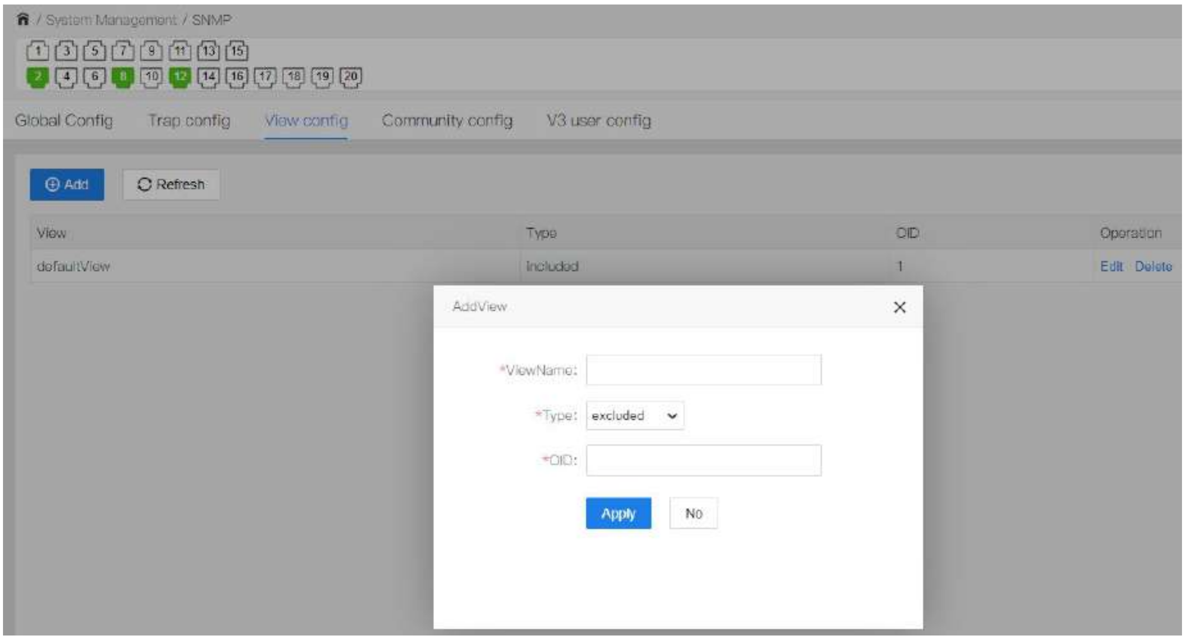
3.1.8.2 Trap configuration



Trap configuration: It is a message actively sent by the managed device to the management station to notify the management station of a specific event or status change. By configuring Trap, administrators can be informed of the switch's operational status in a timely manner, so as to respond and handle problems quickly.

3.1.8.3 View Configuration

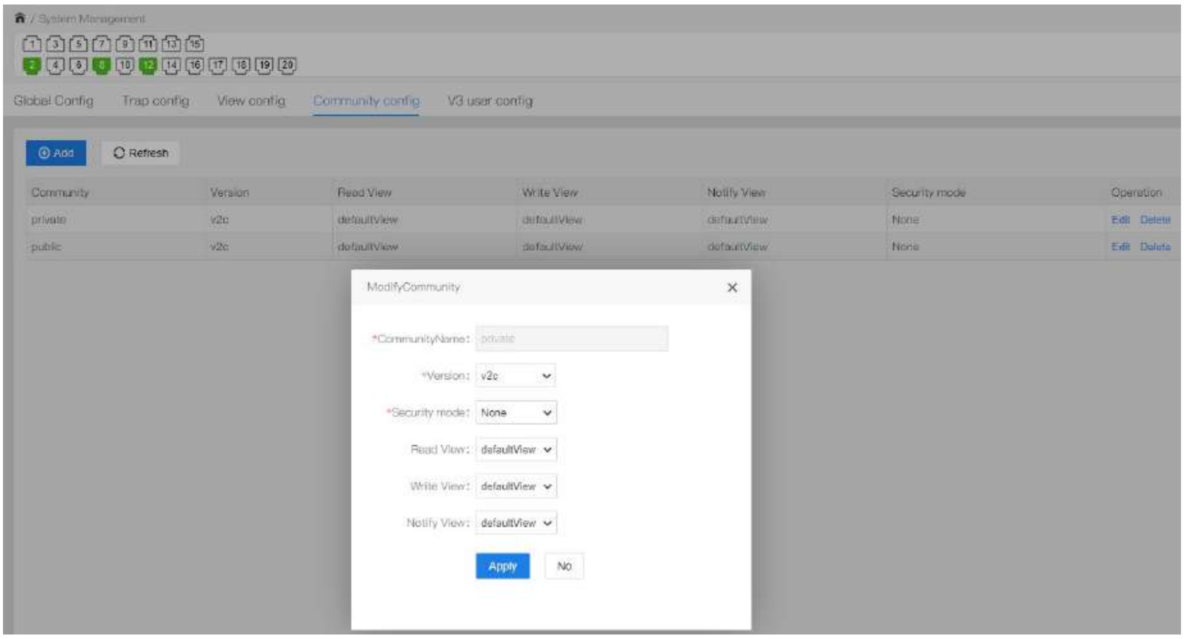


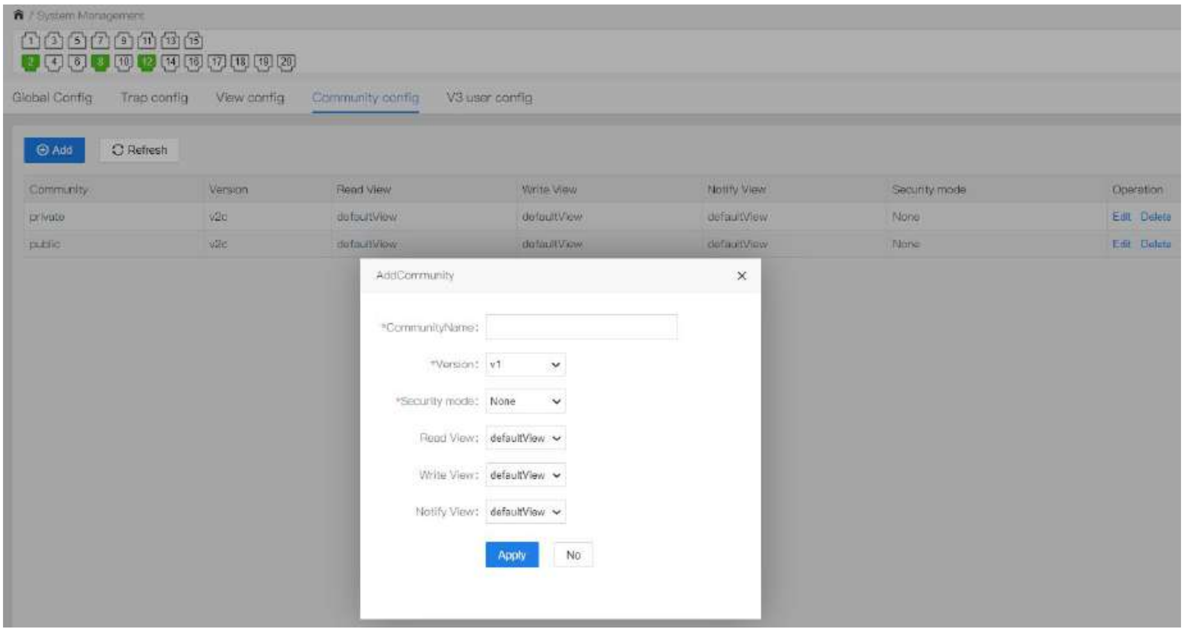


View configuration: Modify a view or add a view.

View configuration**:** A feature for customizing what is displayed and laid out in the user interface, through which administrators can adjust the information presented in the switch management interface according to their own needs and habits for more efficient management and monitoring.

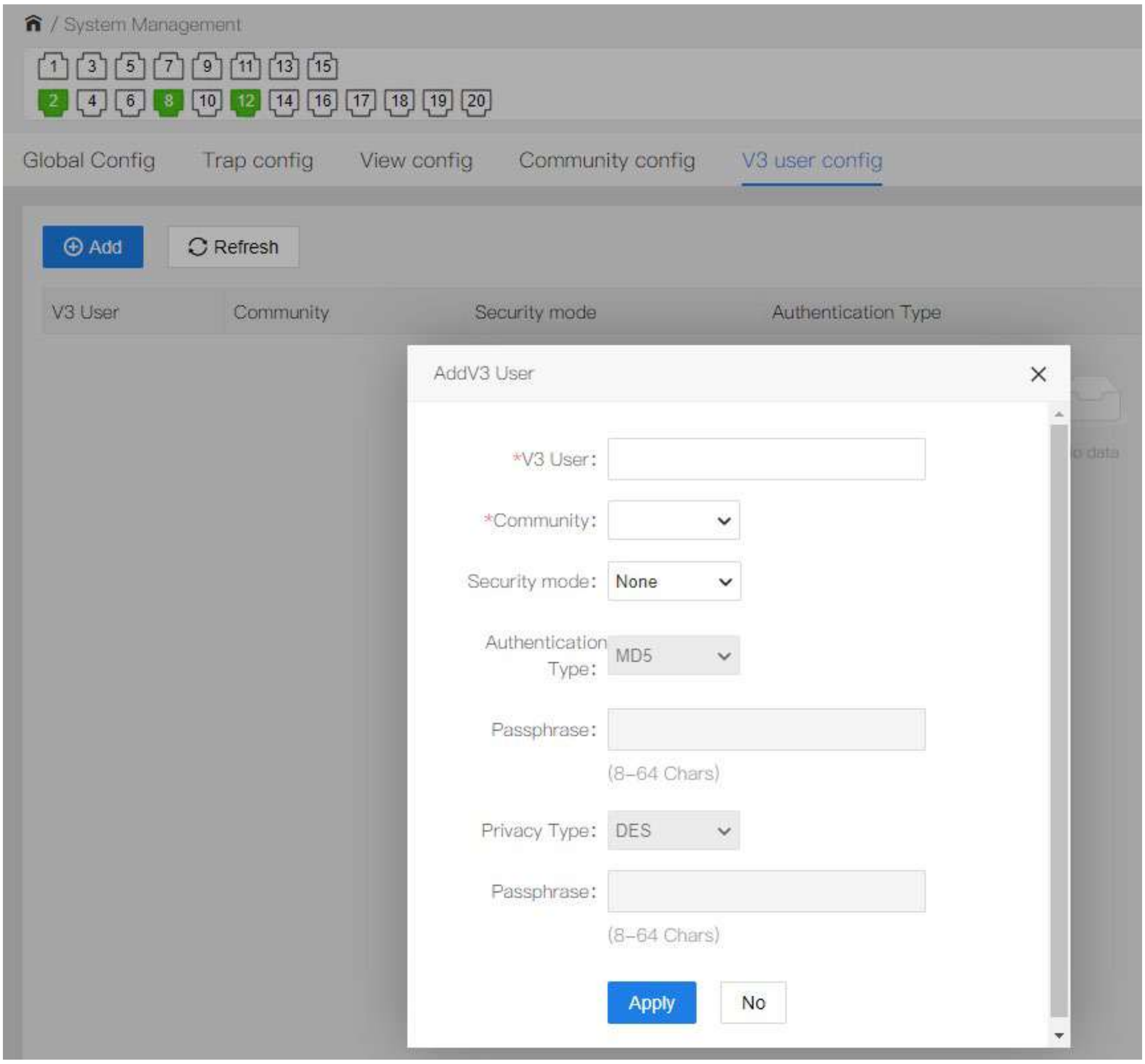
3.1.8.4 Group Configuration





Group configuration: A protocol used to manage network devices, and a Community is an important concept in SNMP. Group configuration involves setting parameters such as the SNMP group name.

3.1.8.5 V3 User configuration

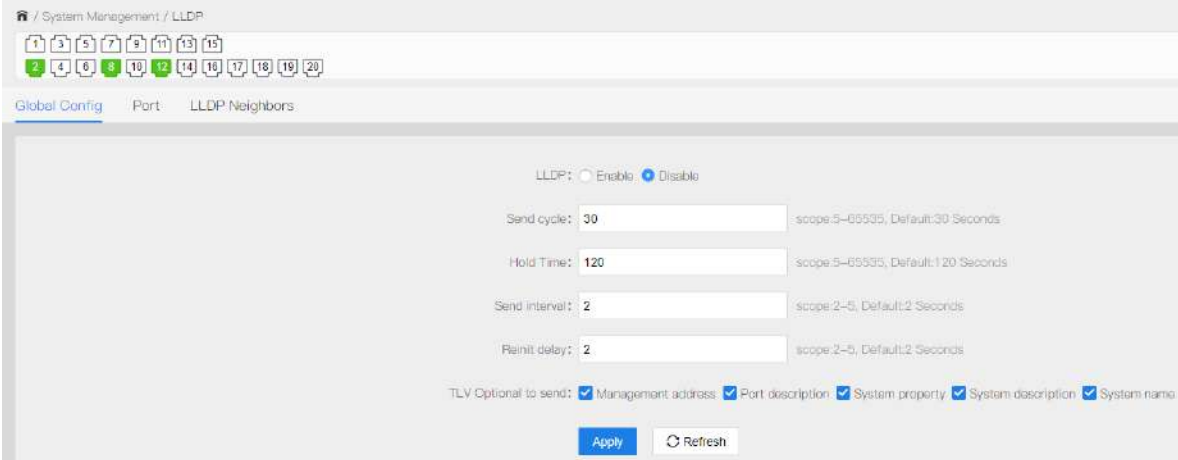


User configuration: Add version V3 user configuration.

3.1.9LLDP

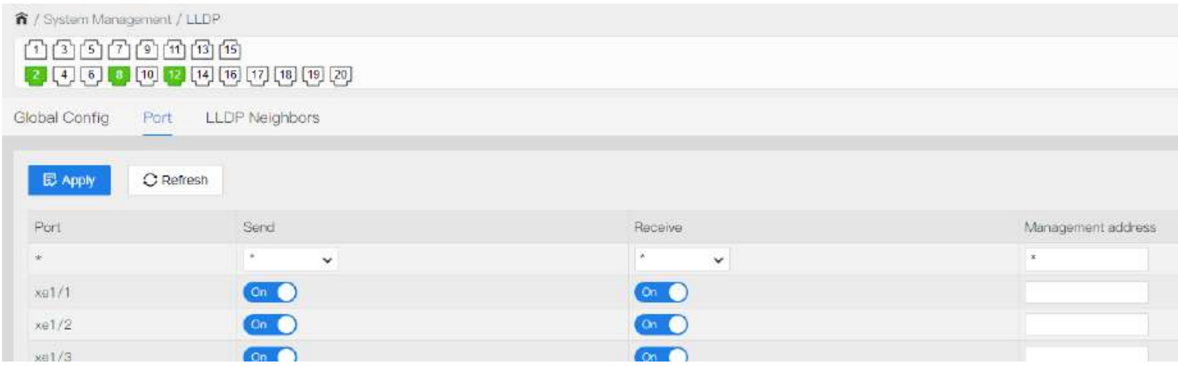
LLDP: includes global configuration, port configuration, and LLDP neighbors.

3.1.9.1 Global configuration



Global configuration: The operation of enabling or disabling link layer discovery protocols to set the overall operating parameters and functions of the switch that affect the global behavior of the switch, rather than targeting a particular port or interface.

3.1.9.2 Port configuration



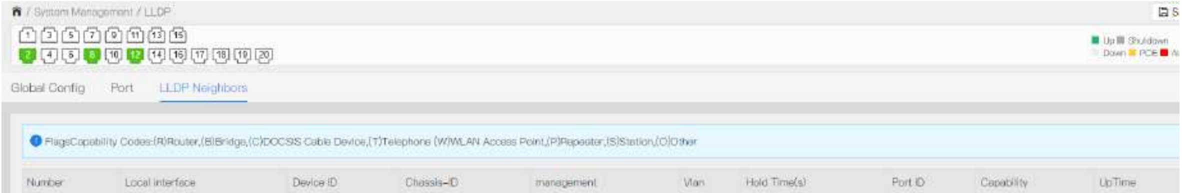
Port configuration: Set the working parameters and functions of each port of the switch to meet different network requirements.

● Port status: Ports can be set to enable or disable. When enabled, the port works normally and can send and receive data; When disabled, the port stops working and does not transfer data.

● Port rate: Set the transfer rate of the port according to the performance of the connected device and network requirements, such as 10Mbps, 100Mbps, 1000Mbps, etc.

● Duplex mode: Half-duplex and full-duplex modes are available. In half-duplex mode, data can only be transmitted in one direction at the same time; In full-duplex mode, data can be transmitted in both directions at the same time, which improves port transmission efficiency.

3.1.9.3LLDP neighbors



LLDP neighbor: Other devices directly connected to this switch that are discovered through the Link Layer Discovery Protocol (LLDP).

3.1.10 UDLD

UDLD: It includes two types: port configuration and UDLD neighbors.

3.1.10.1 UDLD neighbors

UDLD neighbor: A neighbor device identified through the Unidirectional Link Detection (UDLD) protocol.

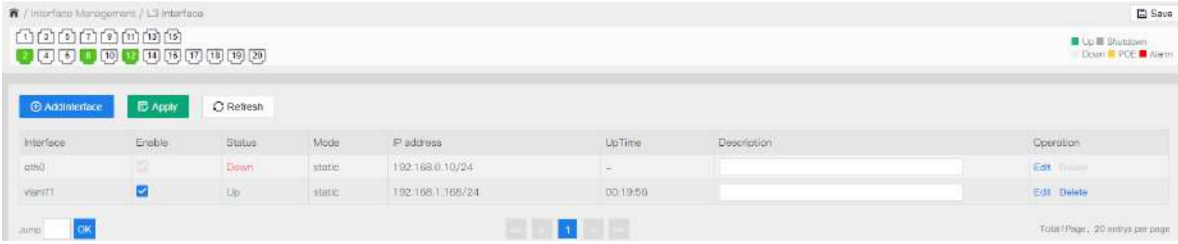
3.2 Interface Management

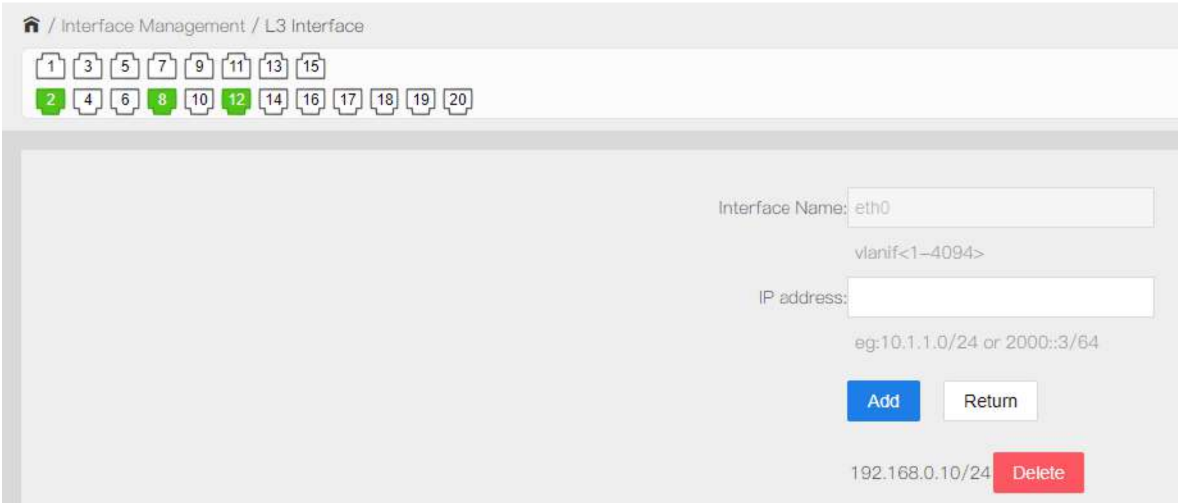
Expand this setup and you can set up physical ports, Layer 3 interfaces, link aggregation, port mirroring, port statistics, bandwidth trend charts, Fiber Info, etc.

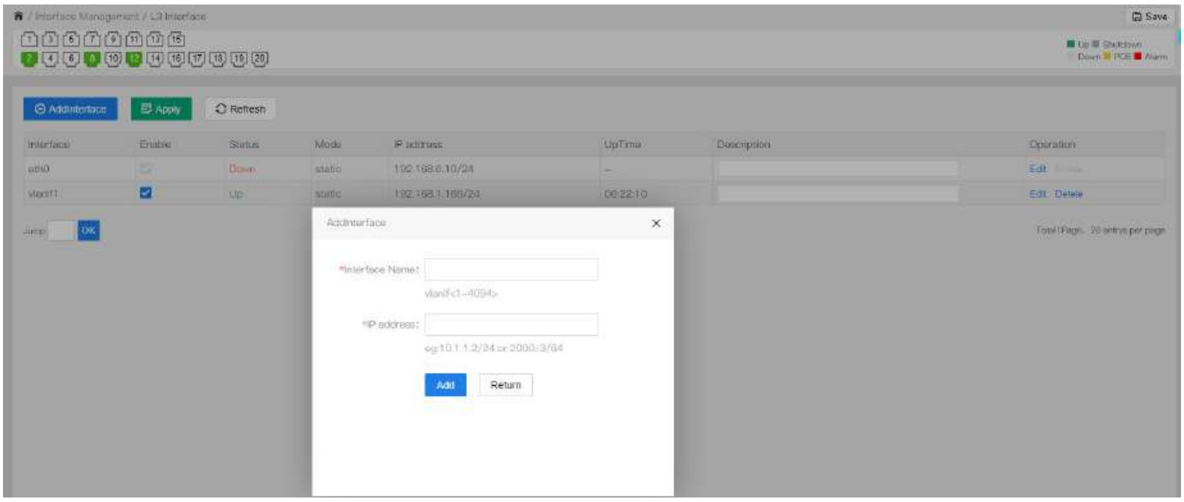
3.2.1 Physical Ports

Physical port: A hardware interface that actually exists on a switch for connecting network devices.

3.2.2 Layer 3 Interface







Layer 3 interface: Can modify the current managed IP address of the switch.

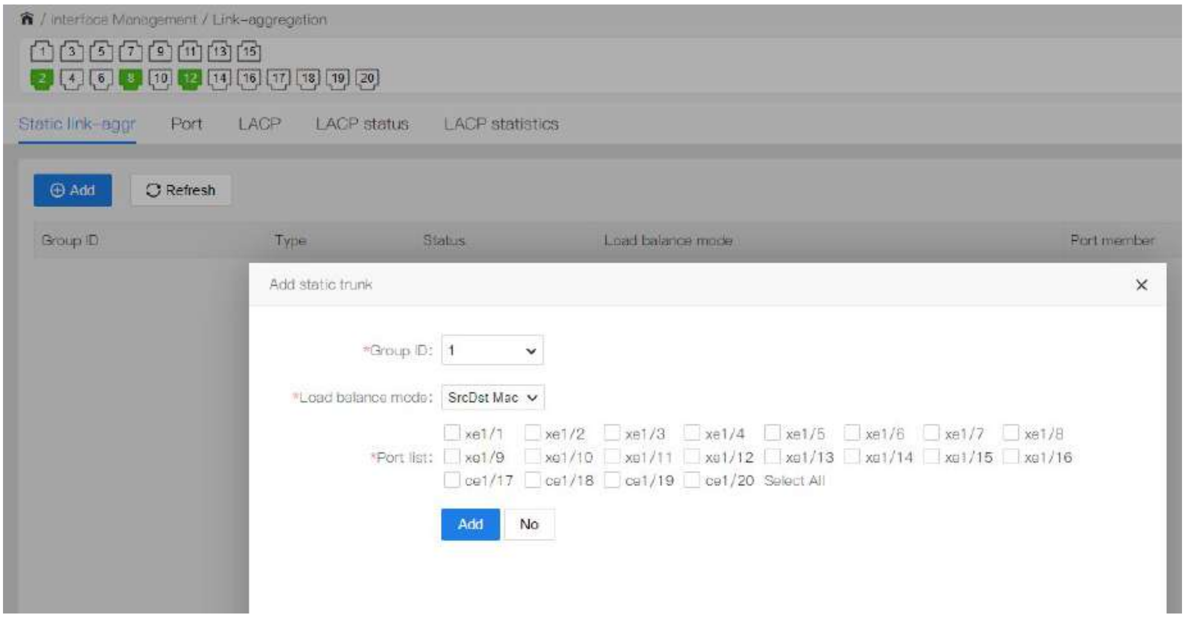
 Interface name: The current vlan group of the switch.

▯ IP address: The IP address of the switch service port vlan1.

3.2.3 Link Aggregation

Link aggregation: includes static link aggregation, port configuration, LACP, LACP status, LACP statistics.

3.2.3.1 Static Link Aggregation



Static link aggregation: Static link aggregation is a way to manually configure link aggregation.

▯ Group ID: Select how many groups of aggregation ports to set.

▯ Load balancing mode: It refers to how the switch distributes data traffic to each member port in the link aggregation group to achieve full utilization of link bandwidth and load balancing.

▯ Port list: All ports.

3.2.3.2 Port configuration

Port configuration: Parameter setting and functional adjustment for each physical port involved in link aggregation to achieve the desired effect of link aggregation.

3.2.3.3 LACP

LACP: A protocol used to bundle multiple physical links into one logical link.

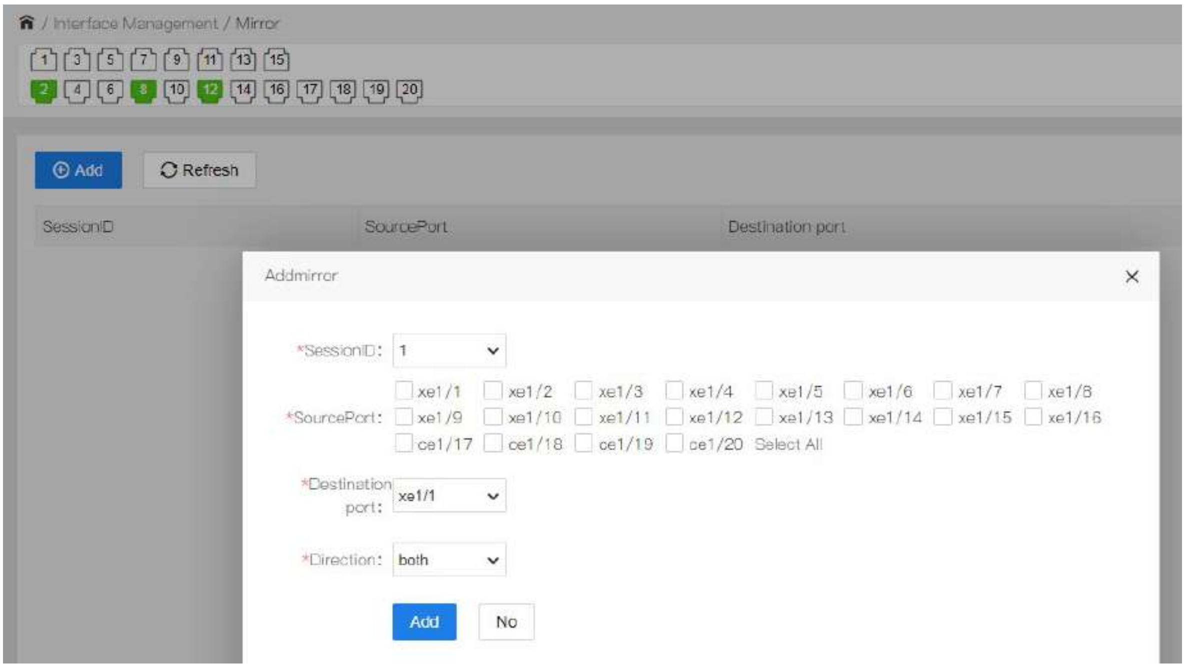
3.2.3.4 LACP state

LACP status: Link Aggregation Control Protocol.

3.2.3.5 LACP statistics

LACP statistics: Link Aggregation Control Protocol statistics are statistics of information about link aggregation groups used to show how LACP works and the performance of link aggregation.

3.2.4 Port mirroring



Port mirroring: refers to replicating traffic from one or more ports (source port) of a switch to another port (destination port) for network monitoring and analysis.

3.2.5 Port statistics

Port statistics: including port rate statistics, port summary statistics, and port detail statistics.

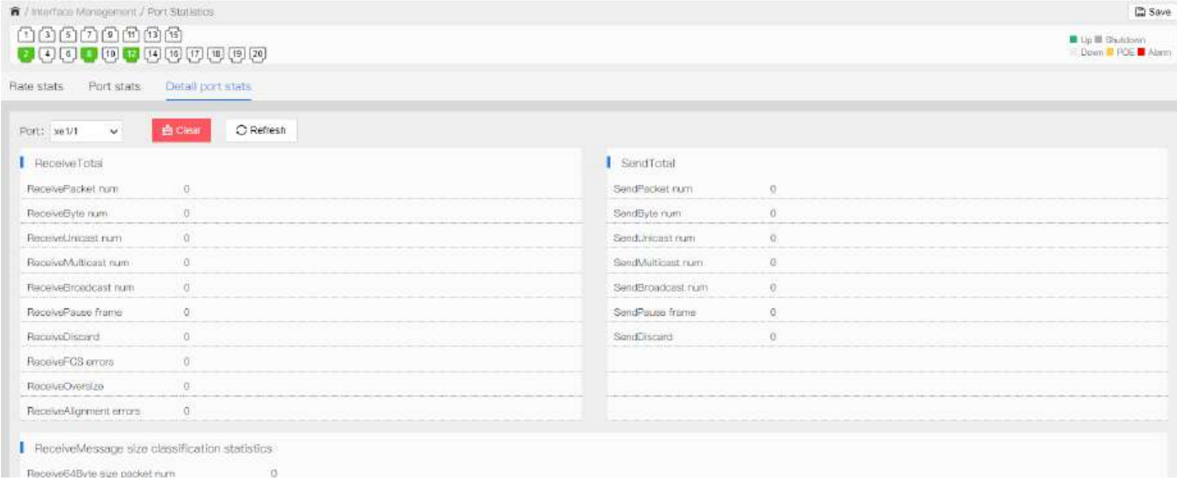
3.2.5.1 Port rate statistics

Port rate statistics: The function of real-time monitoring and statistics of data transfer rates at each port of the switch.

3.2.5.2 Port Summary Statistics

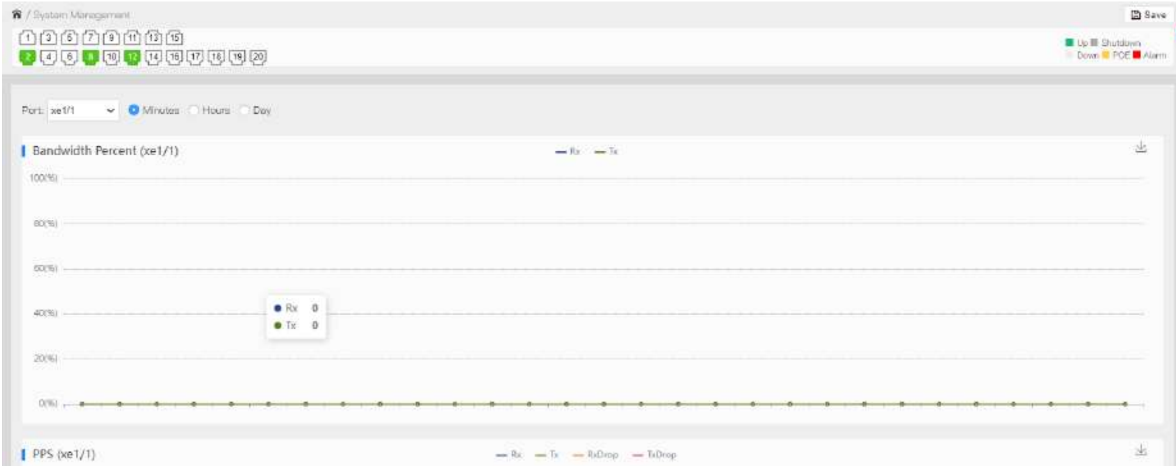
Port summary statistics: A summary and presentation of key information about the switch ports so that administrators can quickly understand the overall operational status of the ports.

