L2 Lite Cloud/WebManaged Switch

(10 Ports+) User Manual

Version：2026.01.21-V1.0.1

Introduction:

This manual is provided for L2 lite managed switch ,The device information (except PoE Settings) displayed in this manual is based on 28ports PoE as a reference. For specific information, please refer to the actual device model used. Please read this manual before managing the device.

Suitable users:

This manual is applicable to network administrators of similar IT and network technologies.

Precautions:

Do not put the product too close to water, for example, in a damp basement or near by a swimming pool. Avoid electric storm. Electric shock may occur in case of lightning.

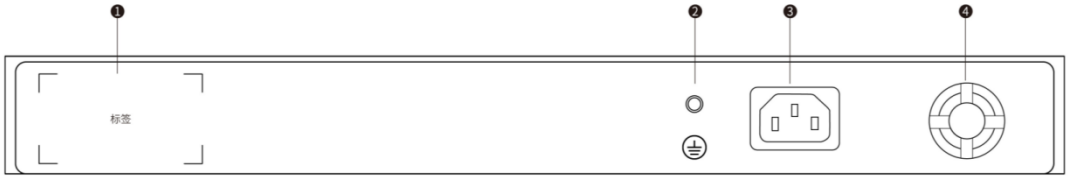
Directory

1. Specifications

Front panel

Device Features	Default
1(Indicator Light)	PoE : Red LED
1(Indicator Light)	L/A(LINK/ACT) : Green LED
1(Indicator Light)	PWR : Red LED
1(Indicator Light)	SYS : Green LED
2(Reset)	Reset Button（Press and hold for about 5 seconds to reset the device）
3(Port 1~24)	PoE Port
4(Port 25~26)	Uplink electrical port
5(Port 27~28)	Uplink optical port

Rear panel



Device Features	Default
1(Tag information)	-
2(Ground screw hole)	-
3(Power supply)	Input AC 90~240V
4(Cooling fan)	-

2. Login device

Environmental requirements
Browser: Supports Google Chrome, IE9.0, IE10.0, IE11.0 and some browsers based on Google/E core (such as 360 Security Browser, it is recommended to use the high-speed mode). When using other browsers to log in to Web Management, abnormalities such as garbled characters or format errors may appear.

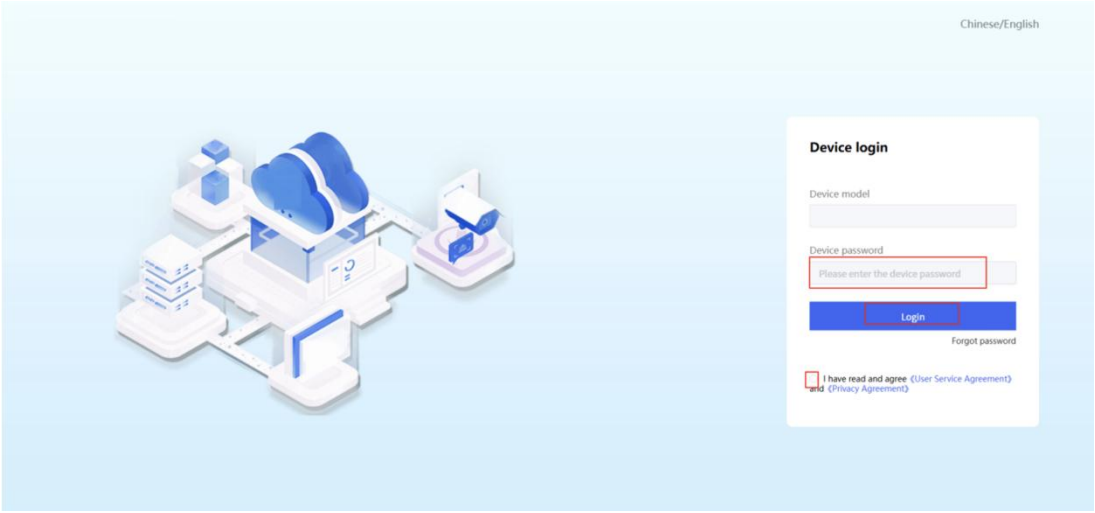
Resolution: It is recommended to set the resolution to 1024*768 pixels or above. At other resolutions, the page font and format may be misaligned, not beautiful enough, and other abnormalities.

2.1 Login Web

Use a network cable to connect the switch port to the PC's network port, configure an IP address for the PC that is in the same network segment as the device's default IP address, and ensure that the PC can ping the switch device. For example, set the PC's IP address to 10.253.10.200.

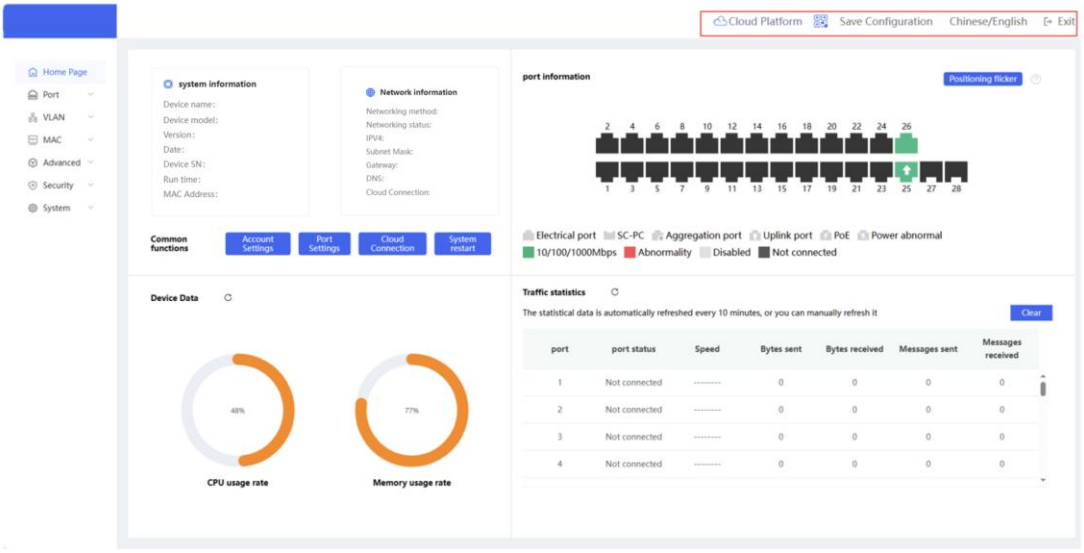
Device Features	Default
Device IP	10.253.10.253(Example)
Password	admin

Enter the device's IP address in the browser address bar to login.
01 Default IP address of the switch 10.253.10.253 (Example)
02 Default IP address of the switch 10._____ (Please check the switch body sticker information)



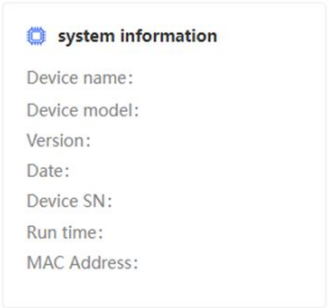
3. Home Page

3.1 Quick Navigation Bar



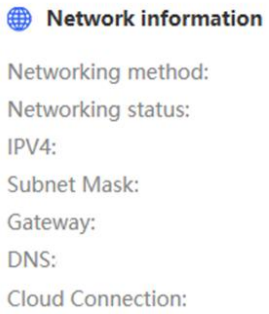
Cloud Platform: Click to automatically redirect to the Cloud Web login page；
QR Code: Hover the mouse here to display QR codes for downloading the APP and binding devices；
Save Configuration: After configuring switch functions, click "Save Configuration" to permanently save settings and prevent configuration loss during power failure；
Chinese/English: Toggle the system language; click to switch language；
Log Out: Exit the current device management login page. The device allows a maximum of 1 concurrent connection. To access the device from another PC, users must log out from the currently connected PC first.

3.2 System Information



This field allows editing the device name, primarily used for custom device identification，It displays detailed device information including model, software version, firmware date, serial number (SN), uptime, MAC address, etc., for easy management and identification.

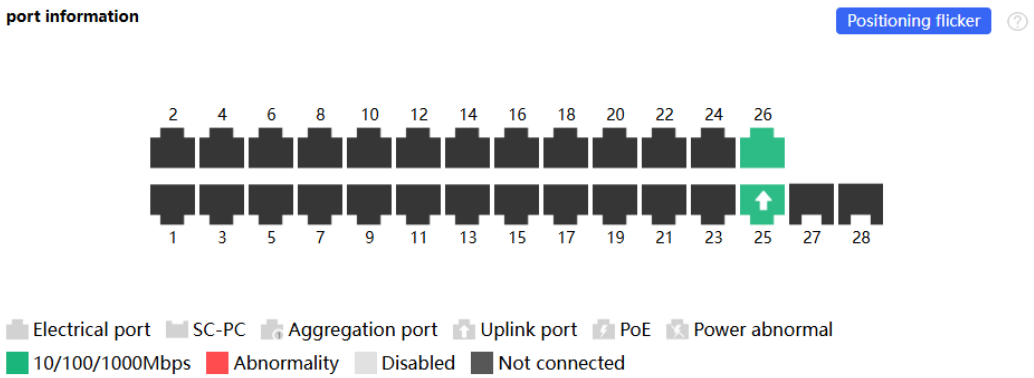
3.3 Network Information



Here you can view the device's IP address information obtained via default IP configuration or DHCP, as well as the current network status and its connection state to the Cloud server.

Note:
If the device's cloud connection status shows "Disconnected", it may be caused by incorrect IP/DNS configurations. Please verify DHCP parameters distributed by upstream devices, or manually modify the IP/DNS addresses to ensure normal cloud connectivity.

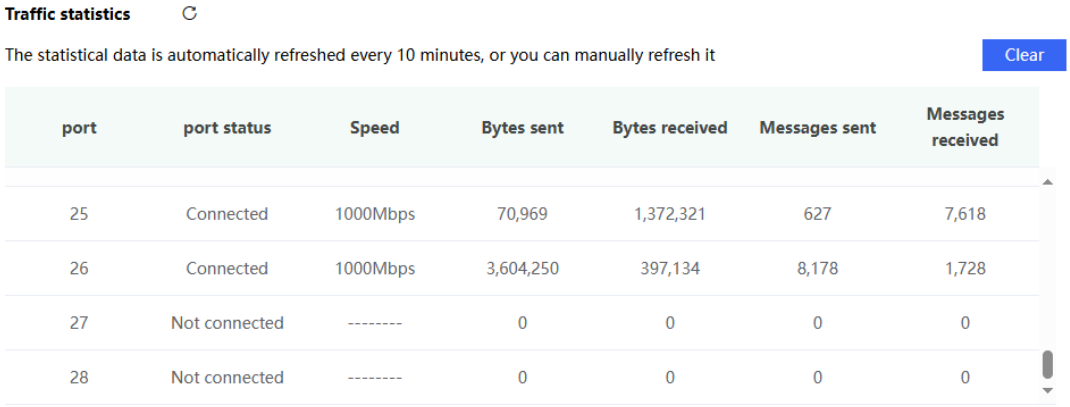
3.4 Port Information



This area displays the real-time status of the device ports for quick access to port information;
After enabling the location indicator mode, all indicator lights on the device will

blink for 30 seconds to assist in physically locating the device.

3.5 Traffic Statistics

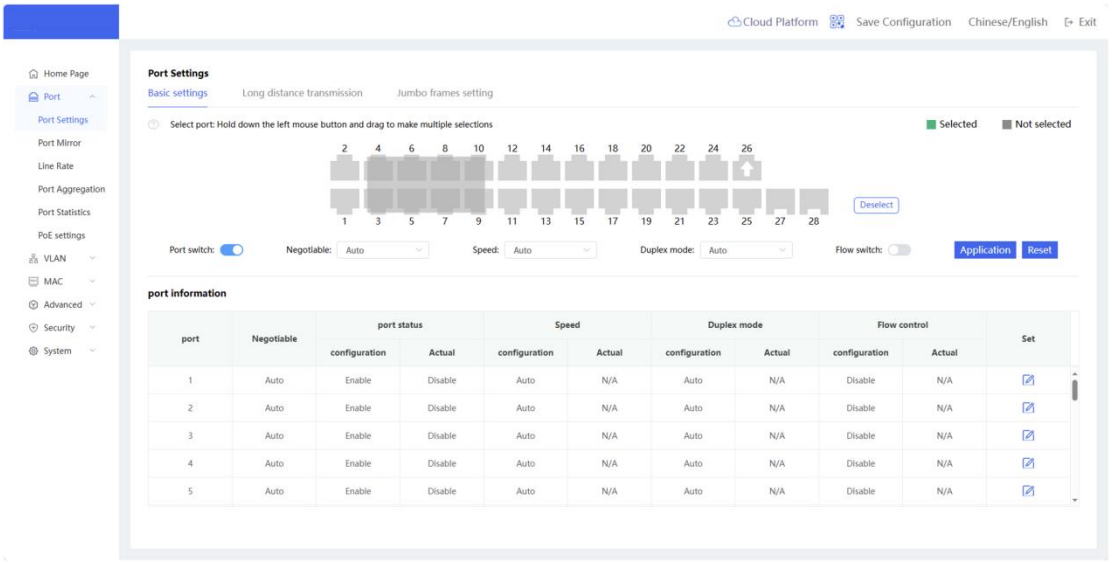


This page displays the device's port status, negotiation speed, total bytes of received/transmitted data, transmitted packet count, and other traffic statistics. You may also click "Clear All" to reset port traffic statistics.
The statistics automatically refresh every 10 minutes. Manual refreshing is also available to view traffic feedback in real-time.

4. Port Settings

4.1 Basic Settings

Set the basic properties of the Ethernet interface, such as speed, duplex, and flow control



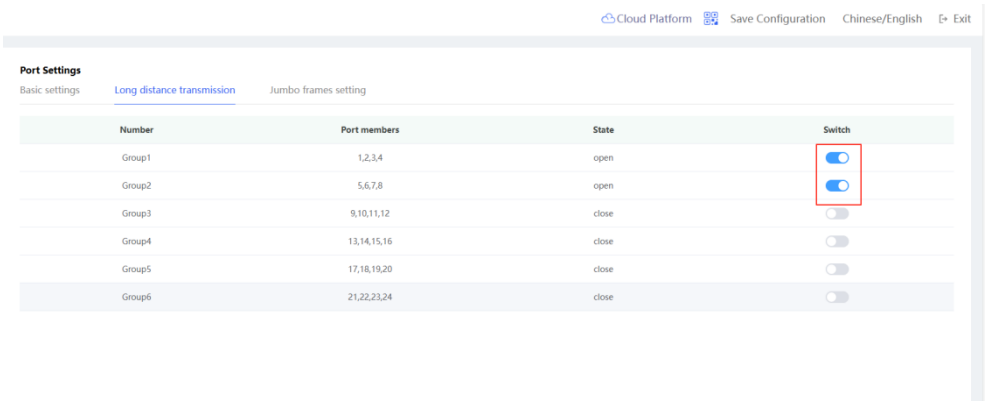
Click a single port icon to select it individually. To select multiple ports, click several icons or hold the left mouse button and drag.
After configuring the selected ports' Status, Negotiation Mode, Speed, Duplex Mode, and Flow Control, click <Apply> to activate the settings.

