The Series Of Cloud-managed SwitchesWeb User Guide（Version 3）

Document version: A/5

Release time: 2025-04-21

Disclaimer:

The products, services or features you purchase should be subject to the company's commercial contracts and terms. All or part of the products, services or features described in this document may not be within your purchase or use scope. This manual is prepared based on existing information. If its content is changed, no further notice will be given. Please pay attention to the latest information provided on the company's website. The company has made every effort to ensure the accuracy and reliability of its content when compiling this manual. However, the company shall not be liable for omissions, inaccuracies or errors in this manual and the resulting losses and damages.

Icon Description:

This guide uses various eye-catching signs to distinguish the areas that need attention in each paragraph. The significance of these signs is as follows:

-  Warnings, precautions
-  Post scripts, questions, application examples
-  Key parameter description
- The item marked with * number is selected according to different product models

Revision Records:

Document Version	Release Time	Modify Description
A/0	2024-03-25	Initialize the product manual according to the test import
A/1	2024-04-16	Update to the latest official firmware
A/2	2024-06-01	Description of characteristics of equipment suitable for new models
A/3	2024-08-08	Add cloud management and hardware description
A/4	2024-09-20	Add new models
A/5	2025-04-21	Add new models and functional management updates

Category

1. Product Overview 4
1.1 Product Introduction 4
1.2 Product Features 6
1.3 Product Appearance 7
1.4 Product Installation 11
1.5 Product Application 17
1.6 Remote Cloud Management 18
1.7 Log Onto The Web Page 20
1.8 Web Page Introduction 22
2. System Management 23
2.1 IP Settings 23
2.2 Change Password 24
2.3 Firmware upgrade 25
2.4 Manage Configuration 25
2.5 Reboot 26
2.6 AI Function Configuration*（Only some models support it） 26
3. Port Configuration 27
3.1 Port Mirroring 27
3.2 Port Management 27
3.3 Spanning Tree Protocol* 29
4. VLAN Management 32
4.1 802.1Q VLAN 33
4.2 MTU-VLAN 37
4.3 Port VLAN 38
5. Safety 39
5.1 storm suppression 39
5.2 Adaptive Power supply 40
5.3 loop detection 40
5.4 MAC Management 41
5.5 DHCP Snooping 42
6. Basic specifications 44
7. Exit 45
8. FAQ 45

1. Product Overview

1.1 Product Introduction

The WEB series of Cloud Network Management switches is an Ethernet management switch independently developed by our company. It provides multiple Ethernet RJ45 ports and can be applied to various monitoring and security, as well as data communication projects. This model supports remote management and can be remotely managed through the App "Amitres IOT". It also supports login management via web pages.

The current included models of the switch are as follows:

Product	Product Model	10/100/1000Mbps RJ45	1000Mbps SFP Port
Full gigabit WEB network management switch	GS105	5	Null
	GS108	8	Null
	GS105L	5	Null
	GS108L	8	Null
	GS116	16	Null
	GFS226	26（Ham2UP.Link）	2
	GFS124	24	1
Full Gigabit WEB management Poe switch	GPS424	26（Ham2UP.Link）	2
	GPS204	5（Ham1UP.Link）	1
	GPS208	10（Ham2UP.Link）	Null
	GPS208F	8	2
100M + 1000M Web management POE switches	PS104G	5（Ham1UP.Link）	Null
	PS105G	5（Ham1UP.Link）	Null
	PS110G	10（Ham2UP.Link）	Null
	PS208G	10（Ham2UP.Link）	Null

	PS308G	6+2+2+1 （Ham2UP.Link）	1
	PS316G	16+2+1 （Ham2UP.Link）	1

The SFP port is compatible with multi-mode and single-mode SFP fiber modules, and the fiber module can be selected according to actual needs and networking conditions; it is recommended to use the company's SFP101P Gigabit SFP electrical port module.

1.2 Product Features

- Follow IEEE 802.3 Ethernet, IEEE 802.3u Fast Ethernet, IEEE 802.3ab protocol standards;
- Cloud network management: visual remote management, on-site problems, remote resolution;
- Support spanning tree protocols: STP (IEEE802.1d), RSTP (IEEE802.1w);
- Local web management, easy to use on-site debugging;
- All ports support Auto-Flip (Auto MDI/MDI-X) function;
- Support IEEE802.3X full duplex flow control and Backpressure half duplex flow control;
- Support port speed limit, port duplex setting, port mirroring and other port management;
- Support DHCP snooping to restrict access to illegal DHCP servers;
- Storm suppression to control unknown multicast and broadcast traffic;
- MAC binding, restricting port access to devices;
- Support 802.1Q VLAN, MTU-VLAN, Port-VLAN suitable for a variety of networking service requirements;
- Support MAC Address Self-learning and Aging and Manual Static MAC Port Binding;
- Three-speed function switch, AI/default/cloud network management three-speed switch (only some models);
- Plug and Play;

1.3 Product Appearance

1.3.1 Full gigabit web management switch

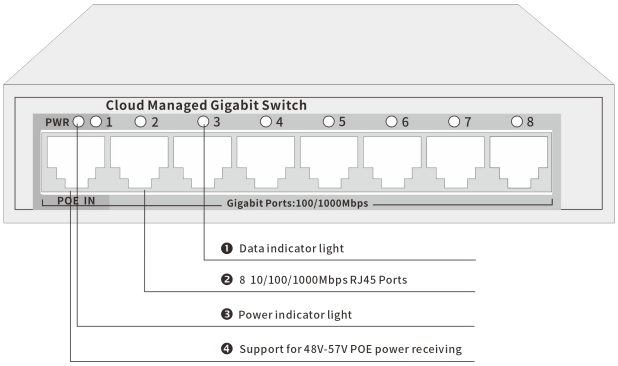


Figure 1-1 Front panel diagram 8 ports (including the following) without function switch

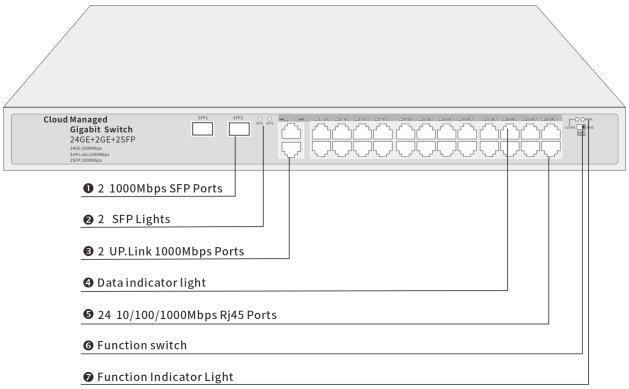


Figure 1-2 Front panel schematic

1.3.2 Full Gigabit Web management Poe switch

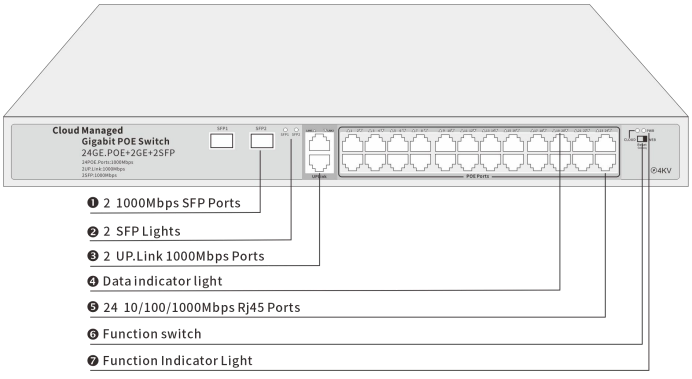


Figure 1-3 Front panel schematic

1.3.3 100M + 1000M Web management POE switches

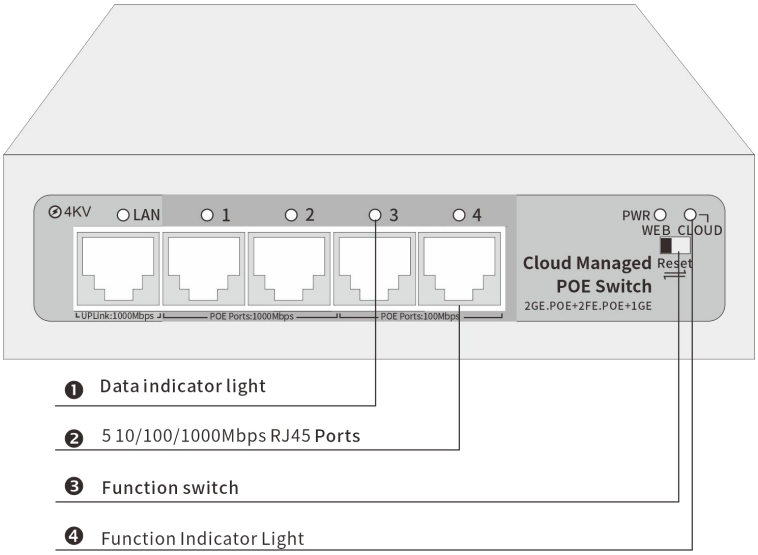


Figure 1-4 Front panel schematic

Attention: The port of PoE power receiving only supports the following switch applications with 8 ports (included).

1.3.4 Indicator Light

The indicator lights of GS105/GS108/GS105L/GS108L, which include PWR, Link/Act. You can monitor the working status of the switch through indicators. The description of indicators is shown in table 1-1/1-2.

Indicator Light	Working Status	Functional Description
PWR	ON	The power supply of system is normal
	OFF	The system is not powered on or the power supply is abnormal
Link/ACT	ON	The link of ports is normal
	Flashing	The port is transferring data.
	OFF	Port unconnected device

Table 1-1 /1-2 indicator working status description

The indicator lights of GS116/GFS226/GFS124/GPS424/GPS204/GPS208/PS104G/PS105G/PS110G/PS208G/PS308G/PS316G/GPS208F and other switches, which include PWR, WEB, CLOUD, Link/Act. You can monitor the working status of the switch through indicators. The description of indicator lights is shown in table 1-2:

Indicator Light	Working Status	Functional Description
PWR	ON	The indicator light of switch power: Light Up: Device is started
	OFF	The system is not powered on or the power supply is abnormal
CLOUD	ON	Local WEB management and APP remote management
Link/ACT	ON	The link of ports is normal
	Flashing	The port is transferring data.
	OFF	Port unconnected device

Table 1-2 working status description of indicators

1.3.5 The description of functional switch

parameter:

Switch	Working Mode	Functional Description
ON	WEB Mode	Only support local WEB management, fixed standby IP: 10.0.0.10
OFF	CLOUD Mode	Support local web management and remote APP management
RESET		Please make sure that the switch is in the WEB position. Then, within 2 seconds, first toggle the switch to the CLOUD position and then back to the WEB position. At this time, the device will restart and be restored to factory settings.