3.2.5.3 Detailed statistics of ports



Port detail statistics: Collect and display relevant data on each port of the switch so that administrators can understand port usage and network traffic conditions.

3.2.6 Bandwidth trend chart



Bandwidth trend chart: A tool that graphically shows how bandwidth usage on a switch port or the entire network changes over time.

3.2.7 Fiber Info

Fiber Info: Fiber optic information.

3.3 Business Management

Expand this setup and you can set up VLAN, MAC, Spanning-tree, ERPS, QINQ, NTP, DHCP Server, ARP, ND, NAT, etc.

3.3.1 VLAN

VLAN: It includes four types: Port configuration, Port, Mac-vlan, Protocol-vlan.

3.3.1.1 Port configuration

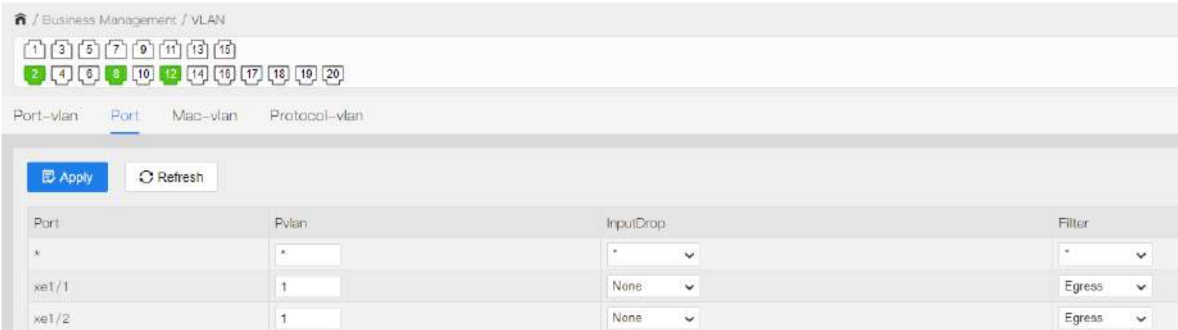
Port configuration: Setting parameters related to vlans for each port of the switch.

● Access mode: Ports can only belong to one VLAN and are typically used to connect terminal devices such as computers, printers, etc. These devices only need to communicate with other devices within the VLAN they belong to and do not need to handle traffic between different vlans.

●Trunk mode: It allows ports to belong to multiple vlans simultaneously and is often used for connections between switches or between switches and servers that support multiple vlans. It adds VLAN tags to the data frame to distinguish data from different vlans, allowing data from multiple vlans to be transmitted over a single link.

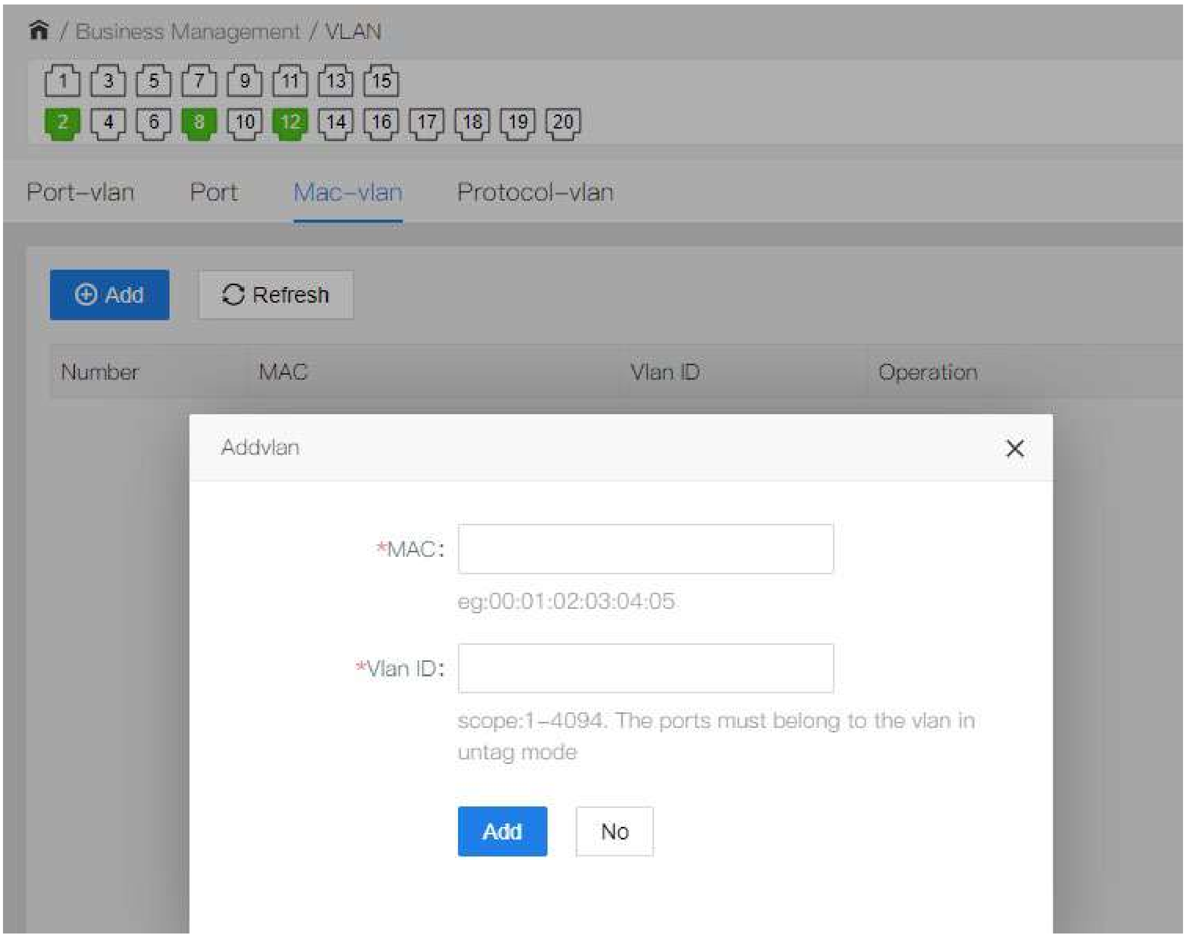
●Hybrid mode: Combines the features of both Access and Trunk modes, allowing for flexible configuration of how ports handle data in different vlans as needed. It can either belong to one VLAN like an Access port and send unlabeled frames, or belong to multiple vlans like a Trunk port and send labeled frames.

3.3.1.2 Port



Port: port.

3.3.1.3 Mac-vlan



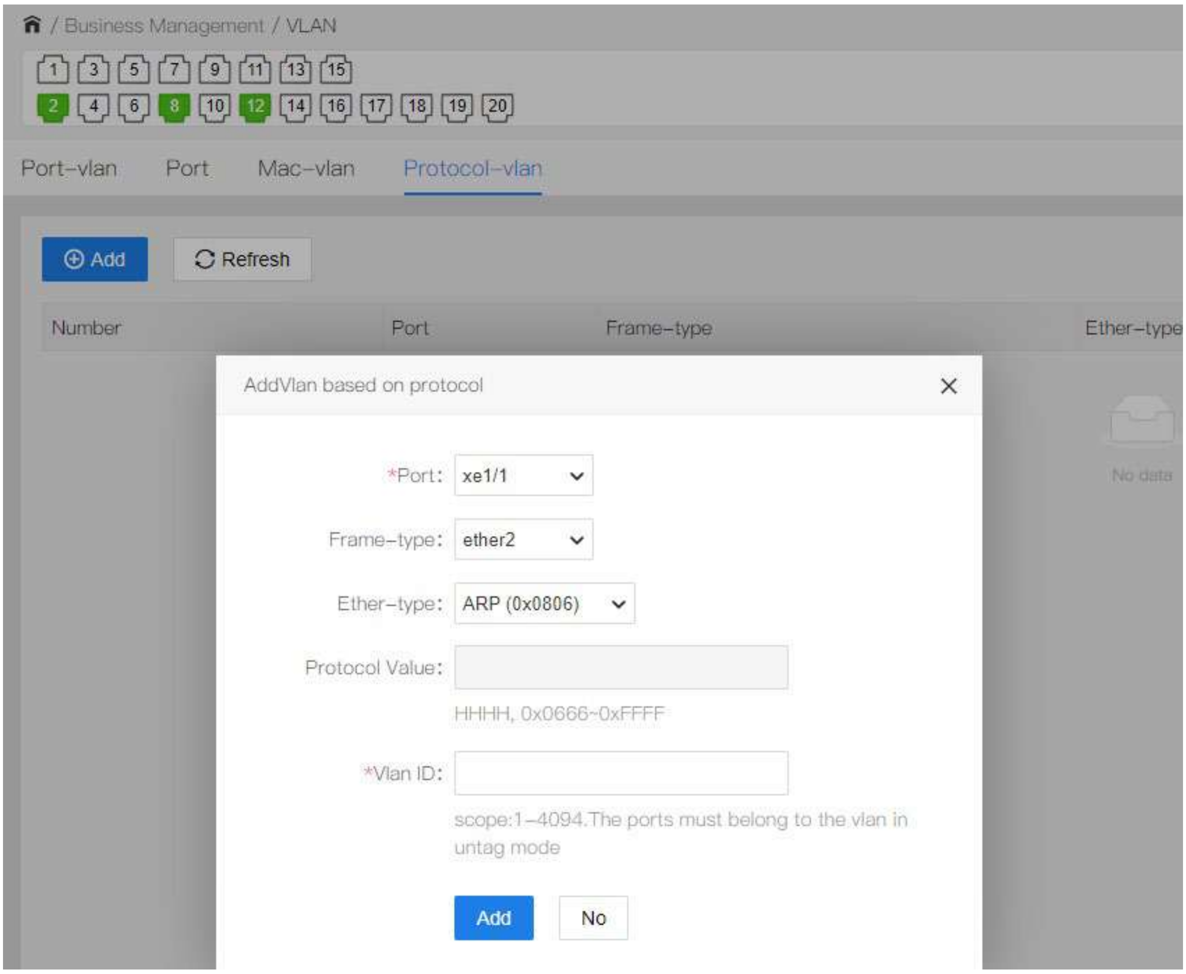
Mac-vlan: A virtual local area network partitioned based on MAC addresses.

 MAC: Custom MAC address.

 MAC mask: A MAC mask is a value used for bitwise logical operations with a MAC address, and it is primarily used for more flexible matching and filtering of MAC addresses in scenarios such as VLAN division based on MAC address or MAC address filtering.

 Vlan ID: A unique identifier used to distinguish different virtual local area networks.

3.3.2.4 Protocol-vlan



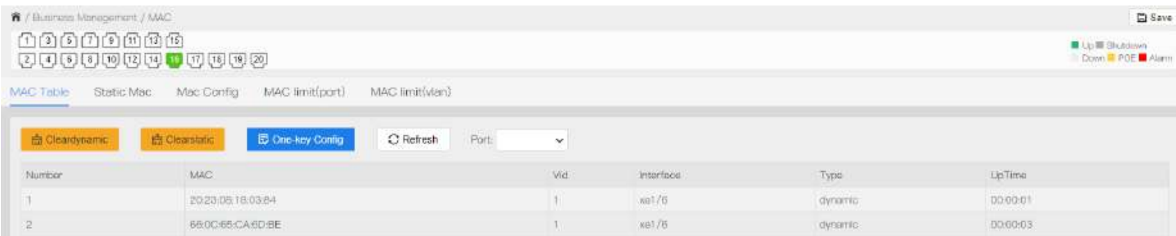
Protocol-vlan: A way to divide a virtual local area network (VLAN) based on the type of network Protocol.

Name	Description
Port	Select a port
Frame type	The data frame formats used by different network protocols
Ethernet type	Field values that identify the upper-layer protocol in an Ethernet frame

3.3.2 MAC

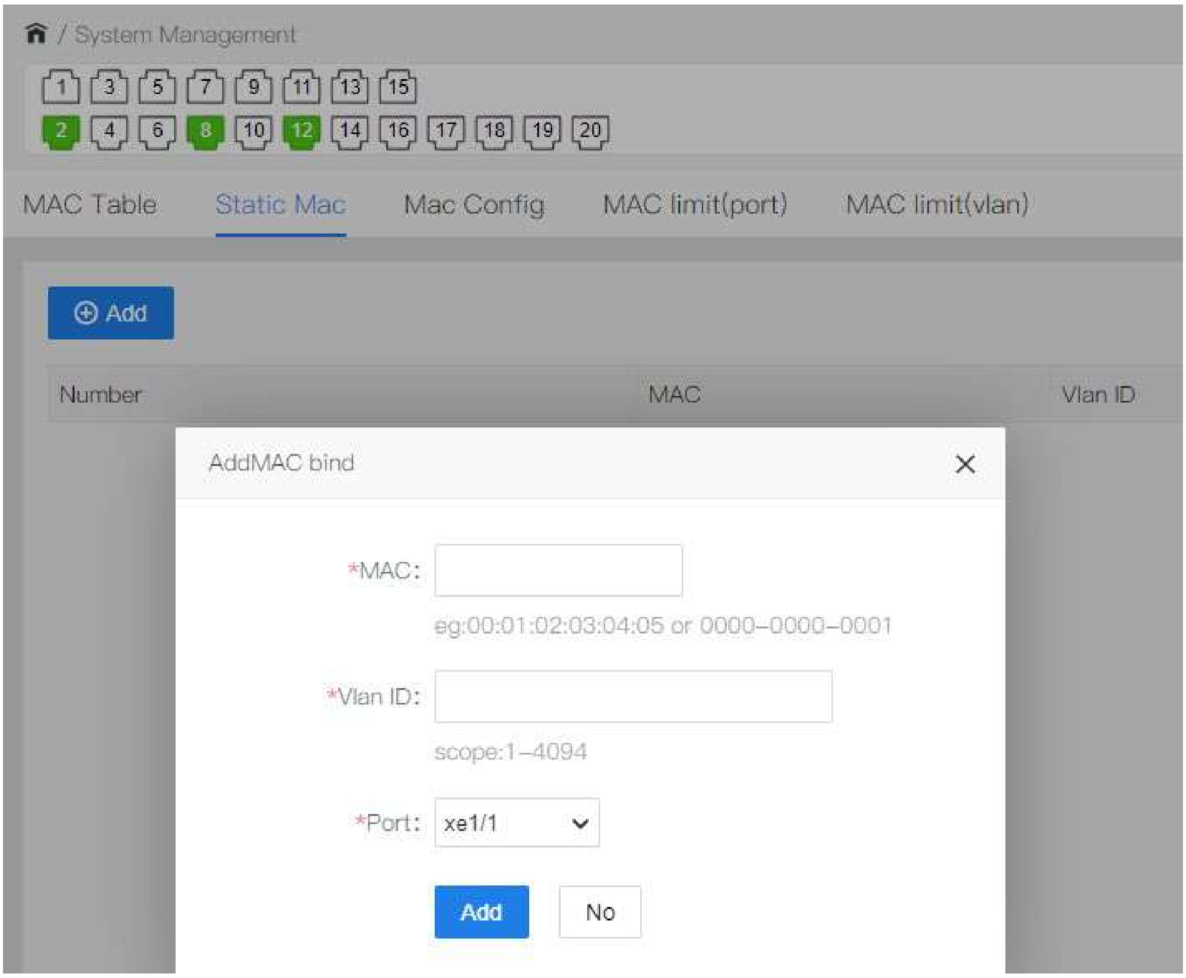
MAC: including MAC table, static Mac, Mac configuration, MAC limi(port), MAC limit(vlan).

3.3.2.1 MAC table



MAC table: A table used by a switch to record the MAC address information of devices connected to its various ports, also known as a MAC address table.

3.3.2.2 Static Mac

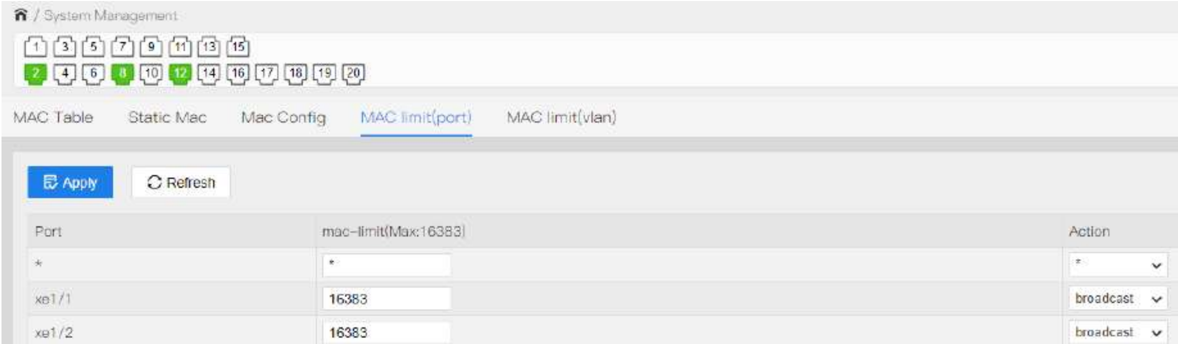


Static Mac: A MAC address that a user manually configures and binds to a specific port of the switch.

3.3.2.3 Mac configuration

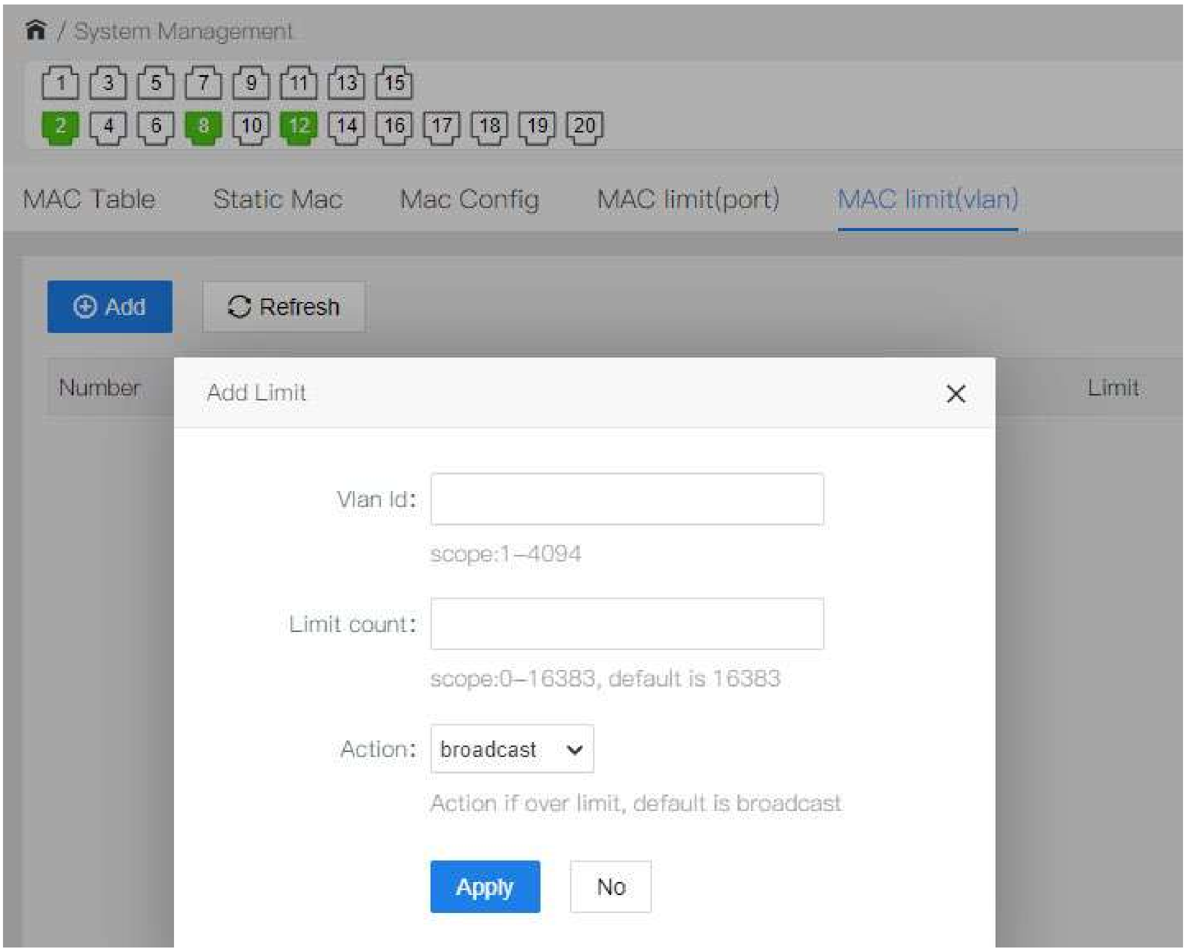
Mac configuration: Setting up various functions and parameters related to the MAC address.

3.3.2.4 MAC limi(port)



MAC limi(port) : Port-based MAC address limit, which is used to set the upper limit of the number of MAC addresses allowed to connect to a certain port of the switch. By setting a "MAC limit (port)" for a specific port, you can control the number of devices connected to that port, prevent unauthorized device access or port abuse, and thereby enhance network security and manageability.

3.3.2.5 MAC limit(vlan)



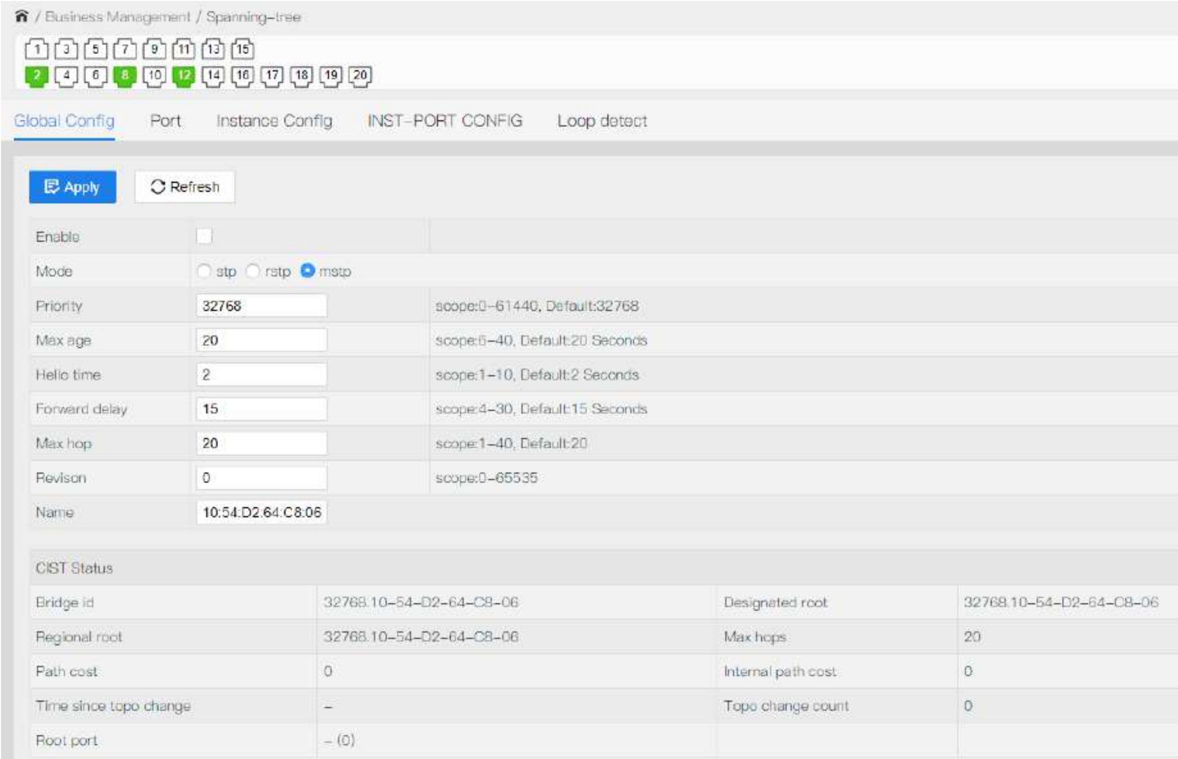
MAC limit(vlan) : MAC address limits based on VLAN.

Name	Description
Vlan Id	A number that uniquely identifies a virtual local area network (VLAN)
Limit count	Limit quantity
Action	The action taken by the switch when the number of MAC addresses reaches a limit

3.3.3 Spanning tree

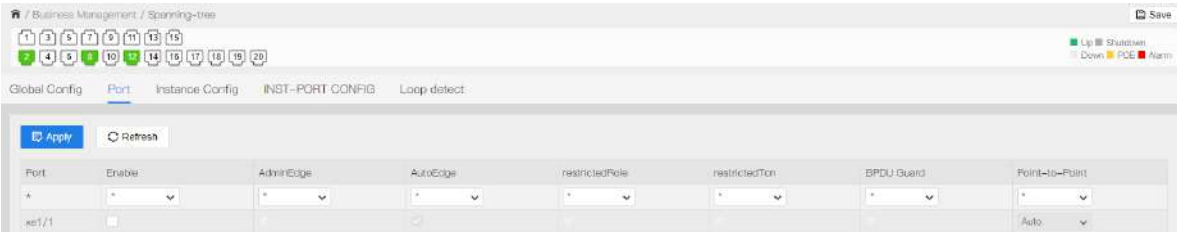
Spanning tree: It includes global layout, port configuration, instance configuration, instance port configuration, and loop detection.

3.3.3.1 Global configuration



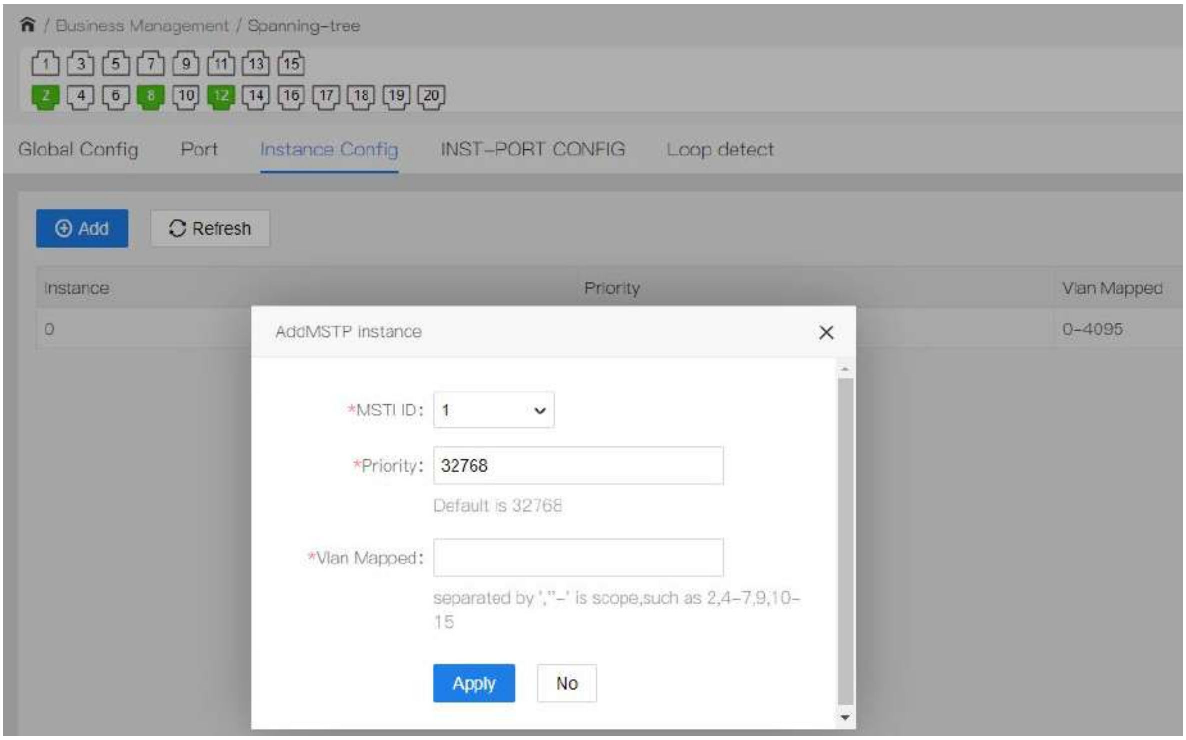
Global configuration: Choose to enable or disable the Spanning Tree protocol feature.

3.3.3.2 Port configuration



Port configuration: Specific parameter Settings for each physical port of the switch in the spanning tree protocol for precise control of port behavior to ensure stable and efficient operation of the network.

3.3.3.3 Instance configuration



Instance configuration: Set the overall runtime parameters and characteristics of the spanning tree to accommodate different network topologies and business requirements.

Name	Description
MSTI ID	Generate the identifier of the tree instance
Priority	Parameters used to determine the role and status of a switch in a spanning tree network
Vlan Mapped	VLAN mapping, which is used to associate and map specific vlans with spanning tree instances

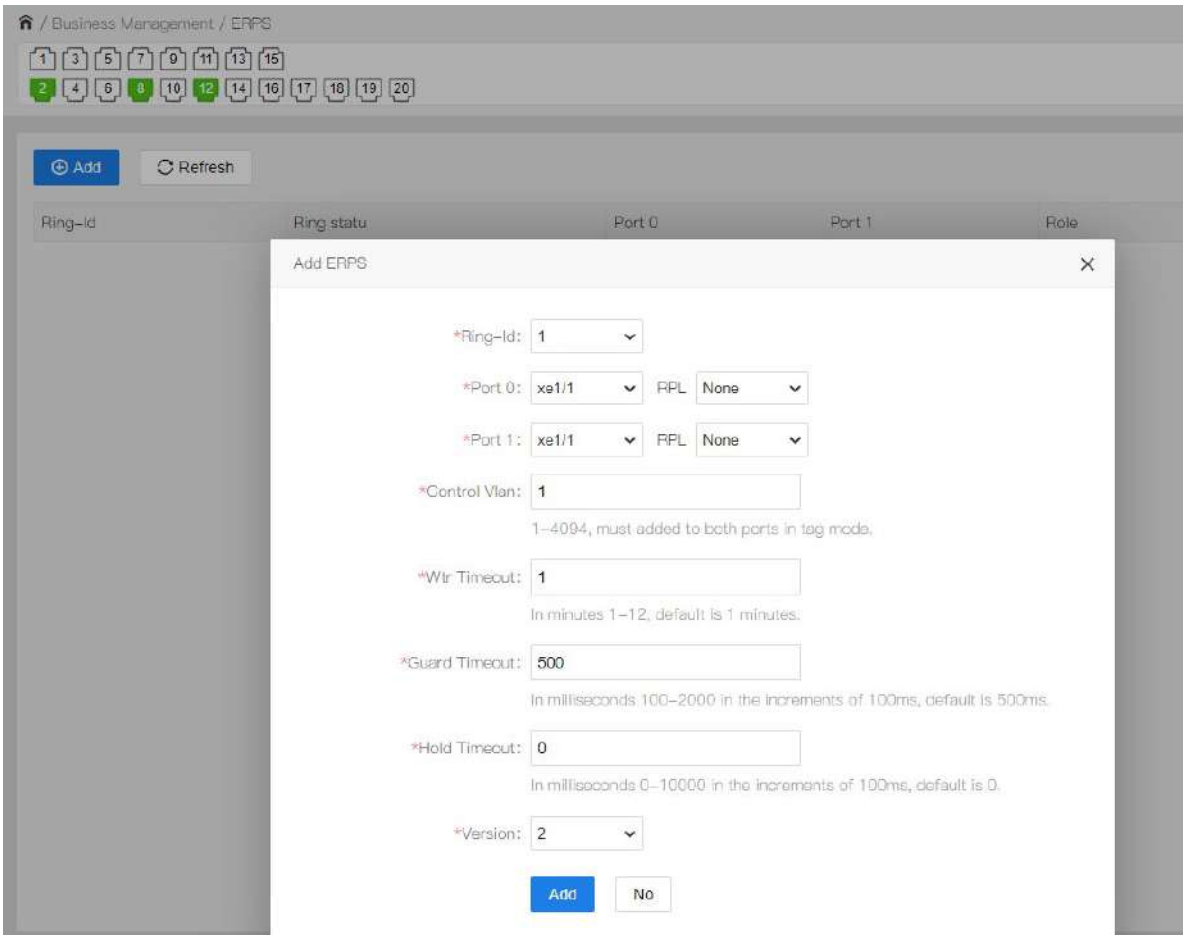
3.3.3.4 Instance Port Configuration

Instance port configuration: Detailed Settings for each port in a spanning tree instance, mainly used to control the behavior of ports in the spanning tree network.