Specification	Introduction	Default
Port	Click the port icon. If it is green, it means it is selected.	N/A
Port Switch	After the port is closed, the port cannot send or receive messages (PoE function is not affected)	Auto
Negotiated Mode	There are two modes: automatic and forced. When set to automatic, the local and remote devices automatically select the best common rate and duplex mode.	Auto
Negotiated Rate	Set the working speed of the Ethernet physical interface. When the negotiation mode is automatic, the negotiation speed can be set to automatic (10M/100M/1000M), 10M/100M, 10M; When the negotiation mode is forced, the negotiation speed can be set to 10M/100M	Auto
Duplex Mode	Full-duplex: enables the port to receive data packets while sending data packets Half-duplex: controls the port to only send or receive data packets at the same time Automatic: the duplex state of the port is determined by automatic negotiation between the local port and the peer port	Auto
Flow Control	After the flow control is turned on, the port will process	Off

	the received flow control frames and send flow control frames when the port is congested to coordinate the data transmission rate between the sender and the receiver.	

4.2 Long Distance Transmission

This function is enabled by group. After it is enabled, the working rate of the group member port will automatically drop to 10M (the group member port is basically set to fixed and cannot be configured) to support long-distance transmission of 250 meters.



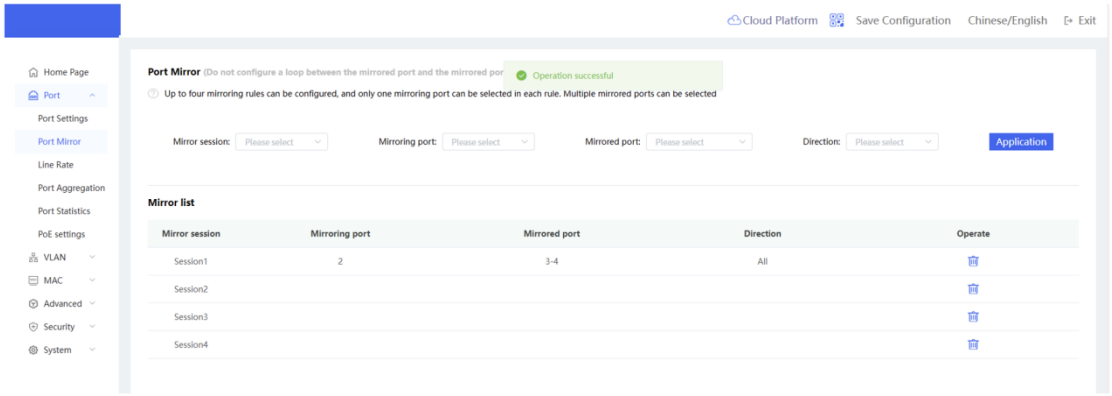
4.3 Jumbo Frames Setting

Jumbo frames are Ethernet frames with a frame length greater than 1522 bytes. The use of jumbo frames can fully utilize the performance of Gigabit Ethernet and increase data transmission efficiency by 50% to 100%.

This page is used to configure jumbo frames on the switch. Turn on <Jumbo Frame Switch>, select the maximum supported frame length (bytes) ranging from 2K to 15K, and click <Save> to take effect.

4.4 Port Mirror

Port Mirror replicates traffic from a specified source port to another port connected to a network monitoring device. Once configured, all packets entering or leaving the source port are copied and forwarded to the destination port. A packet analyzer is typically connected to the destination port to monitor ingress and egress traffic of the source port.



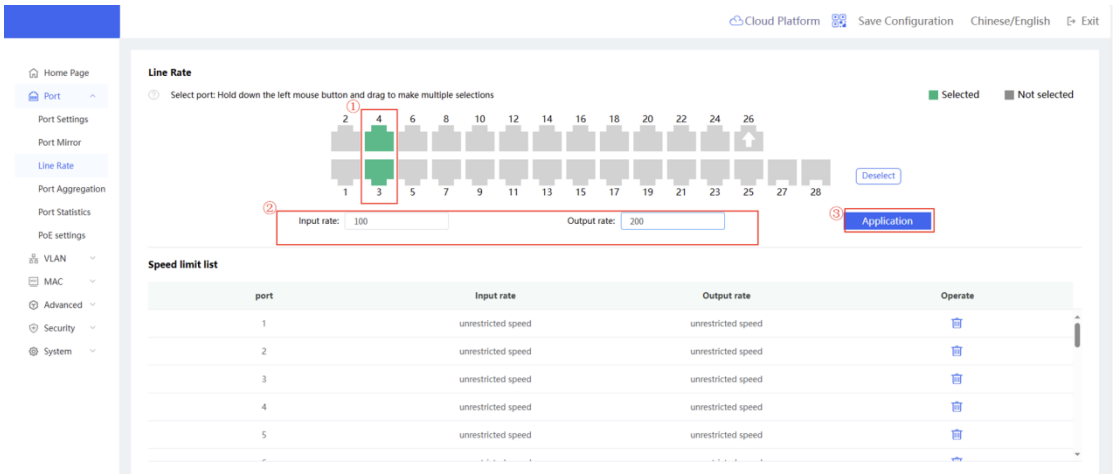
After configuring the mirroring session, mirroring port, mirrored port, and Direction, click <Apply> to take effect.

Note:

You can configure up to four mirroring rules. In each rule, you can only select one mirroring port, but you can select multiple mirrored ports.

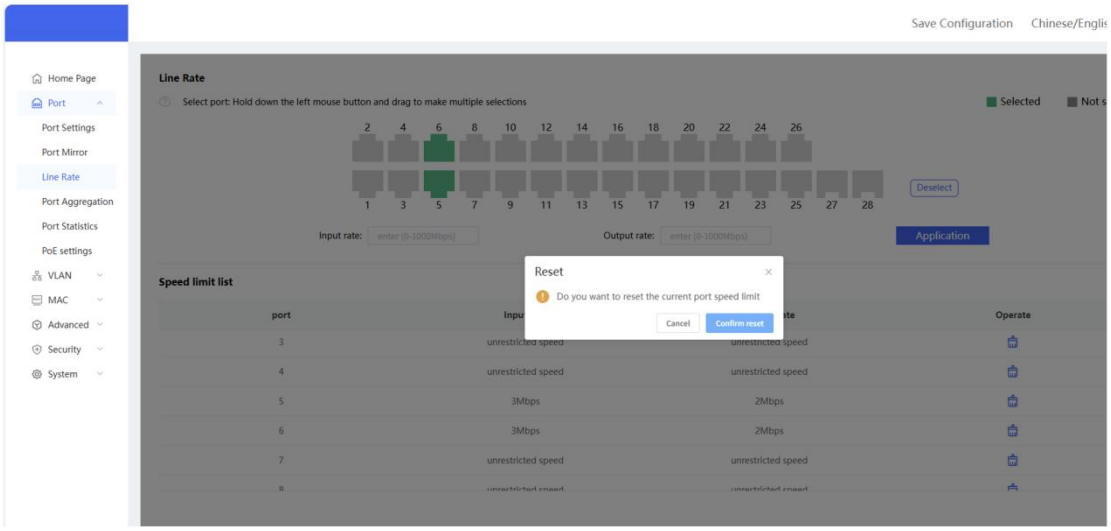
4.5 Line Rate

Line Rate controls traffic throughput on switch ports. By restricting bandwidth, it ensures rational allocation of network resources and prevents specific devices from consuming excessive bandwidth that may affect normal operations of other devices.



Configure traffic limiting rules for ports, including ingress rate limit and egress rate limit.

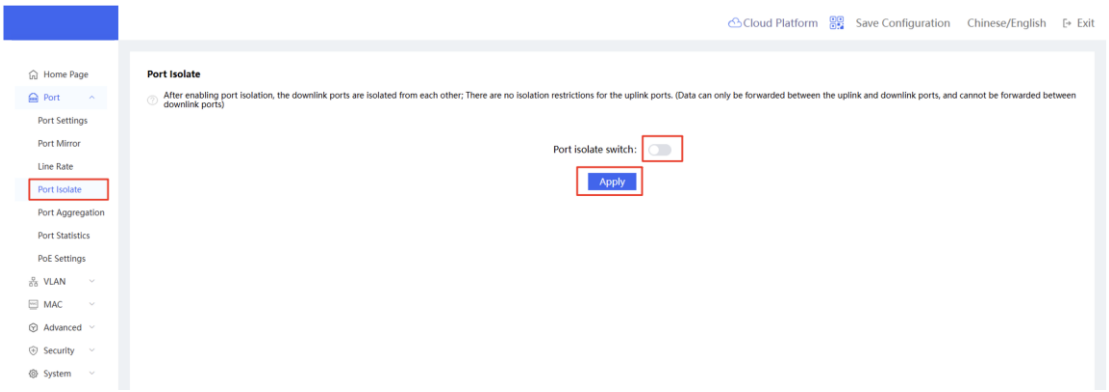
Select ports, enter ingress/egress rates (range: 0-1000 Mbps; 0 = no rate limit), then click <Apply> to activate.



Clear rate limiting configurations (set to no limit) via the <Actions> menu on the corresponding port.

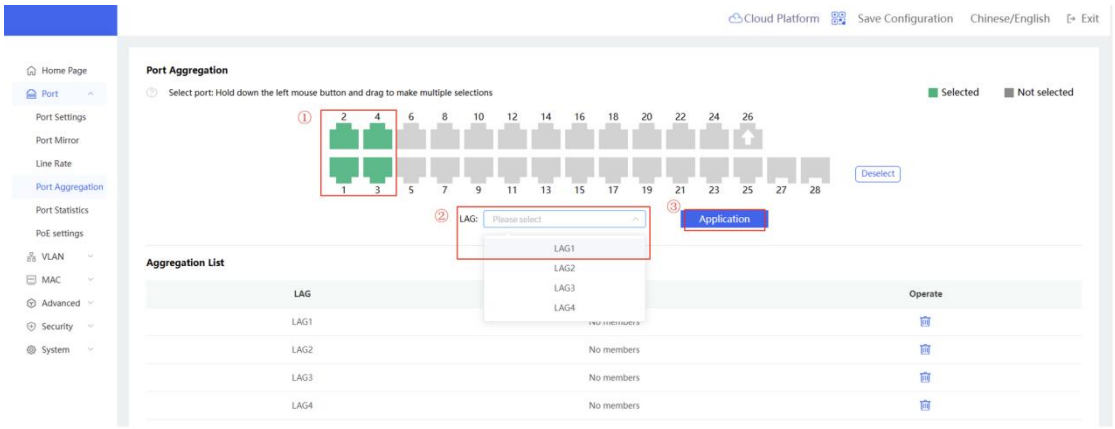
4.6 Port Isolate

After enabling port isolation, the downlink ports are isolated from each other; There are no isolation restrictions for the uplink ports. (Data can only be forwarded between the uplink and downlink ports, and cannot be forwarded between downlink ports)



4.7 Port Aggregation

Port aggregation refers to a logical aggregation port group formed by aggregating multiple physical member ports to increase link bandwidth and achieve mutual link backup.



Select the corresponding port and aggregation group and click <Apply> to add one or more ports to the aggregation group

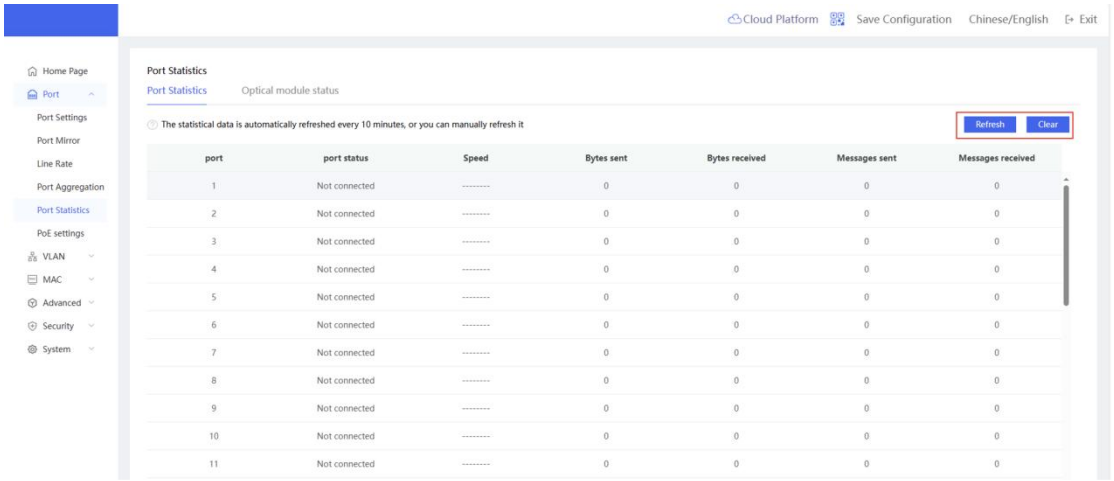
You can clear the members of the aggregation group in the corresponding aggregation group <Operation>.

Note: The maximum number of members in the aggregation group is 8

4.8 Port Statistics

Port Statistics displays traffic information for device ports, including connection status, receive/transmit rates, total bytes received/sent, and transmitted / received packet counts.

The statistics automatically refresh every 10 minutes. Manual <Refresh> is available for real-time traffic monitoring.



Click <Clear All> to reset all port traffic statistics and restart data collection.

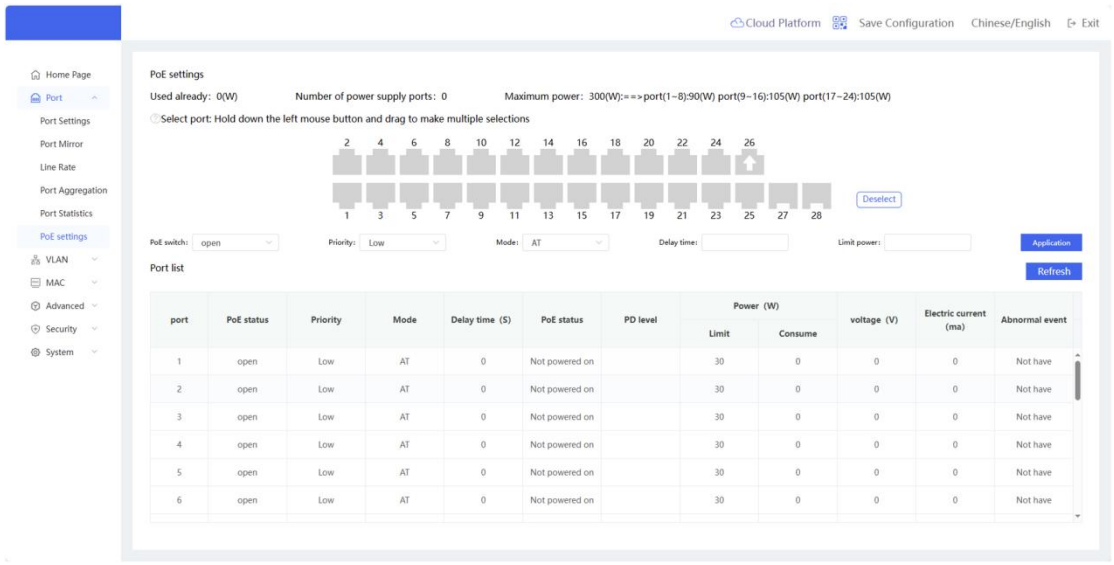
4.9 Optical module status

Displays the optical port module status, module temperature, voltage, current,

transmit power, receive power and signal reception status.