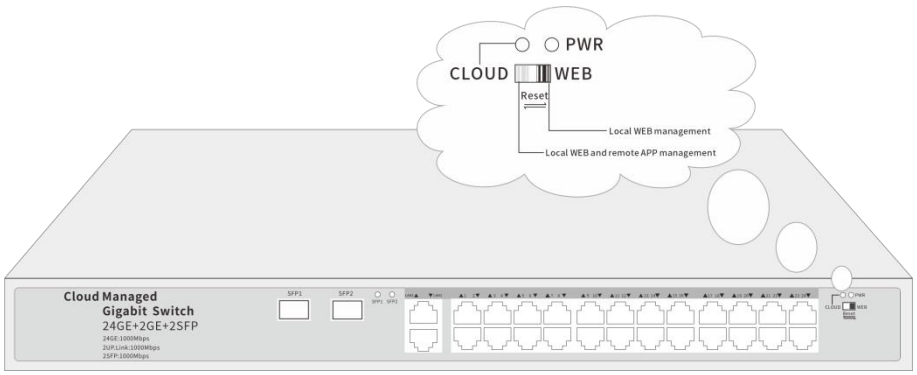


Figure 1-5 Schematic diagram of function switch

■10/100/1000Mbps RJ45 ports and POE RJ45 ports

Support 10Mbps, 100Mbps or 1000Mbps rate adaptation function, and support Auto-MDI/MDIX function.

All models have an indicator light corresponding to each port(Link/Act)

■1000Mbps SFP ports

GFS226/GPS424/GSP204/PS308G and other models provide 1000Mbps SFP ports. Each port corresponds to an indicator light (Link/Act)

1.3.5The connection of power cord

1. Check that the selected power supply is consistent with the power supply requirements marked by the switch;

2. Switch Original power cord Connect switch to power outlet as shown in Figure 1-10/1 -11.

Figure 1-10 shows DC power supply, the power adapter plug is connected to the socket, the DC plug is connected to the switch, the adapter is divided into: 12V/48V/52V voltage optional.

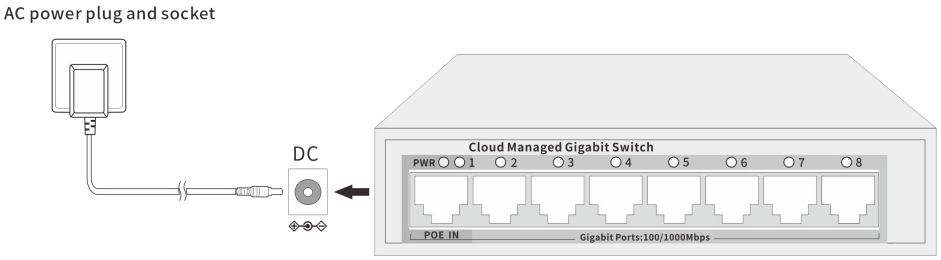


Figure 1-6 Schematic diagram of power cord connection

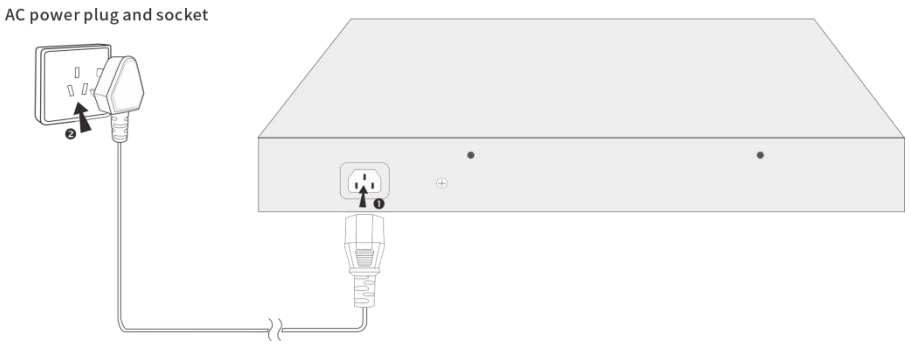


Figure 1-7 Schematic diagram of power cord connection

Figure 1-11 shows three-plug power socket. Connect the negative plug of the power cord to this socket and the positive plug to the AC power supply. The non-PoE switch is connected to the AC power supply of 100-240V~ 50/60Hz.

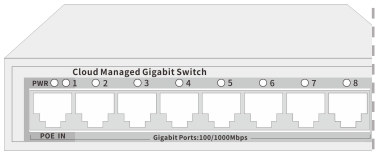
Attention：1. Please use the original power cord.

2. The power supply of the power supply system requires good contact with the earth, and the position of the power supply switch of the equipment is confirmed, so that the power supply can be cut off in time when necessary.

1.4 Product Installation

1.4.1Product Matching List

Switch



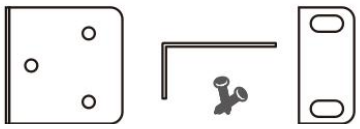
Power adapter (or AC power cord)



user's guide



A kit of accessories (only some models are selected)



Attention：If you find any shortage or damage of accessories, please contact the local dealer in time.

1.4.2 Installation Precautions

Warning：In a living environment, this product may cause radio interference. In this case, the user may be required to take practical measures against the interference.

■ The safety precautions for installation;

■ Keep the power off during the installation process, while wearing an anti-static wrist, and ensure that the anti-static wrist is in good contact with the skin to avoid potential safety hazards;

■ The switch can only work normally under the correct power supply. Please confirm that the power supply voltage matches the voltage marked on the switch;

■ Before the switch is powered on, please confirm that it will not cause the power circuit

to overload, so as not to affect the normal operation of the switch or even cause unnecessary damage;

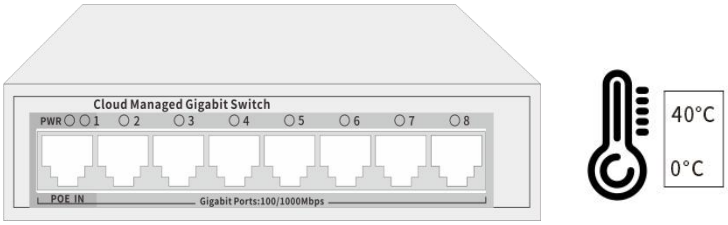
■ To avoid the risk of electric shock, do not open the case when the switch is working, even if it is not charged, do not open it yourself;

■ Before cleaning the switch, the switch power plug should be pulled out, do not wipe with wet fabric, do not clean with liquid;

■ During use, please keep the bottom of the switch facing down and placed horizontally to avoid potential safety hazards.

The environment precautions for installation

Temperature/humidity

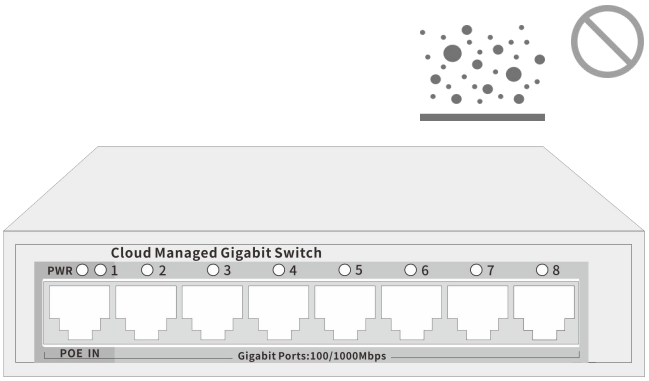


In order to ensure the long-term stable operation of the switch and prolong the service life, please maintain a certain temperature and humidity in the environment. Too high or too low ambient humidity can easily cause leakage, deformation and even rust of metal parts of insulating materials. Too high temperature will accelerate the aging process of insulating materials and seriously affect the service life of equipment. The normal operation and storage temperature/humidity of this series of switches are as follows table 1-1.

Environment	Parameter
Temperature	Working temperature：0°C～40°C Storage temperature：-40°C～70°C
Humidity	Working humidity：10%～90% RH non-condensing Storage humidity：5%～90% RH non-condensing

Table 1-1 Temperature/humidity requirements for normal use of switches

Indoor Dust

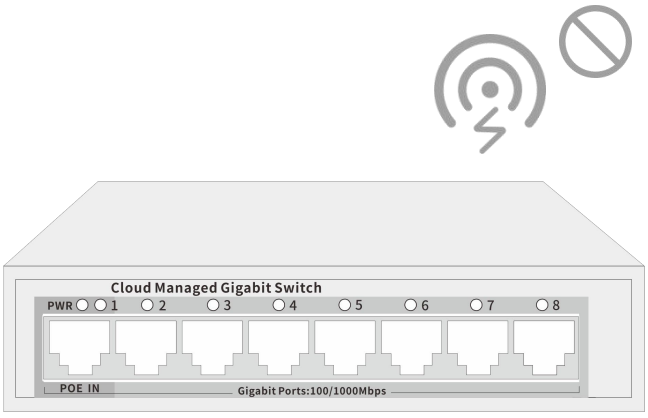


Dust falling on the surface of the switch will cause electrostatic adsorption and poor contact with metal contacts. Although the device itself has taken certain measures in anti-static, when the static electricity exceeds a certain strength, it will still cause fatal damage to the electronic components on the internal circuit board. In order to avoid static electricity affecting the normal operation of the device, please pay attention to the following matters:

■ Regularly remove dust to keep indoor air clean.

■ Confirm that the equipment is well grounded to ensure the smooth transfer of static electricity.

Electromagnetic Interference



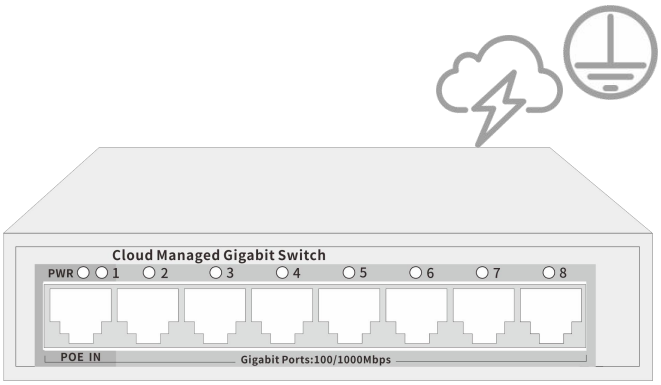
Electromagnetic interference can affect the capacitance, inductance, and other electronic components inside the device through capacitive coupling, inductive coupling, and impedance coupling. To reduce the adverse effects of electromagnetic interference factors, please pay attention to the following matters:

■ The power supply system takes necessary anti-grid interference measures.