3.3.3.5 Loop detection

Loop detection: A function used to monitor and prevent loops in a network.

3.3.4 ERPS

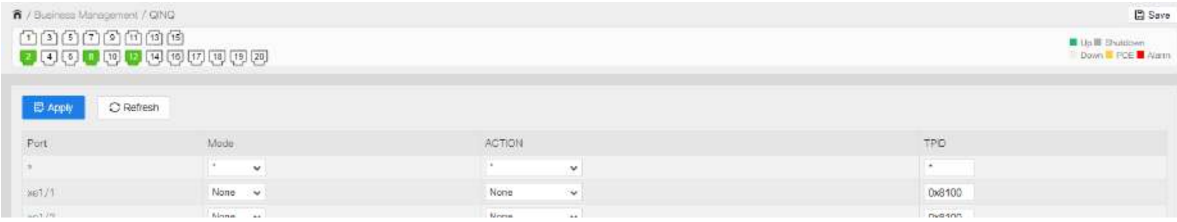


ERPS: A link layer protocol specifically designed for Ethernet ring networks, which can prevent broadcast storms caused by data loops when the Ethernet ring network is intact, and can quickly restore communication between nodes on the Ethernet ring network when a link is broken.

Name	Description
Ring-Id	The unique identifier used to identify different ERPS rings in the Ethernet Ring protection switching protocol
Port 0	Select the port
Port 1	Select the port
Control Vlan	A VLAN dedicated to carrying ERPS protocol control messages. Management and Control of the ERPS ring network can be achieved by encapsulating the ERPS control message in a specific Control Vlan for

	transmission
Wtr Timeout	It is an important parameter in the ERPS protocol used to set the time a port waits to return to its normal forwarding state after a link failure has recovered
Guard Timeout	Protect timeout times
Hold Timeout	Keep the timeout time
Version	Version number of the ERPS protocol

3.3.5 QINQ

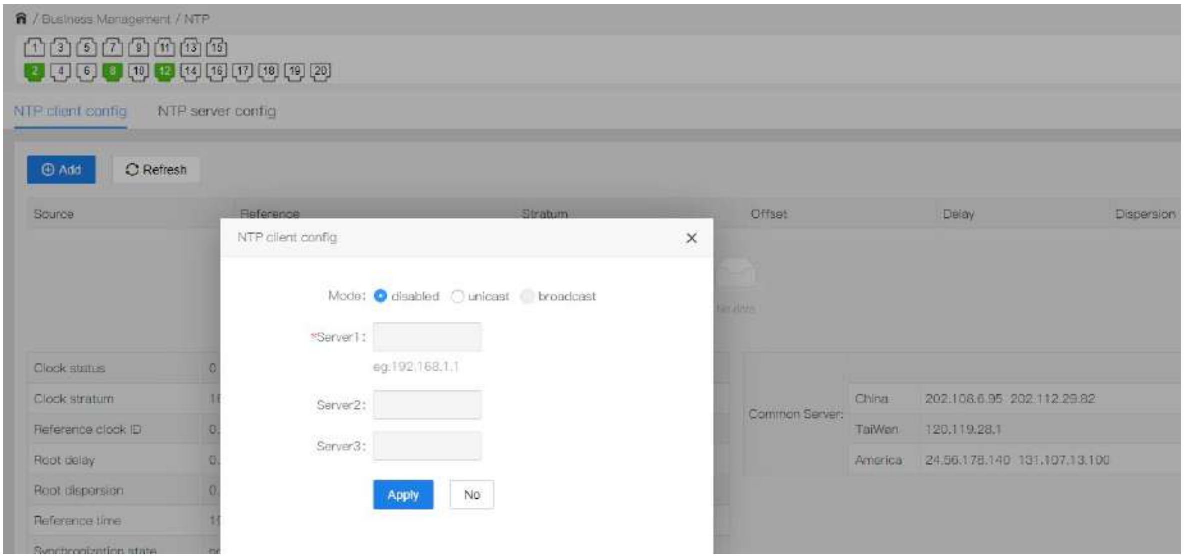


QINQ: Its main function is to add an additional layer of VLAN tags on the basis of the existing VLAN (Virtual Local Area Network), forming a two-layer VLAN tag structure to achieve a more flexible network topology and user management.

3.3.6 NTP

NTP: It includes both NTP client configuration and NTP server configuration.

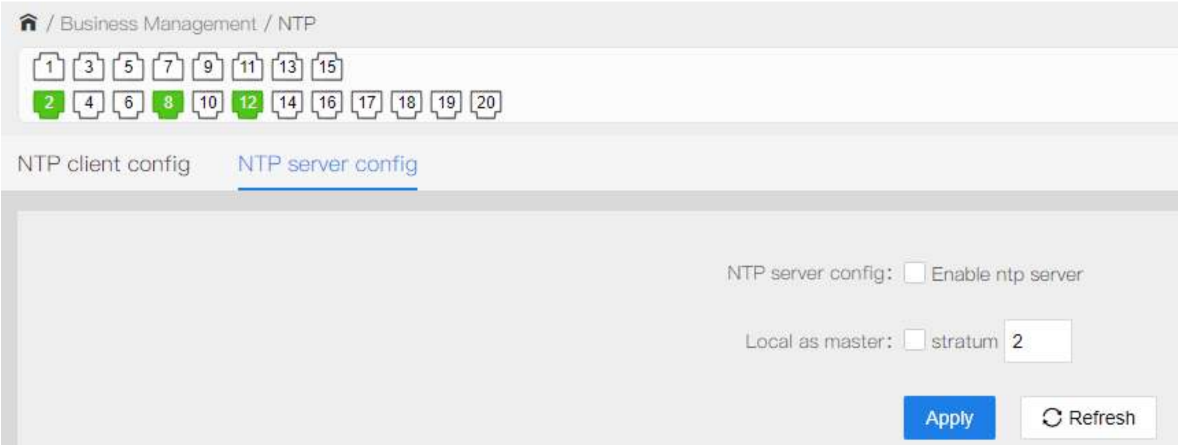
3.3.6.1 NTP client configuration



NTP client configuration: Use the switch as an NTP client and set the parameters related to its interaction with the NTP server and synchronization of time.

Name	Description
Patterns	Select mode Toggle
Server 1	Select the server IP address
Server 2	Select the server IP address
Server 3	Select the server IP address

3.3.6.2 NTP server configuration

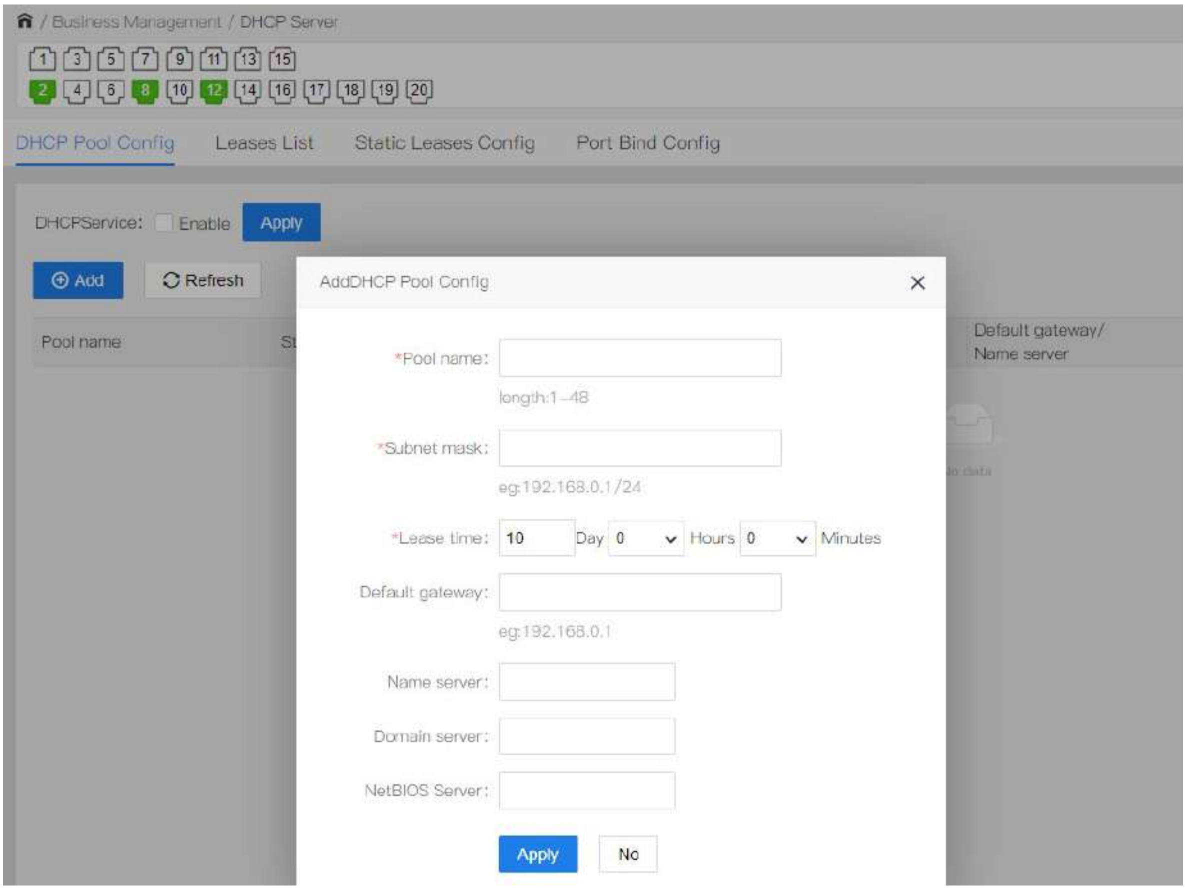


NTP server configuration: The function of setting network time protocols and related parameters of the server.

3.3.7 DHCP Server

DHCP Server: Dynamic Host Configuration Protocol Server.

3.3.7.1 DHCP Pool Config



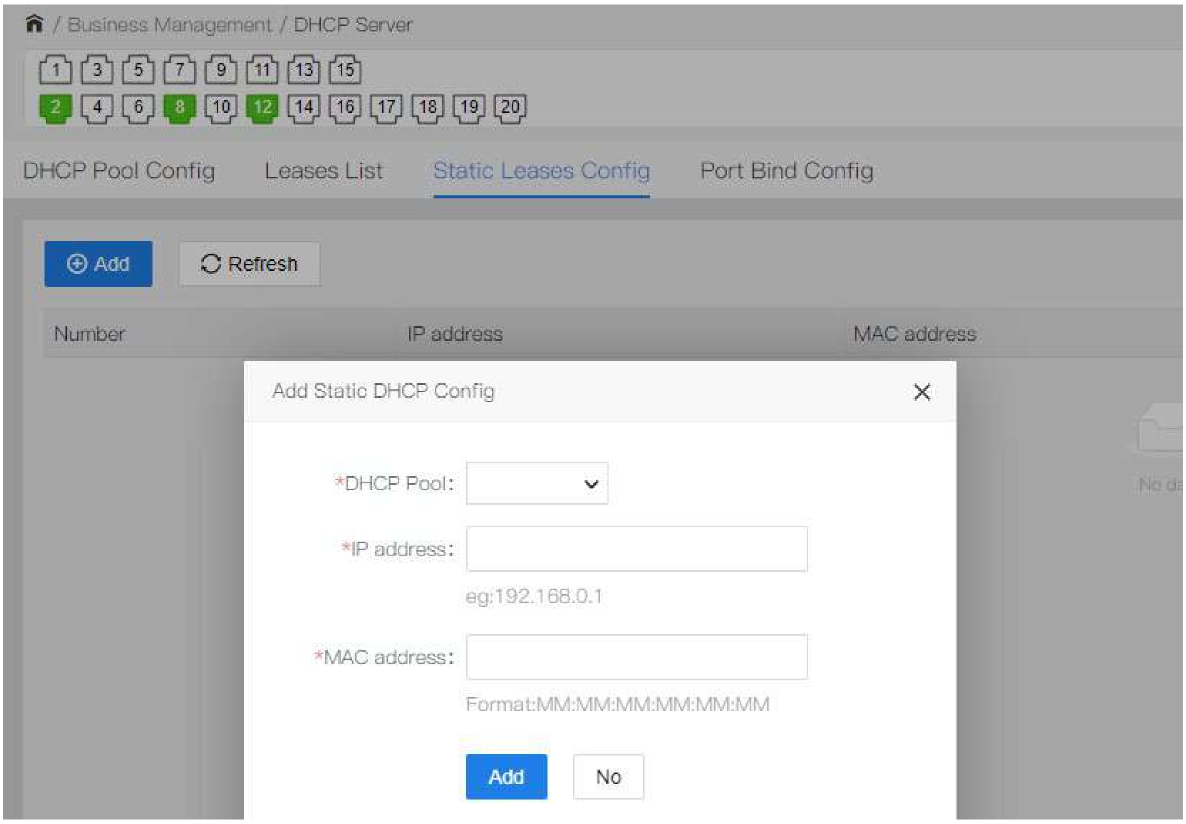
DHCP Pool Config: Dynamic Host Configuration Protocol (DHCP) address pool configuration.

Name	Description
Pool name	DHCP address pool name
Subnet mask	Subnet mask
Lease time	Lease time
Default gateway	Default gateway
Name server	Domain name server
Domain server	A specific related domain name server
NetBIOS Server	NetBIOS Name server

3.3.7.2 Leases List

Youdaoplaceholder0 List: A list of Leases.

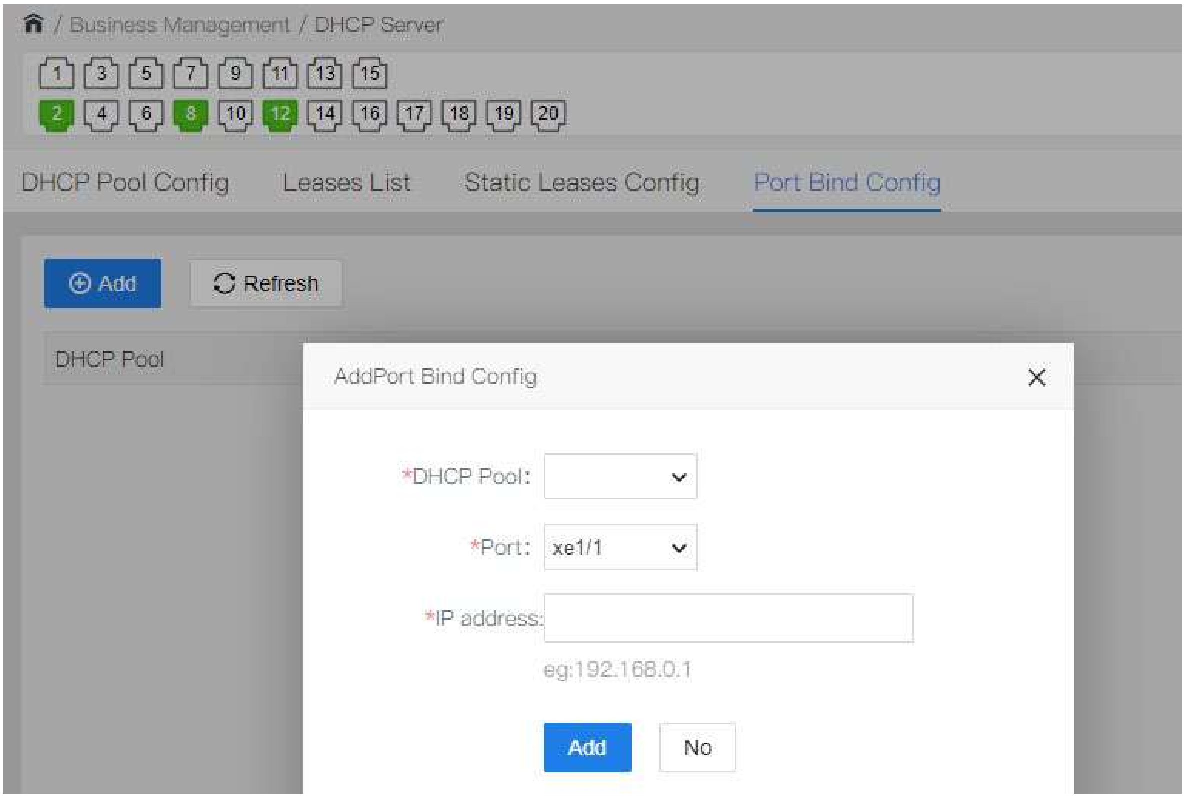
3.3.7.3 Static Leases Config



Static Leases Config: Lease list configuration.

Name	Description
DHCP Pool	DHCP Address Pool
IP address	IP address
MAC address	MAC address

3.3.7.4 Port Bind Config



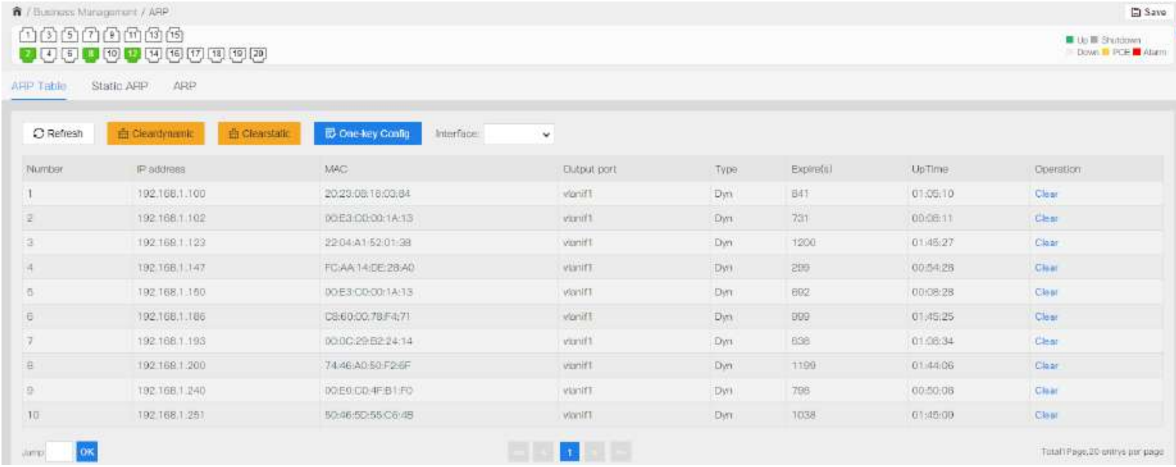
Port Bind Config: Server port binding configuration.

Name	Description
DHCP Pool	DHCP Address Pool
Port	Select a port
IP address	Custom IP address

3.3.8 ARP

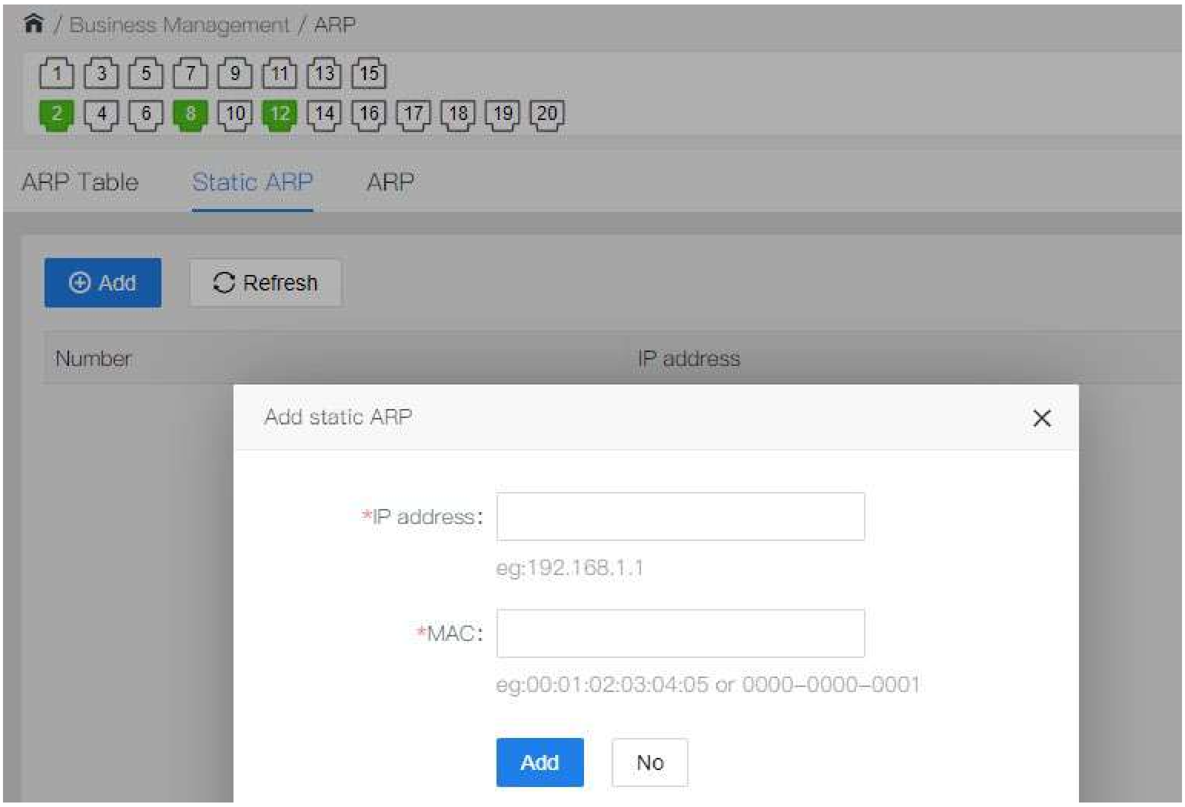
ARP: It includes three types: ARP table, static ARP, and ARP.

3.3.8.1 ARP Table



ARP table: Address Resolution Protocol Table.

3.3.8.2 Static ARP



Static ARP: Static Address Resolution Protocol Table.

Name	Description
IP address	Custom IP address
MAC	Custom MAC address

3.3.8.3 ARP

ARP: Address Resolution Protocol.

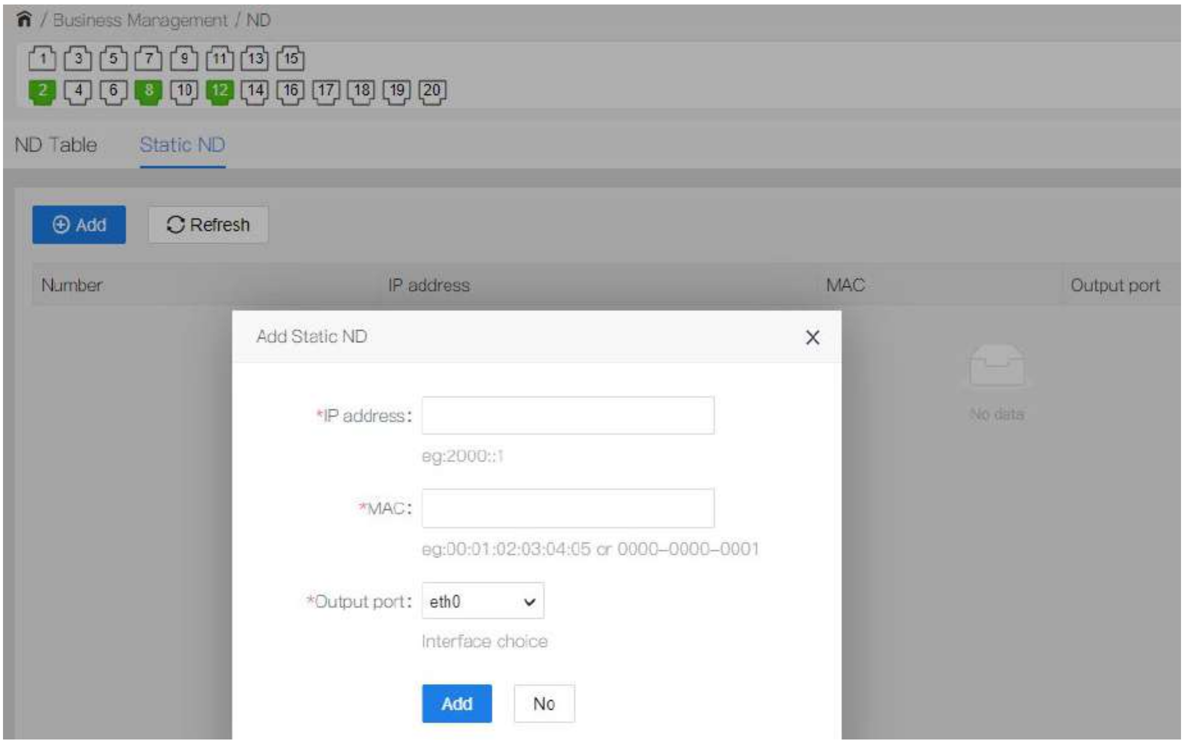
3.3.9 ND

ND: includes ND Table and Static ND.

3.3.9.1 ND Table

ND Table: Neighbor Discovery Protocol (NDP) table.

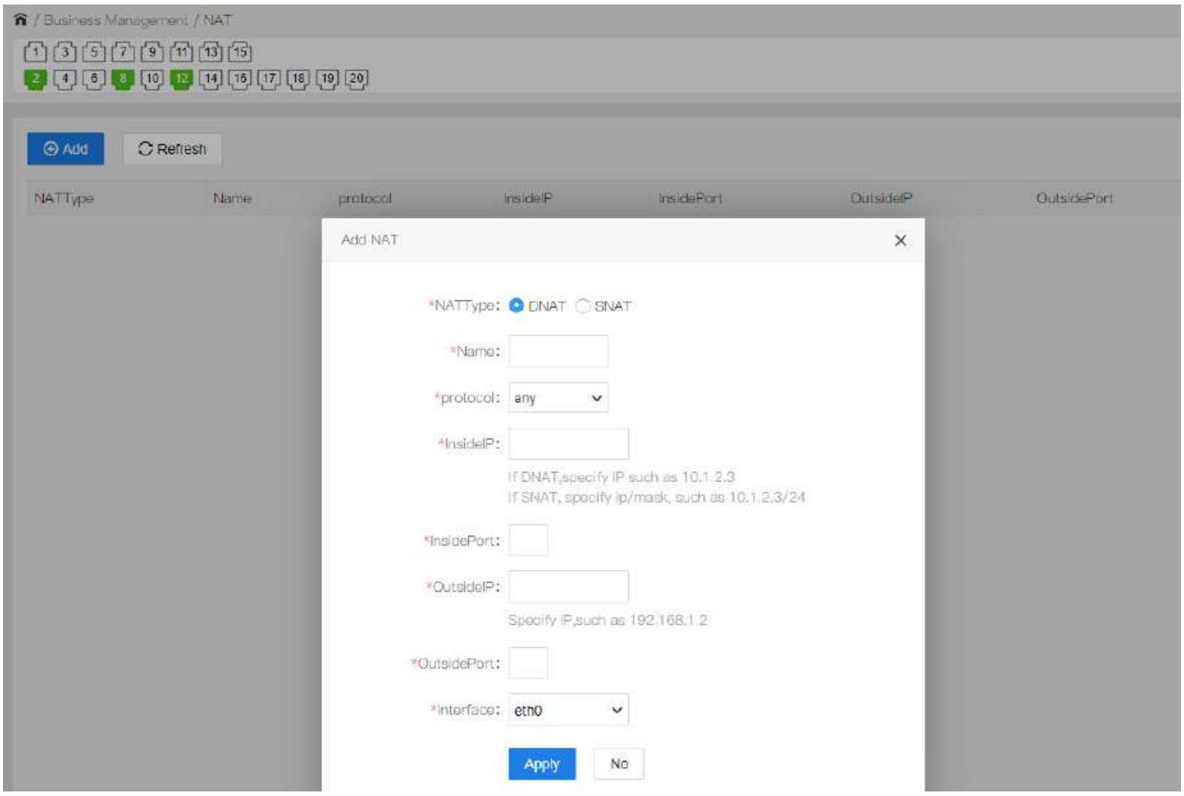
3.3.9.2 Static ND



Static ND: Static neighbor discovery.

Name	Description
IP address	Custom add IP addresses
MAC	Access control addresses, also known as physical addresses or hardware addresses
Exit interface	An exit interface refers to the physical or logical interface that a switch uses to send data packets to a target device.

3.3.10 NAT



NAT: Network Address Translation.

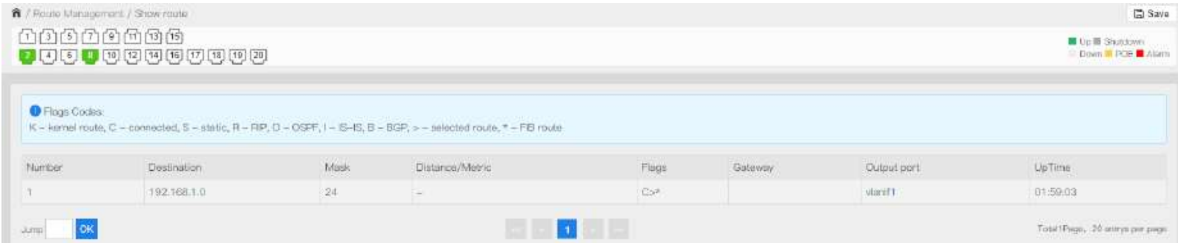
Name	Description
NATType	Network address translation type
Name	Name
protocol	Agreement
InsideIP	Internal network device IP address
InsidePort	Port number
OutsideIP	External network device IP address

OutsidePort	Port number
Interface	Interface

3.4 Route Management

Expand this setup and you can make Settings such as View Routes, Static Routes, RIP, OSPF, VRRP, NQA, etc.