4.10 PoE Settings

The device supports powering PoE-powered devices through ports. Users can view the current power status of the system and ports, and configure port power controls.
This page displays the system's maximum PoE power, used power, and the number of currently powered ports.
In Auto mode, the system allocates power based on the detected PD class. Fixed power values are assigned: Class 0 at 15.4W, Class 1 at 4W, Class 2 at 7W, Class 3 at 15.4W, Class 4 Type 1 at 15.4W, and Class 4 Type 2 at 30W. In this mode, if a port connects to a Class 3 device, the PoE power supply will allocate 15.4W to the port even if the device only consumes 11W.



The port list displays voltage, current, output power, and current power status during port power supply. Users can enable/disable the port's PoE power function using the PoE switch. When turned off, the port ceases power delivery. For ports already powering connected devices, if a power anomaly causes shutdown, you can manually repower the port to restart the powered device.

Note：

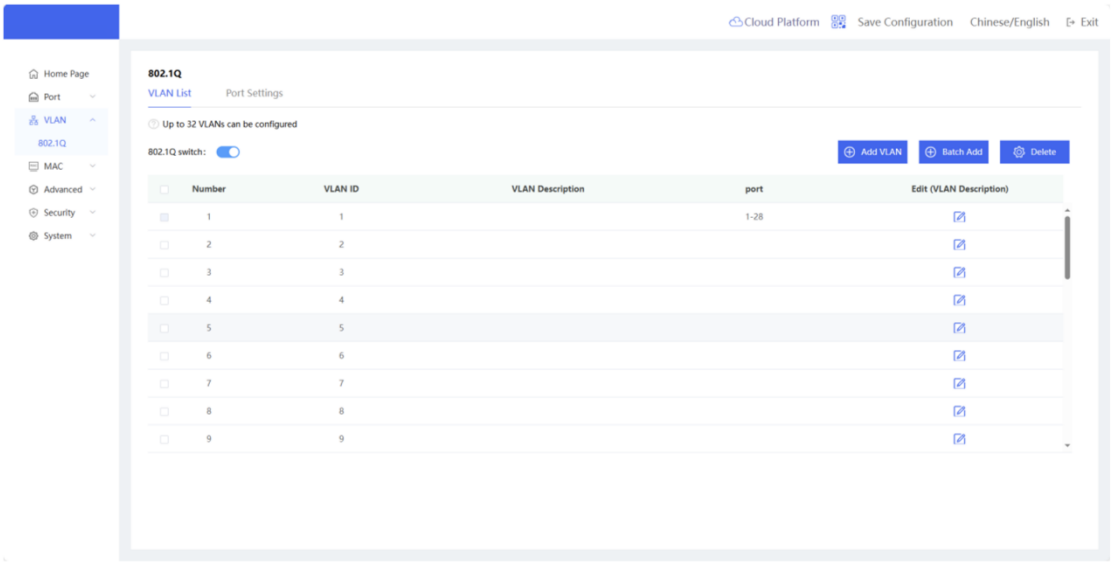
Port(1~8):90(W) port(9~16):105(W) port(17~24):105(W)

5. VLAN Management

VLAN (Virtual Local Area Network) is a logical network partitioned within a physical network. Beyond lacking physical location constraints, VLANs possess the same attributes as standard physical networks. Each VLAN maintains an independent broadcast domain, with Layer 2 isolation between different VLANs. Layer 2 unicast, broadcast, and multicast frames can only be forwarded and propagated within a single VLAN and will not enter other VLANs directly. When a port is assigned to a VLAN, all terminals connected to that specific port become part of the virtual network. The entire network supports multiple VLANs. Inter-VLAN communication is achieved via Layer 3 devices or routed ports. VLAN configuration encompasses two functions: creating VLANs and assigning port VLAN memberships.

5.1 802.1Q Management

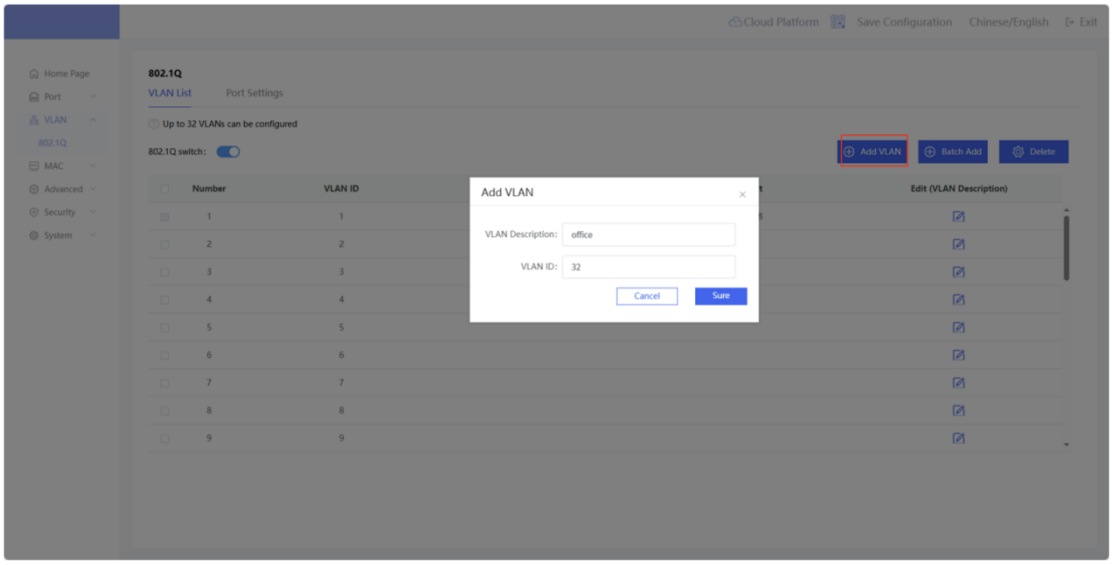
The VLAN list displays all existing VLAN information, allowing modification or deletion of current VLANs and creation of new VLANs (up to 32 VLANs can be created).



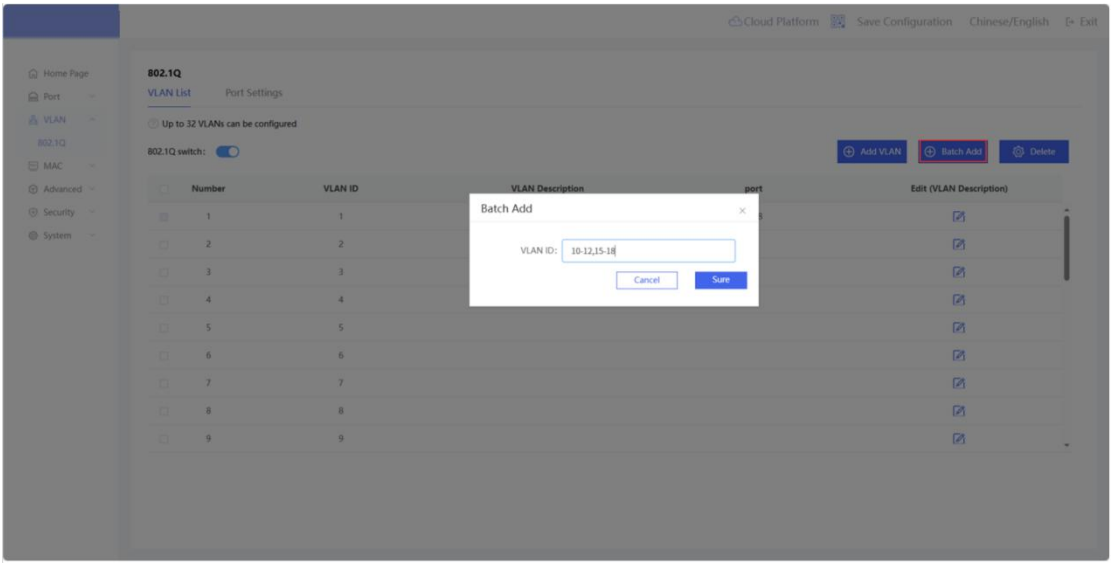
Disabling the 802.1Q VLAN switch will clear all VLAN configurations. When VLAN is disabled, data will be forwarded based on the MAC address table (VLAN passthrough mode).

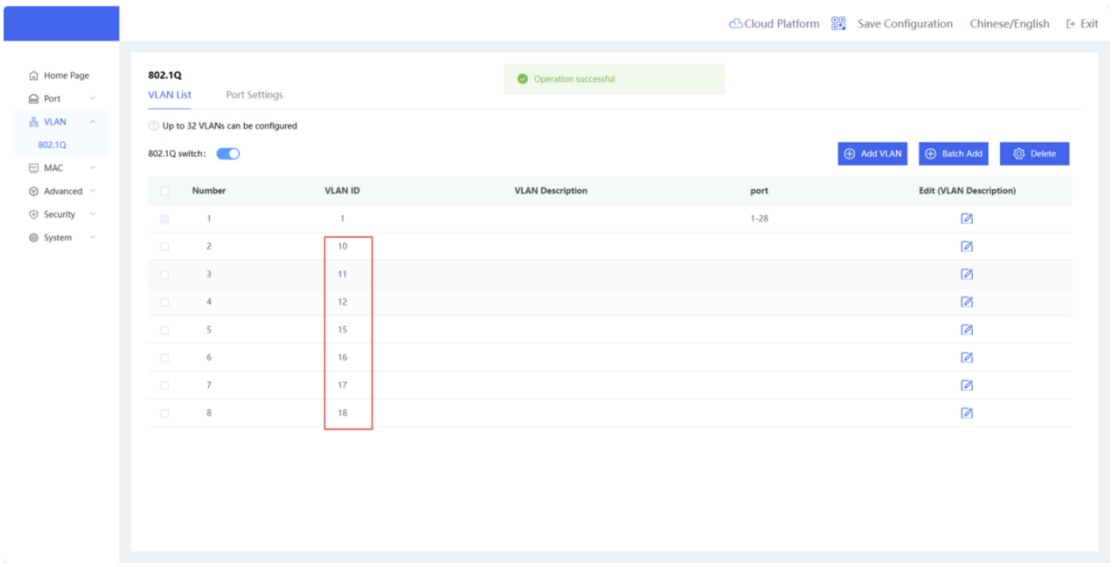
5.1.1 Add VLAN

To create a single VLAN: Click <Add VLAN>, enter the VLAN description (optional) and VLAN ID, then click <Sure>. The newly added VLAN will appear in the VLAN List.
*Note: VLAN descriptions cannot exceed 10 characters and may only contain spaces, 0-9, a-z, A-Z. -_.。



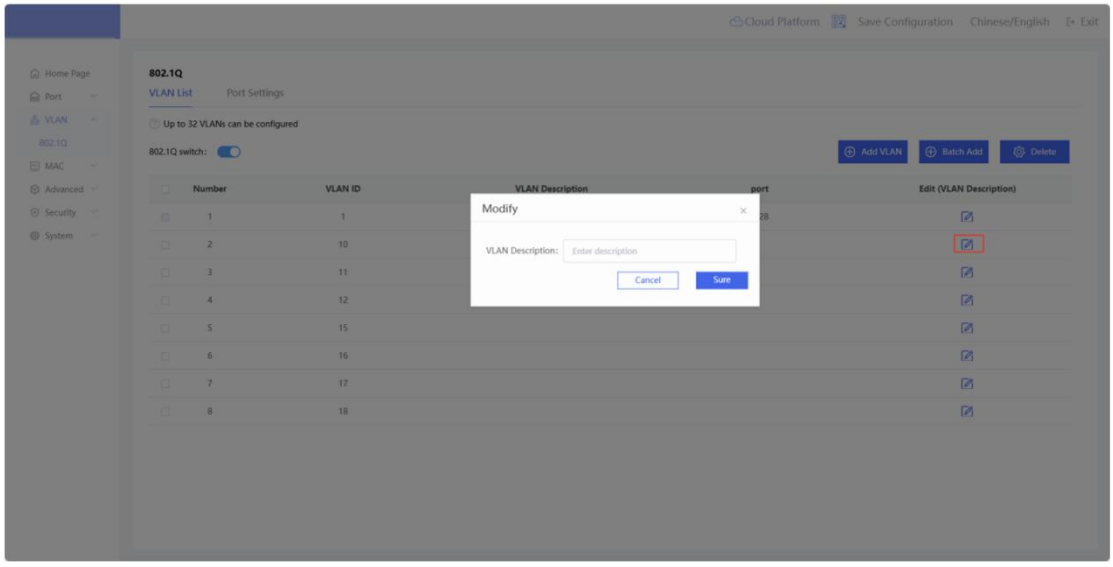
To batch add VLANs: Click <Batch Add>, enter VLAN ID ranges in the pop-up window (multiple ranges separated by commas, or continuous VLAN IDs connected with hyphens), then click <Sure> to create multiple VLANs simultaneously. The new VLANs will appear in the VLAN List.





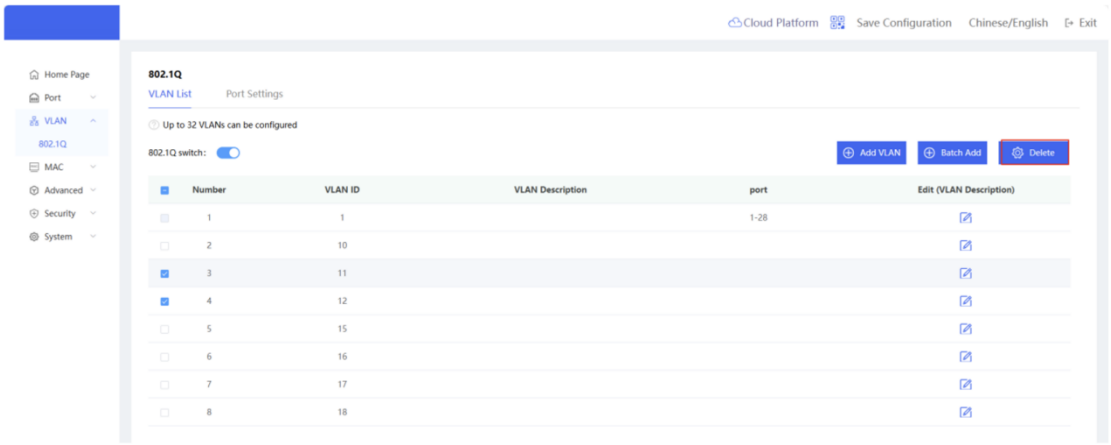
5.1.2 Modify VLAN Description

Click the <Modify symbol> under the "VLAN List" edit (VLAN description) operation column to modify the description information of the specified VLAN. Note: The VLAN description cannot exceed 10 characters and can only use standard characters such as space, 0~9, a~z, A~Z, -_.



5.1.3 Delete VLAN

Batch delete VLANs: Select the VLAN items to be deleted in the "VLAN List", and then click <Delete> to delete multiple/single VLANs at one time.