■ Switch should be away from high-frequency high-power, high-current equipment, such as wireless transmitters;

■ Take electromagnetic shielding measures when necessary

The protection requirements for lightning



When a lightning strike occurs, a strong current is generated in an instant, and the air in the discharge path is instantly heated to 20,000 degrees Celsius. The instantaneous high current is enough to cause fatal damage to electronic devices. In order to achieve better lightning protection, please pay attention to the following matters:

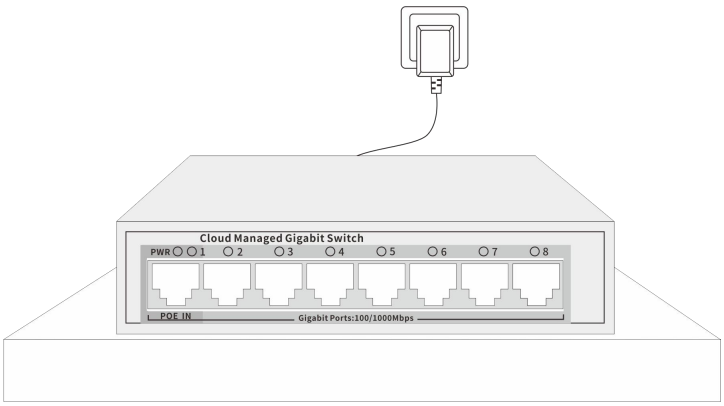
■ Verify that the rack and equipment ground terminals are in good contact with the ground;

■ Make sure the power socket is in good contact with the ground;

■ Reasonable wiring to avoid internal induction lightning;

■ When wiring outdoors, it is recommended to use a signal lightning protector;

1.4.3 Mounting Table



Whether the switch is installed in the rack or on other horizontal tables, please note the following:

■ Verify that the rack or table is stable, secure, and capable of withstanding at least 5.5Kg weight;

■ Make sure the rack itself has a good cooling system, or keep the room well ventilated;

■ Confirm that the rack is well grounded and the distance between the power socket and the switch does not exceed 1.5 meters;

Attention: Leave a 5~ 10cm gap around the switch case to ensure heat dissipation and air circulation, and avoid placing other heavy objects on the switch surface.

1.4.4 Mounts on a 19-inch standard rack

This series of switches is designed according to the size of a 19-inch standard rack and can be easily installed on the rack. The specific installation steps are as follows:

1. Check the grounding and stability of the rack;

2. Install the two L-angle iron in the accessories on both sides of the switch panel and fix them with the screws provided in the accessories, as shown in Figure 1-1 ; L-angle iron screws

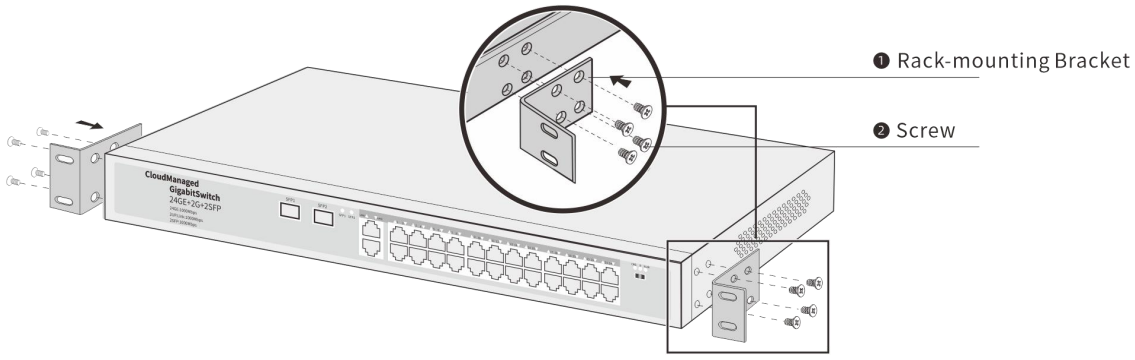


Figure 1-1 ,Schematic diagram of angle iron installation

3. Place the switch in place in the rack, supported by the bracket;

4. Fix the L-angle iron on the guide grooves fixed at both ends of the frame with screws to ensure that the switch is installed stably and horizontally on the rack

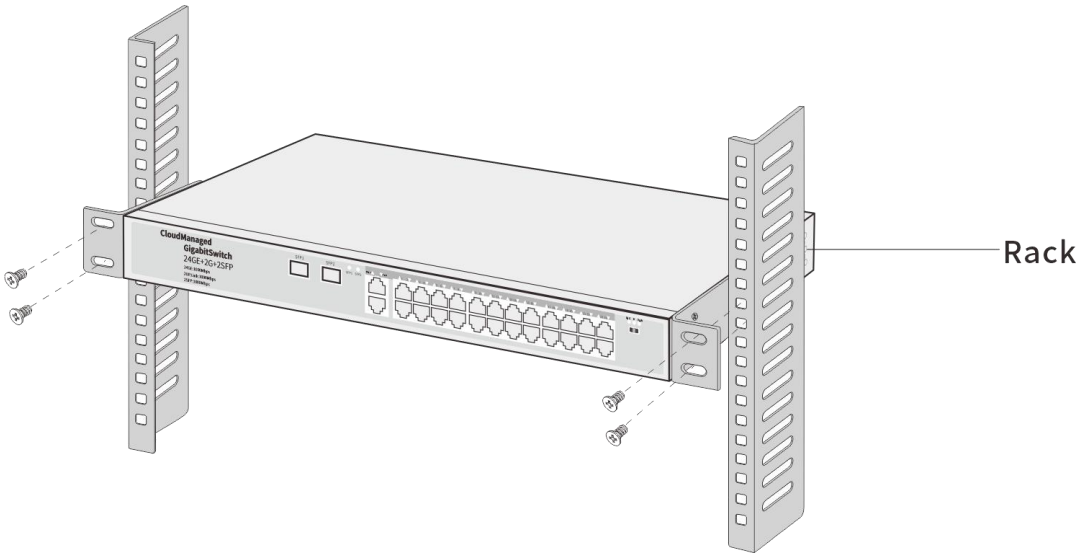


Figure 1-2, Schematic diagram of rack installation

Attention:

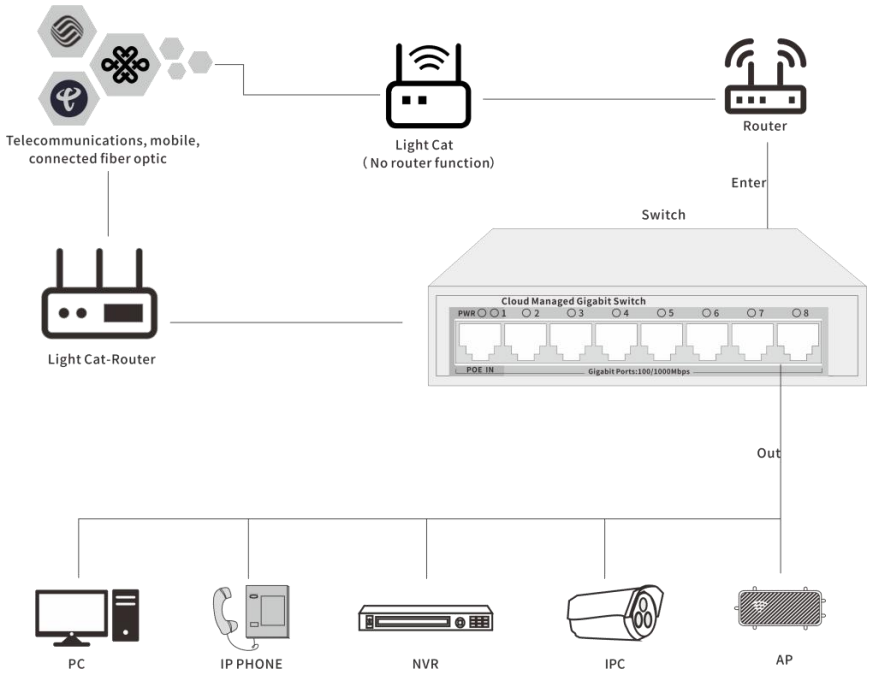
■ Good grounding of the rack is an important guarantee for anti-static, anti-leakage, lightning protection and anti-interference of the equipment, so please ensure that the grounding wire of the rack is installed correctly;

■ The equipment installed in the rack is generally from bottom to top to avoid overload installation;

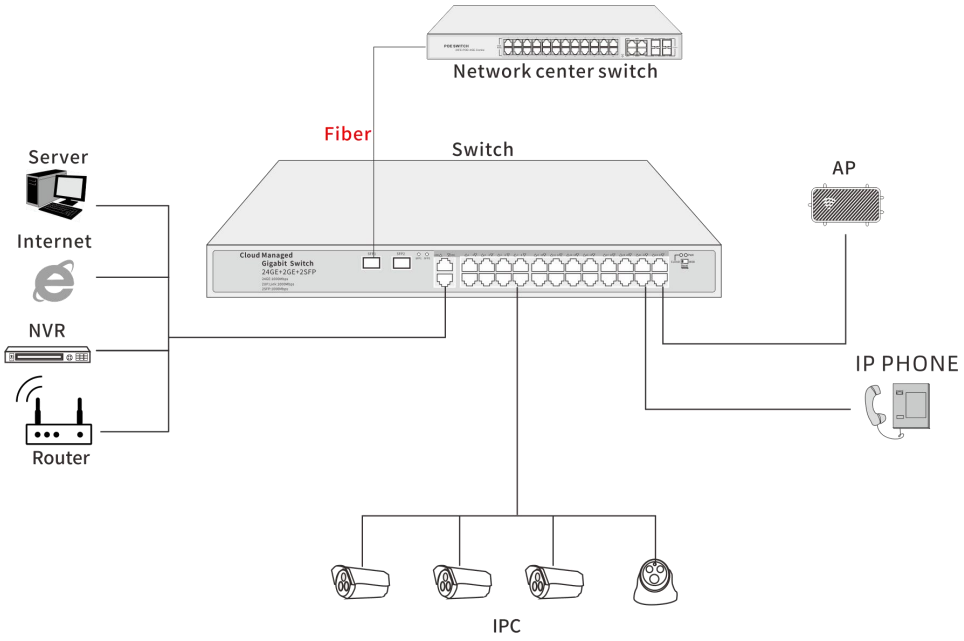
■ Avoid placing other heavy objects on the switch surface to avoid accidents;

■ Ensure heat dissipation and air circulation;

1.5 Product Application



Product application Figure 1-1 GS105/GS108/GS105L/GS108L is for reference only



Product application Figure 1-2

GS116/GFS226/GPS424/GPS204/GFS124/PS104G/PS105G/PS308G/PS208G/GPS208F/PS316G is for reference only

Parameter Description:

■ 1000Base-T: 4 pairs of Super Category 5 (Cat5e) or higher UTP/STP (≤ 100m)

■ 100Base-TX: 2 pairs of Category 5 (Cat5) or higher UTP/STP (≤ 100m)

■ 10Base-TX: 2 pairs of Category 5 (Cat5e) or higher UTP/STP (≤ 250m)

■ Switch Ethernet port Auto-MDI/MDIX function is turned on by default. When using Category 5 twisted pair to connect Ethernet, standard network cable or cross network cable can be used.

Attention:

■ The port of POE power receiving only supports the following switch applications with 8 ports (included)*.

■ SFP port is only supported by some models*.

■ POE power receiving port only supports the following switch applications with 8 ports (included).

■ The port of POE power receiving only supports the following switch applications with 8 ports (included).

■ The power supply of the power supply system requires good contact with the earth, and the position of the power supply switch of the equipment is confirmed, so that the power supply can be cut off in time when necessary.

Items marked with*are selected according to different product models

■ Check whether there is enough heat dissipation space around the switch and whether the air circulation is smooth.

■ Check whether the power supply from the power socket meets the switch specifications.

■ Check that power supplies, switches, racks and other equipment are properly grounded.