3.4.1 View the Route

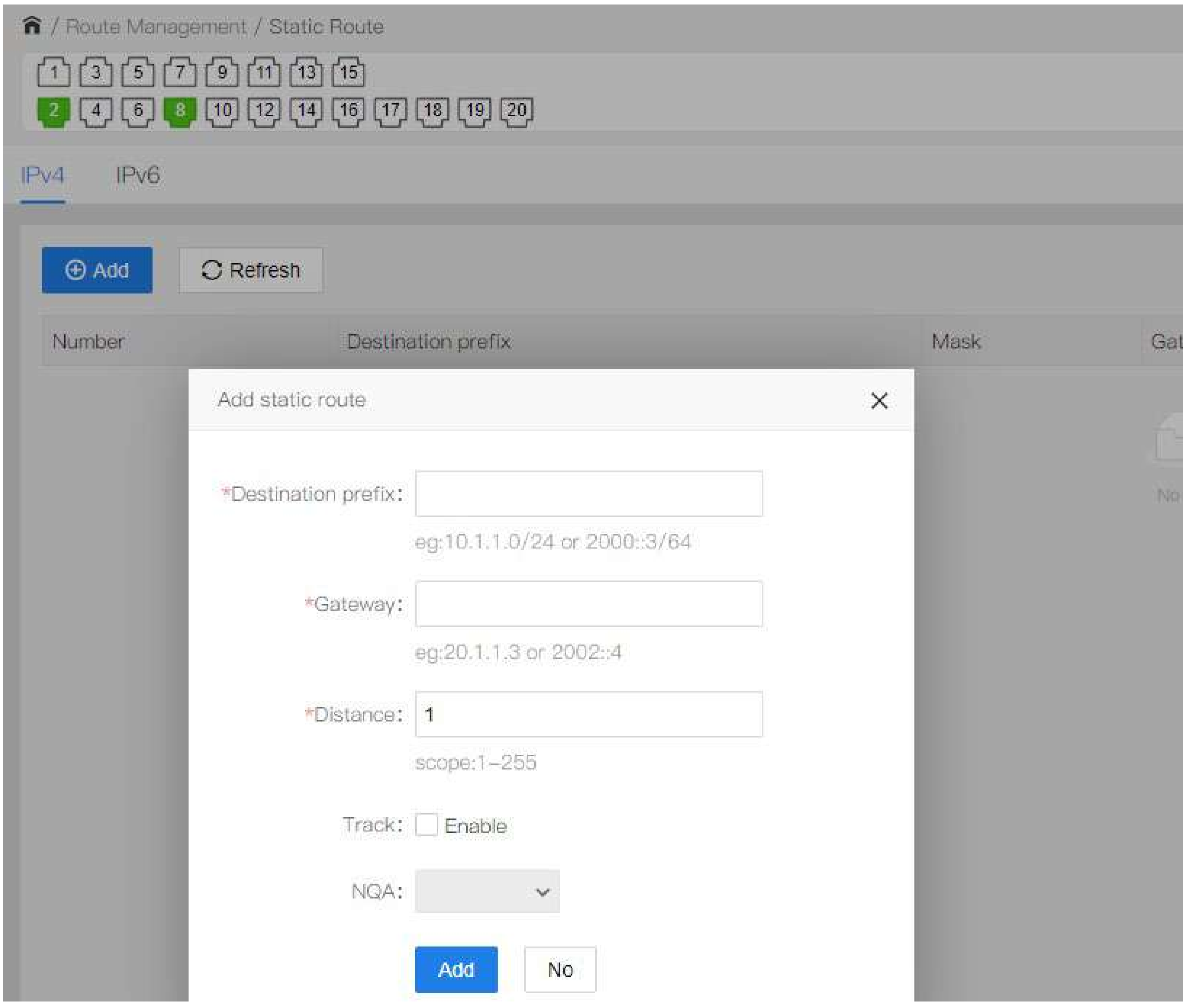


View routes: Administrators can view the current routing table information of the switch.

3.4.2 Static routing

Static routing: It includes two types, IPv4 and IPv6.

3.4.2.1 IPv4

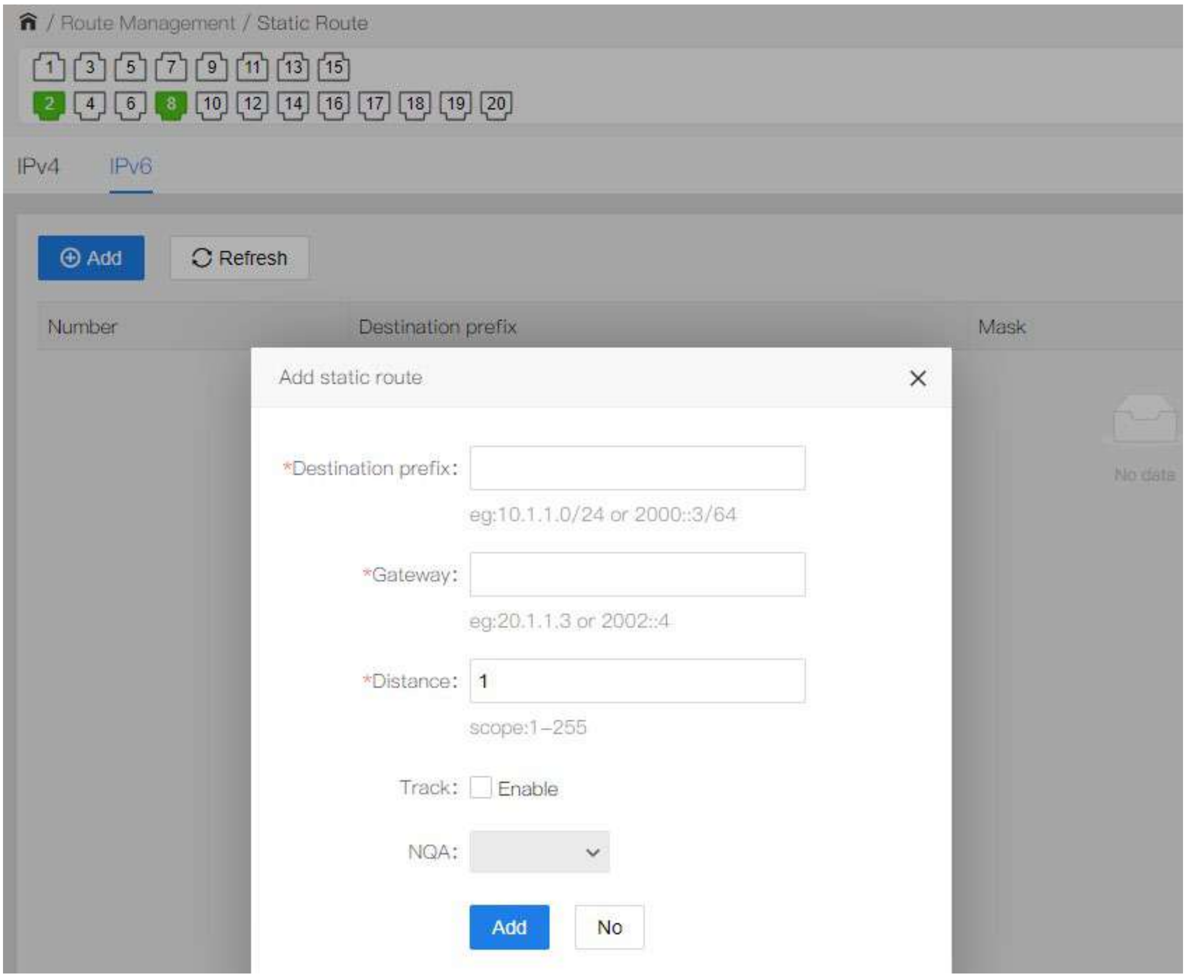


IPv4: IPv4, short for Internet Protocol Version 4, is a widely used network layer protocol that enables communication and data transmission between devices in a network.

Name	Description
Destination in prefix	Custom IP address
Gateway	Custom gateway address
Distance	A routing metric, or hop count, is used to measure the cost of a path to the destination network
Monitoring	Switch/Enable

NQA	Network Quality analyzer

3.4.2.2 IPv6



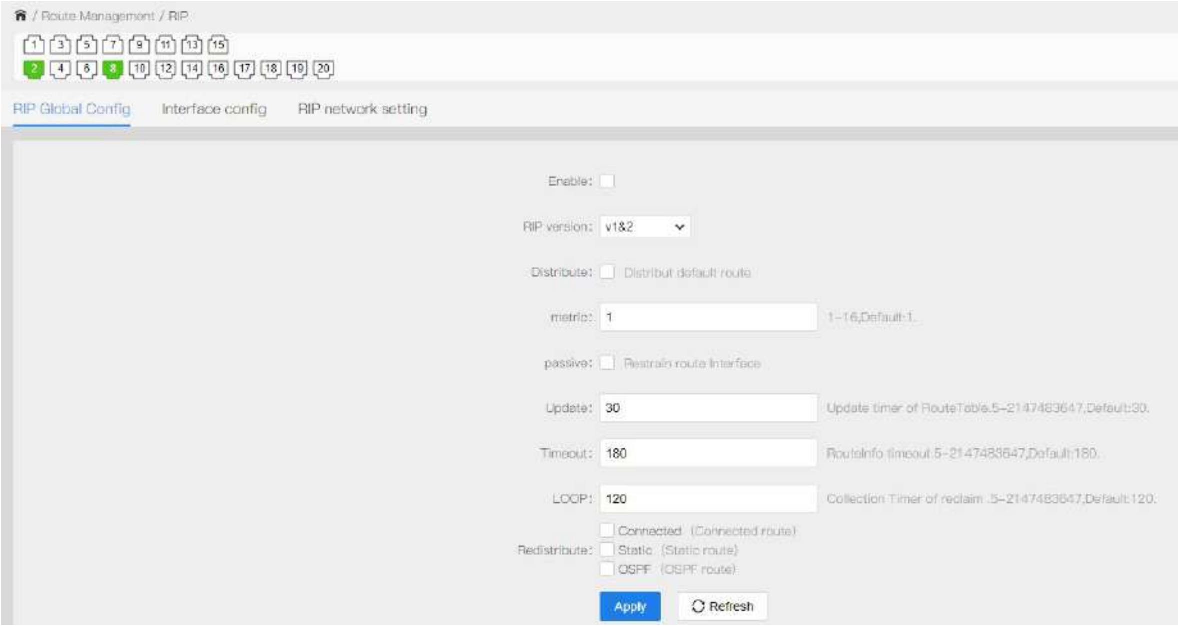
IPv6: An abbreviation for Internet Protocol Version 6, it is a new generation of network layer protocol designed to replace IPv4.

Name	Description
Destination in prefix	Custom IP address
Gateway	Custom gateway address
Distance	A routing metric, or hop count, is used to measure the cost of a path to the destination network
Monitoring	Switch/Enable
NQA	Network Quality analyzer

3.4.3 RIP

RIP: It includes RIP global configuration, interface configuration, and RIP network configuration.

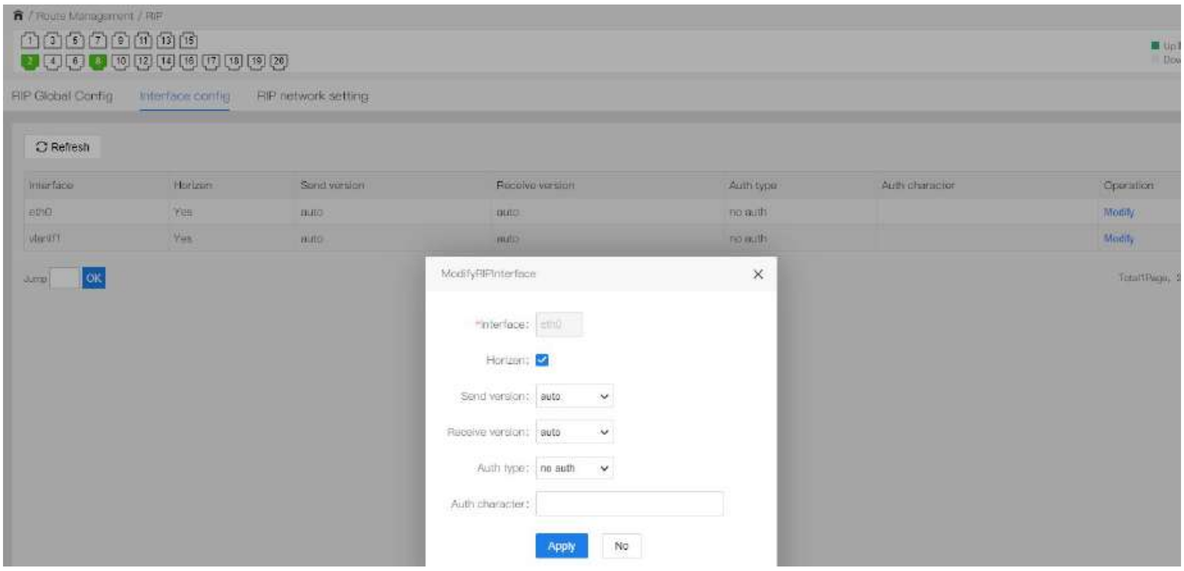
3.4.3.1 RIP Global Configuration



RIP global configuration: The overall Settings made for the RIP (Routing Information Protocol) running across the entire switch.

Name	Description
Start	Switch/Enable
RIP version	The specific version of the RIP routing protocol used by the switch
Allocation	Switch/Enable
Metrics	Numbers that measure the quality of a route
Passive	Switch/Enable
Updates	Time interval/Event-triggered update/Routing information update
Timeout	When a routing information is not updated within a certain period of time, the switch will consider that there may be a problem or failure with the route
Loop	Loop processing in the horizontal segmentation reversal mechanism
Redistribution	Introduce routing information from other routing protocols or different routing processes into the RIP protocol, or redistribute RIP routing information to other routing protocols or different RIP processes in order to achieve routing information sharing among different routing domains

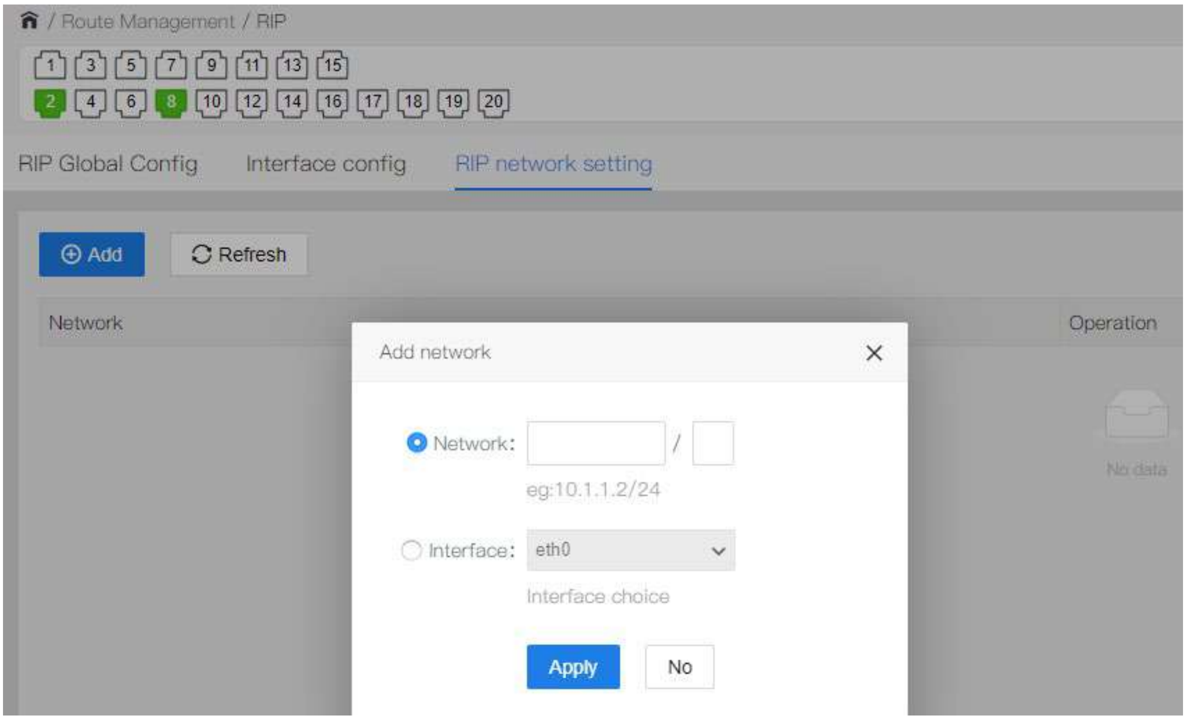
3.4.3.2 Interface configuration



Interface configuration: Set parameters related to routing functions for each interface of the switch. By configuring the interface, you can precisely control how the routing protocol operates on each interface, ensuring the correct exchange of routing information and data forwarding between the switch and other network devices.

Name	Description
Horizontal segmentation	A technique for preventing routing loops, mainly used in distance vector routing protocols
Send version	The version of the protocol that a switch uses when sending routing protocol information through a specific interface
Accepted version	The specific interface of the switch is prepared to receive and process the version of the routing protocol information
Authentication type	Ensure that only authorized devices can participate in the exchange of routing information, enhance the security of the network, and prevent illegal devices from accessing and tampering with routing information
Authentication characters	The key information for authentication, also known as the authentication key

3.4.3.3 RIP Network configuration



RIP network configuration: refers to setting up Routing functions based on RIP (Routing Information Protocol) to enable the exchange of routing information and path selection between routers in a network.

 Network: Custom IP address

 Interface: Custom select interface mode

3.4.4 OSPF

OSPF: It includes OSPF global configuration, interface configuration, OSPF network configuration, and OSPF neighbors.

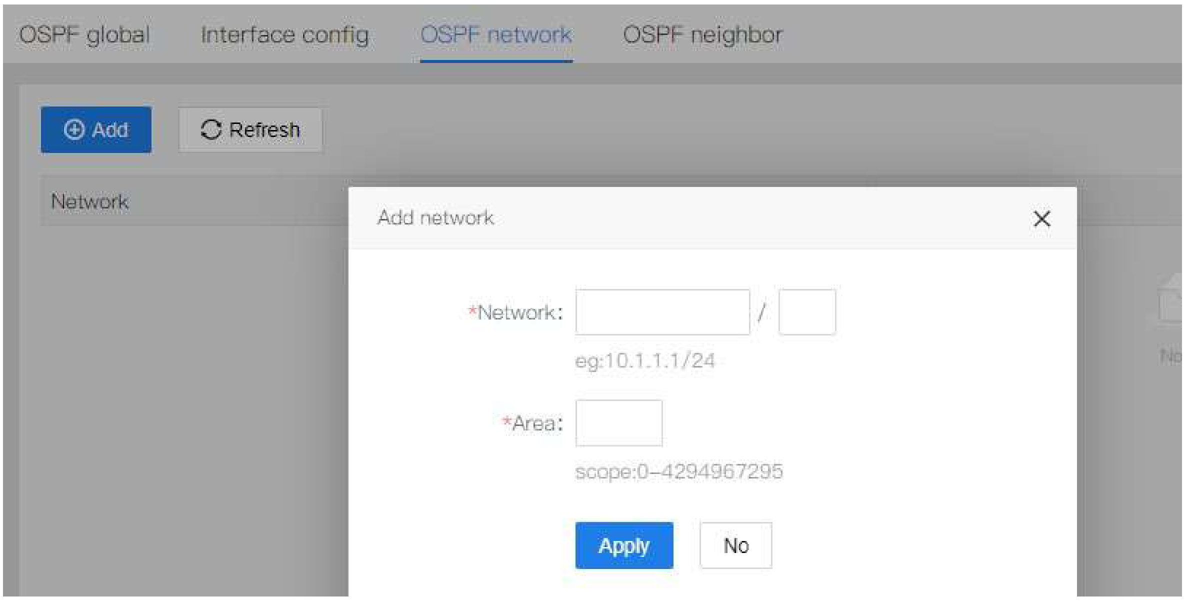
3.4.4.1 OSPF Global Configuration

OSPF Global configuration: OSPF Global configuration is the setting of overall parameters and functions for the entire OSPF protocol to run on a switch, and these Settings have a global impact on all OSPF processes and related interfaces on the switch.

3.4.4.2 Interface Configuration

Interface configuration: Set parameters related to OSPF for specific physical or logical interfaces on the switch.

3.4.4.3 OSPF Network configuration



OSPF network configuration: Used to set the operating parameters and working mode of a switch in an OSPF protocol-based network for efficient routing and network communication.

 Network: Different segments or subnets connected to the switch, the main purpose of configuring the "network" is to enable the switch to communicate with other devices in these networks via the OSPF protocol and to achieve routing functions.

 Shore: It is an important concept for the logical division of an OSPF network.

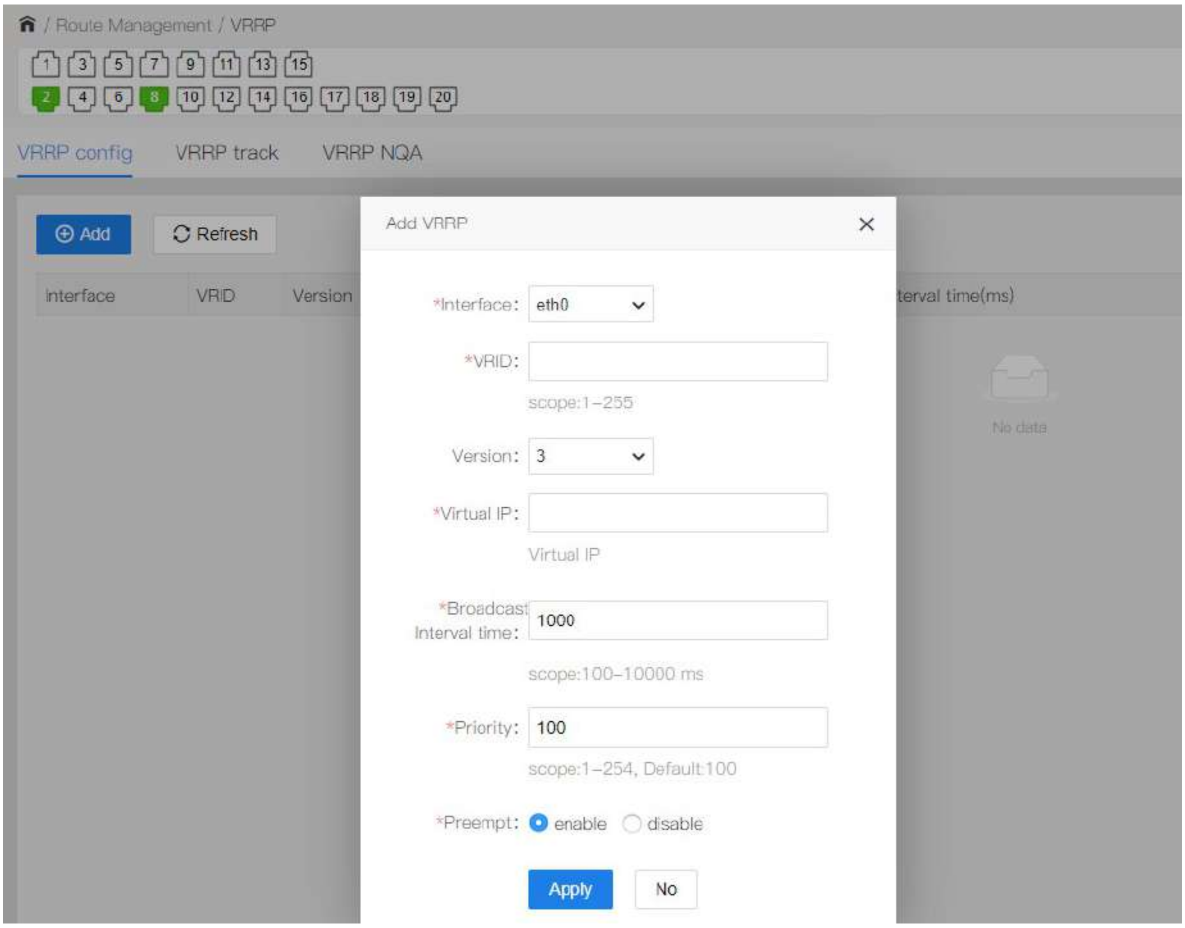
3.4.4.4 OSPF Neighbors

OSPF neighbor: Other routers that have established an adjacency relationship with this switch via the OSPF protocol.

3.4.5 VRRP

VRRP: Includes VRRP configuration, VRRPP monitoring, and VRRP NQA.

3.4.5.1 VRRP configuration

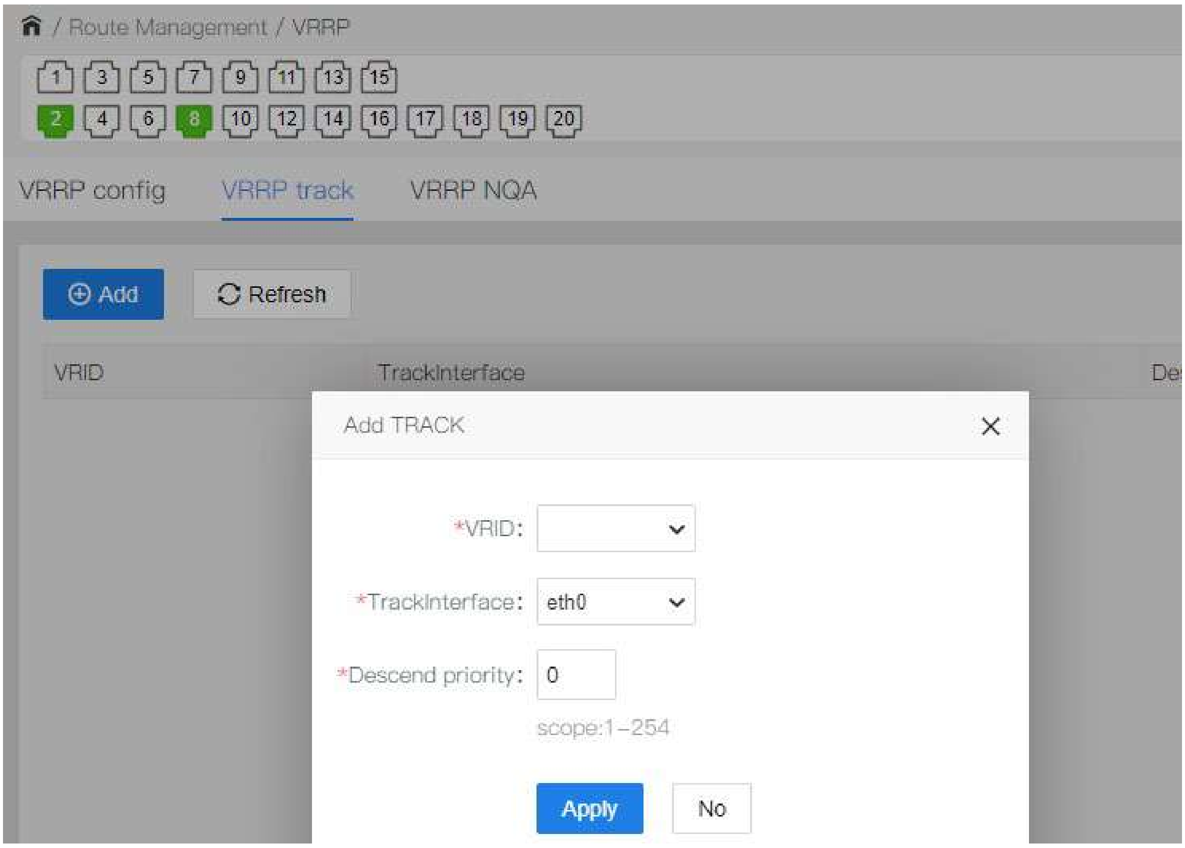


VRRP configuration: Setting relevant parameters for the redundancy protocol of the virtual router to achieve network reliability and fault tolerance.

Name	Description
Interface	A specific physical or logical interface used by VRRP to monitor the state of the network.
VRID	Virtual router identification
Version	Different version numbers of the Virtual Router Redundancy Protocol (VRRP)
Virtual IP	A virtual IP is a logical IP address that does not actually exist on a certain physical device but is jointly maintained by the routers in the VRRP group
AD intervals	The time interval for the main router to send VRRP notification messages
Priority	Important parameters for determining the roles of each router in the VRRP

	group
Preemption	A mechanism for router role switching in a VRRP group

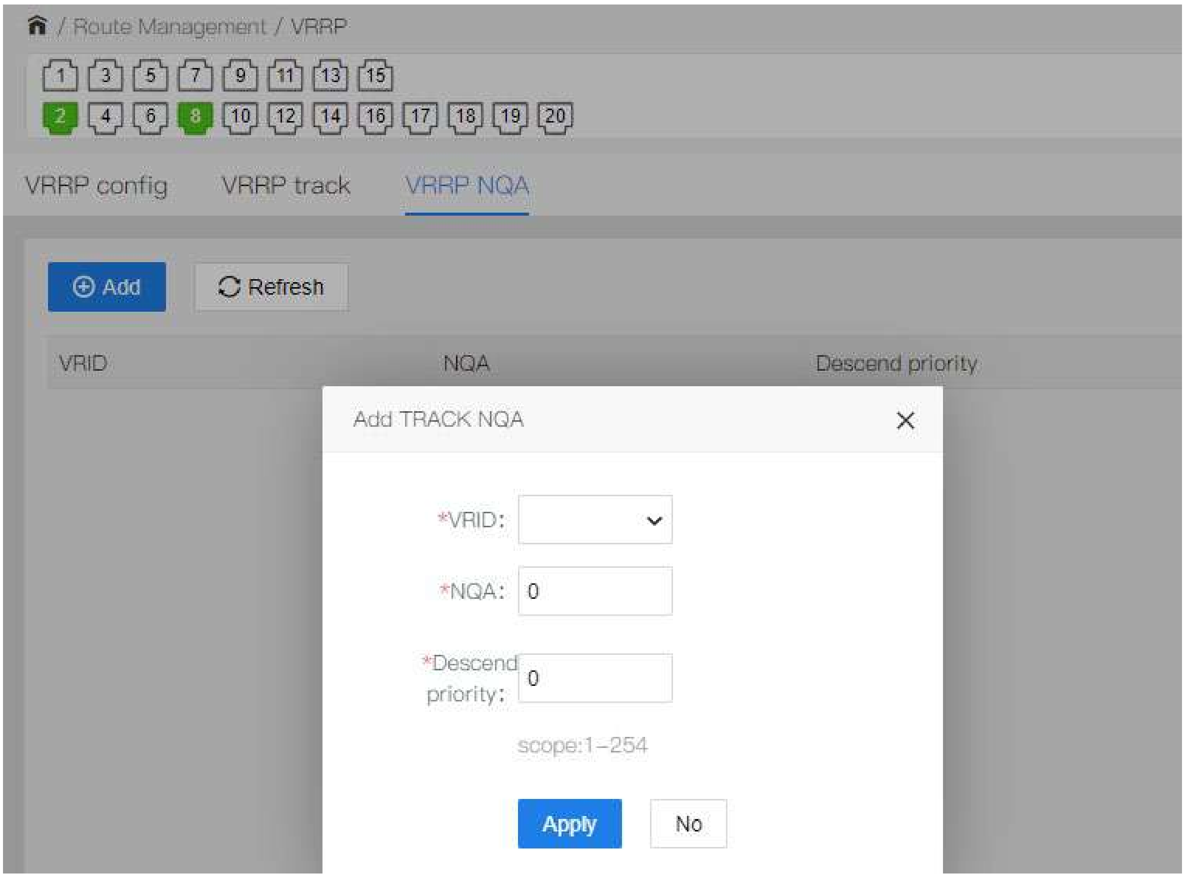
3.4.5.2 VRRPP monitoring



VRRPP monitoring: The function of real-time monitoring of the relevant operational status and parameters of the Virtual Router Redundancy Protocol (VRRP).