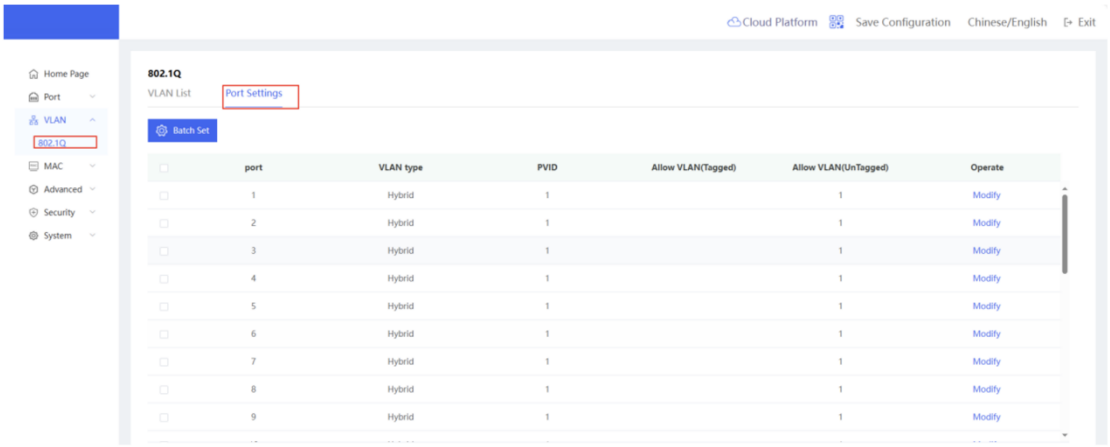


Note:

VLAN1 is the default VLAN and cannot be deleted.

5.2 Port Settings(VLAN)

This page displays the current port VLAN division. Please create VLANs in the VLAN list first, and then perform VLAN-based port configuration.



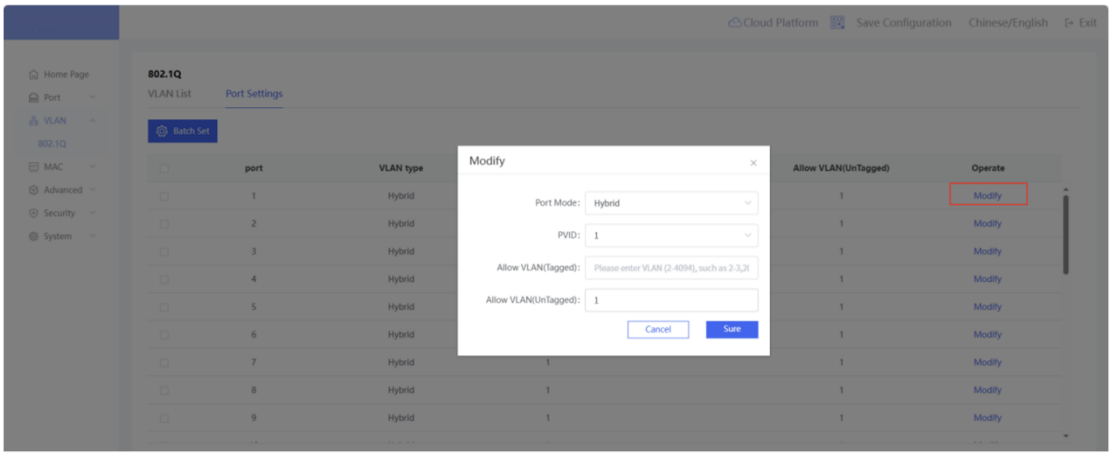
By configuring the port mode and VLAN members of a port, you can determine the VLANs that the port allows to pass and whether the port carries a TAG when forwarding packets.

Port Type	Introduction
Access	An Access port belongs to only one VLAN, permitting frames solely from that VLAN (known as the Access VLAN). Frames sent from an Access port carry no VLAN TAG. If an Access port receives an untagged frame from a connected device, it assigns the frame to the Access VLAN and internally adds the Access VLAN ID. Access ports are typically used to connect end devices.
Trunk	A Trunk port can have one Native VLAN and multiple Permit VLANs. It forwards frames from the Native VLAN untagged, while frames from Permit VLANs are tagged with the VLAN ID. Typically used for inter-switch connections, the permitted VLAN range controls which VLAN frames can traverse the port. Note: The Native VLAN must be configured identically on both ends of the trunk link.
Hybrid	A Hybrid port supports one Native VLAN and multiple Permit VLANs, categorized into Tag VLANs and Untag VLANs. The port forwards frames from Tag VLANs with VLAN tags, while frames from Untag VLANs are forwarded untagged.

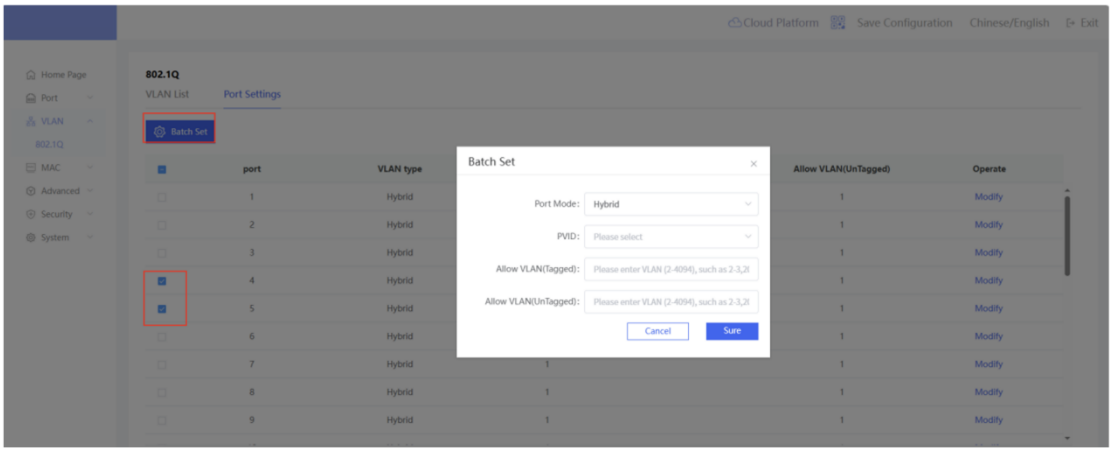
5.2.1 Port VLAN Configuration

To configure VLAN settings for a single port:
Click <Modify> in the operation column for the target port.

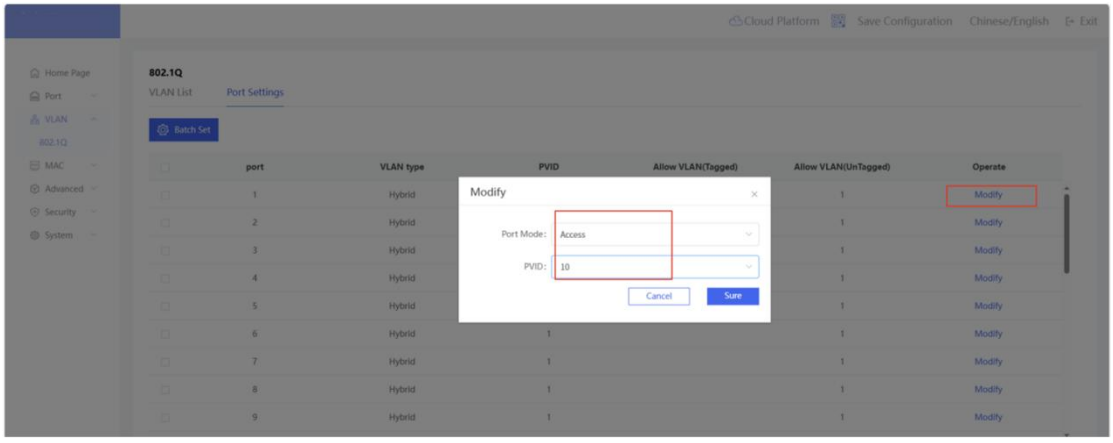
Select the Port Mode (Access/Trunk/Hybrid) from the dropdown menu.
Choose an existing VLAN from the VLAN List as the PVID.



To configure multiple ports with identical VLAN settings: Select the corresponding ports, click <Batch Set>, and follow the same steps as single-port VLAN configuration

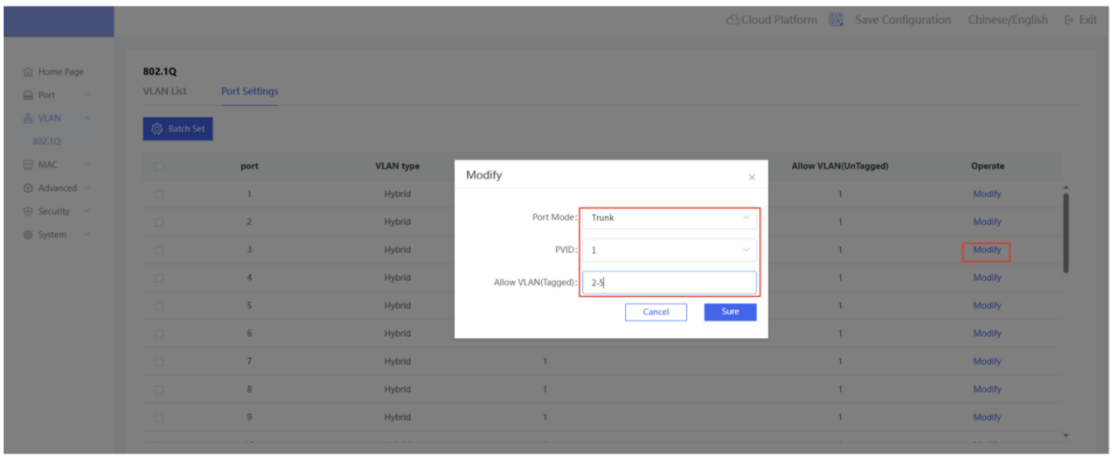


To configure an Access port:
With VLANs 1-5 existing in the VLAN List, click <Modify> in the operation column for the target port, select Access as the port mode, choose a PVID, then click <Sure>

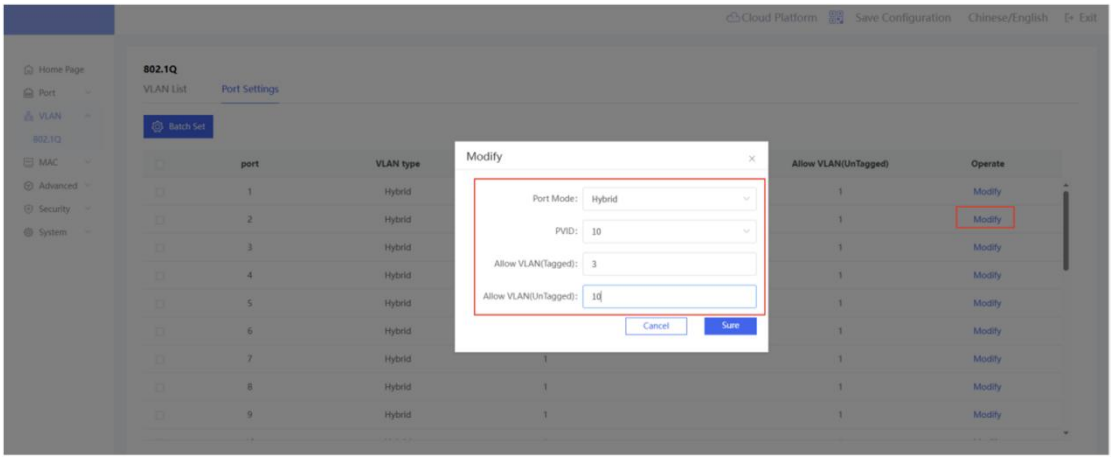


To configure a Trunk port:
With VLANs 1-5 existing in the VLAN List, click <Modify> for the target port,

select Trunk as the port mode, configure the PVID, enter Permitted VLANs (Tagged), then click <Sure>.
Note: The VLAN corresponding to the PVID must be included in the Permitted VLANs (Tagged) list.

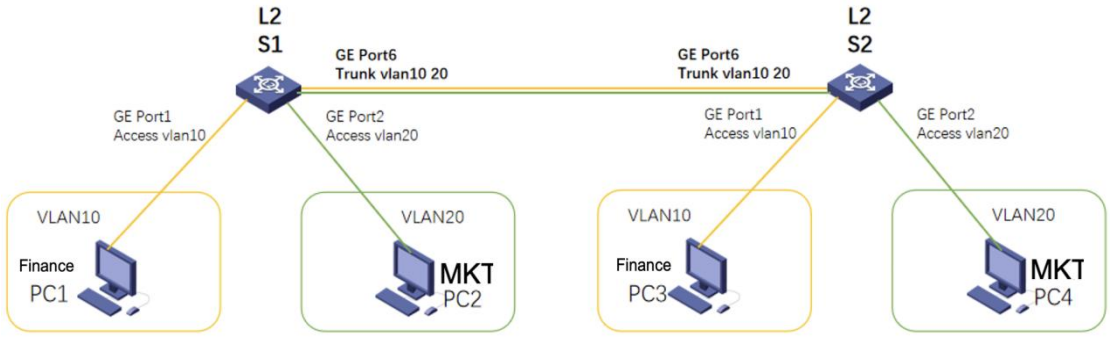


To configure a Hybrid port:
With VLANs 1-5 existing in the VLAN List, click <Modify> for the target port, select Hybrid as the port mode, configure the PVID, optionally enter Permitted VLANs (Tagged) and Permitted VLANs (Untagged), then click <Confirm>.
Note: The VLAN corresponding to the PVID must exist in either the Permitted VLANs (Tagged) or Permitted VLANs (Untagged) list. VLANs cannot overlap between these two lists.