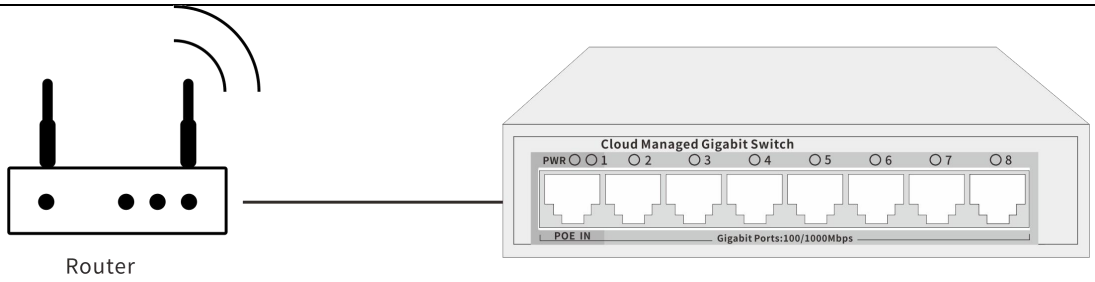
■ Check whether the switch is connected properly to other network devices.

1.6 Remote Cloud Management

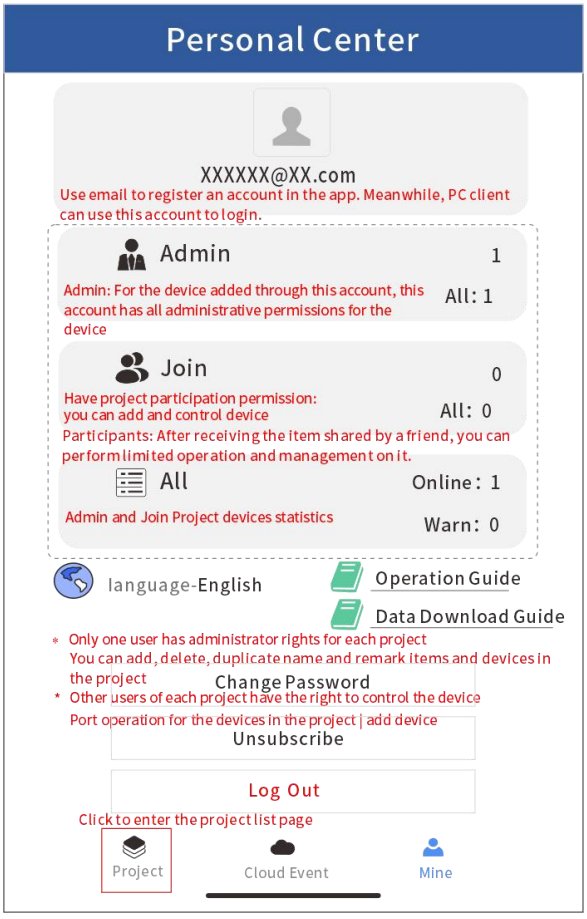
All models in this manual support cloud management, which is explained in the APP management interface. Please refer to the following steps to bind:

1.6.1 Make sure the switch is connected to the network for Internet communication.

Connect the router that is connected to the Internet to LAN port of the device. (the router needs to enable DHCP).



1.6.2 Download the app "Amitres IOT". Then, register an account by email in the app. Meanwhile, PC client can use this account to login.

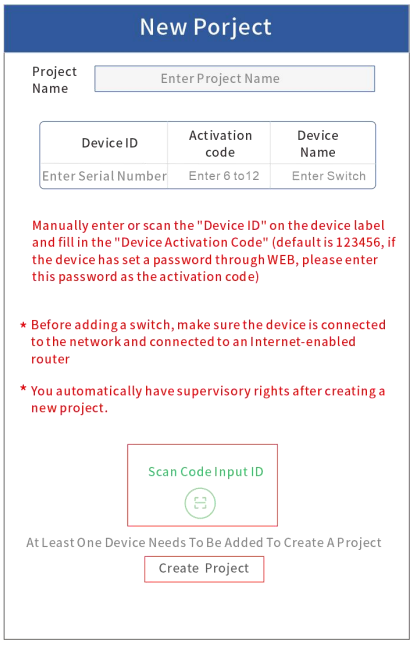


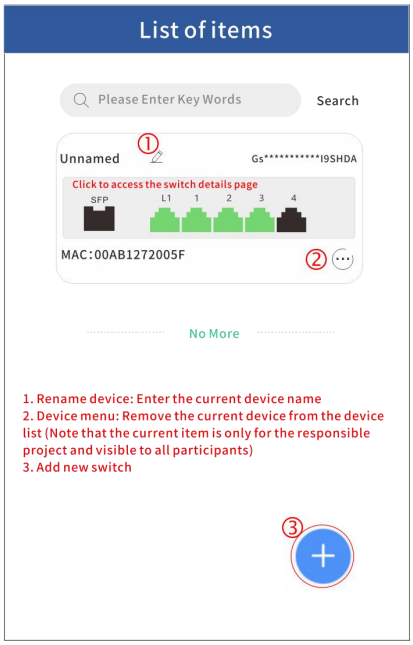
1.6.3 Add device:

■New project: Click "+" to scan the equipment ID QR code (located on the fuselage) and enter the project name and other corresponding information to create it.



■Existing project: Enter the submenu of project, click "+" to add switch to scan the QR code of device ID and enter corresponding information to add.





Attention:

■ When adding a new device, you need to enter the initial password of the device by default (the default is 123456).

■ To add the device ID, make sure that the current device is connected to the Internet router.

■ For more instructions, please visit the App.

1.7 Log Onto The Web Page

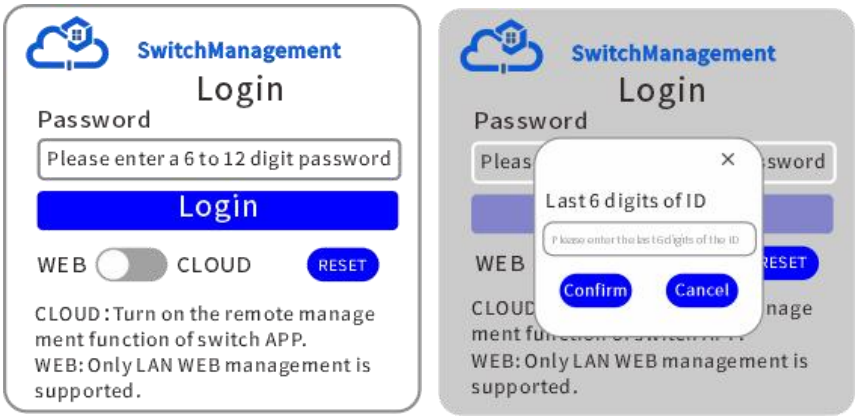
Open the PC browser and enter the Internet Protocol Address of the device in the address bar to manage the switch. The URL format in the address bar is http://xxx.xxx.xxx.xxx, where xxx represents the Internet Protocol Address of the switch (when directly connecting the device, the fixed default management IP is: 10.0.0.10，The computer needs to be the same network segment as the Internet Protocol Address).

1.7.1Log onto the WEB page via fixed IP

Web pages are divided into two types: a normal login page, and another page with administrative mode switching



Normal WEB login page



WEB login with management mode switch page

Parameter Description:

Parameter	Description
WEB	Local WEB management, fixed standby IP: 10.0.0.10;
CLOUD	Local WEB and remote APP management;
RESET	On the WEB login interface, click the RESET button and enter the last 6 digits of the device ID to restore factory settings;

•When switch is not connected to the extranet environment, it will automatically turn on the fixed IP10.0.0.10 and configure the computer with an Internet Protocol Address on the same network segment as switch.

•Open a browser on your computer and enter the switch Internet Protocol Address 10.0.0.10 login page WEB.

1.7.2Log onto the management page with the IP obtained through the router.:

•The factory status of the switch is turned on by default to automatically obtain IP. When the local area network of the switch is connected to the extranet, the IP

automatically obtained by the switch needs to be logged in to the web interface of the switch for management.

•For devices that obtain IP through the router, log in to the router to check the Internet Protocol Address in the connected device where the hostName is the device model (such as GS108). Login to WEB Management.

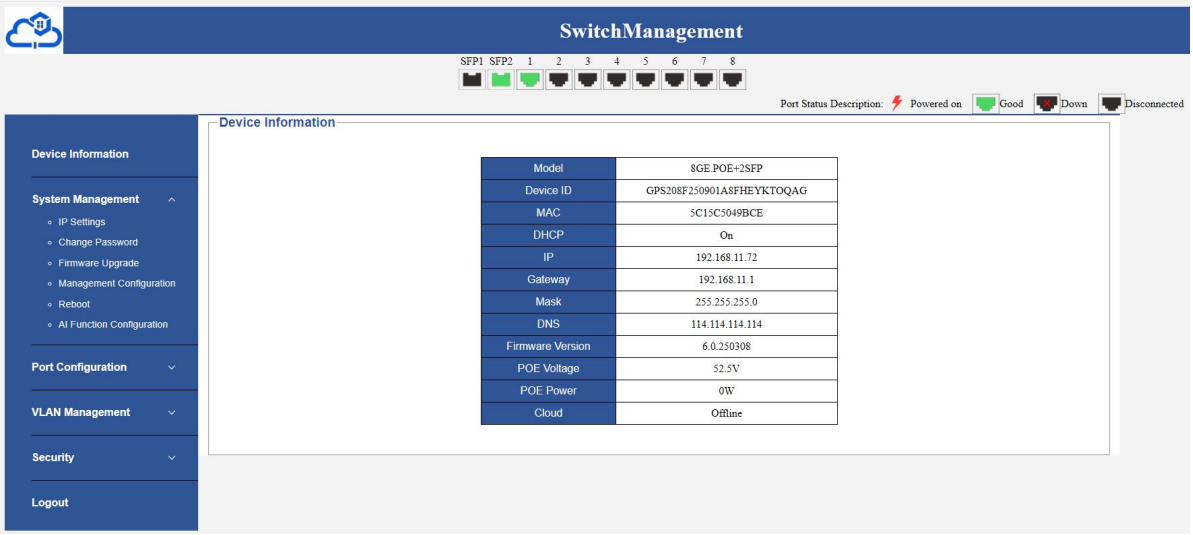
SN	IP Address	MAC Address	hostName	type	status	Lease expiration time
1	192.168.1.105	5C-15-C5-00-00-EC	GFS226	assign	online	2024-08-16 00:00:00
2	192.168.1.106	5A-15-C5-00-00-EC	GS116	static	online	--
3	192.168.1.107	5B-15-C5-00-00-EC	GPS424	static	online	--

Enter the device password (the activation password set when binding through the App) to log into the management page.

⚠Attention：If the device is brand new and inactive, the password will be initialized（Please remember this setting password, which will be used when the device is bound to the App）

⚠Attention：This device can only log in to one web side at the same time. When you need to switch to log in to a PC or browser, please use the "Exit" button in the function menu to perform the login operation.

1.8 Web Page Introduction



The icon area of port status:



The navigation bar area of function Menu:



Device information：You can view the current model, SN, MAC, IP, firmware version and other information of the device here.

System Management：System management related operations or configurations can be performed on this column (IP settings, password change, firmware upgrade, factory restore, device restart).

Port Configuration：Device function configuration (port mirroring, port duplex, port speed limit, * STP) can be performed on this column.