Name	Description
VRID	Virtual router identification
Monitor Interface	A specific physical or logical interface used by VRRP to monitor the state of the network
Downpriority	A mechanism that dynamically lowers the priority of a router based on NQA's monitoring of network status when VRRP is used in combination with NQA

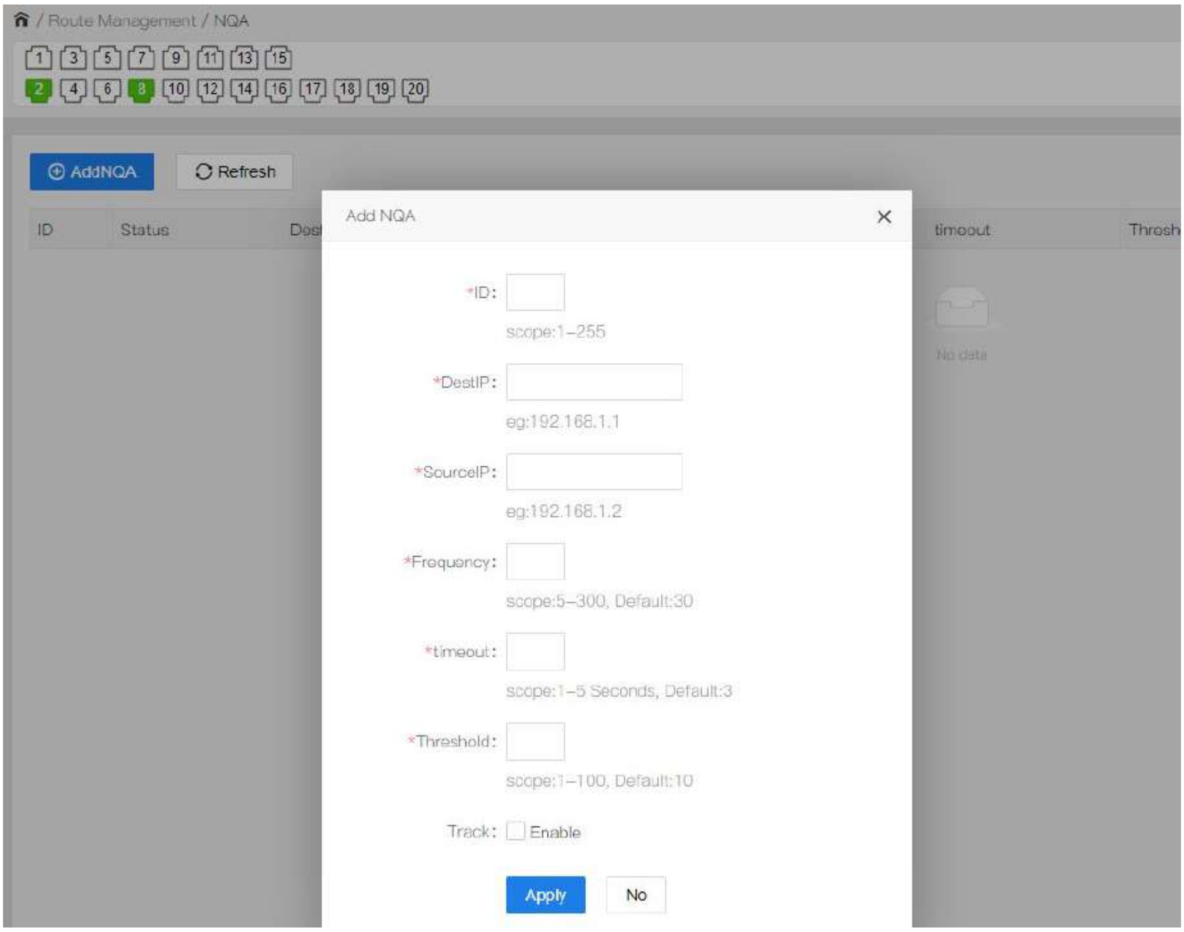
3.4.5.3 VRRP NQA



VRRP NQA: A feature that combines the Virtual Router Redundancy Protocol (VRRP) with Network Quality Analysis (NQA).

Name	Description
VRID	Virtual router identification
NQA	It is primarily used for real-time monitoring of network performance metrics such as latency, packet loss rate, jitter, etc
Descent priority	It refers to the mechanism of dynamically reducing the priority of a certain router based on the monitoring results of NQA on the network status when VRRP is used in combination with NQA

3.4.6 NQA

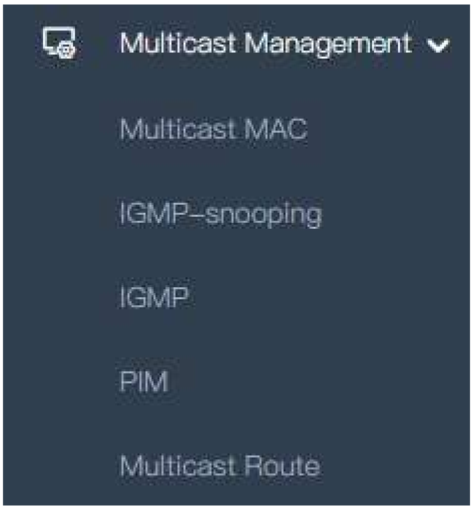


NQA: Network quality analysis.

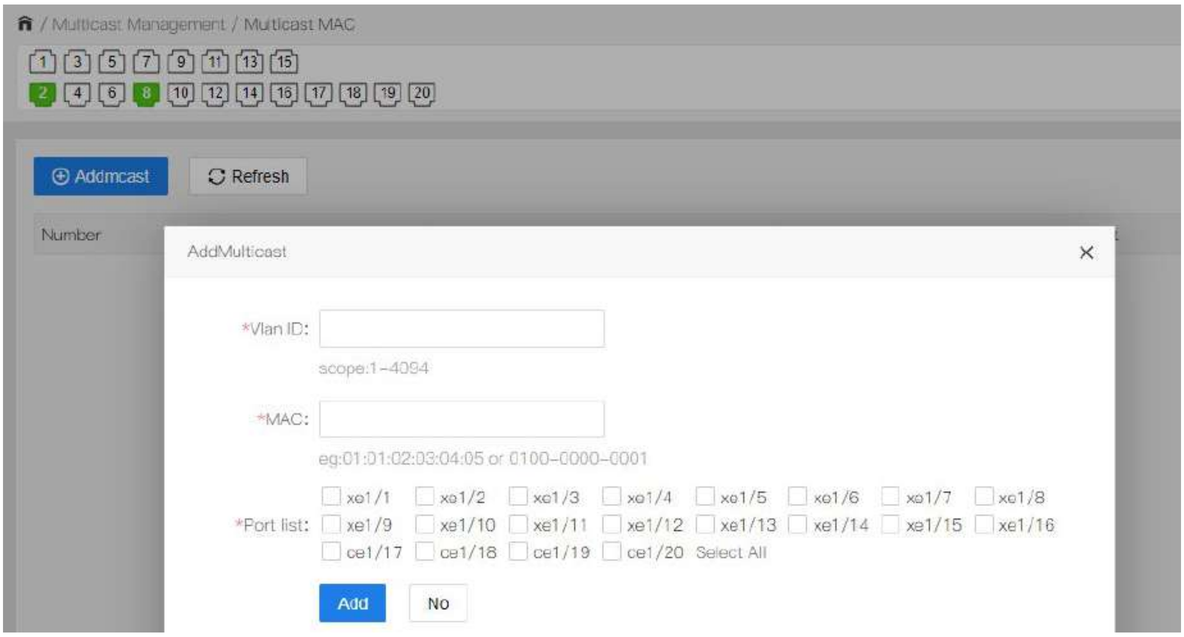
Name	Description
ID	Customize your ID
Destination IP	The IP address of the target device to which the NQA probe message is to be sent
Source IP	The source address used when the NQA probe message is sent, that is, the IP address of the interface configured on the switch for sending the probe message.
Frequency	The time interval for NQA to send probe messages.
Timeout	The maximum time that the switch waits to receive the corresponding response message after sending the NQA probe message.
Threshold	A key indicator limit value used to judge the performance status of the network.
Monitoring	Enable/Turn off switches

3.5 Multicast Management

Expand this setup and you can set up multicast MAC, IGMP-Snooping, IGMP, PIM, multicast routing, etc.



3.5.1 Multicast MAC



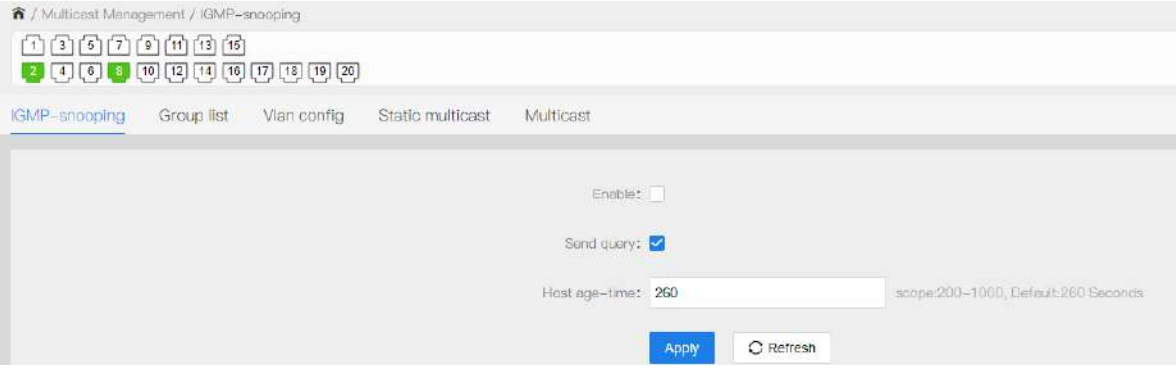
Multicast MAC: A special MAC address used to identify multicast groups at the data link layer.

Name	Description
Vlan ID	Customize your ID
MAC	Customize your MAC Settings
Port list	All ports

3.5.2 IGMP-snooping

IGMP-snooping: It includes four types: IGMP-snooping, Group list, Vlan configuration, and static multicast.

3.5.2.1 IGMP-snooping



IGMP-snooping: The meaning of peer group management protocol snooping.

 Enable: switch

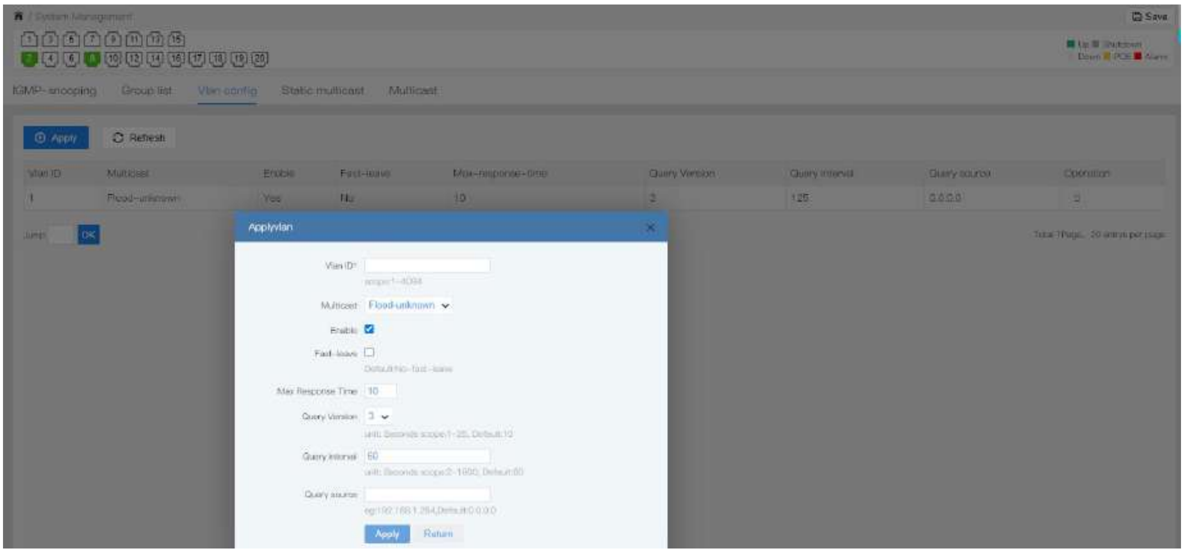
 Active query: A mechanism by which the switch actively sends IGMP query messages to know the status of multicast group members.

 Host aging time: The time set by the switch to wait for a host to be removed from the multicast group member list if it has not received an IGMP report message or specific relevant information from a host.

3.5.2.2 Group list

Group list: Refers to a list of multicast groups.

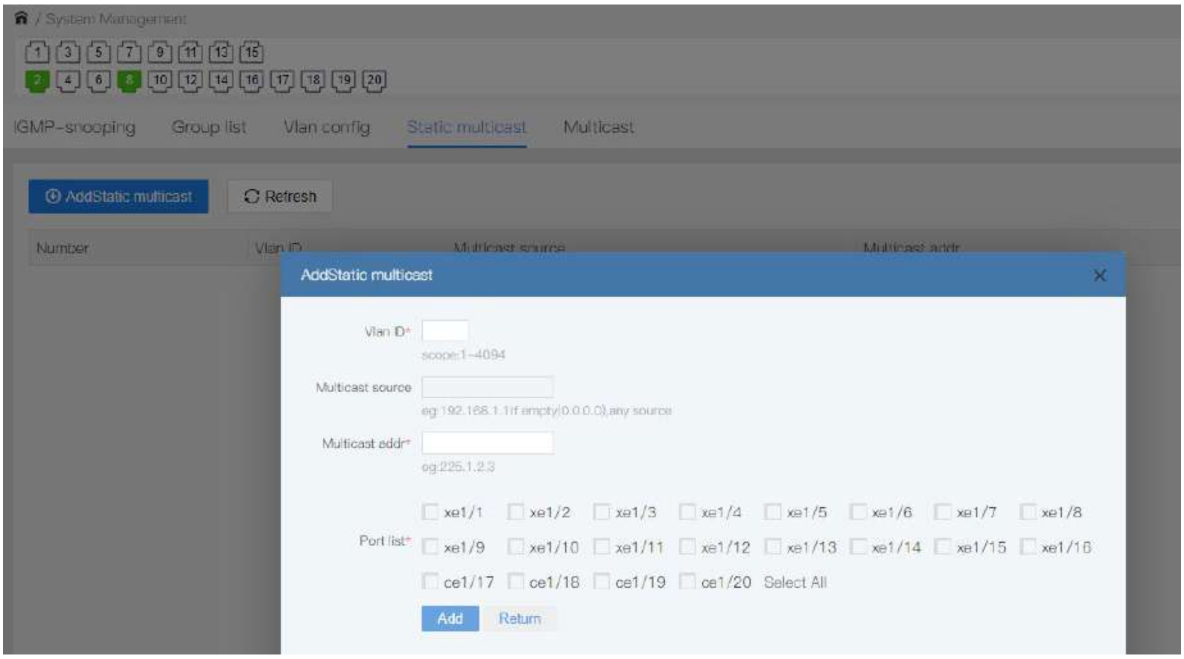
3.5.2.3 Vlan configuration



Vlan configuration: Associate and configure multicast functionality with a specific virtual local area network (VLAN).

Name	Description
Vlan ID	Identification of a virtual local area network (VLAN)
Multicast	A network communication method that allows a data source to send the same data to multiple target devices simultaneously without the need to establish separate connections and send data to each target device.
Enable	Enable
Get off multicast quickly	Quick Leave multicast is a mechanism that optimizes the handling of multicast members leaving.
Max Response Time	Maximum response time
Active Query	The switch actively sends query messages to connected devices to learn about the members of the multicast group in the network.
Query Version	Query version
Query message intervals	The time interval for the switch to send multicast query messages.
Query the source address of the message	The source IP address used by the switch when sending multicast query messages.

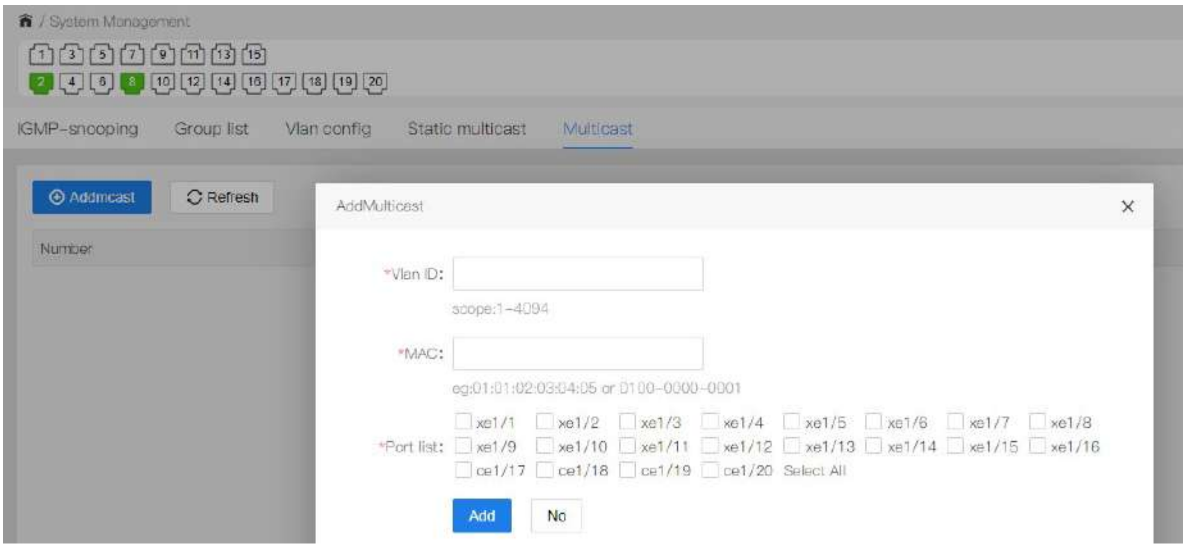
3.5.2.4 Static multicast



Static multicast: It means setting multicast parameters on a switch through manual configuration, allowing specific multicast traffic to be forwarded along pre-set paths and rules.

Name	Description
Vlan ID	Identification of a virtual local area network (VLAN)
Multicast source	The device or node that initiates the multicast data transmission
Multicast address	A special IP address used to identify a multicast group
Port list	All ports

3.5.2.5 Multicast



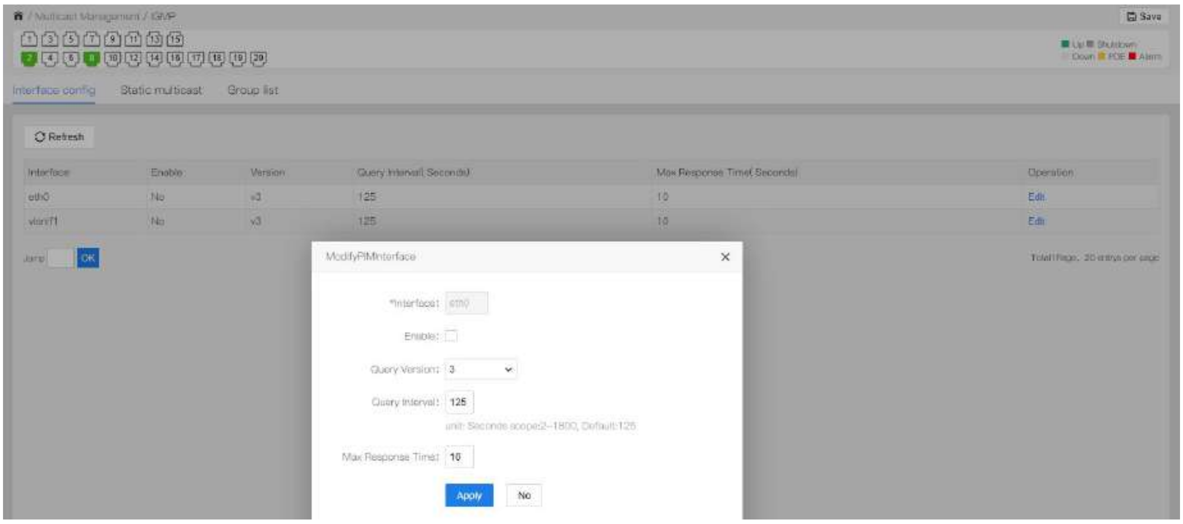
Multicast: A data transmission method that allows one device to send data to multiple target devices simultaneously without having to send a separate copy of the data to each target device, thereby improving network efficiency and reducing network bandwidth usage.

Name	Description
Vlan ID	Custom VLAN-ID
MAC	Custom MAC
Port list	Port list

3.5.3 IGMP

IGMP: includes interface configuration, static multicast, and Group list.

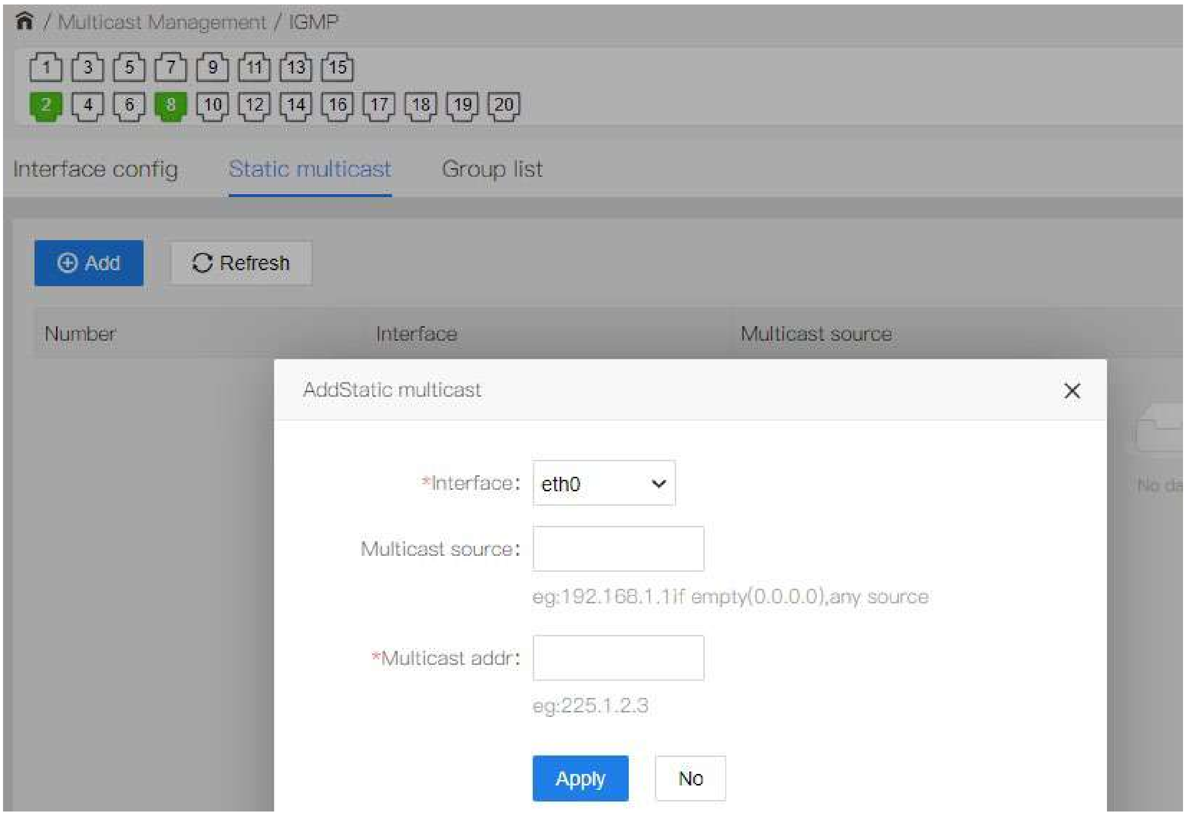
3.5.3.1 Interface configuration



Interface configuration: Primarily used for managing and controlling multicast port forwarding modes.

Name	Description
Enable	Switch
Query Version	Query version
Query Interval	Query interval
Max Response Time	Maximum response time

3.5.3.2 Static multicast



Static multicast: It means setting multicast parameters on a switch through manual configuration, allowing specific multicast traffic to be forwarded along pre-set paths and rules.

 Interface: A physical or logical port on a switch used to connect to other devices.

 Multicast source: A device or node that sends multicast data.

 Multicast address: A special IP address used to identify a multicast group.

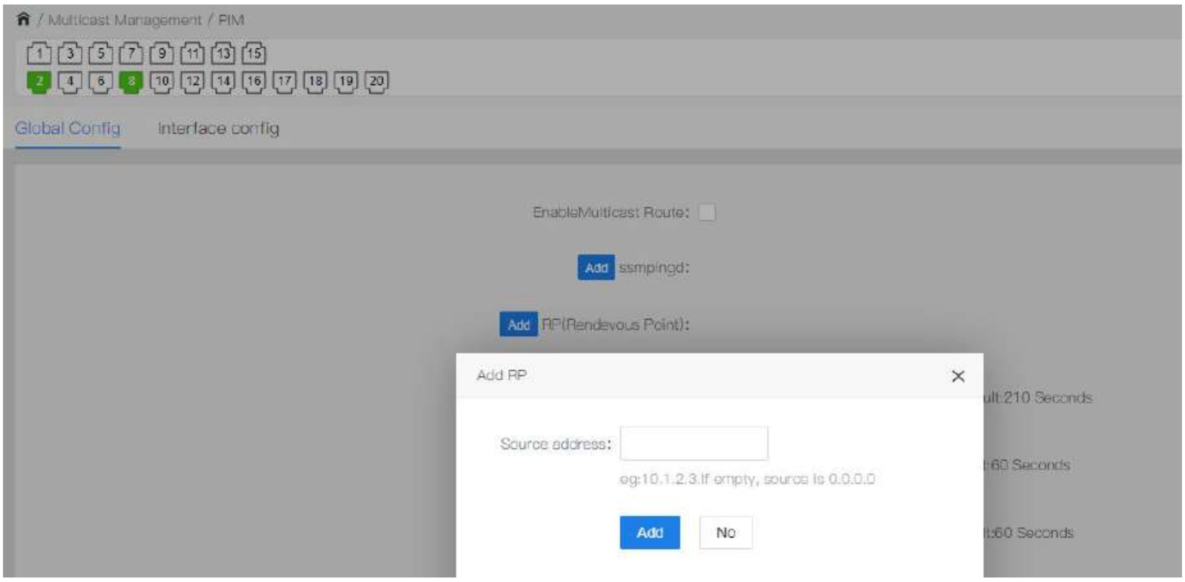
3.5.3.3 Group list

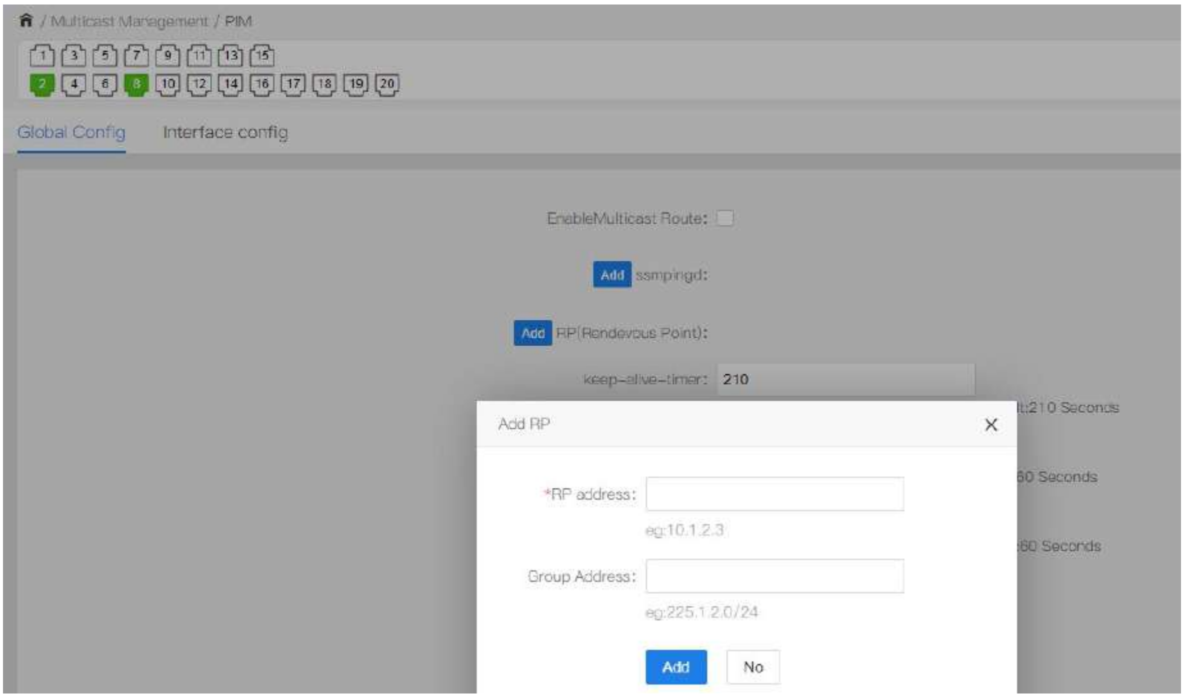
Group list: It is a display of information about the various groups configured on the switch. These groups can be created based on different functions or purposes.

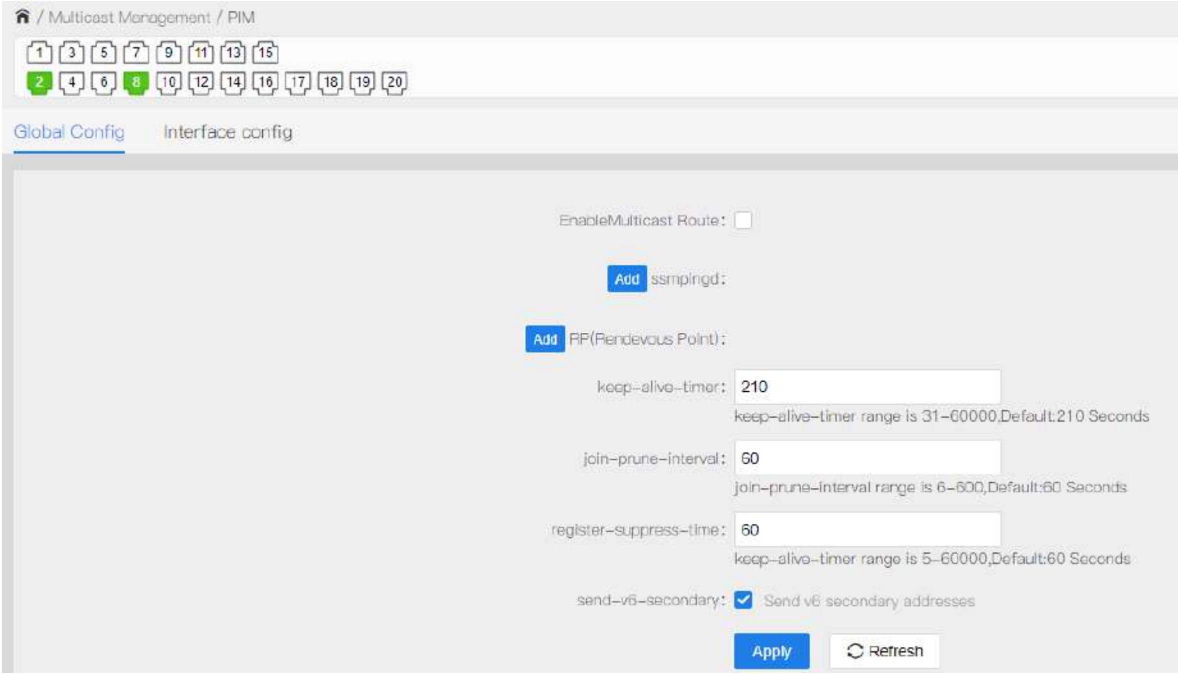
3.5.4 PIM

PIM: It includes both global configuration and interface configuration.