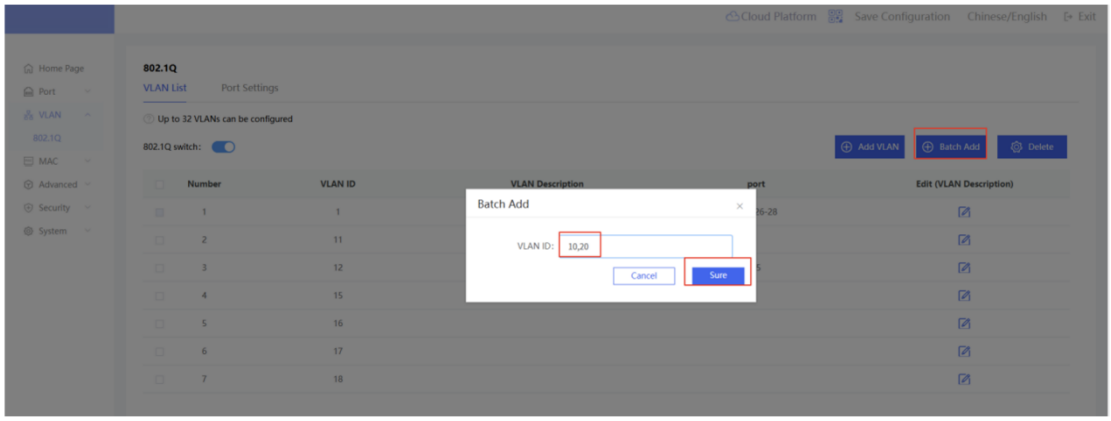


5.3 VLAN Configuration Example

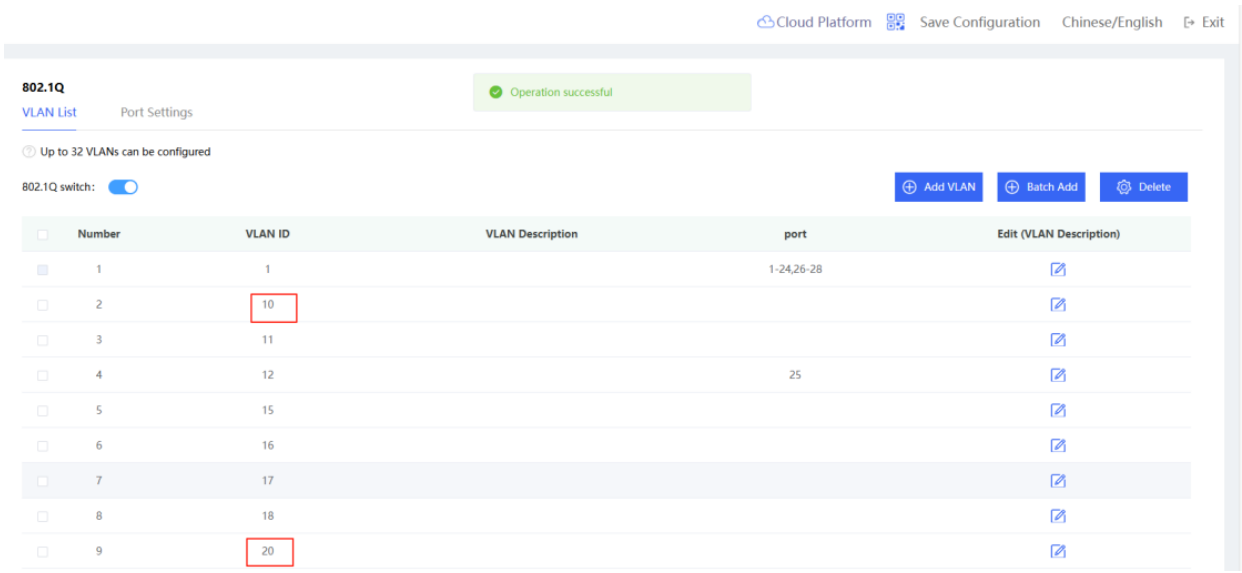
A company's equipment connects two departments, namely the Finance Department and the MKT Department, and needs to access the company network through different devices. For the security of communication and to avoid the flooding of broadcast messages, it is now required that the hosts within the department can communicate with each other, and the hosts in different departments cannot communicate with each other.
At this time, you can configure VLAN division based on interfaces on the device, and divide the interfaces connecting users in the same department into the same VLAN. Users in the same VLAN can communicate directly with each other, and users in different VLANs cannot communicate directly at the second layer.
According to the known requirements, it is now planned that the PCs belonging to the Finance Department are divided into VLAN10, and the PCs belonging to the MKT Department are divided into VLAN20



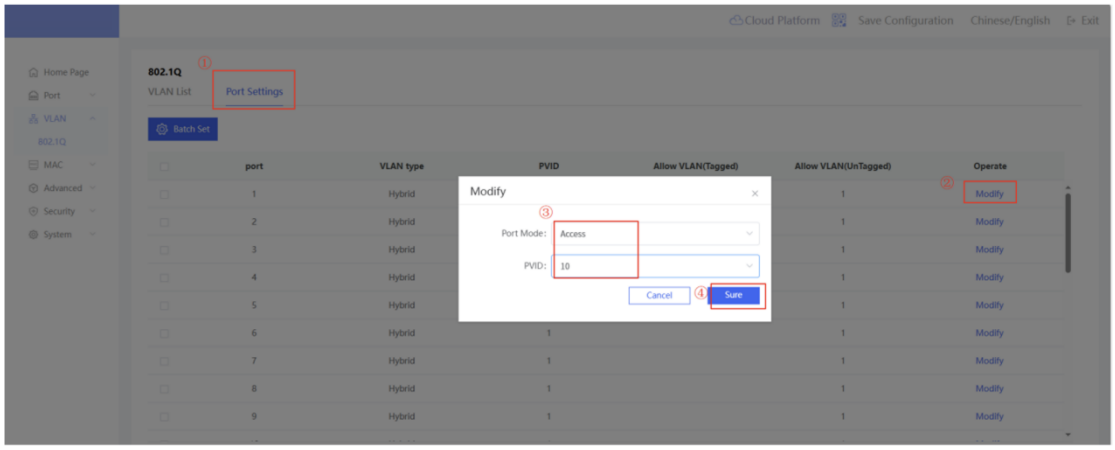
1. Create VLAN10 and VLAN20. <802.1Q Configuration - VLAN List - Batch Add - Enter "10,20" <Sure>



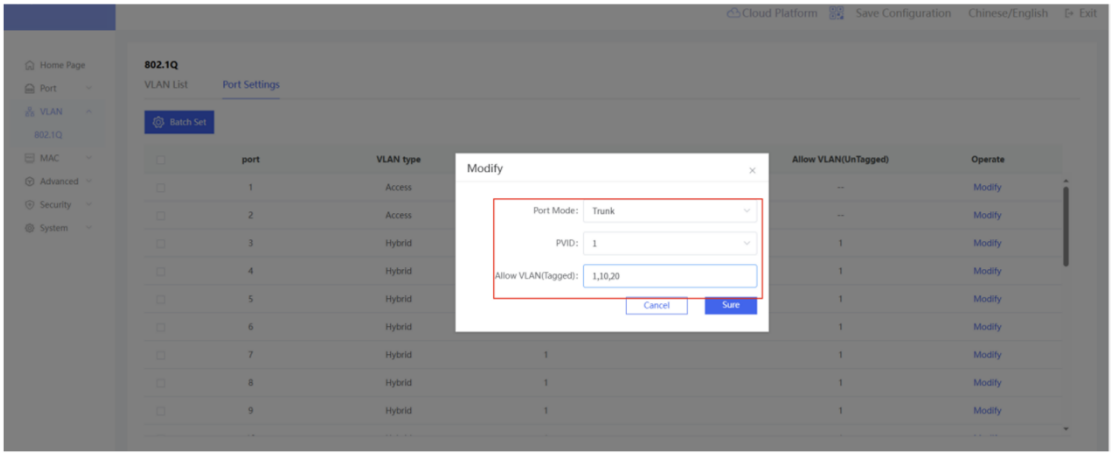
As shown in the figure, the creation is successful.



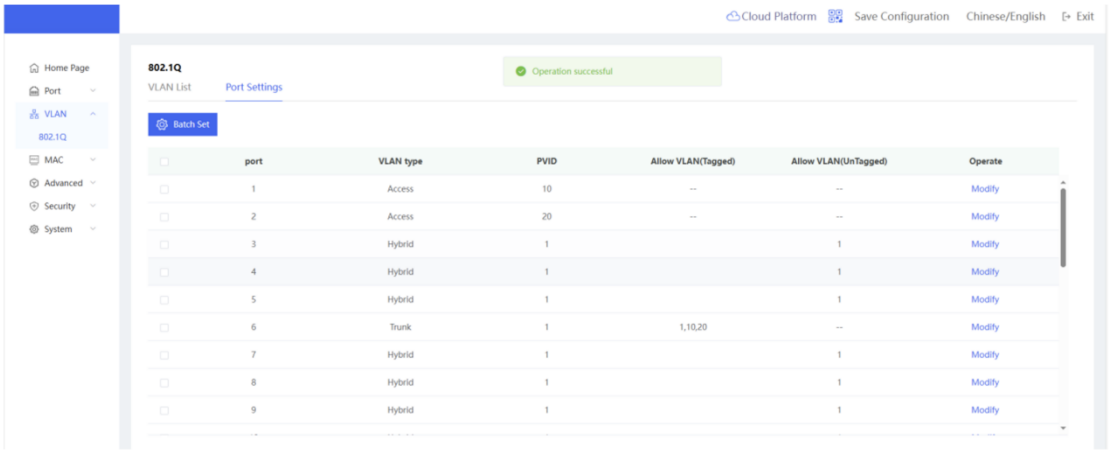
2. Configure S1, port 1 port mode: Access, PVID select 10, <Sure>,Configure S1, port 2 port mode: Access, PVID select 20, <Sure>



3. Configure S1, port 6 port mode: Trunk, allow VLAN input "1,10,20" <Sure>



4. Configuration Complete



Note:

The configuration of S2 is the same as that of S1, so I will not go into details here.

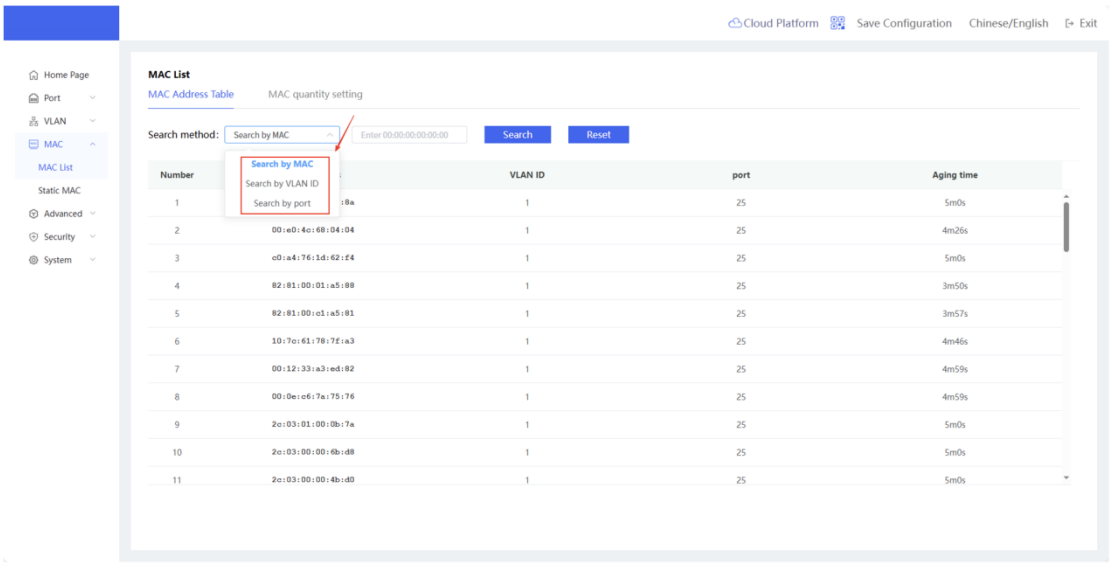
6. MAC management

The MAC address table records correspondences between MAC addresses, ports, and their associated VLANs.
The device checks the destination MAC address in a packet against this table. If a matching entry exists, the packet is unicast through the port specified in the entry. If no match is found, the device broadcasts the packet to all other ports within the same VLAN except the receiving interface.
MAC address entries are categorized as:
Static MAC Address Entry: Manually configured by users. Ensures packets destined to the specified MAC address are forwarded through the designated port.
Dynamic MAC Address Entry: Automatically generated by the device through dynamic MAC address learning.

6.1 MAC List

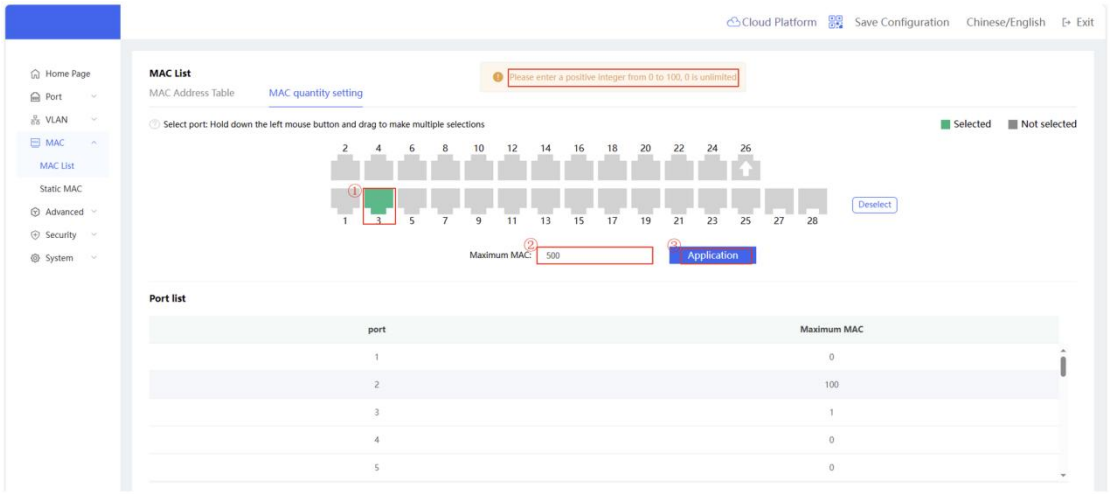
6.1.1 MAC Address List

This page supports MAC address search. The system provides three search methods: Search by MAC address, Search by VLAN ID, and Search by port. Users can select the appropriate search method as needed to quickly locate information.



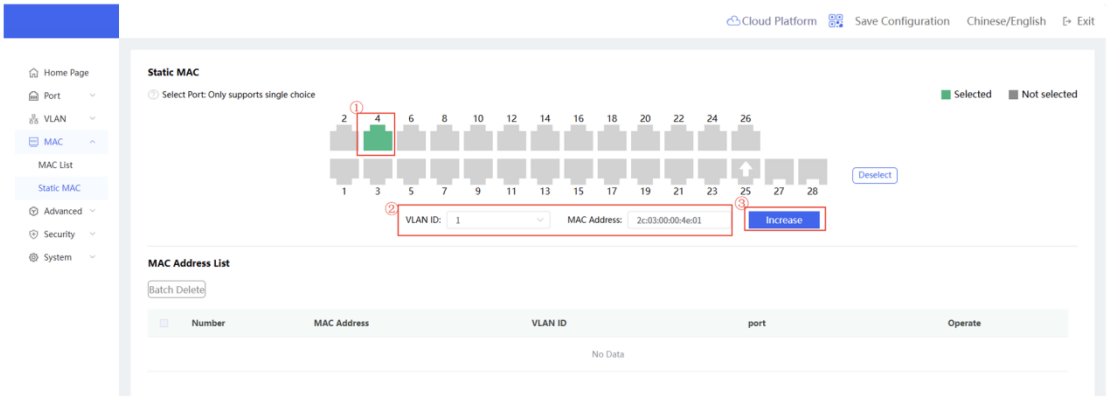
6.1.2 MAC Quantity Setting

By configuring individual or multiple ports, you can impose restrictions on the number of MAC addresses dynamically learned by the selected port(s).

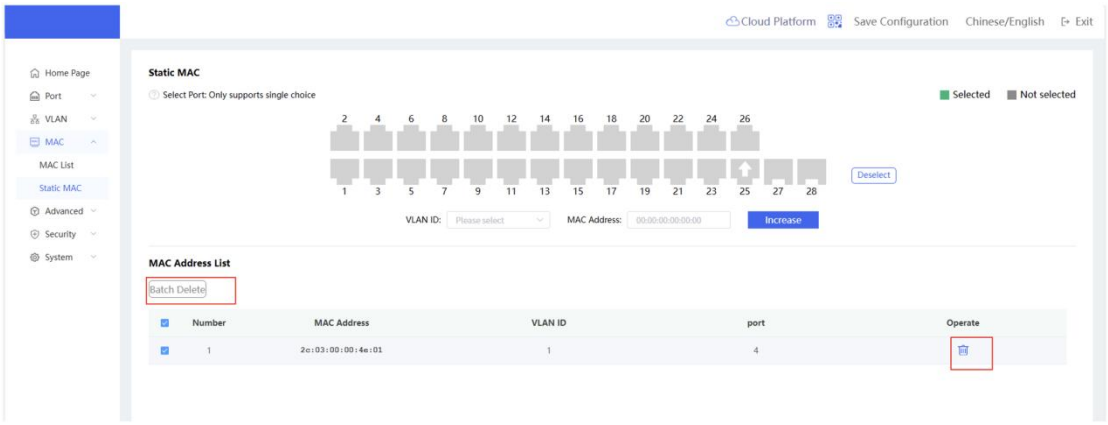


6.2 Static MAC

Users can manually bind the MAC addresses of network devices connected to this equipment to specific ports and VLAN IDs by configuring static MAC address entries. Once a static entry is added, when a frame destined for that MAC address is received within the VLAN, it will be forwarded to the designated port.