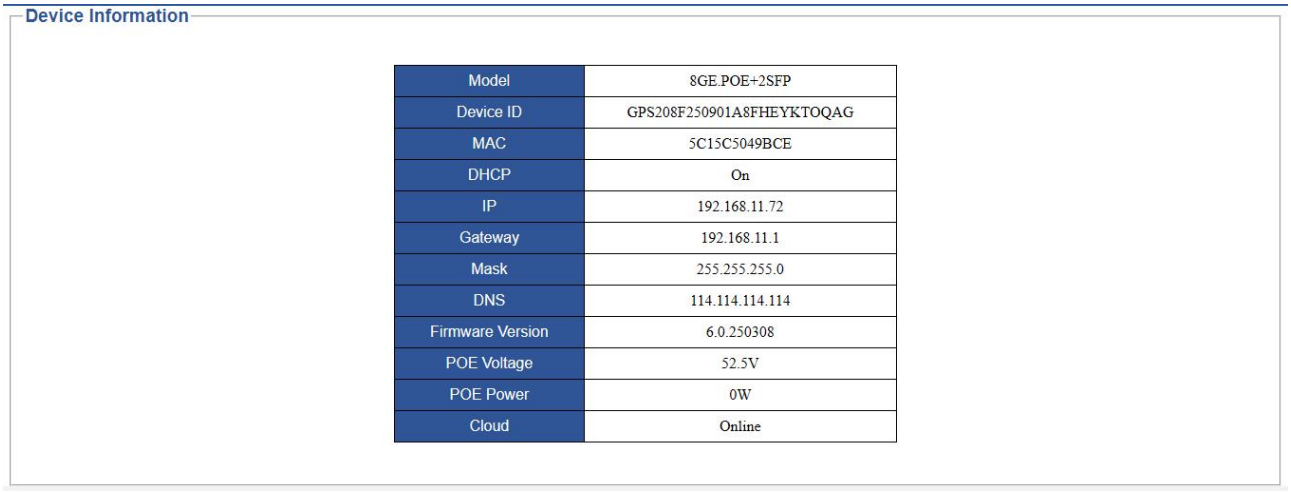
VLAN Management：VLAN related configuration (1Q_VLAN, port VLAN) can be performed on this column；

Security：Device security-related configurations (storm suppression, loop detection, MAC management, * DHCP snooping) can be performed here.

Logout：Logout for user authentication.

* Mark * function, currently only available in the test version.

Information and settings page area：

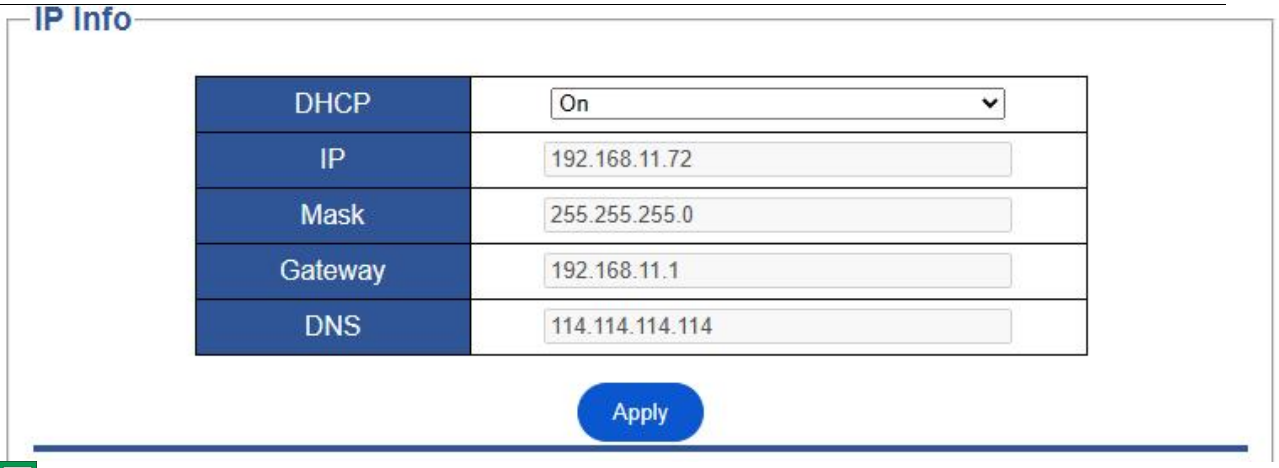


This page allows for relevant information viewing and settings；

2. System Management

2.1 IP Settings

⚠Attention：Direct connection device, login device Web standby fixed Internet Protocol Address is 10.0.0.10 (note that the PC manually configures IP).



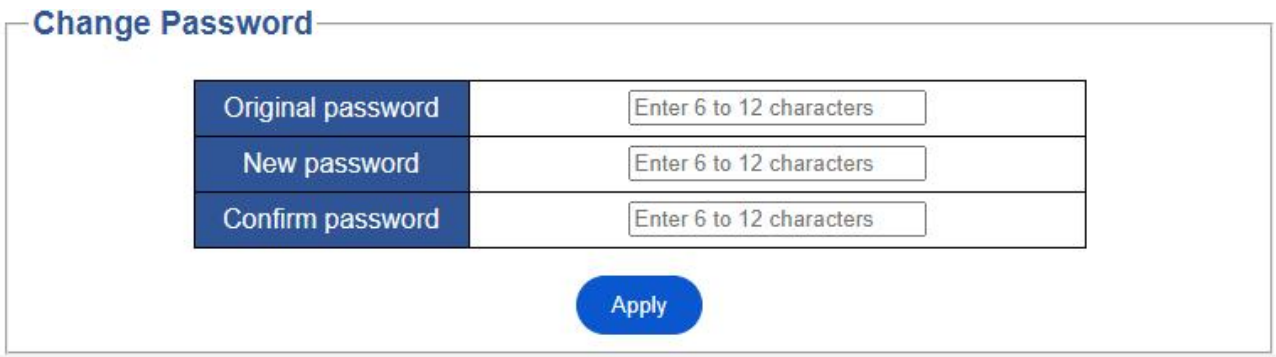
Parameter Description:

Parameter	Description
DHCP	The default is enabled, and when set to disabled, the following parameters can be entered manually.
IP	Enter a static IP v4 address.
Mask	Enter a static IP v4 mask.
Gateway	Enter a static IP v4 gateway, the gateway needs to be on the same subnet as the IP.
DNS	Enter static DNS. The device needs to have correct DNS resolution when connecting to the cloud server. If you are not sure, you can fill in the gateway address.

Enter or select and 

click to execute the operation.

2.2 Change Password



Parameter Description:

Parameter	Description
Old Password	Enter the original password.
New Password	Enter new password.
Confirm Password	Confirm the input, the same as the new password.
*Supported password characters	“abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ 0123456789!@#$%^&*()-=_+[]{}|;':,.<>?/”

Enter or select and click Apply to execute the action.

2.3 Firmware upgrade

This function is the local firmware file upgrade function. Click Choose File to open the correct upgrade file, and then click Sure to perform the device upgrade operation.

⚠ Note: During the process of upgrading and programming the firmware, please pay attention to keep the power supply powered.

2.4 Manage Configuration

Reset To Factory:

After clicking the "Reset" function button, the device will wipe the relevant device configuration information other than the password and restore the factory default state.

Backup Switch Configuration:

Click "Backup Configuration" to automatically download the Json file of current device configuration to the local directory.

Restore Switch Configuration:

Select the json file that originally backed up, click OK to upload the configuration information, and the device will be restored to the state where the configuration file was saved.

2.5 Reboot

After clicking the "Reboot" function button, the device will be powered on again.

2.6 AI Function Configuration* (Only some models support it)

Port Watchdog:

Parameter Description:

Parameter	Description
ON	After turning on this function, the device will monitor the port data status. When the connected device is abnormal or freezes and the data traffic is disconnected, the port will restart the connected device through POE power supply;
OFF	Turn off the AI watchdog function

After entering or selecting, click Apply to execute the current selection settings and save.

Automatic Port Extension:

Parameter Description:

Parameter	Description
ON	When the network cable is too long or the network signal strength is not enough, the port will automatically reduce the port speed to 10Mbps, enhance the network signal and extend the port transmission distance. The ideal connection distance can reach 200 meters to 250 meters.
OFF	Turn off the smart ultra-far function, and the port duplex is an adaptive effect.

After entering or selecting, click Apply to execute the current selection settings and save.

*AI function:

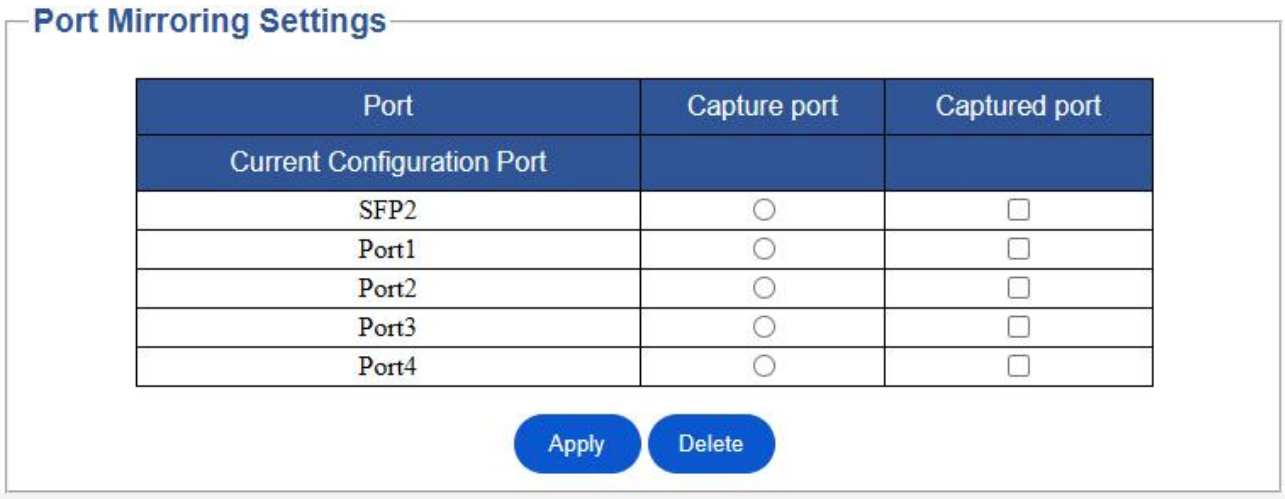
AI watch dog: Turn on POE port detection, access the device abnormally, automatically detect the powered port device, find a crash and immediately power off and restart the device, and restore PoE power supply (watchdog);

AI ultra-long: When it is detected that the device is powered normally but the continuous link fails,

modify the port duplex mode and enable the port remote transmission mode;

3. Port Configuration

3.1 Port Mirroring



Port Mirroring: All captured ports will be cloned to the captured port without destroying the original communication state for network data analytics processing.

Parameter Description:

Parameter	Description
capture port	Select the port for capturing network data (radio only); mirror destination port
captured port	Select the port of the captured network data (multiple selectable); mirror the source port

After entering or selecting, click Apply to execute the currently selected mirror port settings and save.

Click Delete to delete the current mirror port settings.