3.5.4.1 Global configuration







Global configuration: A series of parameters and instructions that set the overall operational status and functionality of the switch, which affect the global operational characteristics of the switch rather than local objects such as specific ports or vlans.

 Enable multicast routing: Switch

 Ssmpingd: Placing specific multicast groups within the SSM range enables more precise multicast forwarding and management, allowing the switch to perform more precise multicast data forwarding based on the source address and multicast group address, improving the efficiency and security of multicast communication.

①Source address: Multicast source address.

Rp(rendevous point) : Multicast convergence point.

①RP address: The address of the convergence point.

②Group Address: Multicast address.

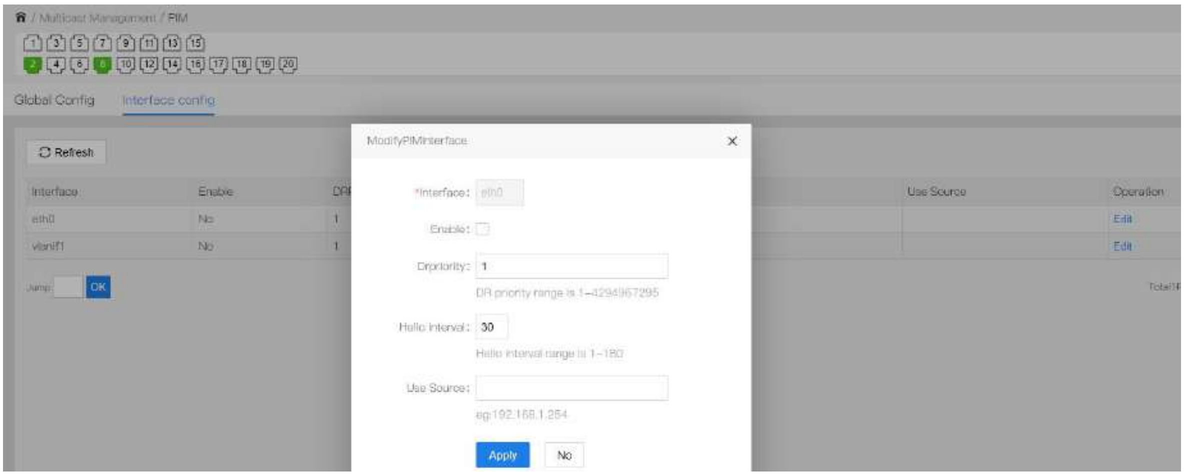
- Keep-alive timer: Multicast alive timer.

 Join-prune-interval: Refers to the priority of the interface when electing the specified router.

 the Register - suppress - time: refers to the multicast registered holding time.

 Send-v6-secondary: Send IPv6 helper (multicast) related functional Settings.

3.5.4.2 Interface configuration



Interface configuration: Setting the parameters and functions of each physical or logical port of the switch to meet different network connection and service requirements.

- Enable: Switch
- Drpriority: Refers to the priority of the interface when electing the specified router (DR).
- Hello Interval: Refers to the time interval for sending the Hello message."
- Use Source: usually refers to the source address of the specified data packet.

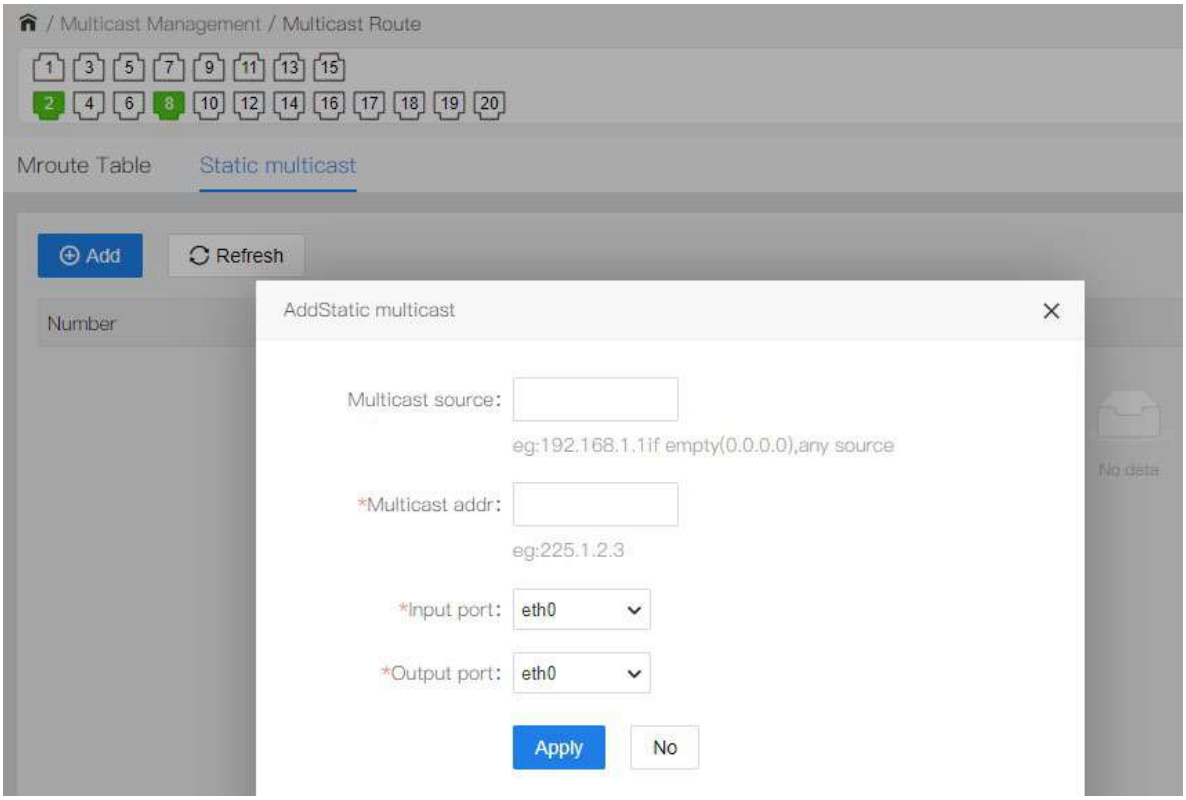
3.5.5 Multicast routing

Multicast routing: includes Mroute Table and static multicast.

3.5.5.1 Mroute Table

Mroute Table: Multicast Routing table.

3.5.5.2 Static multicast



Static multicast: A manually configured multicast method used to implement specific multicast data transmission control over a network.

 Multicast source: A device or node that sends multicast data.

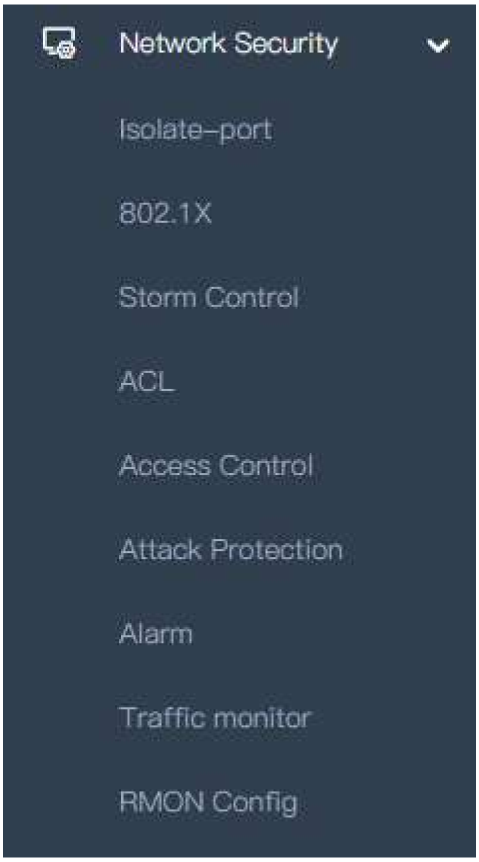
 Multicast address: A special IP address used to identify a multicast group.

 Inbound interface: Refers to a switch port that is statically configured for receiving multicast traffic.

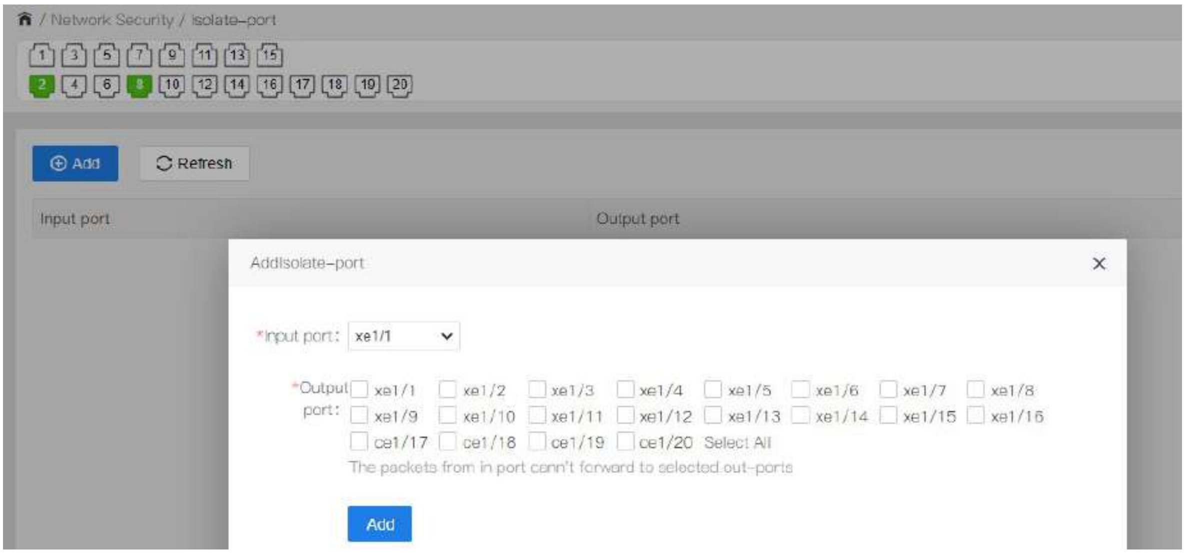
 Outgoing port: The port on which the switch forwards multicast data out.

3.6 Security Management

Expand this setup and you can set up Settings such as port isolation, 802.1X, storm suppression, ACL, access control, attack protection, alerts, traffic monitoring, RMON configuration, etc.



3.6.1 Port Isolation



Port isolation: Port isolation is a feature that isolates ports on a switch to limit communication between ports.

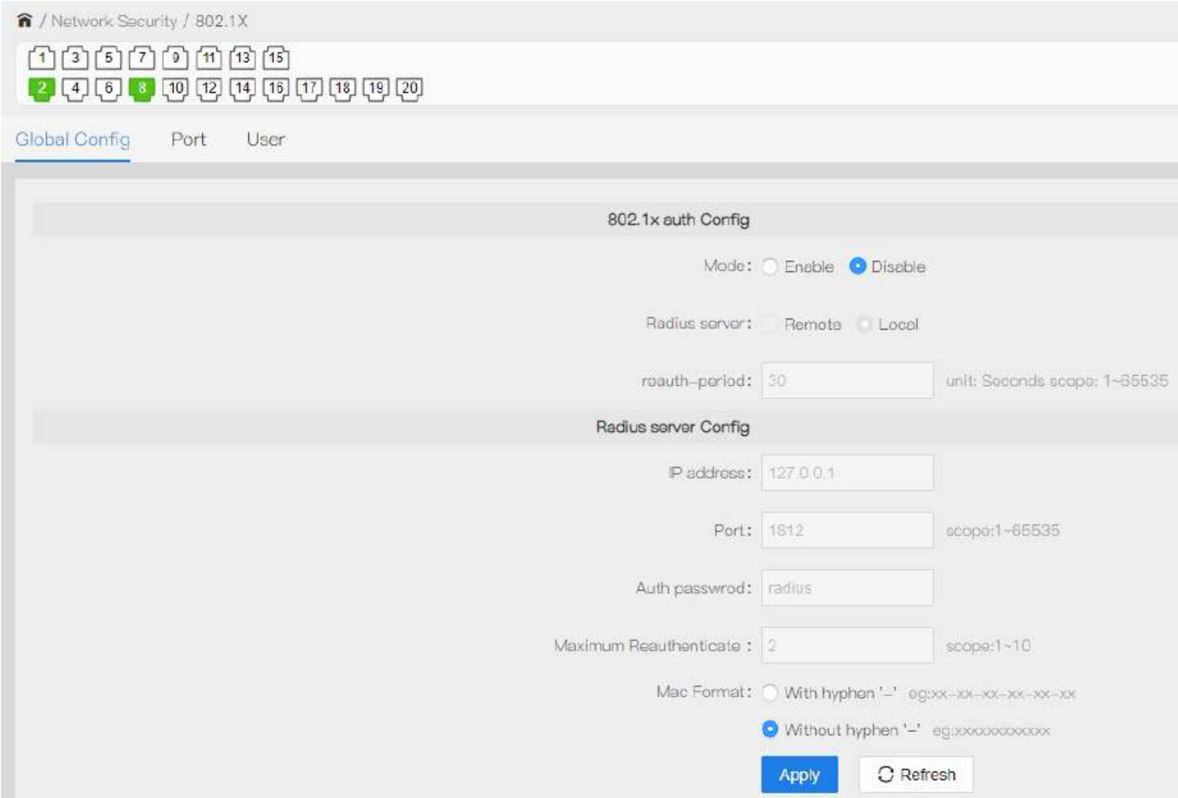
 Access interface: Refers to a port that allows devices to connect and communicate normally.

 Exit port: Refers to the port used when data is sent out from an isolated area.

3.6.2 802.1X

802.1X: includes global configuration, port configuration, and user.

3.6.2.1 Global Configuration

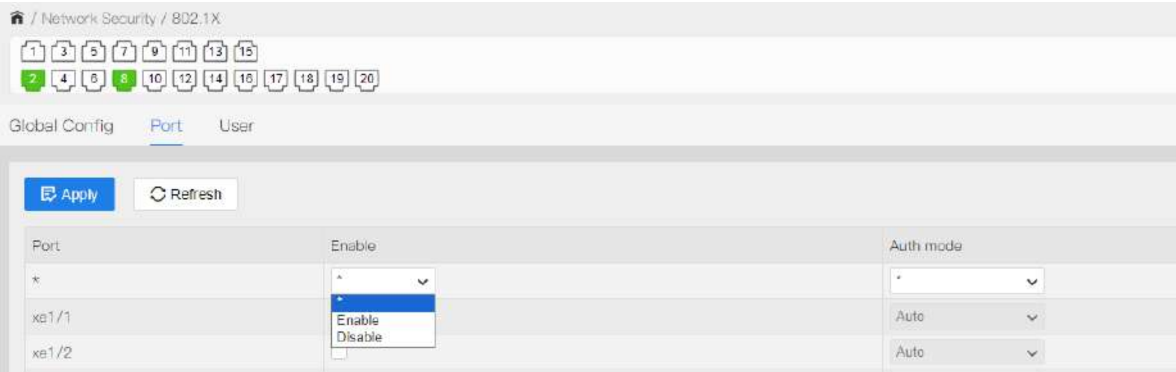


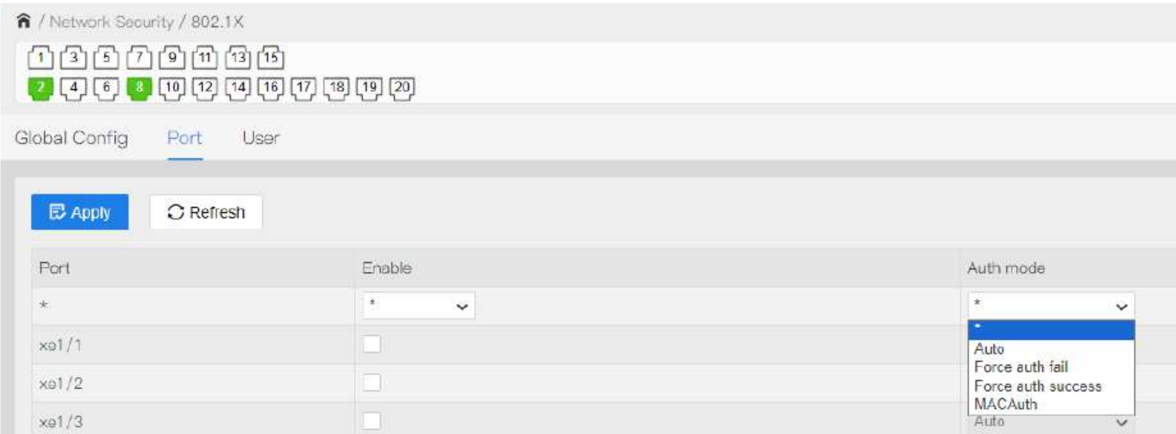
Global configuration: All business ports

802.1x authentication configuration	
Name	**Description**
Patterns	Choose enable or disable.
Radius server	To be used for centralized authentication, authorization, and billing management of network users.
Authentication update intervals	The time interval between the switch and the authentication server for regular updates of user authentication information.
Radius server configuration	
Name	**Description**
IP address	The network address set by the switch itself.
Port	The physical interfaces on a switch used to connect other network devices also involve some logical Settings related to ports.
Authentication Shared password	A security key used when a switch communicates with an authentication server, such as a Radius server.

Number of authentication retries	The maximum number of times a switch attempts to communicate with the authentication server to verify the user's identity while the user authenticates the network.
Mac authentication address format	The address representation used by the switch for MAC address authentication and related specifications.

3.6.2.2 Port configuration





Port configuration: Select the port

 Authentication mode: The way devices or users connected to that port are authenticated. By setting the authentication mode, the switch ensures that only authorized devices or users have access to network resources, thereby enhancing the security of the network.

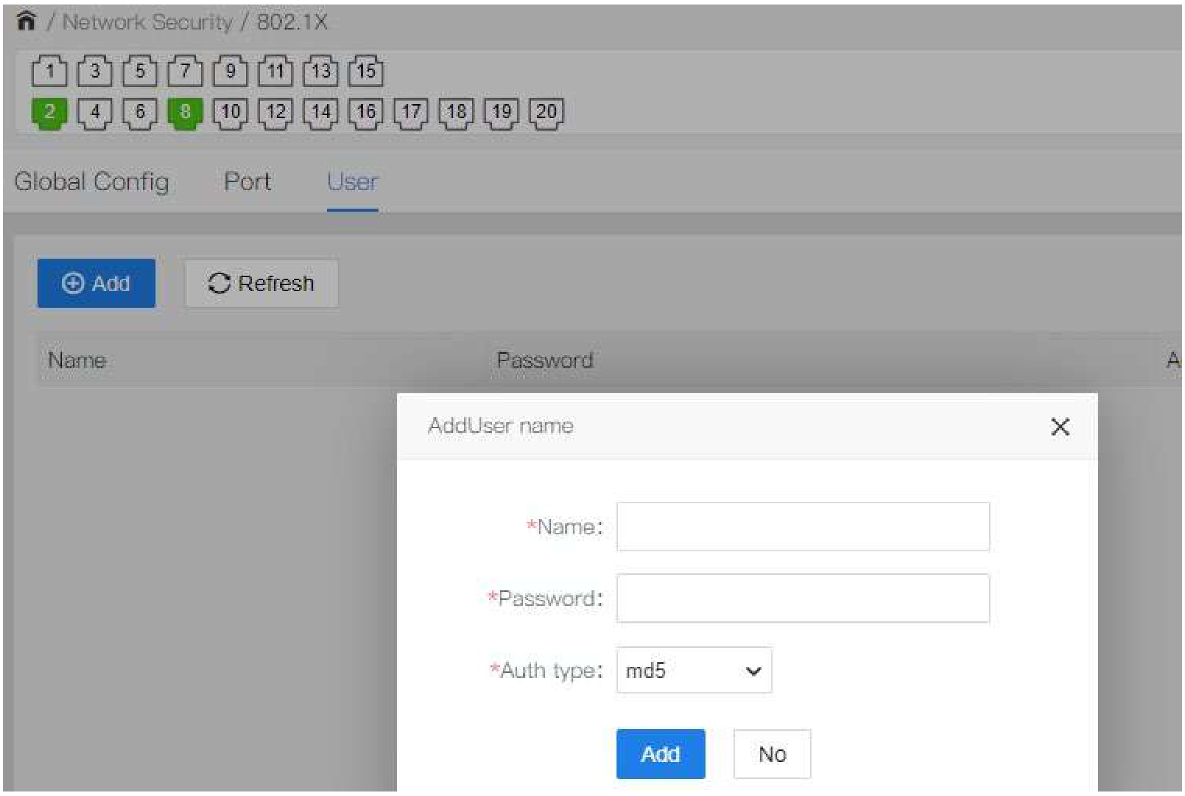
① Automatic: The switch can automatically detect and adapt the authentication method supported by the connected device.

② Forced authentication fails: Set a specific port so that it is not allowed to access the network through authentication regardless of the authentication information provided by the connected device or user.

③ Forced authentication pass: The switch defaults the device connected to the port to authentication pass regardless of whether it is authenticated or the authentication information it provides is correct, allowing the device to access the network.

④MAC authentication: The administrator configures a list of MAC addresses allowed to access in the switch in advance. When a device connects to a port, the switch compares its MAC address with the list and allows access if it matches. This is suitable for network environments where devices are relatively fixed and the number is limited.

3.6.2.3 Users



User: Create a new user.

 Name: Custom name.

 Password: Custom password.

 Authentication type: The way a switch authenticates a user attempting to access the network or use network resources.

①Md5: Used to encrypt information such as user passwords to enhance security during the authentication process.

②Tls: Used to provide encryption and authentication functions in network communications to ensure the security and integrity of data transmission.

③Mschapv2: A protocol used to verify user identity, mainly used in the Windows network environment, functioning when the switch interacts with the user's device for authentication.

④Peap: It is a security protocol used for user authentication in wireless networks. Here are its features and functions.

⑤Ttls: Tunnel Transport Layer Security Protocol.

⑥Tlv: A data encoding format, not a common type of user authentication.

⑦Gtc: Authentication or generic two-factor authentication.

⑧Sim: Authentication type SIM refers to the authentication method based on the user identification module.

3.6.3 Storm suppression

Storm suppression: A function used to prevent abnormal situations such as broadcast storms, multicast storms, or unicast storms in a network.

 Broadcast: When there are a large number of broadcast packets in the network, it causes the network bandwidth to be greatly occupied, affecting normal data transmission.

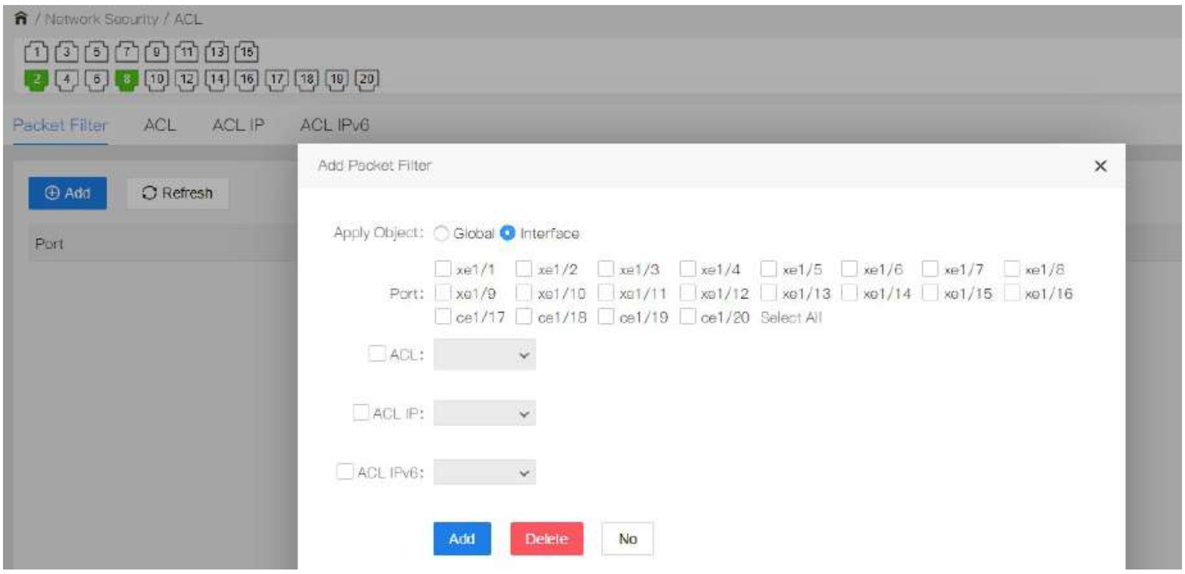
 Unknown multicast: Excessive multicast data flooding the network can also cause network congestion.

 Unknown unicast: A large number of unicast data packets of unknown or incorrect purpose are constantly spreading in the network, which also consumes network resources.

3.6.4 ACL

ACL: includes Packet Filter, ACL, ACL IP, ACL IPv6.

3.6.4.1 Packet Filter



Packet Filter:

 Application Object: Select all ports/individual ports.

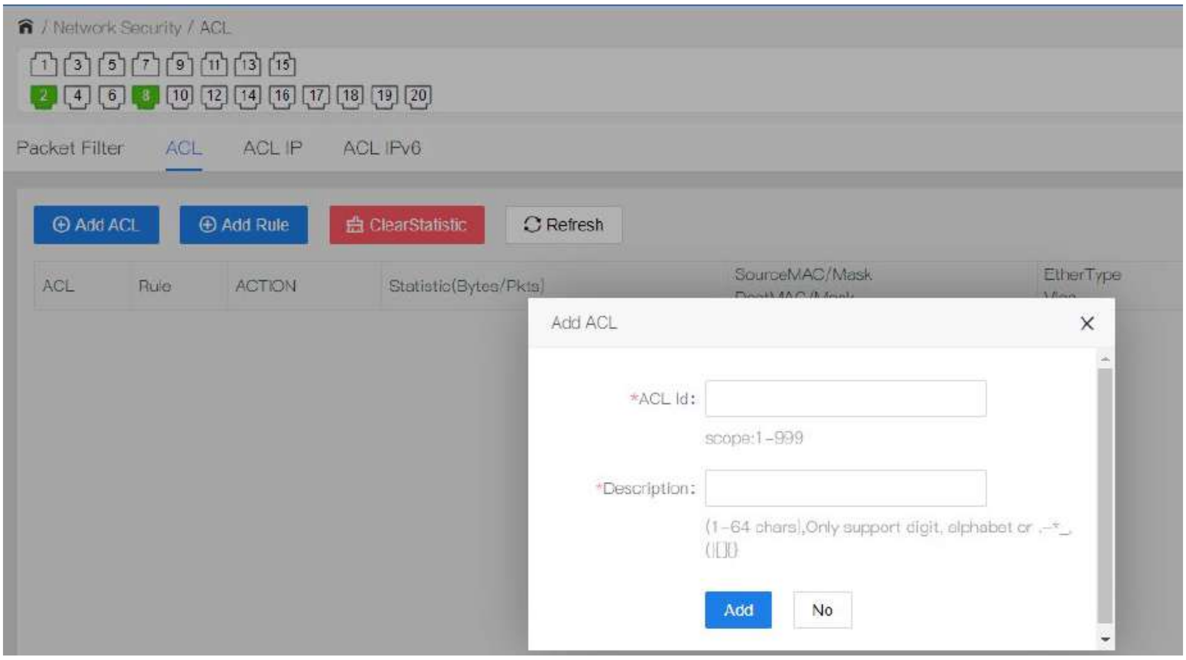
 Port: All ports.

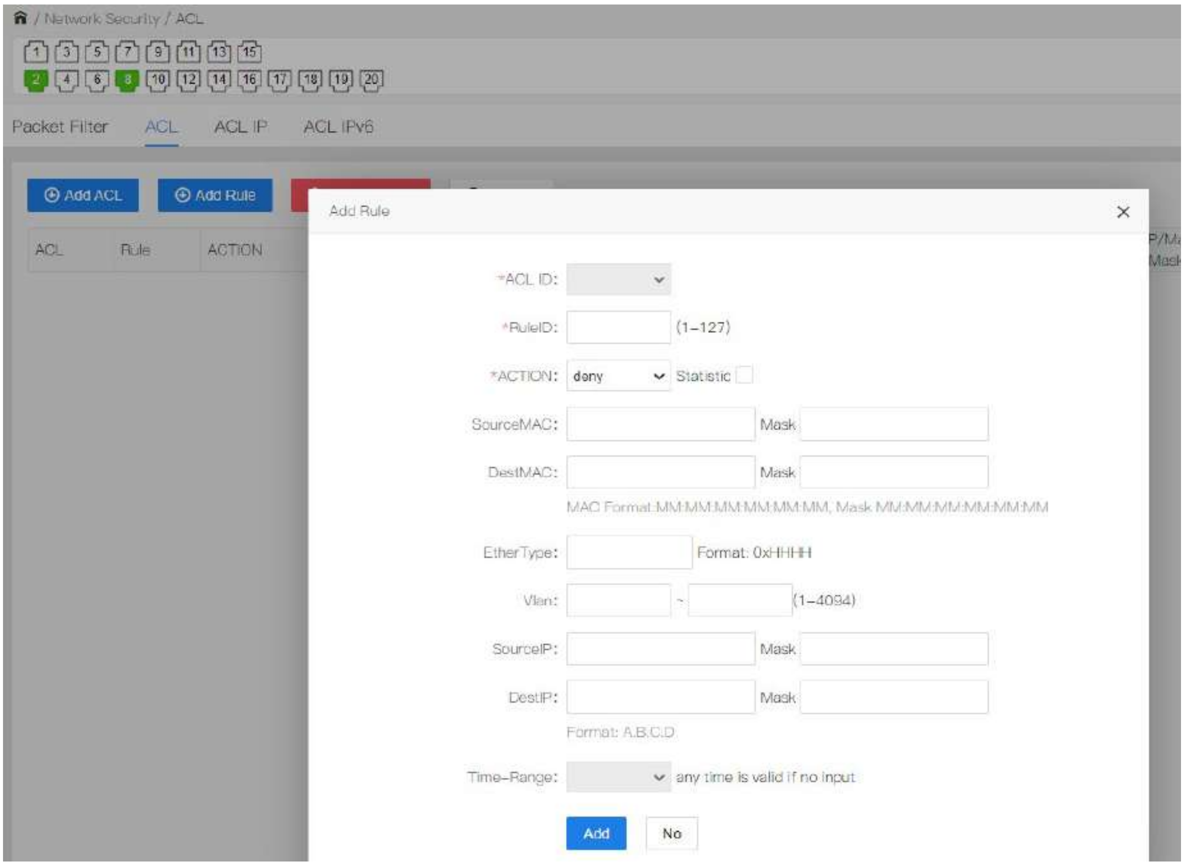
 ACL: It is a packet-filtering access control technique used to control how a switch forwards network packets.

 ACL IP: A collection of Access Control rules for IPv4 addresses in an Access Control List.

 ACL IPv6: A mechanism used to control access rights to IPV6 network traffic.