Deleting static MAC entries supports both individual deletion and batch deletion.

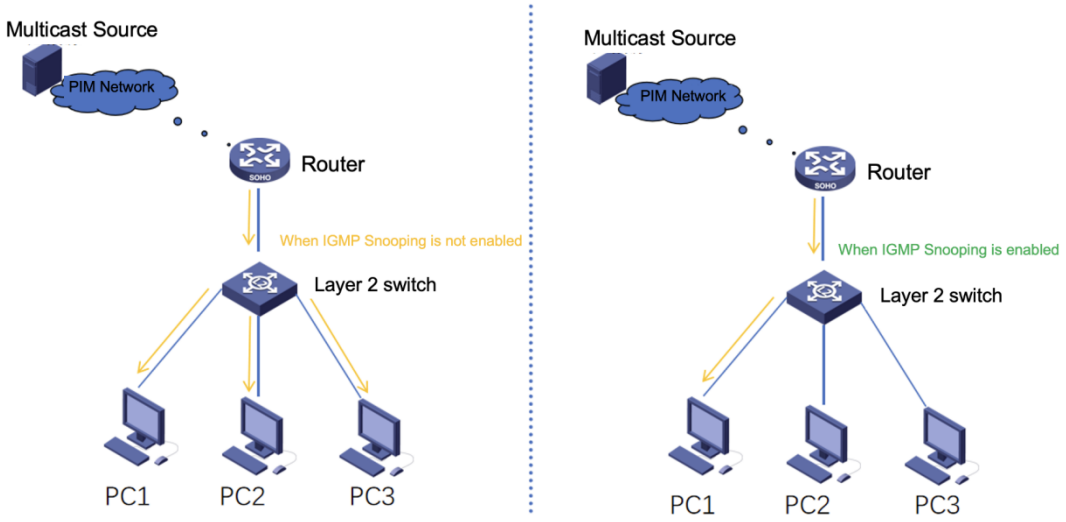


7. Advanced Features

7.1 IGMP Snooping introduction

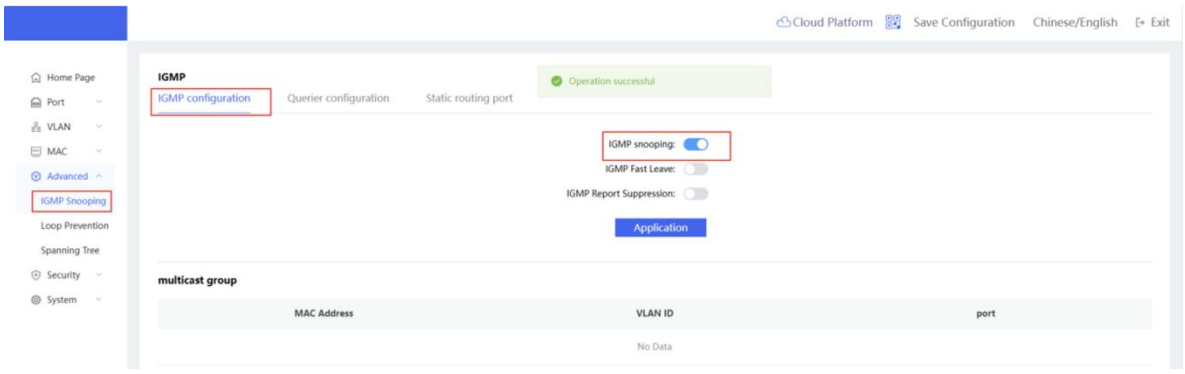
IGMP Snooping (Internet Group Management Protocol Snooping) is an IP multicast snooping mechanism operating at the VLAN level. It manages and controls the forwarding of IP multicast traffic within a VLAN, enabling Layer 2 multicast functionality. Typically, especially in LAN environments, multicast traffic must traverse Layer 2 switches. When IGMP Snooping is not enabled on a Layer 2 switch, IP multicast frames are flooded (broadcast) throughout the VLAN. However, when IGMP Snooping is enabled, the Layer 2 switch listens to IGMP messages exchanged between host devices and upstream PIM multicast routers. This allows the switch to build a Layer 2 multicast forwarding table, ensuring IP multicast traffic is only sent to member ports and preventing unnecessary flooding within the Layer 2 domain.

Comparison before and after IGMP Snooping is enabled



PC1 needs the multicast data, while PC2 and PC3 do not need the multicast data.

7.1.1 IGMP Snooping



Specifications	Introduction	Default
IGMP Snooping	Enable IGMP Snooping globally	Off
IGMP Fast Leave	When enabled, upon receiving an IGMP Leave message on a port, the switch immediately removes that port from the multicast group without waiting for the aging timer to expire. Subsequently, when the device receives Group-Specific Query messages or multicast data traffic for that group, it will no longer forward them to this port This feature is applicable when only a single host is connected to a port, and is typically enabled on access switches directly connected to end-user devices.	Off
IGMP Report message	When enabled, if multiple downstream hosts simultaneously send IGMP Report messages to join	Off

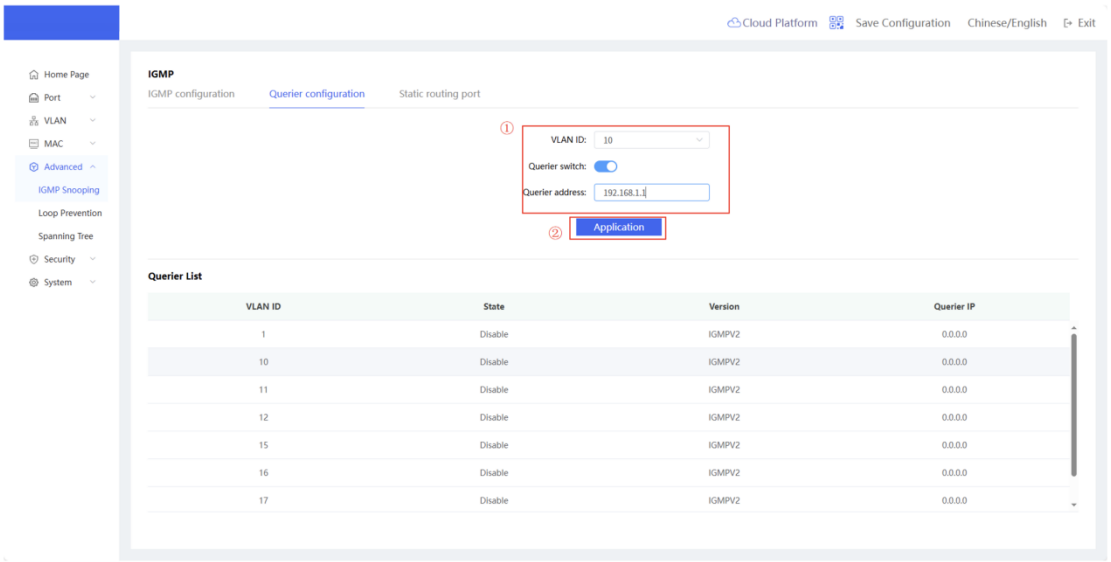
suppression	the same multicast group, the switch will only forward a single copy of the Report message upstream towards the multicast router. This reduces protocol traffic on the network, conserving bandwidth and reducing processing overhead on IGMP multicast devices.	

7.1.2 Configuring IGMP Snooping Querier

By enabling IGMP Snooping, Layer 2 devices can dynamically build Layer 2 multicast forwarding entries by listening to IGMP messages exchanged between hosts and the IGMP querier. This enables efficient Layer 2 multicast delivery.

However, in the following two scenarios, even if IGMP Snooping is enabled on the Layer 2 device, it will fail to dynamically build the Layer 2 multicast forwarding entries correctly because it cannot snoop any IGMP protocol messages:
1. The upstream Layer 3 multicast device has static multicast groups configured on its interface and is not running the IGMP protocol.
2. The multicast source and the user hosts reside within the same Layer 2 network, eliminating the need for a Layer 3 multicast device.

In these cases, the issue can be resolved by configuring an IGMP Snooping Querier on the Layer 2 multicast device. The IGMP Snooping Querier acts as a proxy for the Layer 3 multicast device, sending IGMP Query messages to the user hosts.



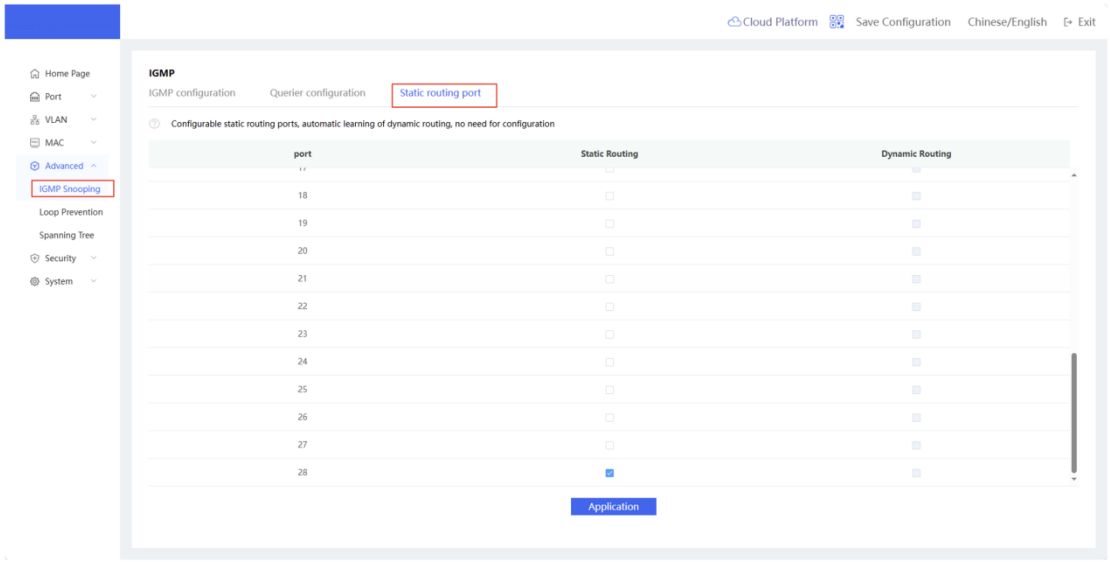
7.1.3 Configuring IGMP Snooping Static Routing Ports

A router port is typically an interface on a Layer 2 device facing upstream towards a Layer 3 multicast device (such as a multicast router or Layer 3 switch). After enabling IGMP Snooping within a VLAN, interfaces belonging to that VLAN learn entries by inspecting multicast protocol messages. When an interface receives an IGMP Query message or a PIM Hello message, the Layer 2 device designates that interface as a dynamic router port. Router ports serve two primary functions:

1.Receiving multicast data from upstream.

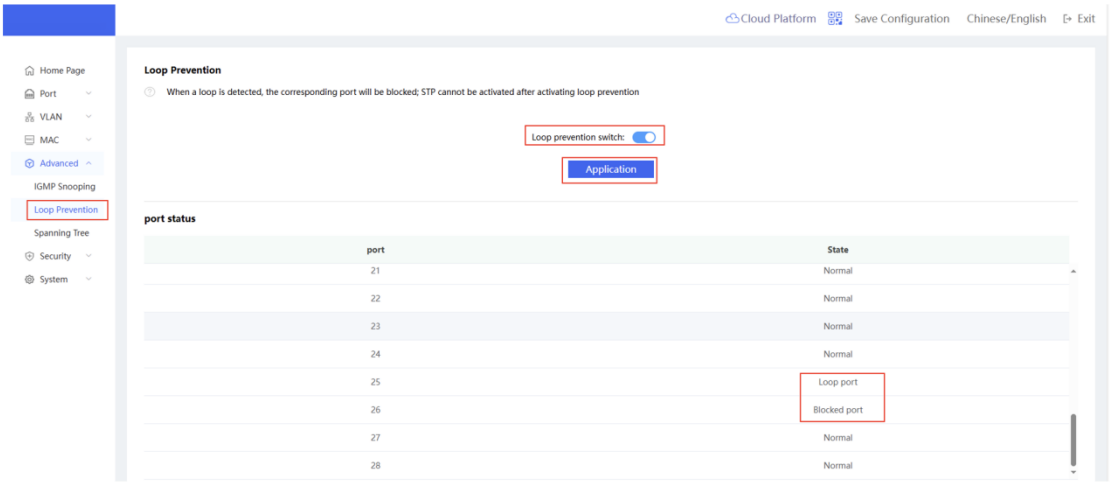
2.Directing IGMP Report/Leave message forwarding. When an IGMP Report or Leave message is received within the VLAN, it is only forwarded to router ports within that VLAN.

Dynamic router ports age out based on a timer. If a dynamic router port does not receive an IGMP Query or PIM Hello message before its aging timer expires, the device will remove that interface from the router port list. To ensure an interface persistently forwards IGMP Report/Leave messages upstream to the IGMP Querier, you can configure it as a static router port.

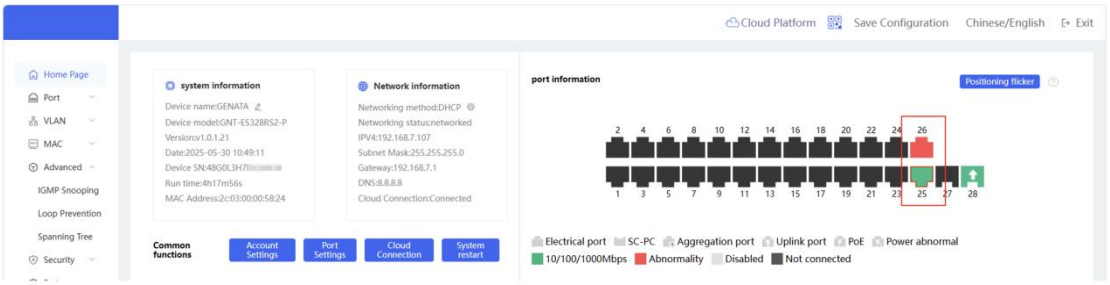


7.2 Loop Prevention

After loop protection is enabled, if a loop exists on the current device, the port causing the loop will be automatically blocked; the port will automatically recover after the loop is resolved. This function is enabled by default.



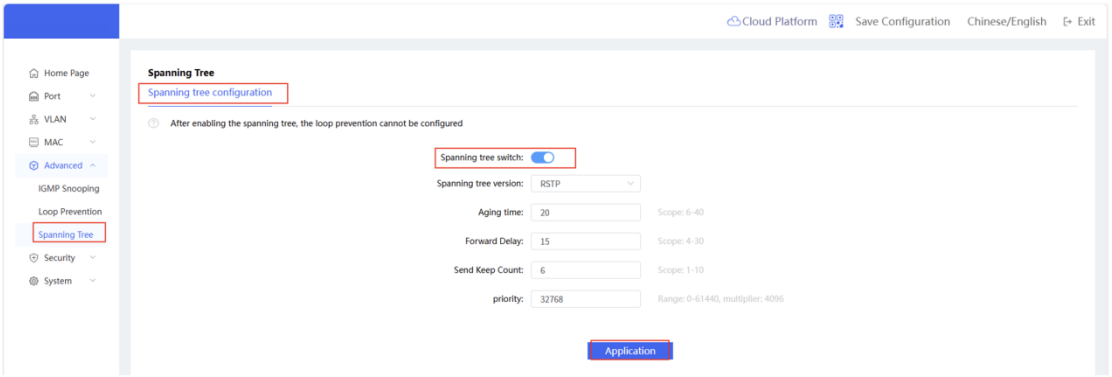
Note: After enabling loop prevention, the STP spanning tree function cannot be enabled. If you want to enable the spanning tree function, you need to disable loop prevention in advance.