3.2 Port Management

Parameter Description:

The list of port information: Reboot, after clicking the "reboot" function button, the corresponding port of the device will be powered on again.

Port Info Table

Port	TX	RX	power	POE	Duplex	Flow Control	Up Speed Limit(Mbps)	Down Speed Limit(Mbps)	Status	Reboot
SFP1	---	---	---	---	1000M full	On	0M	0M	Off	Reboot
SFP2	16Kb	8Kb	---	---	1000M full	On	0M	0M	1000M	Reboot
Port1	---	---	---	On	1000M full	On	0M	0M	Off	Reboot
Port2	8Kb	16Kb	---	On	1000M full	On	0M	0M	1000M	Reboot
Port3	---	---	---	On	1000M full	On	0M	0M	Off	Reboot
Port4	---	---	---	On	1000M full	On	0M	0M	Off	Reboot
Port5	---	---	---	On	1000M full	On	0M	0M	Off	Reboot
Port6	---	---	---	On	1000M full	On	0M	0M	Off	Reboot
Port7	---	---	---	On	1000M full	On	0M	0M	Off	Reboot
Port8	---	---	---	On	1000M full	On	0M	0M	Off	Reboot

Flow Control Settings:

Flow Control Settings

Port	Flow Control
Port5 Port6 Port7 Port8	Off

Apply

Parameter Description:

POE Settings

POE Settings

Port	POE
Port1 Port2 Port3 Port4	Off

Apply

After entering or selecting, click Apply to execute the current selection settings and save.

Port Duplex Settings:

Port Duplex Settings

Port	Duplex
Port1 Port2 Port3 Port4	Disable

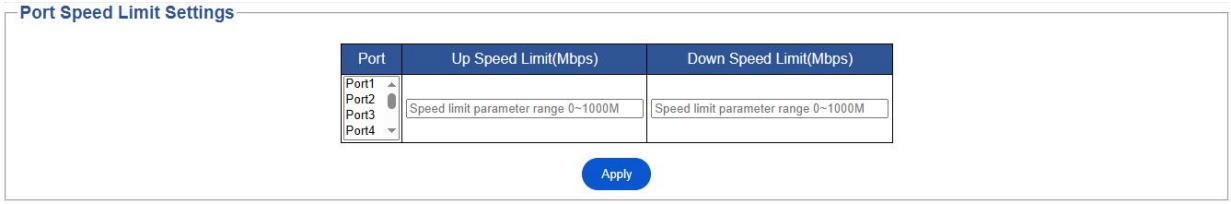
Apply

Parameter Description:

Parameter	Description
Disable	The user chooses to disable the specified port (the access device is no longer linked);
1000/100/100H/10/10H	User selects duplex mode for specified port (backward compatibility);

After entering or selecting, click Apply Execute the current selection settings and save.

Port Speed Limit Settings:



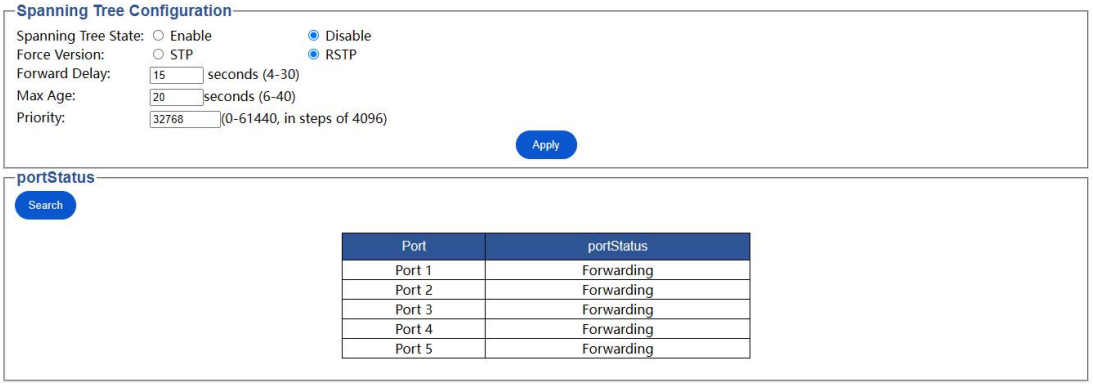
Parameter Description:

Enter integers within 0-1000.

After entering or selecting, click Apply to execute the current selection settings and save.

Note: When the port speed is full duplex and its actual mode is 1000M full duplex/100M full duplex/10M full duplex, the flow control function can be enabled and effective.

3.3 Spanning Tree Protocol*



Spanning Tree related instructions:

3.3.1. The use of STP

STP is a protocol for eliminating the physical loop of the data link layer in a local area network, which is based on the 802.1D standard developed by the IEEE Consortium. Devices running this protocol discover loops in the network by interacting with each other and selectively block some ports. Finally, the loop network structure is trimmed into a loop-free tree network structure, thus preventing the continuous proliferation and infinite circulation of packets in the loop network, and avoiding the problem of the packet processing ability of the host due to repeated receipt of the same message.

STP contains two meanings. STP in the narrow sense refers to the STP protocol defined in IEEE 802.1D, and STP in the broad sense refers to the STP protocol defined in IEEE 802.1D and various improved spanning tree protocols (such as RSTP protocol) based on it.

3.3.2. STP protocol message

The protocol message used by STP is BPDU, also known as configuration message.

STP determines the topology of the network by passing BPDUs between devices. The BPDUs contain enough information to ensure that the device completes the spanning tree calculation process.

BPDUs are divided into two categories in the STP protocol：

• Configuring BPDU: packets for spanning tree calculations and maintaining spanning tree topologies.

• TCN BPDU：When the topology changes, a message is used to notify the relevant device that the network topology has changed.

3.3.3. Basic Concepts of STP

(1) Root Bridge

A tree-like network structure requires a tree root, so STP introduced the concept of a root bridge.

There is only one root bridge in the whole network, and the root bridge will change according to the change of network topology, so the root bridge is not fixed.

(2) path cost

The path cost is the reference value used by the STP protocol to select links. The STP protocol calculates the path cost, selects more "strong" links, blocks redundant links, and prunes the network into a tree network structure without loops.

(3) port role

• Root（Root port）：The port responsible for forwarding data to the root bridge.

• Designated（specified port）：The port responsible for forwarding data to the downstream network segment or switch.

• Blocking（Blocking port）：The port that is blocked by the specified port of the other party.

(4) port status

• Forwarding：The port in this state can send and receive BPDUs and also forward user traffic.

• Learning：This is a transitional state. In this state, the device builds a MAC address table based on the user traffic it receives (but still does not forward traffic).

• Listening：This is a transition state. In this state, the selection of the root bridge, root port, and designated port is completed.

- Blocking：Only receive and process BPDU packets, do not forward user traffic.
- Disabled：STP is closed or the physical link is down.

3.3.4. Fundamentals of STP

The STP determines the topology of the network by passing BPDUs between devices. The configuration message contains enough information to ensure that the device completes the spanning tree calculation process. Some important information is as follows：

- Root bridge ID：It consists of the priority and MAC address of the root bridge；
- Root Path Cost: The shortest path cost to the root bridge；
- Designated Bridge ID: Consists of the priority and MAC address of the specified bridge；
- Specify port ID: Consists of the priority and port name of the specified port；
- Message Age：Configure the lifetime of messages propagating through the network；
- Max Age：Maximum lifetime of configuration messages that can be saved in switch；
- Hello Time：Configure the message sending cycle；
- Forward Delay：Port state migration latency；

3.3.5. RSTP Introduction

RSTP is an optimized version of the STP protocol. Its "fast" is reflected in that when a port is selected as the root port and the designated port, the delay in entering the forwarding state is greatly reduced under certain conditions, thus shortening the time required for the network to finally reach topological stability.

(1) port role

The port role of RSTP adds Alternate port and Backup port to STP, and cancels Blocking port.

- Alternate port: is a replacement port for the root port for fast switching. When the root port is blocked, the Alternate port will become the new root port.
- Backup port: is the port blocked by the specified port of this device.

(2) port status

The port state of RSTP is relative to STP, reducing the original five states to three states.

- Forwarding state: both forwarding user traffic and receiving/sending BPDU packets.
- Learning status: does not forward user traffic, only receives/sends BPDU packets.
- Discarding status: does not forward user traffic, only receives BPDU messages.

configuration parameter description：

parameter	description
Spanning Tree status	Turn on or off Spanning Tree Protocol features (enable/disable).
mandatory version	Spanning Tree (STP) or Rapid Spanning Tree (RSTP) options.
forwarding delay	STP, this parameter is the default message waiting timeout time.
Maximum valid period	A parameter used to determine whether the configuration message is "outdated" in the switch, and the switch will discard the outdated configuration message.
Send hold count	The upper limit of message forwarding processing per unit time.
priority	The root bridge campaign priority of the device, 4096 digits, the smaller the priority, the higher the priority.

After entering or selecting, click 

Execute the current selection settings and save

4. VLAN Management

This series of devices supports the following three VLAN function modes:

•**802.1Q VLAN Mode**: Defined by the IEEE 802.1Q protocol, the message is processed by identifying the tag in the message (including information such as 802.1p priority and VLAN ID).

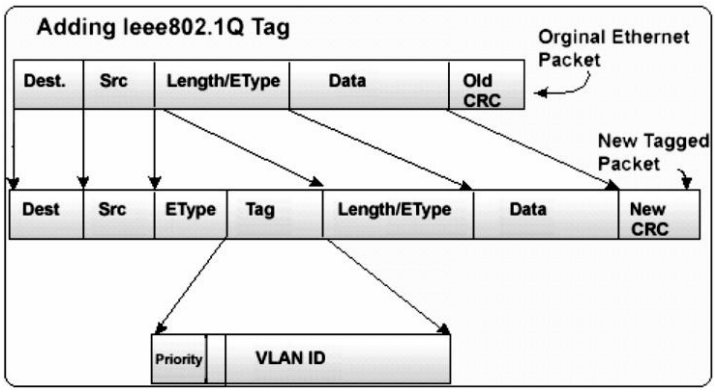
•**MTU VLAN Mode**: Ports set by the user to isolate (vlan flag) cannot communicate with each other, only with ports set to UP-LINK ports.

•**Port VLAN Mode**: In the port-based VLAN (Port VLAN) mode, ports in the same VLAN can communicate with each other, which can effectively shield broadcast storms and improve cyber security performance.

Attention: The device supports three VLAN modes, and only one mode can be selected to be turned on at a time. When the other mode is enabled, the other modes are automatically turned off and all setting parameters are deleted.

4.1 802.1Q VLAN

When IEEE 802.1Q Tag VLANs were first used, the switches of various manufacturers were not recognized and could not be compatible due to the lack of a unified standard. Therefore, IEEE 802.1Q, a new virtual local area network standard, was developed so that devices from different manufacturers can be used in the same network at the same time. Switches that comply with the IEEE 802.1Q standard can communicate with each other. The IEEE 802.1Q standard defines a new frame format, which adds a Tag header after the source address of the standard Ethernet frame, as shown in the figure:



IEEE 802.1Q-based Tag VLANs use VIDs to divide different VLANs. When data frames pass through the switch, the switch identifies the VLAN in which they are located based on the VID information of the Tag header in the frame (but if there is no Tag header in the frame, we call this frame an Untag frame, and use the default VID information of the port through which the frame passes to identify the VLAN in which they are located. Untag frames can also be processed differently by setting), which makes all data frames belonging to the VLAN, whether unicast frames, multicast frames or broadcast frames, limited to propagate in the logical VLAN. Hosts in the group can communicate with each other without being affected by other hosts, just as if they existed in separate local area networks.