3.6.4.2 ACL



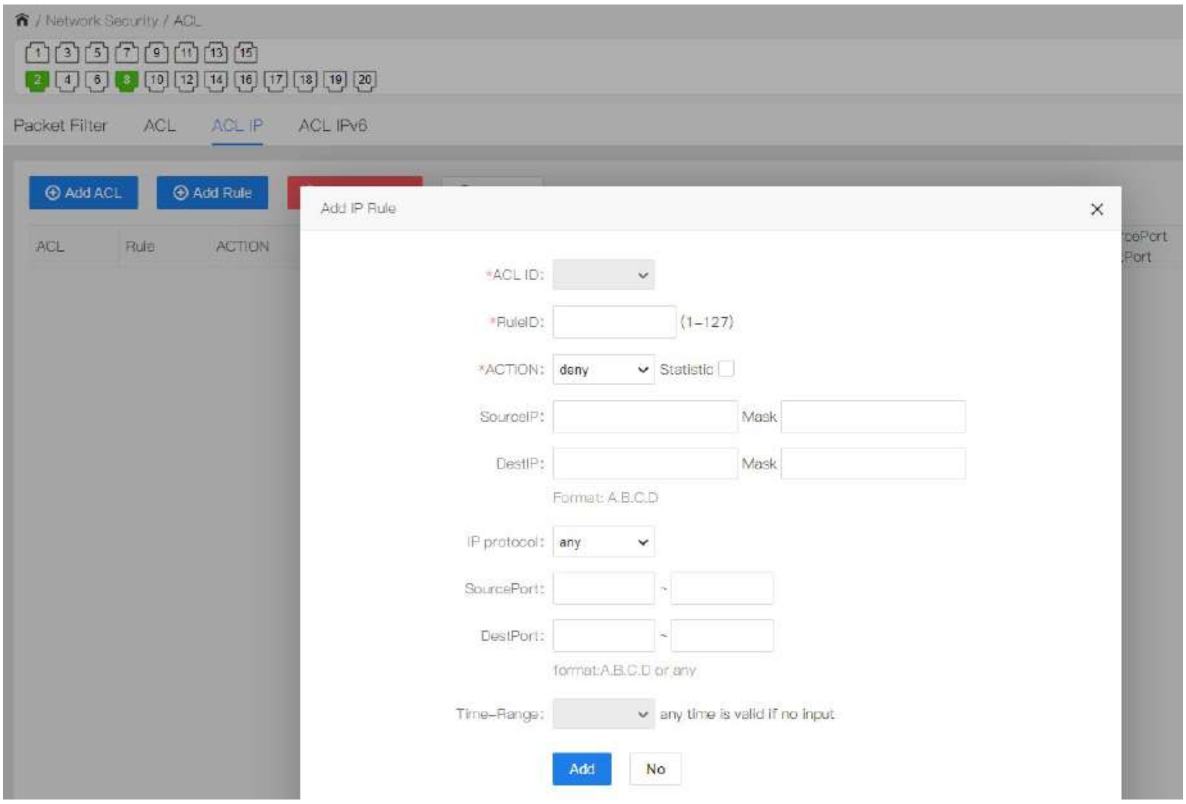


ACL: It is a packet filtering access control technique used to control how a switch forwards network packets.

Add ACL	
Name	**Description**
ACL id	It is a number used to identify different lists of access control
Description	Notes
Add Rule	
Name	**Description**
ACL ID	It is a number used to identify different lists of access control
Rule ID	It is a number used to uniquely identify the rule
Action	Select Mode
Source MAC	The MAC address of the source device in the packet
Mask	A mask is used in conjunction with an IP address or MAC address to specify an address range
Purpose MAC	The MAC address of the target device to which the data packet is to be

	sent
Mask	A mask is used in conjunction with an IP address or MAC address to specify an address range
Ether type	Ethernet frame type, used to identify the upper-layer protocol carried in an Ethernet frame
Vlan	Quasi-local Area network
Source IP	The IP address of the packet sender device
Destination IP	The IP address of the target device to which the packet is going
Time-Range	The time range in which ACL rules take effect. By setting a time range, it is possible to control network access based on different time periods

3.6.4.3 ACL IP



ACL IP: A collection of Access Control rules for IPv4 addresses in an Access Control List.

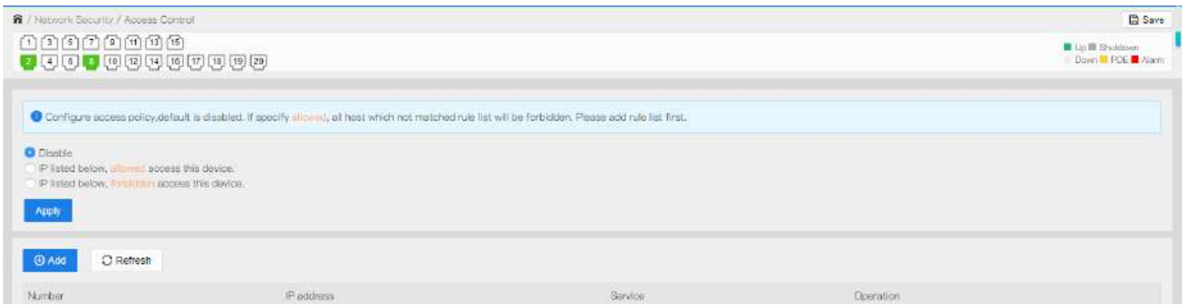
Add IP Rule	
Name	**Description**
ACL ID	The identifier of the access control list. It is a unique number or name used

	to distinguish different access control lists.
Rule ID	It is a number used to identify each specific rule in the access control list.
Actions	Actions are actions taken against IP packets that meet certain conditions, and there are mainly the following two common actions.
Source IP	It is the IP address of the device that initiates a network connection or sends a packet.
Mask	It is mainly used in conjunction with the destination IP address to specify a range of destination IP addresses.
Destination IP	Refers to the IP address of the destination device to which the data packet is to reach.
IP Protocol	The type of protocol used by the network layer to define how data packets are transmitted and processed in the network.
Source port	It is the port number used by the application or process that sends network data packets.
Destination port	The port number listened to by the application or service on the destination device to which the packet is going.
Time-Range	It is used to specify the time period during which ACL rules take effect.

3.6.4.4 ACL IPv6

ACL IPv6: A mechanism used to control access rights to IPV6 network traffic.

3.6.5 Access control

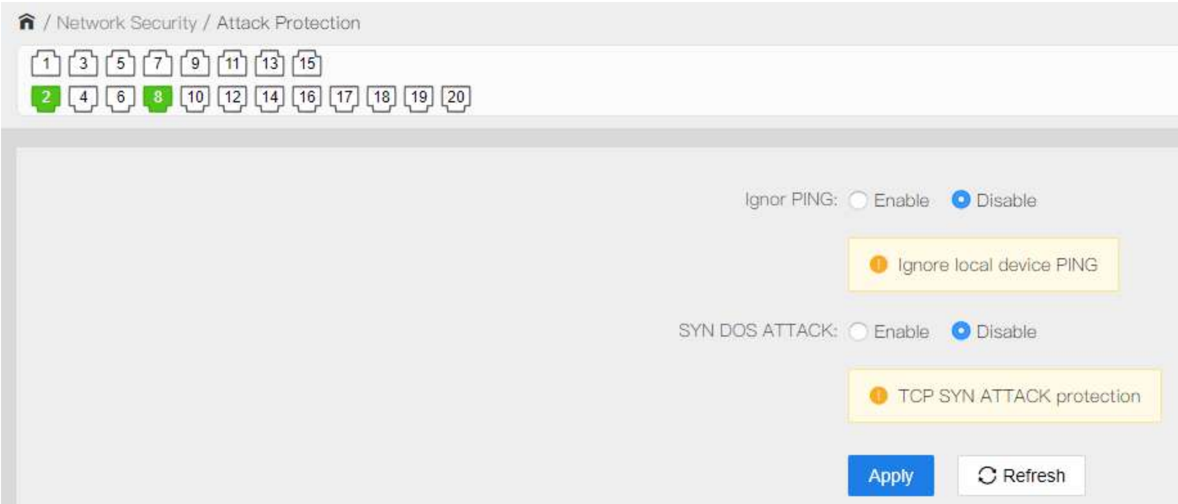


Access control: It is the fine-grained management of data traffic in an IPv6 network based on the rules configured by the administrator on the switch to determine which traffic is allowed through the switch and which is denied.

 IP address: The IP address of IPV6.

 Service: A network service or application based on a particular IP address.

3.6.6 Protect against attacks



Anti-attack: refers to a series of security protection functions that a switch has to detect and defend against various network attacks in order to protect the security and stable operation of the network.

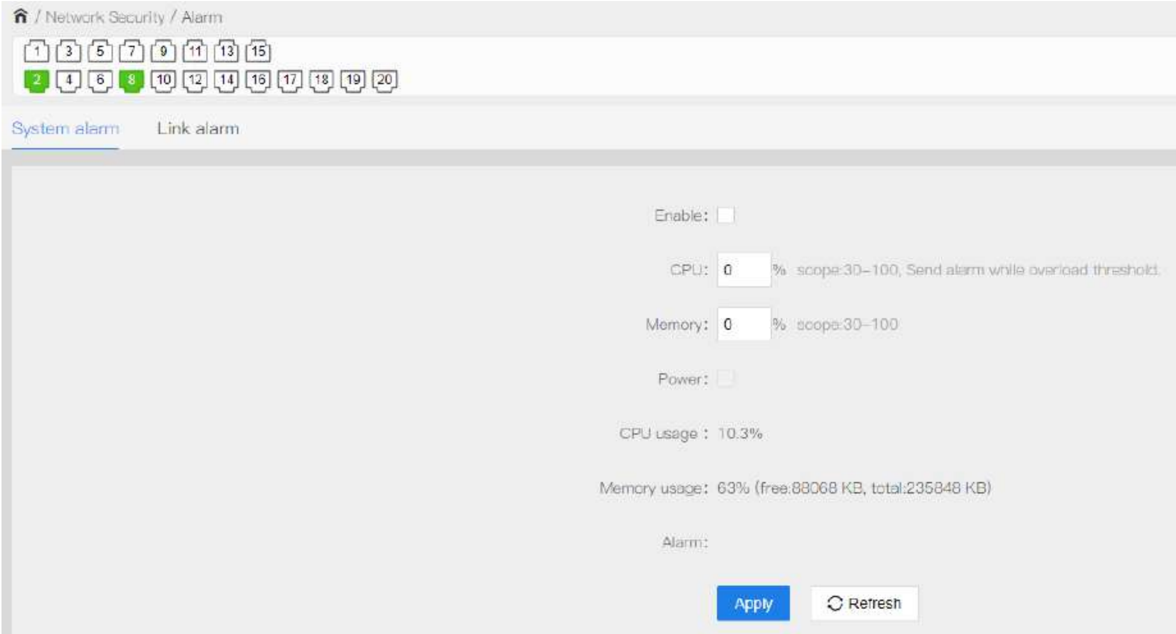
 - Ignore PING packets:

 Guard against SYN DOS attacks:

3.6.7 Alerting

Alarm: It includes two types: system alarm and link alarm.

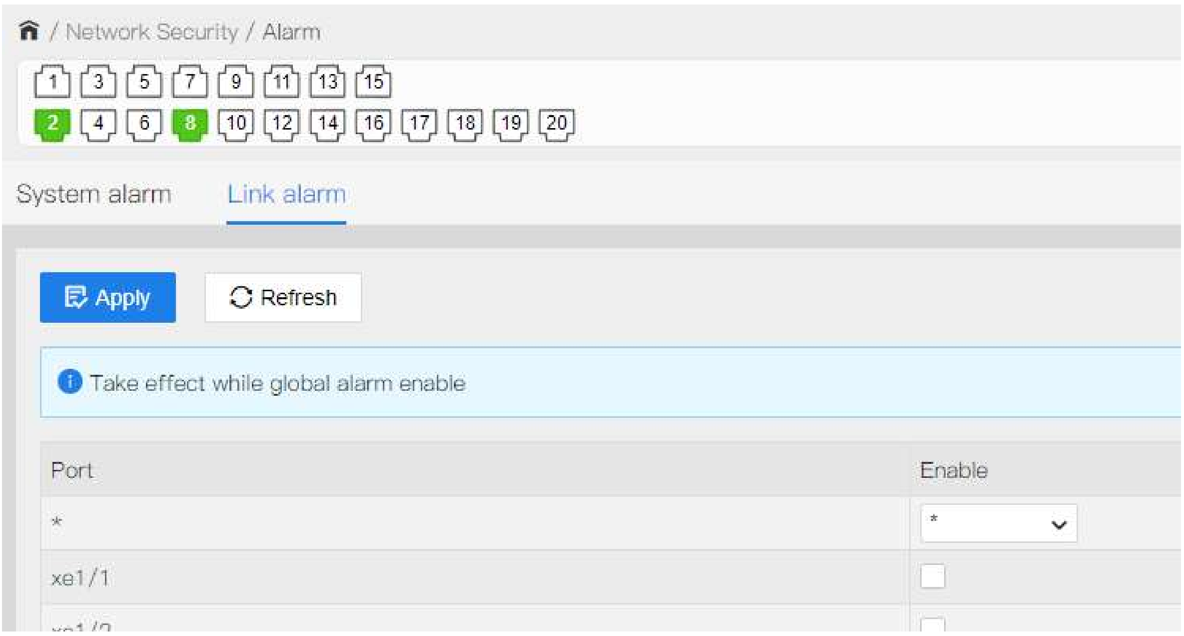
3.6.7.1 System alerts



System alert: An alert message sent by the switch in response to various abnormal conditions of its own system, used to alert the administrator that there is a problem with the system operation of the switch.

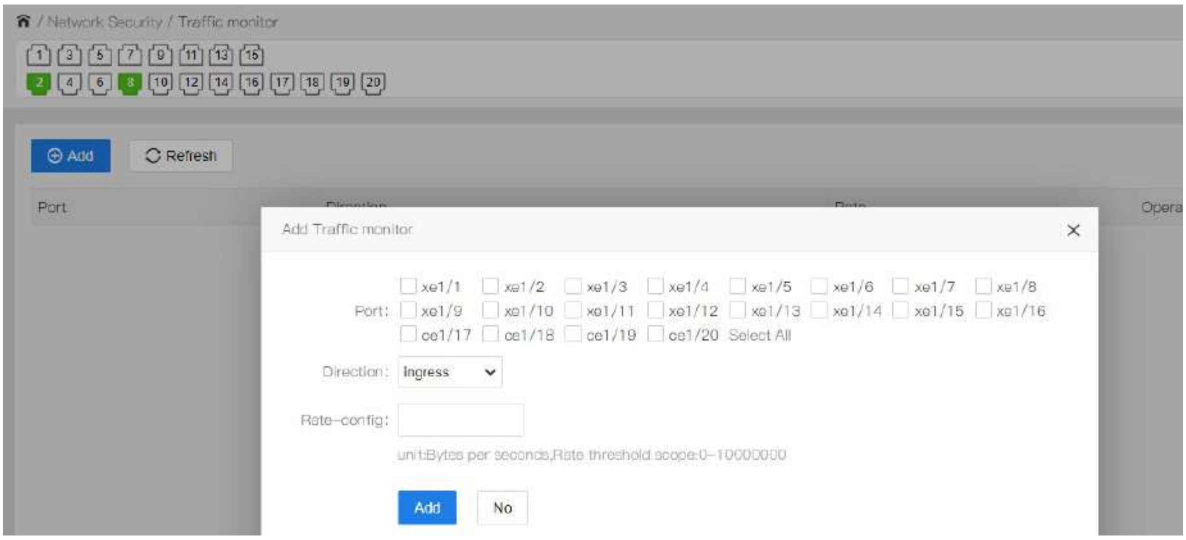
- Enable: Switch
- CPU: Monitor to view the CPU
- Memory: Monitor to view memory
- Power: Monitor to view power

3.6.7.2 Link alerts



Link alert: An alert message sent by a switch when it detects an anomaly in the physical link to which it is connected.

3.6.8 Traffic monitoring



Traffic monitoring: The function of monitoring and controlling the traffic flowing through switch ports in a network.

 Ports: Select all ports.

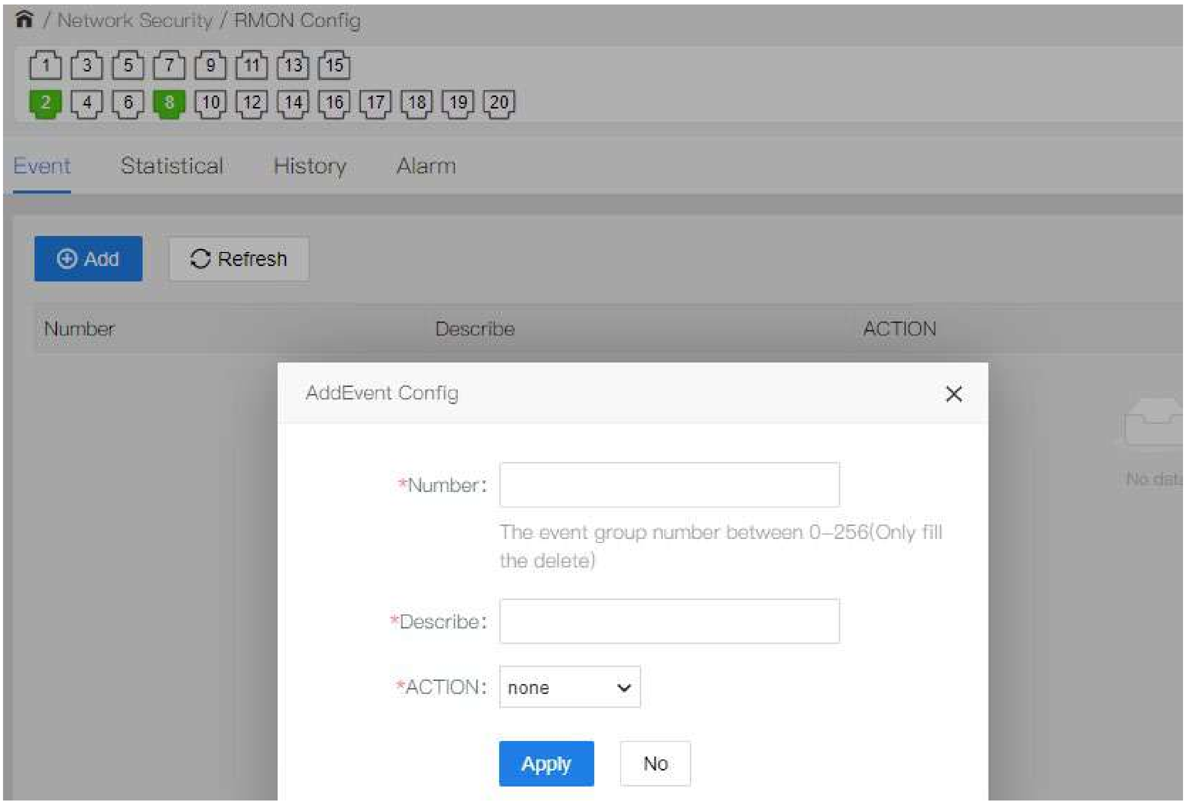
 Direction: Select the entry/exit.

 Rate configuration: Configure the port rate.

3.6.9 RMON configuration

RMON configuration: includes four types: event group, statistics group, history group, and Alert group.

3.6.9.1 Event Group



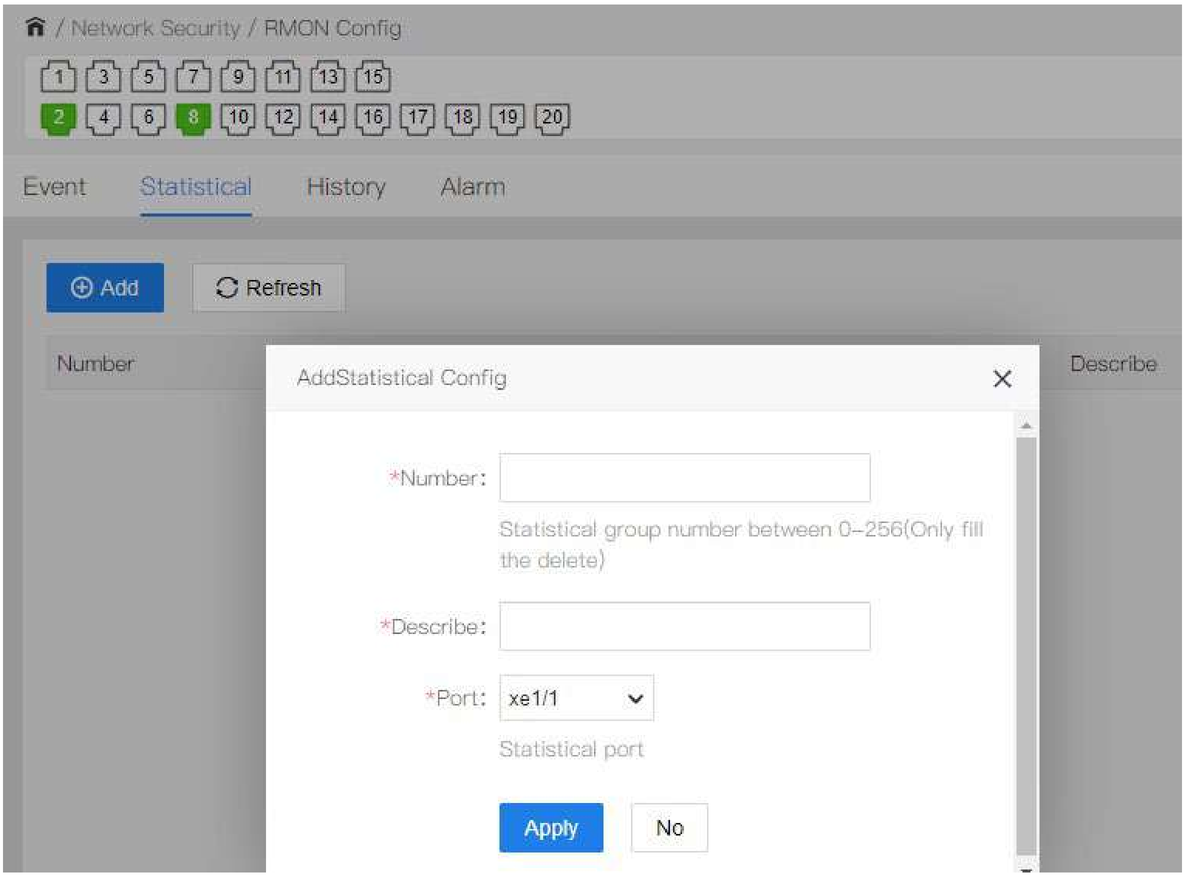
Event group: A set of rules and operations defined for monitoring, documenting, and responding to specific events that occur in a network.

 Serial number: Serial number.

 Description: Remarks.

 Action: Configure mode options.

3.6.9.2 Statistical groups



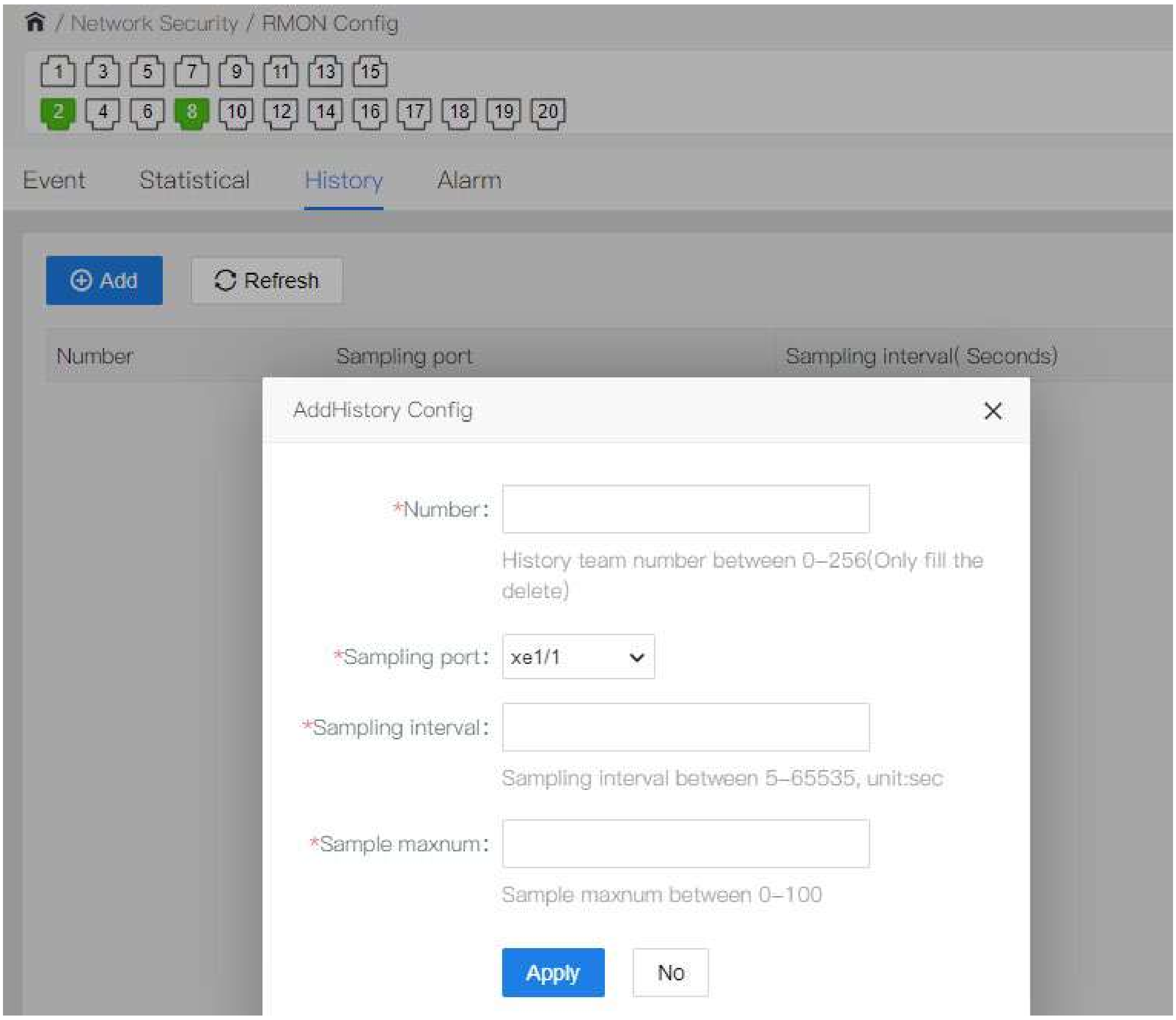
Statistical Group: The statistical group is an important component of RMON for collecting and counting various information about the network interface.

 Serial number: Serial number.

 Description: Remarks.

 Port: Select the port.

3.6.9.3 History Group



History Group: A history group is a functional module used to regularly collect and store statistics on network interfaces.

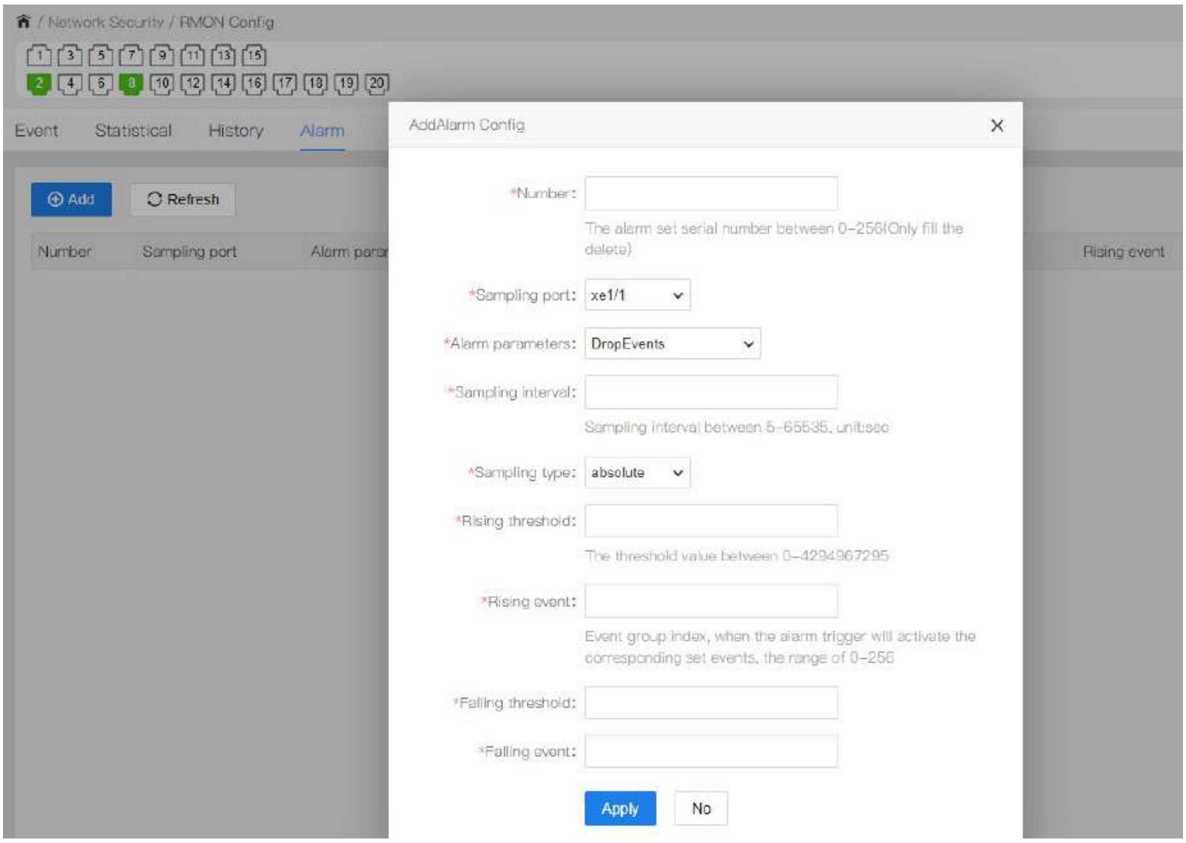
 Serial number: Serial number.

 Sample port: Select port.

 Sampling gap: Refers to the time period during which a switch samples relevant data from a network interface.

 Maximum number of sampling bars: The maximum amount of sampling data that can be stored in the history table.