Ports 25 and 26 on this page are in a loop-blocked state.

7.3 Spanning Tree(STP)

This device supports the following two spanning tree protocols:
STP (Spanning Tree Protocol)
STP is a Layer 2 management protocol that eliminates network loops by selectively blocking redundant links while providing link backup capabilities.
RSTP (Rapid Spanning Tree Protocol)
RSTP, an evolution of STP, enables rapid network topology convergence. However, like STP, it still operates with a single spanning tree instance shared across all VLANs, preventing load balancing.



Specifications	Introduction	Default
Spanning tree switch	Controls whether to enable the STP function. It takes effect globally. Only after it is enabled can STP related attributes be configured.	Off
Spanning Tree Version	N/A	RSTP
Aging time	The maximum lifetime of a BPDU message. When this time is exceeded, the message will be discarded. If a non-root device does not receive the root BPDU information before the aging time expires, it is considered that the root bridge or the link to the root bridge has failed.	20 seconds
Forwarding Delay	The time interval for the port state to change, that is, the time interval for the port to change from Listening to Learning, or from Learning to Forwarding	15 seconds
Send hold count	Limit the burst number of BPDUs, the maximum number of BPDUs that the interface can send per second	6 counts
Priority	Bridge priority. When electing a root bridge, the device will first compare the bridge priority. The smaller the value, the higher the priority.	32768

Note:

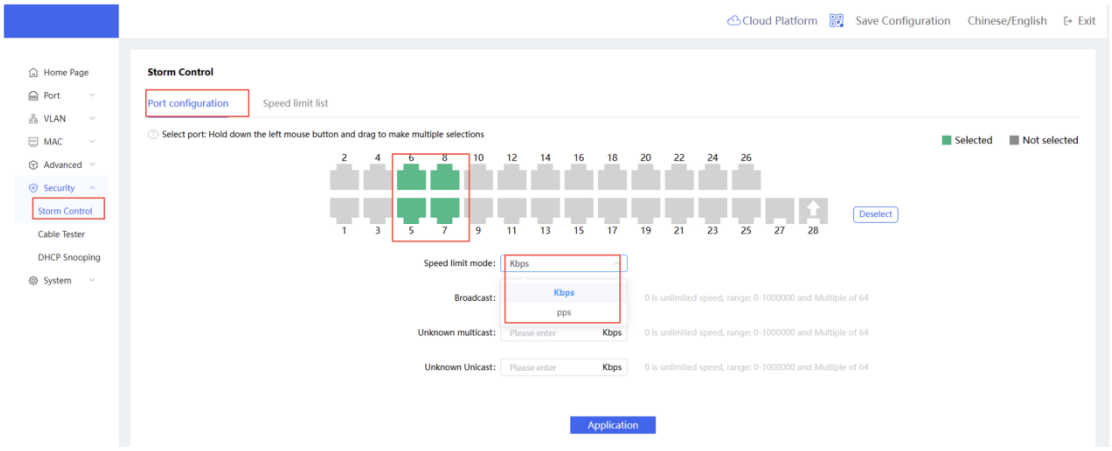
After enabling STP, the loop prevention function cannot be enabled. If you want to enable loop prevention, you need to disable STP in advance.

8. Cybersecurity

8.1 Storm Control

When a local area network (LAN) experiences excessive broadcast, unknown multicast, or unknown unicast traffic, it consumes substantial bandwidth and CPU resources on network devices (such as switches and routers), increasing the likelihood of packet transmission delays. This condition is referred to as a LAN storm. Protocol implementation errors or network misconfigurations can trigger such storms.

8.1.1 Port Configuration

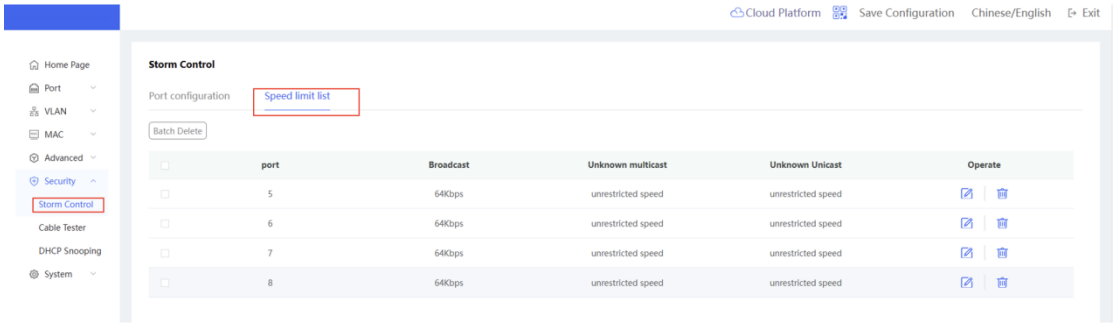


	Specifications	Introduction
Speed Limit Mode	Kbps	Storm control based on **kilobits per second**: When the rate of data flow received by the device port exceeds the set kilobits per second, the device will only allow the set kilobits per second to pass through, and the data flow exceeding the allowed kilobits per second will be discarded until the data flow returns to normal. 0 or no input means no speed limit, range: 0~1000000 and a positive integer multiple of 64

	pps	Storm control based on the number of **packets per second**: When the rate of data flow received by the device port exceeds the set number of packets allowed per second, the device will only allow the set number of packets per second to pass through, and the data flow exceeding the allowed number of packets per second will be discarded until the data flow returns to normal. **0 or no input means no speed limit, range: 0~1488095**

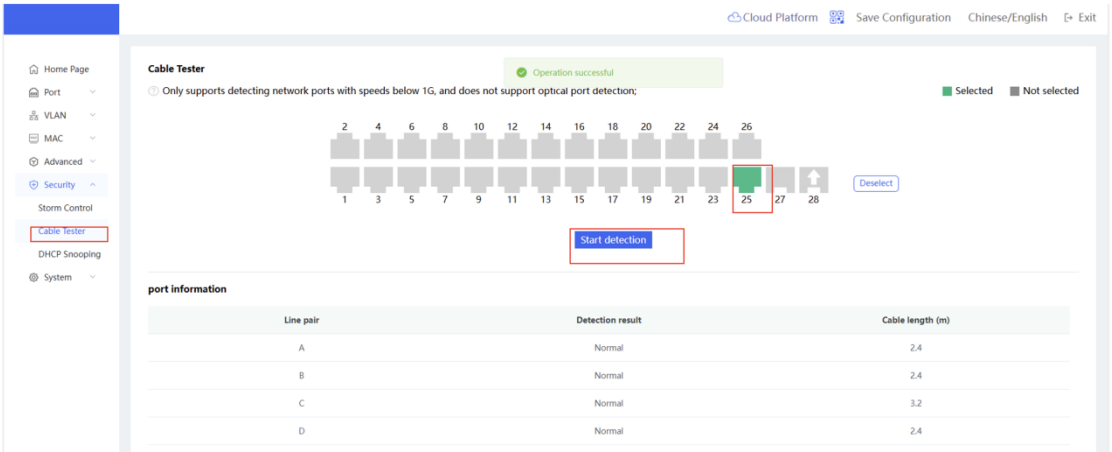
8.1.2 Speed Limit List

In the speed limit list, you can delete (unlimited) and edit the speed-limited ports.



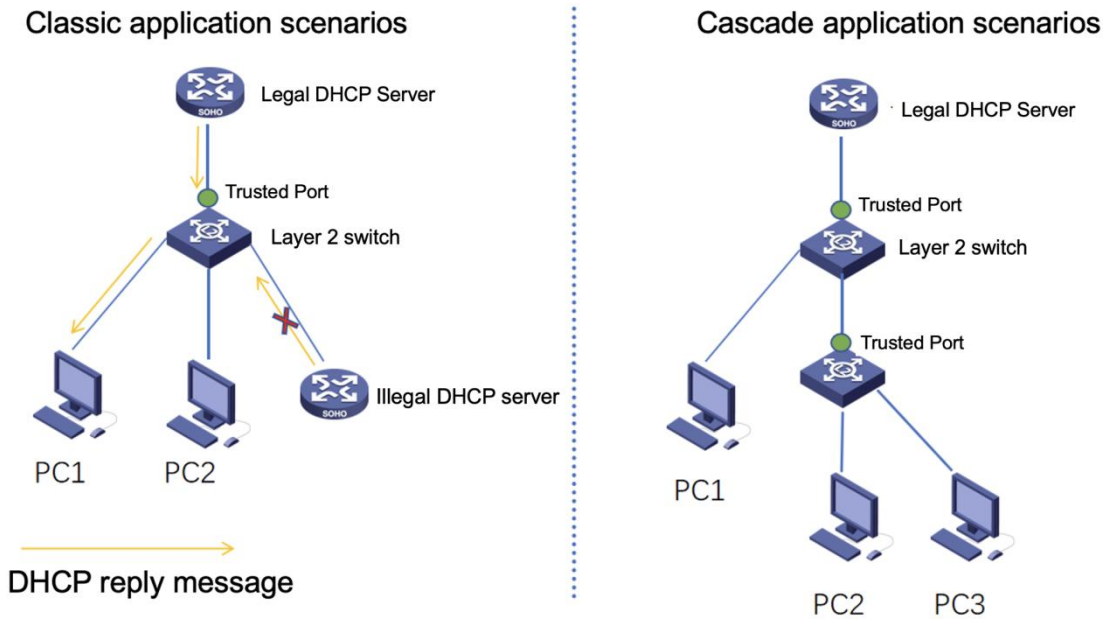
8.2 Cable Tester

Only supports detection of 1G rate electrical ports, does not support optical port detection (single choice).

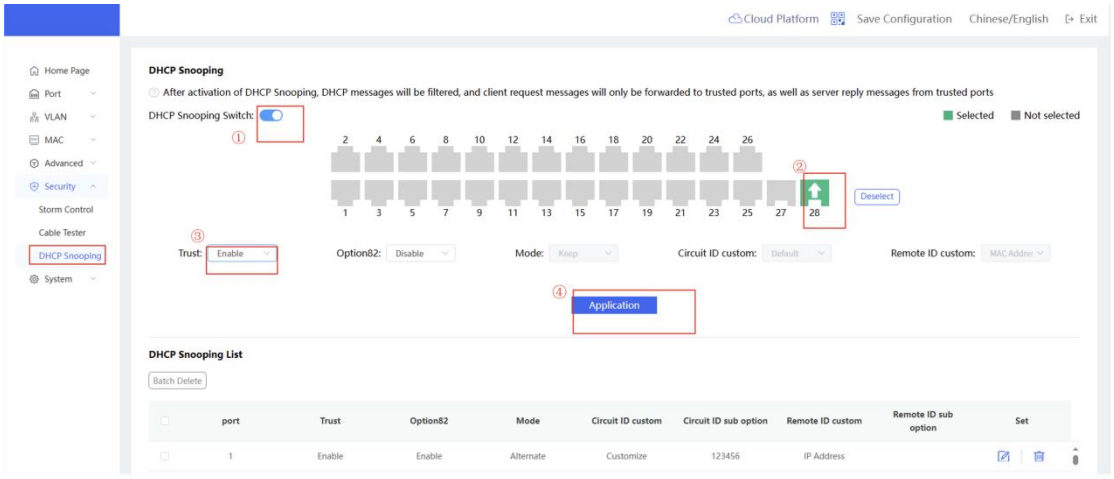


8.3 DHCP Snooping(Anti-private routing)

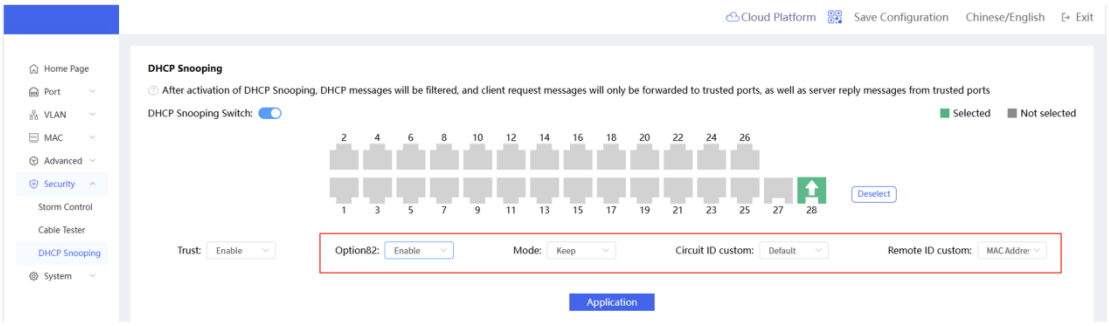
When enabled, DHCP messages will be filtered, and client request messages will only be forwarded to the trusted port, and server reply messages from the trusted port will also only be forwarded.



Enable DHCP Snooping function, and the device can identify the "uplink port" as a trusted port during the initial quick configuration.