802.1Q VLAN:

(1) VLAN Tags

In order for the switch to be able to distinguish messages from different VLANs, a field identifying the VLAN needs to be added to the message. Since the switch works at the data link layer of the OSI model (the three-layer switch is not within the scope of this chapter), it can only identify the data link layer encapsulation of the message. Therefore, the identification field needs to be added to the data link layer encapsulation.

In 1999, IEEE published the draft IEEE 802.1Q protocol standard to standardize VLAN

implementations, unifying the message structure with VLAN tags.

Traditional Ethernet data frames encapsulate the upper layer protocol type field after the destination MAC address and source MAC address. Take the following ICMP message as an example:

```
> Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
v Ethernet II, Src: 08:10:7a:18:87:94 (08:10:7a:18:87:94), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: 08:10:7a:18:87:94 (08:10:7a:18:87:94)
    Type: ARP (0x0806)
    Padding: 00000000000000000000000000000000000000
> Address Resolution Protocol (request)
```

Where Dst represents the destination MAC address, Src represents the source MAC address, and Type represents the type field of the upper layer protocol of the message The IEEE 802.1Q protocol stipulates that a 4-byte VLAN Tag is encapsulated after the destination MAC address and the source MAC address to identify the relevant information of the VLAN.

```
> Frame 2: 64 bytes on wire (512 bits), 64 bytes captured (512 bits)
v Ethernet II, Src: Shenzhen_0c:88:2c (7c:83:34:bc:88:2c), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: Shenzhen_0c:88:2c (7c:83:34:bc:88:2c)
    Type: 802.1Q Virtual LAN (0x8100)
v 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 66
    000. .... .... .... = Priority: Best Effort (default) (0)
    ...0 .... .... .... = DEI: Ineligible
    .... 0000 0100 0010 = ID: 66
    Type: ARP (0x0806)
    Padding: 000000000000000000000000000000
    Trailer: 00000000
> Address Resolution Protocol (request)
```

***It is used to identify that this data frame is a data frame with VLAN Tag. The length of this field is 16bit, and the default value is 0x8100 specified in the protocol.

Priority: Used to represent the priority of 802.1p. This field is 3 bits long.

DEI: Used to identify whether the MAC address is encapsulated in a standard format. The length of this field is 1bit, and the value of 0 means that the MAC address is encapsulated in a standard format. 1 means that it is encapsulated in a non-standard format. The default value is 0.

VLAN ID: The number used to identify the VLAN to which the message belongs. The length of this field is 12bit, and the value range is 0~ 4095.

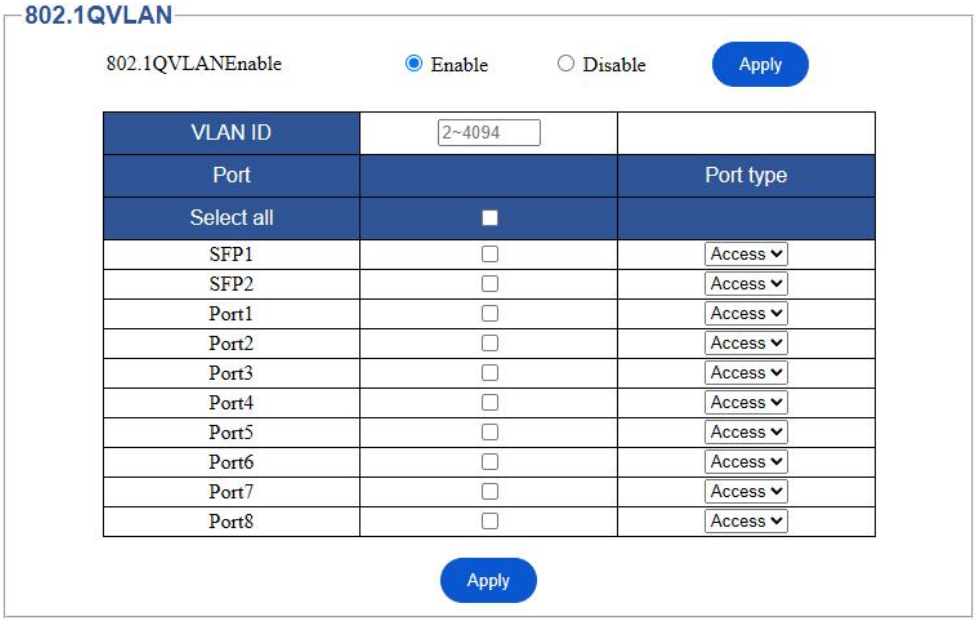
Since 0 and 4095 are usually not used, 1 is reserved for the default management VLAN, so the value range of this series of management switch VLAN IDs is generally 2~ 4094.

(2) Port link type

This series of switches supports two types of port links:

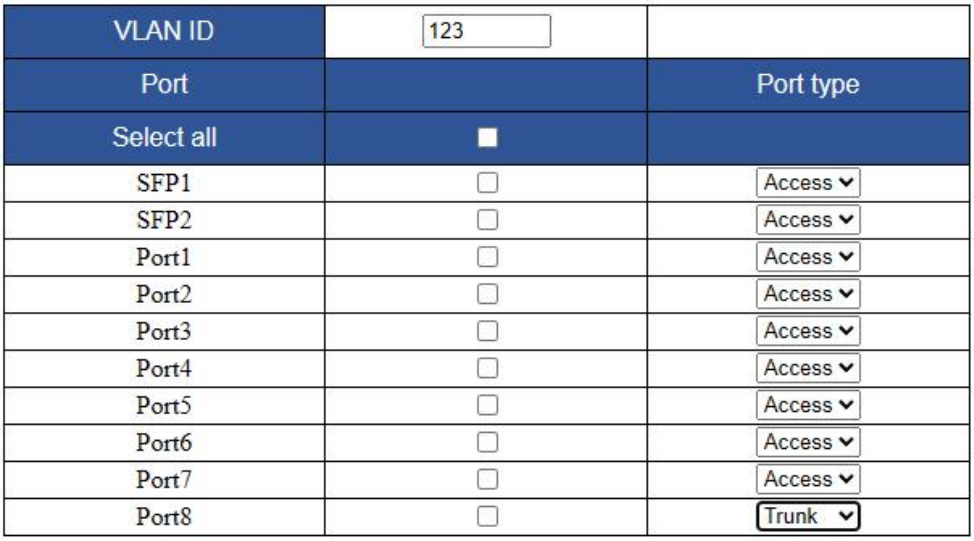
Access: Ports can only belong to one VLAN and are generally used to connect user devices. By default, all ports belong to Access ports;

Trunk: The port can belong to multiple VLANs, can receive and send messages from multiple VLANs, and is generally used to connect to other network devices (the default PVID of this series of devices is 1, which can forward all data that has been configured with a VLAN ID on the machine, and cannot be modified);



Configuration example description:

4.1.1、Create a VLAN 123 that is not configured to the port (check the 802.1Q VLAN bar switch for the VLAN to take effect):



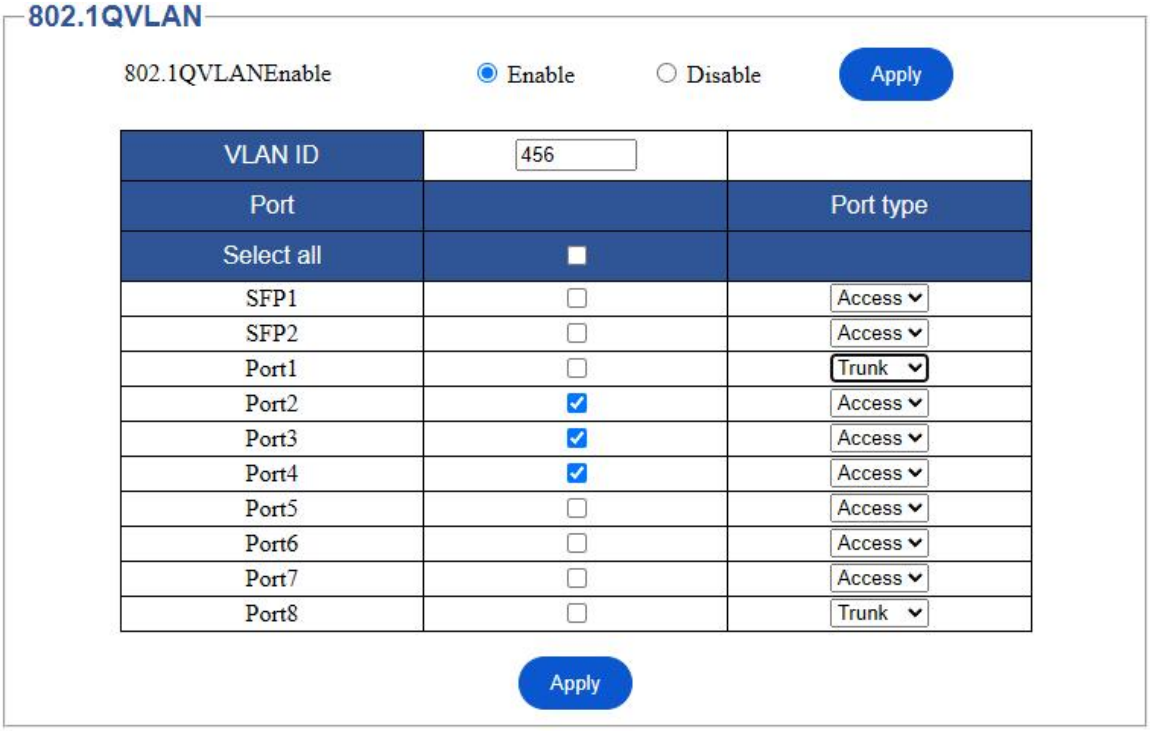
Sometimes in order to pass through business data, it is necessary to increase the vlan of Trunk pass through

4.1.2、Create a vlan and configure it to the port:

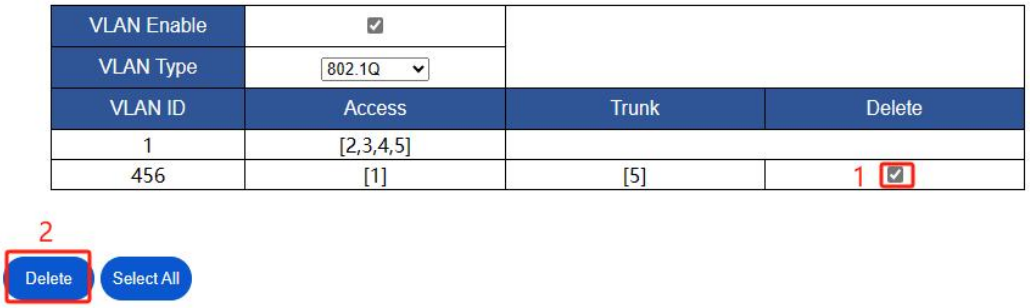
*Note that at least one Trunk port needs to be selected when configuring (to ensure management of vlan data communication).