3.6.9.4 Alarm Group



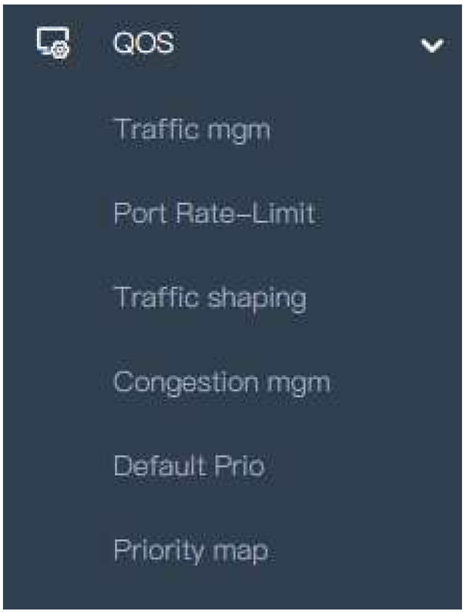
Alert Group:

Add alert group configuration	
Name	**Description**
Serial numbers	Serial number
Sampling port	Select the port
Alarm parameters	Select Mode
Sampling intervals	Intervals are measured in seconds
Sample type	Select the sampling mode
Rising edge threshold	Used to determine when the upper limit alarm event is triggered
Rising edge event	When sampling a specified alert variable, if the current sampling value is greater than or equal to the rising edge threshold (upper limit threshold) and the previous sampling value was less than that threshold, the rising edge event is triggered, generating an alert
Fall edge threshold	A lower limit alert is generated if the current sampling value is less than or

	equal to the falling edge threshold and the last sampling value was greater than that threshold
Fall edge event	A falling edge event is triggered when a specified alert variable is sampled and the current sampling value is less than or equal to the falling edge threshold (lower limit threshold), and the previous sampling value was greater than that threshold, resulting in an alert

3.7 QOS

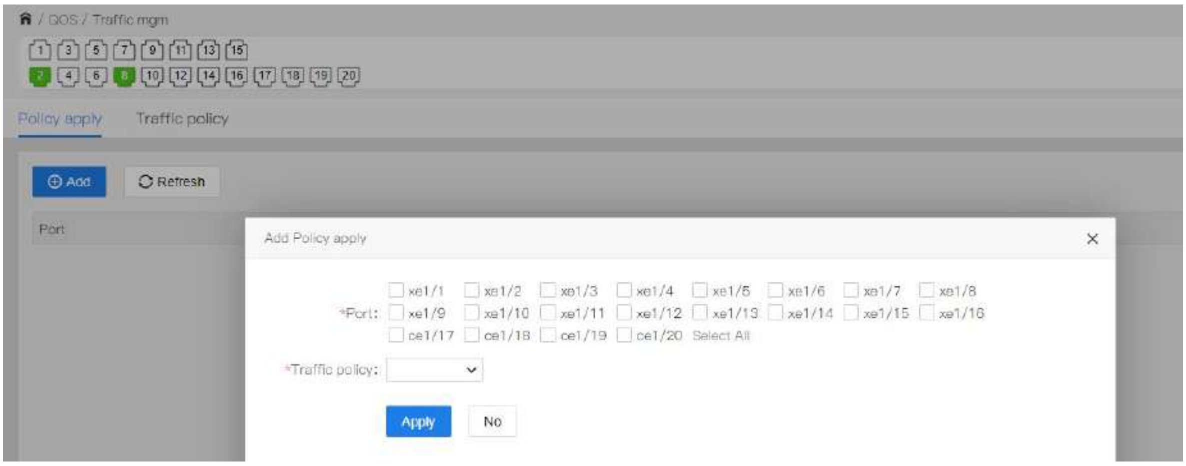
Expand this setting and you can set up traffic management, port speed limiting, traffic shaping, congestion management, port priority, priority mapping, etc.



3.7.1 Traffic Management

Traffic management: includes flow policy application and flow policy.

3.7.1.1 Application of Flow policy

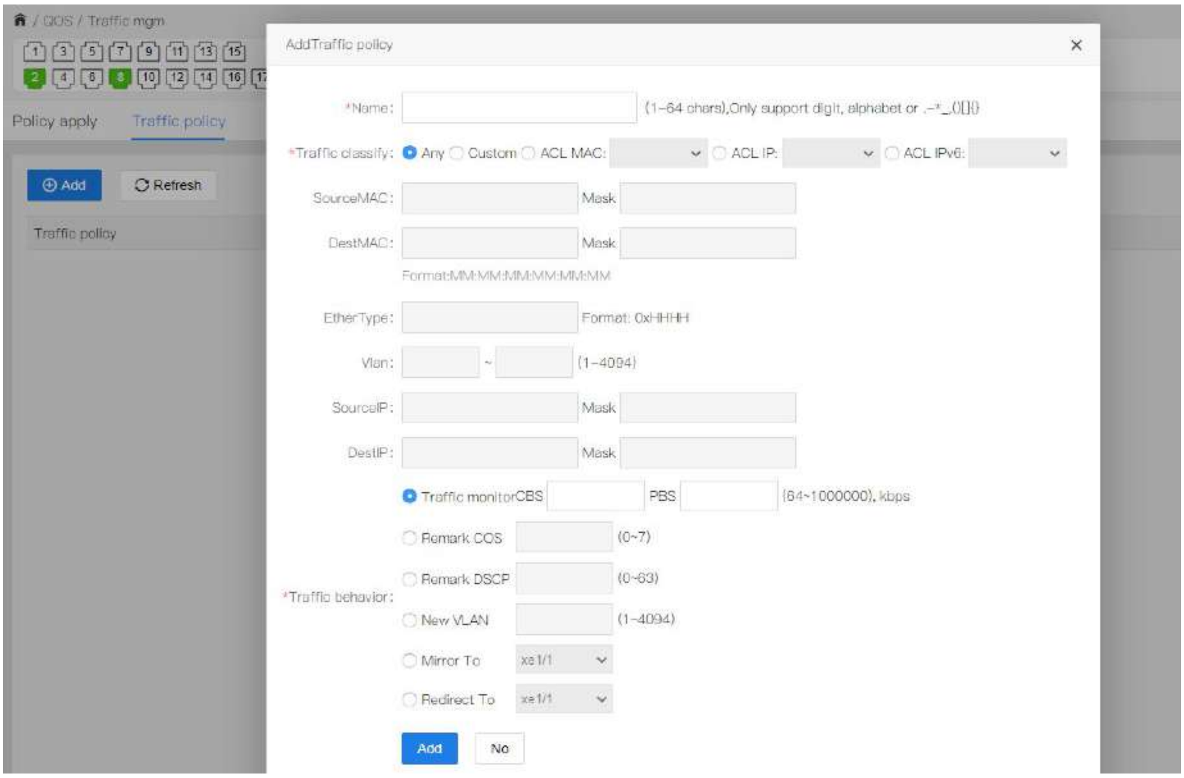


Flow policy application:

 Ports: All business ports.

 Flow policy: A flow policy is a collection of rules used to control and manage network traffic. It can perform operations such as classification, tagging, shaping, and scheduling of network traffic based on different conditions to achieve the rational allocation and optimal utilization of network resources.

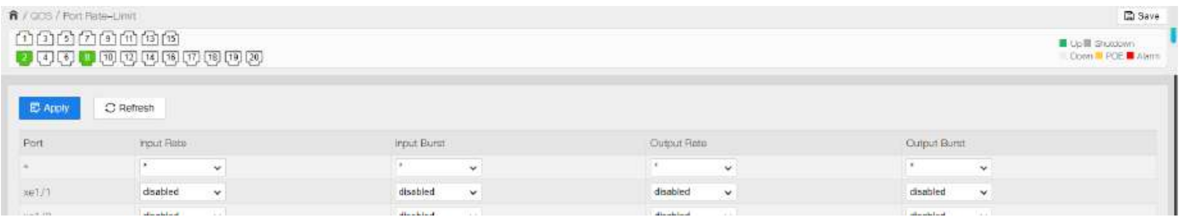
3.7.1.2 Flow Policy



Add stream strategy

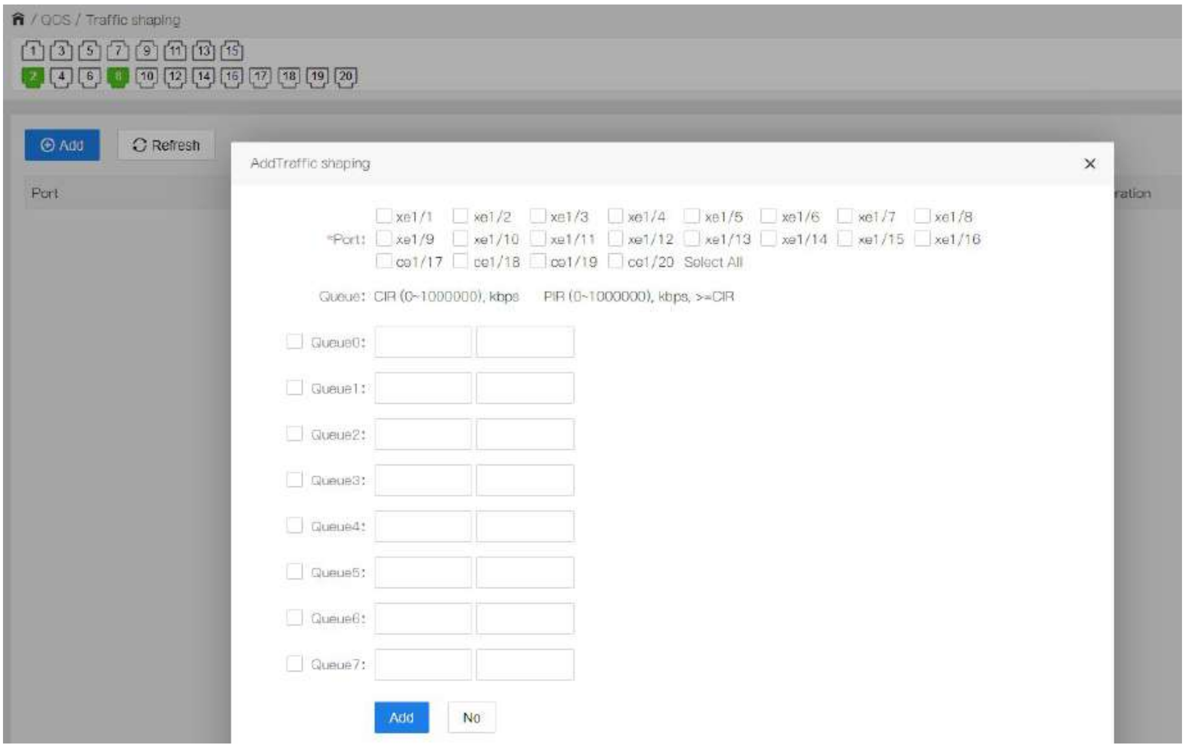
Name	Description
Name	Custom name
Stream classification	Any: Match all flows. 2.Custom: Customize.
Source MAC	Classify network traffic based on the source MAC address of the packet.
Mask	A number that specifies which parts of an IP address are the network address and which parts are the host address.
Destination MAC	It means classifying network traffic based on the destination MAC address of the data packet.
Ether type	Refers to the protocol type field in an Ethernet frame, which is used to identify the upper-layer protocol carried in the frame.
Vlan	It means classifying network traffic based on the virtual local area network (VLAN) to which the data packet belongs.
Source IP	It means classifying network traffic based on the source IP address of the data packet.
Destination IP	It means classifying network traffic based on the destination IP address of the data packet.
Popular	Points to the specific actions or treatments taken on classified network traffic.

3.7.2 Port speed limit



Port speed limit: In the Web interface of a switch, a port speed limit is a function that limits the rate of network traffic on a specific port of the switch.

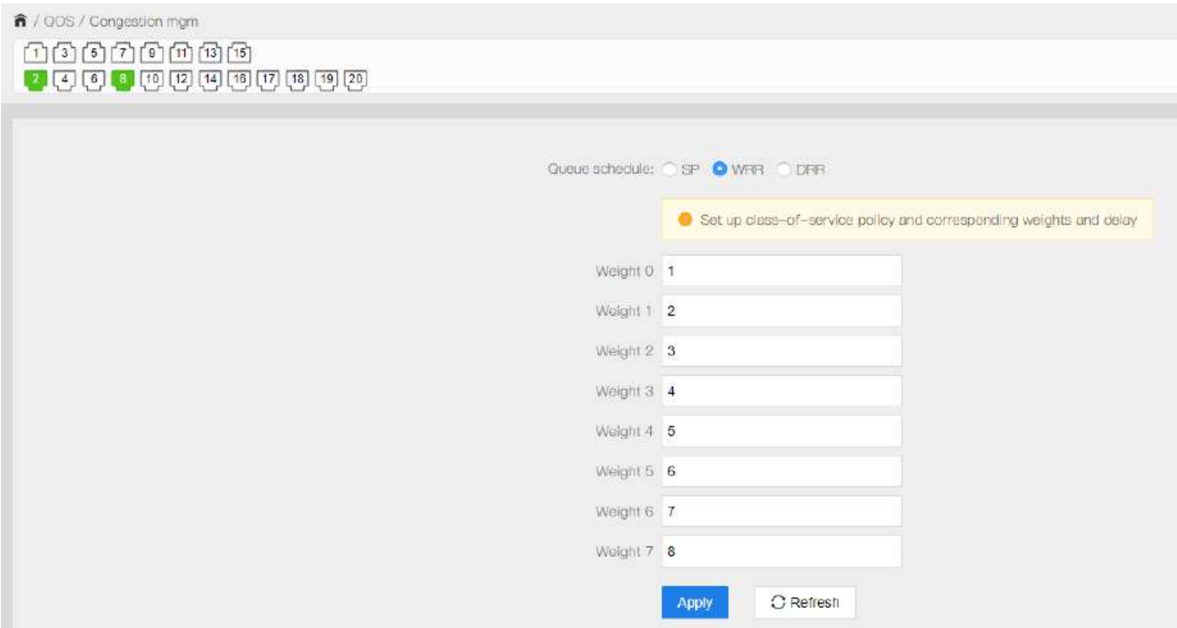
3.7.3 Traffic shaping



Traffic shaping: A technique for controlling and adjusting network traffic to optimize network performance, avoid network congestion, and ensure quality of service for different businesses.

- Port: All service ports.
- Queue: Grouping.

3.7.4 Congestion management



Congestion management: Refers to the mechanism by which a switch controls and manages network traffic when congestion occurs in the network. Its purpose is to ensure the rational allocation of network resources and guarantee the quality of service for critical business.

 Queue scheduling: 1.SP (Strict Priority, strict priority)

2.WRR (Weighted Round Robin)

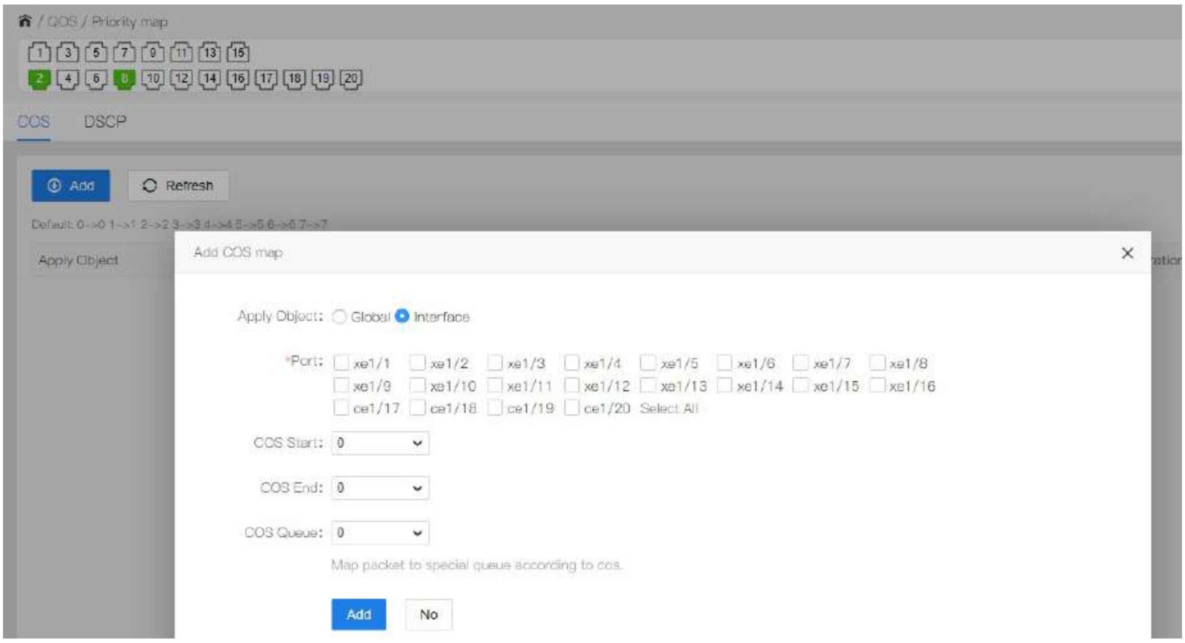
3.DRR (Deficit Round Robin)

3.7.5 Port priority

3.7.6 Priority mapping

Priority mapping: includes COS and DSCP.

3.7.6.1 COS



COS: Service level.

 Application object: Switch between all ports and individual ports.

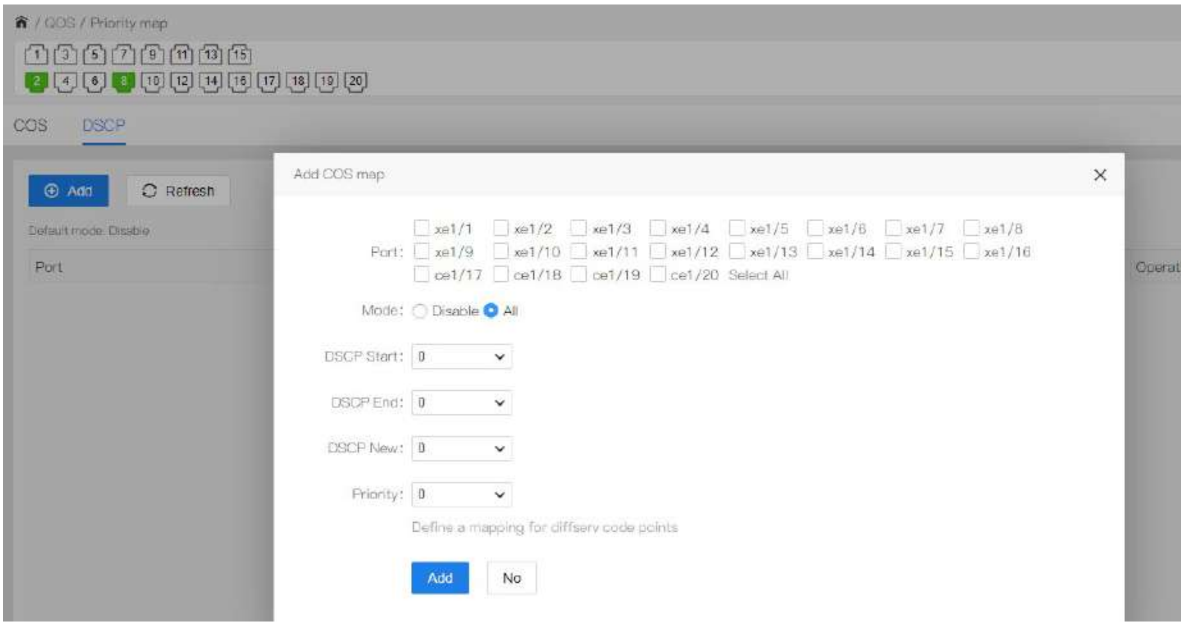
 Ports: All business ports.

 COS Start: Initial value for service level.

 COS End: Service level end value.

 COS Queue: Service level queue.

3.7.6.2DSCP



DSCP: Differential Service Code Point.

 Port: Business port.

 DSCP Start: It is the starting value setting for the new Differentiated Services Code Point (DSCP)."

 DSCP End: is the end value setting for Differentiated Services Code Point (DSCP).

 DSCP END: is the New differential services code point setting.

 Priority: Priority.

3.8 Extended Management

Expand this setup and you can set up DNS, ONVIF, Time Range Config, Devices, VOIP, Diagnosis, etc.

3.8.1 DNS

DNS: Domain Name System.

 Primary DNS: Primary Domain Name System server.

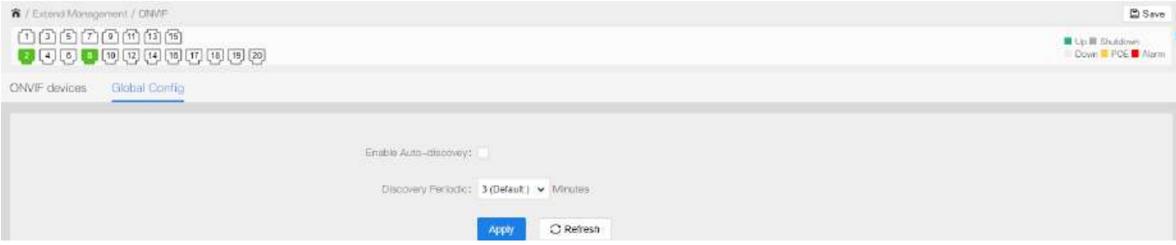
 Secondary DNS: Standby Domain Name System server.

3.8.2 ONVIF

ONVIF: includes devices and configurations.

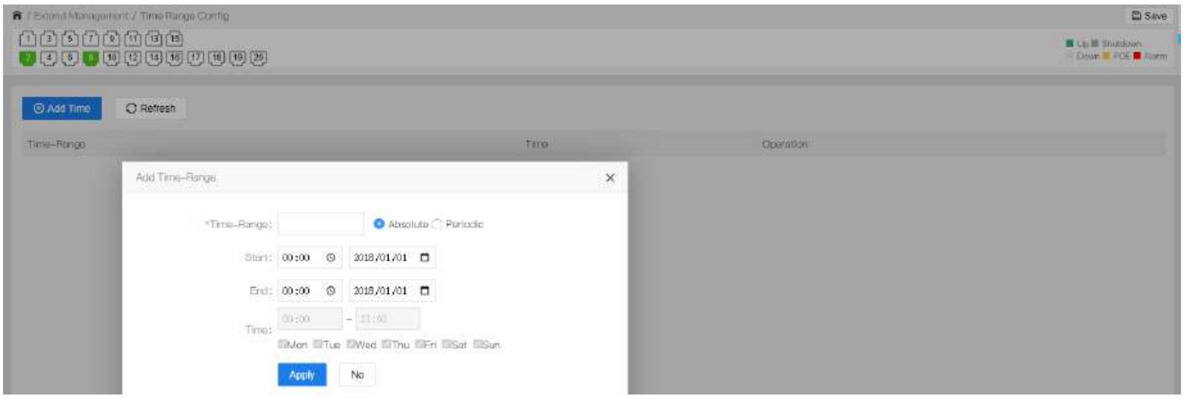
3.8.2.1 Devices

3.8.2.2 Configuration



Configure to enable Auto-discovey: Once this feature is enabled, the switch will automatically collect data such as device type connected, port status, VLAN information, etc., and can use this information for network management and monitoring. For example, it helps network administrators quickly understand device connections in the network, facilitating tasks such as troubleshooting, resource allocation and network planning, and improving the efficiency and convenience of network management.

3.8.3 Time Range Config

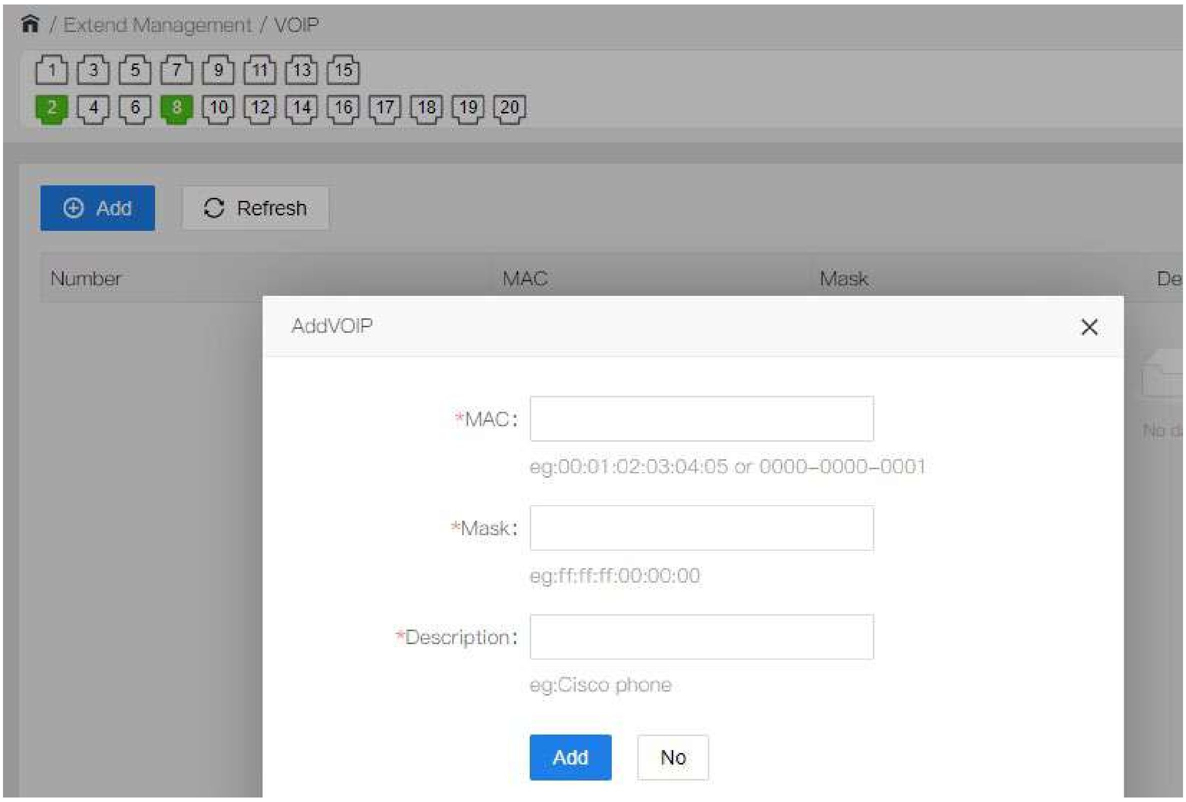


"Time Range Config:" refers to the configuration of the time range.

3.8.4 Devices

Devices: device-related information.

3.8.5 VOIP



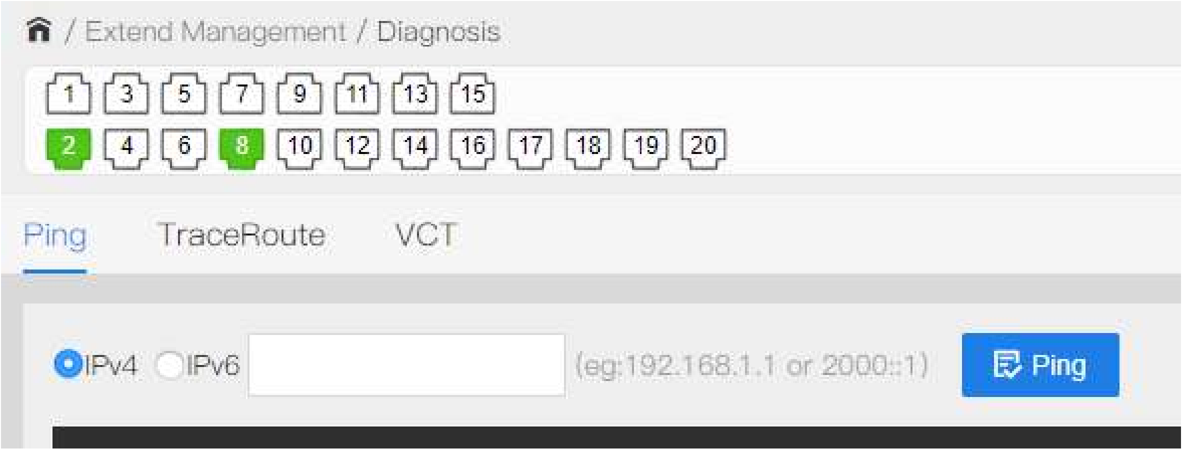
VOIP: Voice over the network.

Add VOIP	
Name	**Description**
MAC	Custom MAC address
Mask	Mask
Description	Description information

3.8.6 Diagnostic tests

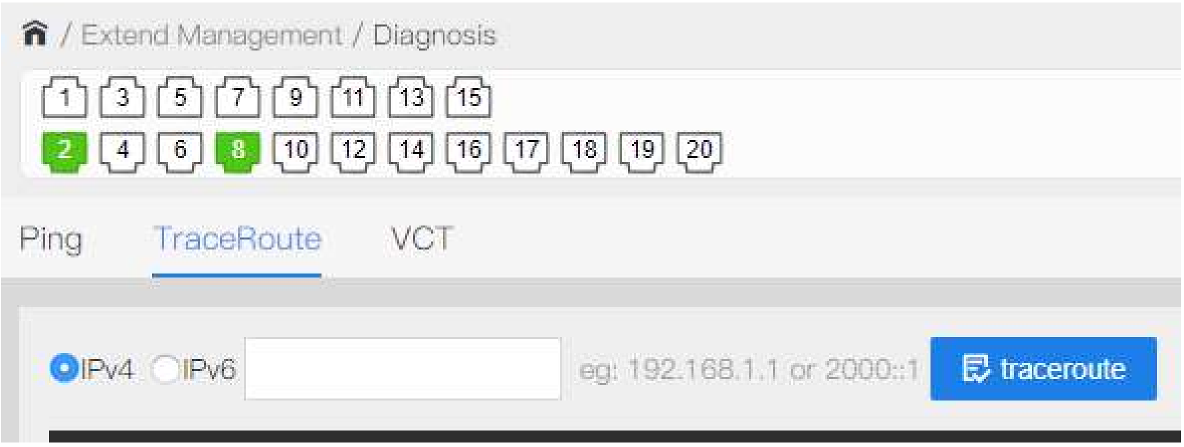
Diagnostic tests: including Ping, TraceRoute, VCT.

3.8.6.1 Ping



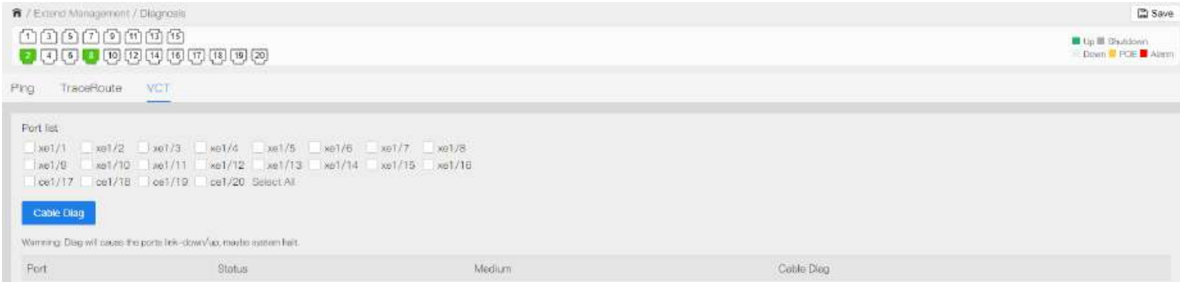
Ping: A function used to test network connectivity. It determines whether the network between the source device and the target device is reachable and the connection is normal by sending an ICMP Echo Request packet to the target device and waiting to receive an ICMP Echo Reply packet from the target device. Specifically, if the switch successfully receives the reply from the target device, it indicates that the network connection between the two is normal; If no response is received, it may indicate that the network is faulty, the target device is unreachable, or there is a device in the middle blocking the transmission of the data packet. In addition, some information about the network connection, such as round-trip time (RTT), can be obtained through the Ping command, which can be used to assess network latency.

3.8.6.2 TraceRoute



TraceRoute: A function used to track the path that network data packets take from the source device to the destination device. It works by sending a series of packets with different time to Live (TTL) values to the destination address, and each time the packet passes through a router in the network, the TTL value decreases by 1. When the TTL drops to 0, the router returns an ICMP (Internet Control Message Protocol) timeout message to the source device. By analyzing these returned messages, TraceRoute can determine the IP address and response time of each router the packet passes through, thereby showing the packet's transmission path in the network. It helps network administrators diagnose network connection problems, determine the location of network delays, and detect network topologies, etc.

3.8.6.3VCT



VCT: The VCT of the switch is the Virtual Cable Test function. It uses TDR (Time Domain Reflectometry - time-domain reflectometry) technology to detect the physical condition of network cables.

The VCT works by the switch actively sending a pulse signal to the wire, and when the signal encounters the end of the cable or the point of failure, part or all of the pulse energy is reflected back to the source. VCT technology calculates the distance the signal travels to or back to the point of failure by measuring the transmission time of the pulse signal in the wire.