8.3.1 DHCP Snooping Option82

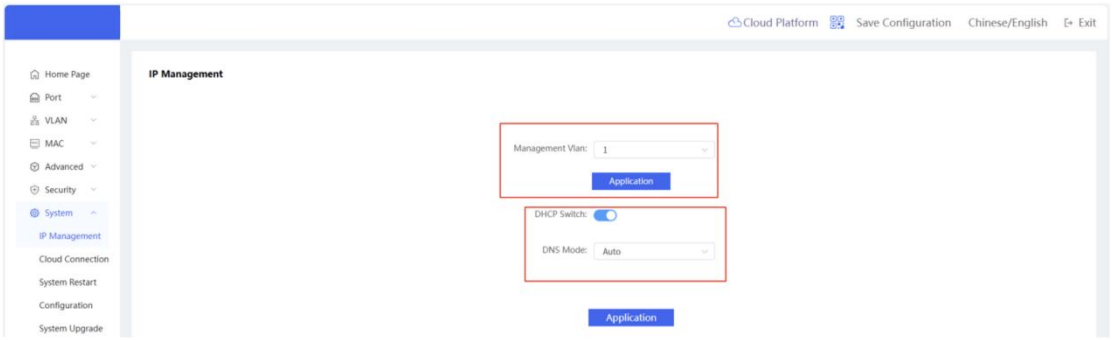


Specifications	Introduction	Default
Option82	Option 82 is a DHCP option proposed to enhance the security of the DHCP server and improve the IP address allocation strategy. After the Option 82 switch is enabled, Option 82 information will be carried in the DHCP request message.	Off
Mode	Discard: If a DHCP request message containing Option 82 is received, the message is discarded.	Keep
	Replace: When receiving a DHCP request message with Option 82, fill Option 82 according to the filling mode, content, and format configured on DHCP Snooping, replace the original Option 82 in the message, and forward it.	
	Keep: When receiving a DHCP request message containing Option 82, the device forwards the message without modifying the Option 82 field.	
-	When receiving a DHCP request message without Option 82, the device dynamically adds Option 82 according to the configured padding mode, content template, and format settings before forwarding the modified message.	-
Circuit ID	The circuit ID sub option is mainly used to identify the VLAN and interface where the (DHCP) client is located.	Default
Remote ID	The remote ID sub option is mainly used to identify the device to which the (DHCP) client is connected. It is the MAC address of the device.	MAC Address

9. System

9.1 IP Management

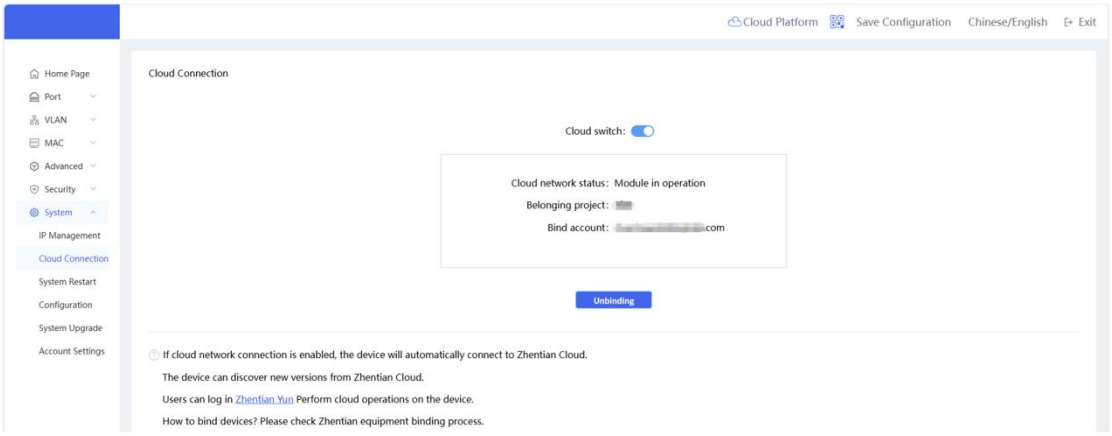
Configure the management IP address of the device. Users can configure and manage the device by accessing the management IP.
The device supports the following two ways to obtain the IP address:
Dynamic IP: Turn on the "DHCP switch" switch to use the IP address dynamically assigned by the upper-level DHCP server.
Static IP: Turn off the "DHCP switch" to use the fixed IP manually configured by the user.
When the "DHCP switch" is turned on, the device will automatically obtain various parameters from the DHCP server. You can choose whether to automatically obtain the DNS address from the DHCP server. If you turn off the "DNS mode" and select manual, you need to manually set the DNS server address.
When the "DHCP switch" is turned off, you need to manually enter the IP address, subnet mask, gateway IP and DNS server address. Click <Apply> to take effect.



Note:
The management VLAN defaults to VLAN 1.
The management VLAN must be selected from the created VLANs. If it is not created, go to VLAN Management to add it first.
It is recommended to bind the configured management VLAN to the current uplink port, otherwise it will cause the inability to access the device Web and disconnect the cloud connection. If the 802.1Q VLAN function is disabled, the management VLAN configuration will not be displayed.

9.2 Cloud network connection

If cloud network connection is enabled, the device will automatically connect to the Cloud. The device can discover new versions from the Cloud.
Users can log in to the Cloud (click to automatically jump to the Cloud Management Platform) to perform cloud operations on the device.

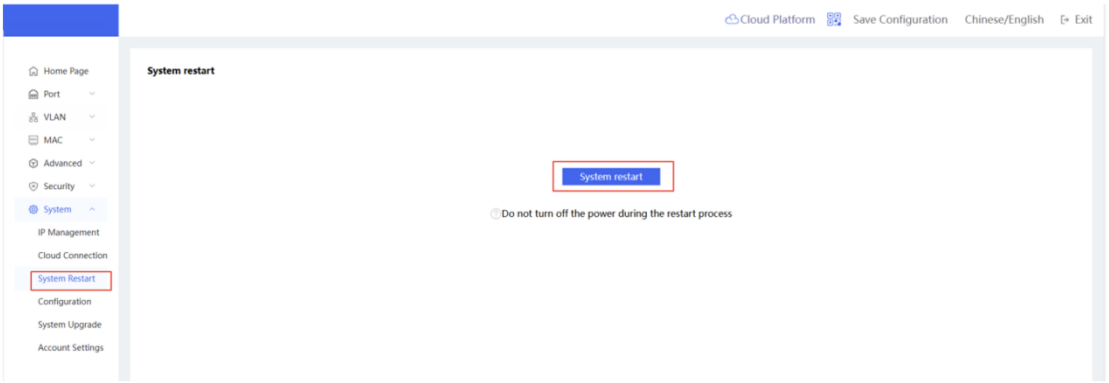


Device unbinding methods include hard unbinding and soft unbinding
Hard unbinding: Use a pin to press and hold the Reset button on the front panel of the device for about 5 seconds to unbind the device
Soft unbinding: Use the "one-click unbinding" function on this page to unbind the device

Note:
Device unbinding requires the cloud connection status to be "connected"

9.3 System Restart

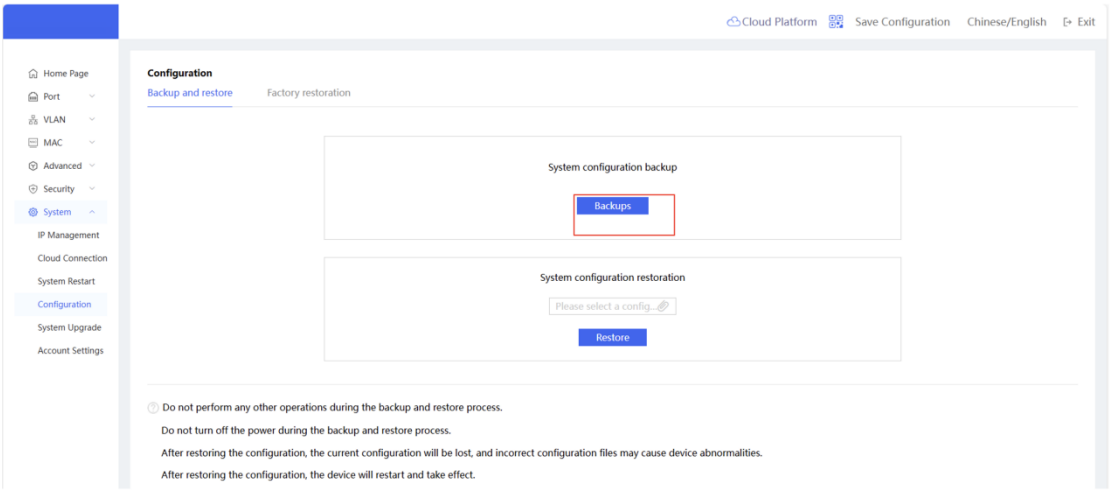
Click <System Restart> to restart the current switch device.



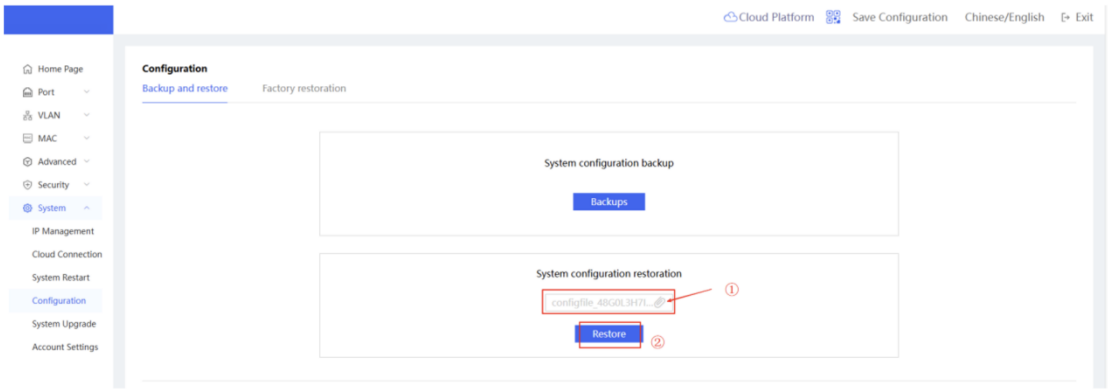
Note:
Before restarting the device, if you need to save the configuration permanently, please click <Save Configuration> in the upper right corner of the device page to avoid loss of configuration due to restart.

9.4 Configuration

System configuration backup, supports downloading the current system configuration file to the local computer, and can import it into the local machine or device of the same model, suitable for scenarios such as rapid maintenance or environmental preservation



Configuration restore, import the downloaded .json configuration file to the device, select the configuration file and click <Restore> to implement this function.



Note:

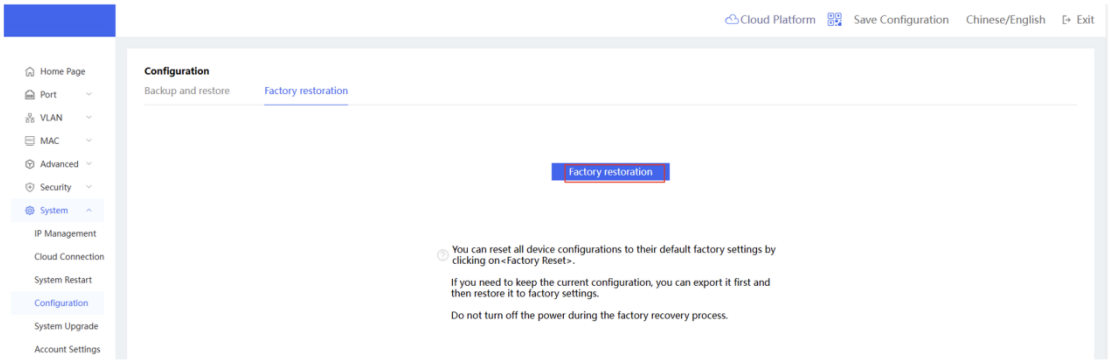
Do not perform other operations during the backup and restore process.

Do not power off during the backup and restore process.

After restoring the configuration, the current configuration will be lost, and incorrect configuration files may cause device abnormalities.

9.5 Factory Restoration

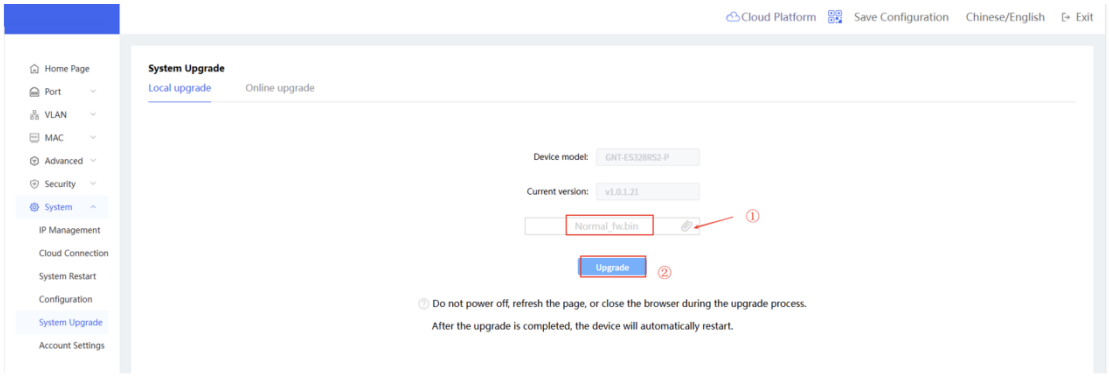
You can click <Factory restoration> to reset all device configurations to the factory default settings.
If you need to keep the current configuration, you can export the current configuration and then restore the factory settings.
Do not turn off the power during the factory reset process.



Note:
Restoring the device to factory default will clear all device configurations. Please operate with caution. The device login password after restoration is the default admin.

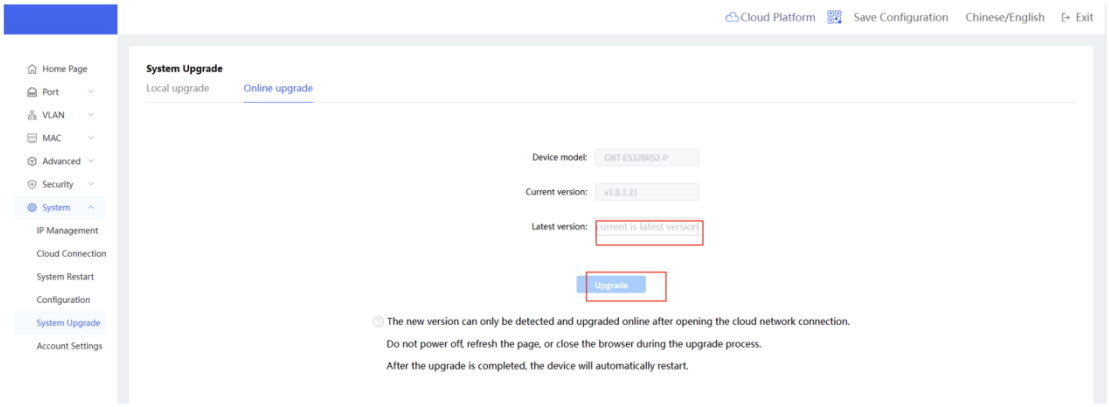
9.6 System Upgrade

System upgrades are divided into local upgrades and online upgrades. For local upgrades, please select the upgrade file xx.bin for upgrades.



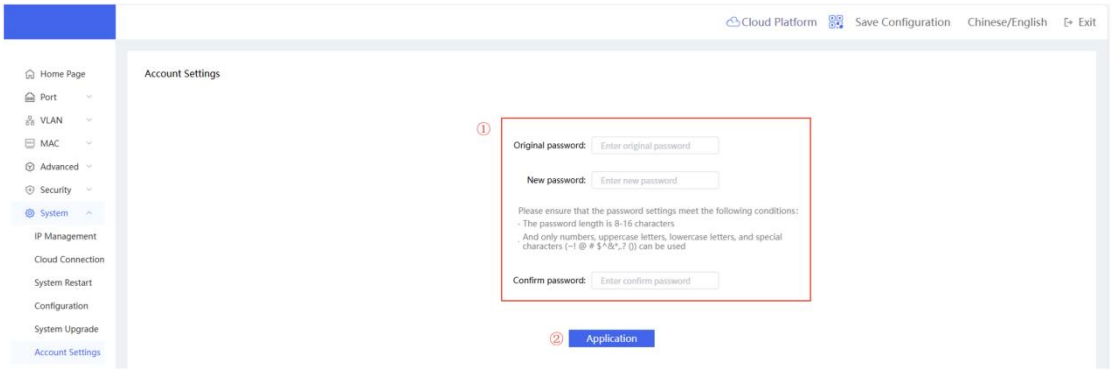
Only after the cloud network connection is turned on and the network is connected can the new version be detected and upgraded online.

During the upgrade process, please do not power off, refresh the page, or close the browser. The device will automatically restart after the upgrade is complete.



9.7 Account Settings

This page is used to modify the device login password. If the factory password has not been modified, please enter admin in the "Original Password" field.



Note:

Please make sure that the password setting meets the following conditions:

The password length is 8 to 16 characters

And only numbers, uppercase letters, lowercase letters and special characters (~!@#$^&*,.?()) can be used.