*The selected port cannot conflict with other vlan id port data. When you need to modify the PVID of the port, please remove it from the original vlan data first (remove the tick).

*In order for the configuration to take effect, the "802.1Q VLAN" switch needs to be checked. At the same time, please note whether the port of the current device connection management PC is the default port or the Trunk port.



4.1.3、Delete a vlan and port configuration:



5.1.4、Modify the port configuration of a VLAN:

VLAN ID	2~4094	
Port		Port type
Select all	☐	
SFP1	☐	Access
SFP2	☐	Access
Port1	☑	Access
Port2	☐	Access
Port3	☐	Access
Port4	☐	Access
Port5	☐	Trunk
Port6	☐	Access
Port7	☐	Access
Port8	☐	Access

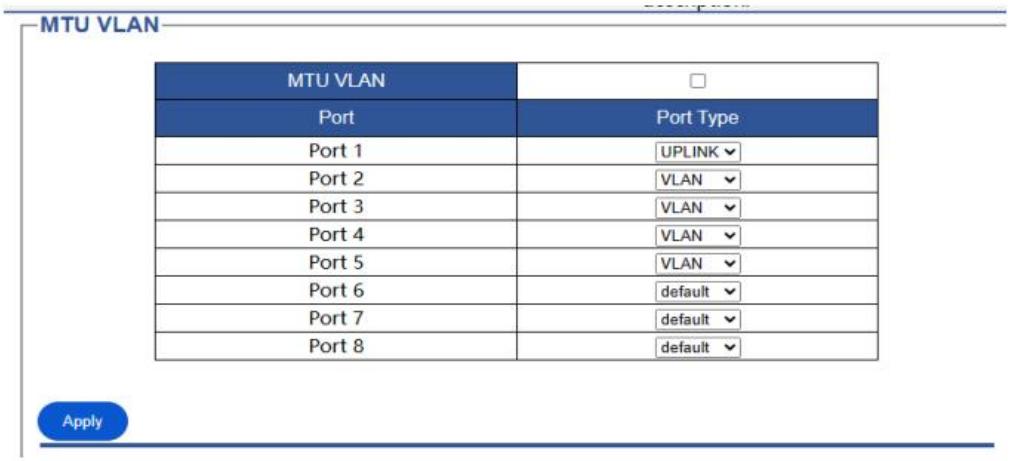
Enter the original vlan id, remove the check of the corresponding port, and click "Apply".

4.1.5、Turn off VLAN:

Remove the check of 802.1Q VLAN and click "Apply" to turn off the vlan function.

4.2 MTU-VLAN

MTU VLAN (Multi-Tenant Unit VLAN) divides the port occupied by each user and the uplink port into a separate VLAN. Users of different ports cannot communicate directly to ensure the security of the network. This situation is very suitable for use in smart cells, where users cannot directly access each other, thus ensuring the cyber security of residents.



parameter description：

Parameter	Description
Default	Default state, all Default ports can communicate with each other, with UPLINK, but not with VLAN ports;
VLAN	Isolation group, ports configured as VLAN attributes cannot communicate with each other, only with UPLINK ports;
UPLINK	It is usually an upstream communication port and can communicate with all other ports;

Enter or select and 

click to execute the action.

4.3 Port VLAN

Port VLAN: Based on the port grouping implementation of this switch, each port can only belong to one vlan. Ports in the same vlan can communicate with each other, and ports in different vlans cannot communicate;

Parameter description：

parameter	description
VLAN ID	Enter the ID number of the VLAN, ranging from 2 to 4094.
port	Show port number.
member	Click the checkbox to select the port of the VLAN, which is optional. If this field is selected, it indicates that the port belongs to the current VLAN.
enable	Enabling the current mode will automatically turn off other modes and delete all settings.
disable	Clicking Disable will close all current functions and delete all set parameters.

Enter or select and 

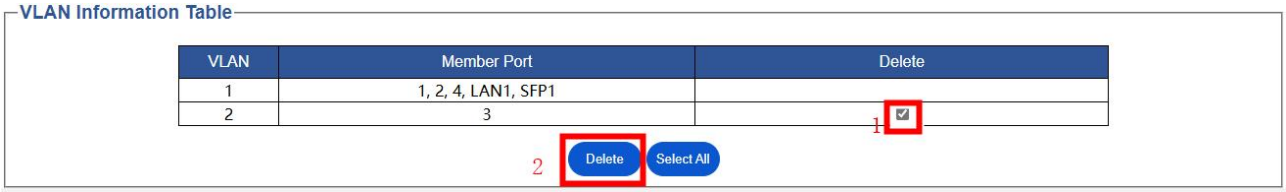
click to execute the action.

Attention：Only the VLAN1 port can be managed to switch, be careful to keep the management port!

disable：Changing the VLAN mode will cause the previous VLAN configuration to be

deleted. Please proceed with caution!

Delete a vlan and its member ports or modify the member ports of a vlan



Enter or select a member port and click Delete Execute to delete the current member port setting.

Attention:

After the current version port is configured as Trunk port, the PVID is fixed to 1, and the Facility Management vlan vid is 1.

*VLAN: It refers to the MTU-VLAN function, which isolates network ports other than the LAN port (including the SFP port) from each other and shields other internal network interference such as broadcast storms.

5. Safety

5.1 storm suppression

About storm suppression:

In a complex network environment, limit the forwarding rate of broadcast and group broadcast packets to avoid interference caused by excessive responses to device communication.



parameter description:

Parameter	Description
ON	Enable broadcast and multicast storm suppression functions, the broadcast and multicast data traffic rates of all ports are limited to about 4Mbps (8Mbps in total), and the excess part is discarded;

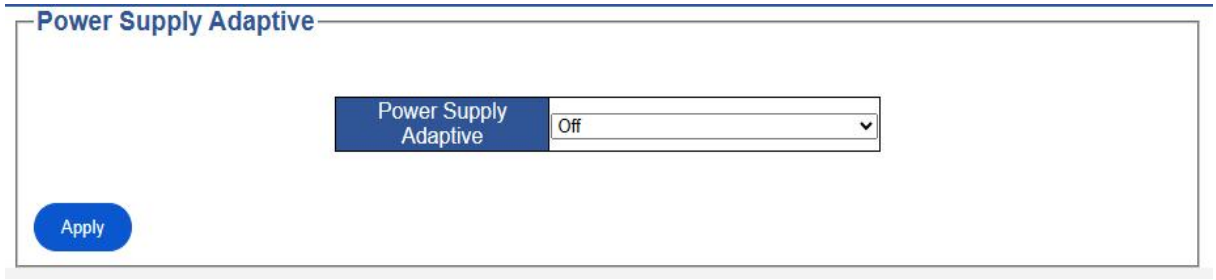
OFF	Broadcast, multicast (multicast) data traffic rates are not limited;

Enter or select and click Apply to execute the action.

5.2 Adaptive Power supply

About power supply adaptation:

Device sends LLDP bulletin supporting POE-AT standard, supports 25.5W power supply mode;



parameter description:

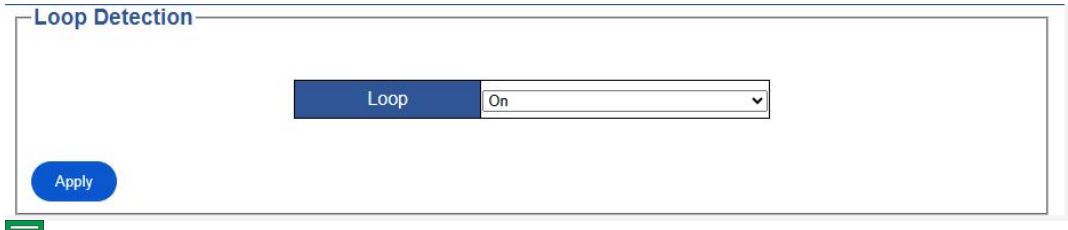
Parameter	Description
Power Adaptive = On	LLDP Announcement for Devices to Turn on POE-AT Standard

After entering or selecting, click Apply to perform the action.

5.3 loop detection

About loop detection:

When the device's own ports are looped, block one of the designated ports.



parameter description:

Parameter	Description
ON	When the device loops itself, close one of the ports (the largest port number is preferred).

OFF	Turn off loop detection.

After entering or selecting, click Apply to execute the action.

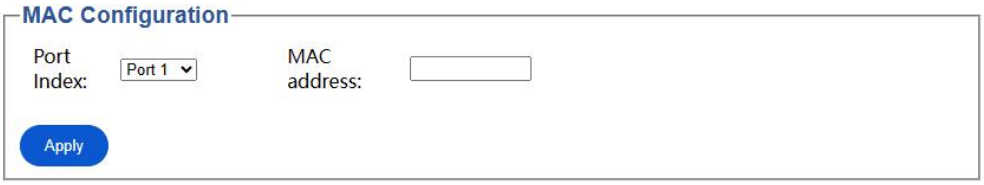


⚠As shown in the figure, when a loop occurs, the closed state shown in the figure may occur.

Device restart, reconfigure duplex or click port restart in the port configuration to restore port communication.

5.4 MAC Management

Add static MAC:



parameter description:

Parameter	Description
port number	Optional all ports of the current device;
MAC	Enter an uppercase or lowercase hexadecimal MAC address (without delimiters);

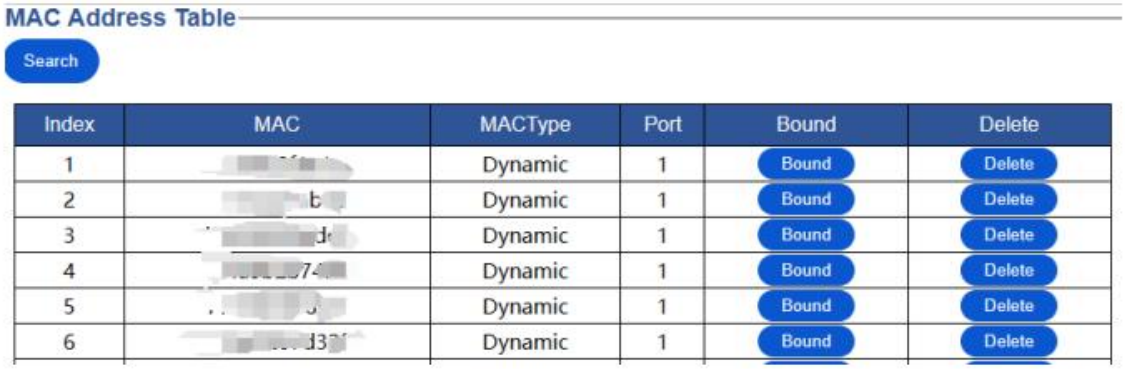
Enter or select and Apply click to execute the action.

Query MAC Address:

Click the "Query" button to display the current device MAC address table.

Delete MAC: Click the "Delete" button to delete the MAC address item in the current list.

Bind MAC: Click "Bind", and the corresponding MAC entry will be changed from dynamic to static (recommended only for non-cascading ports).



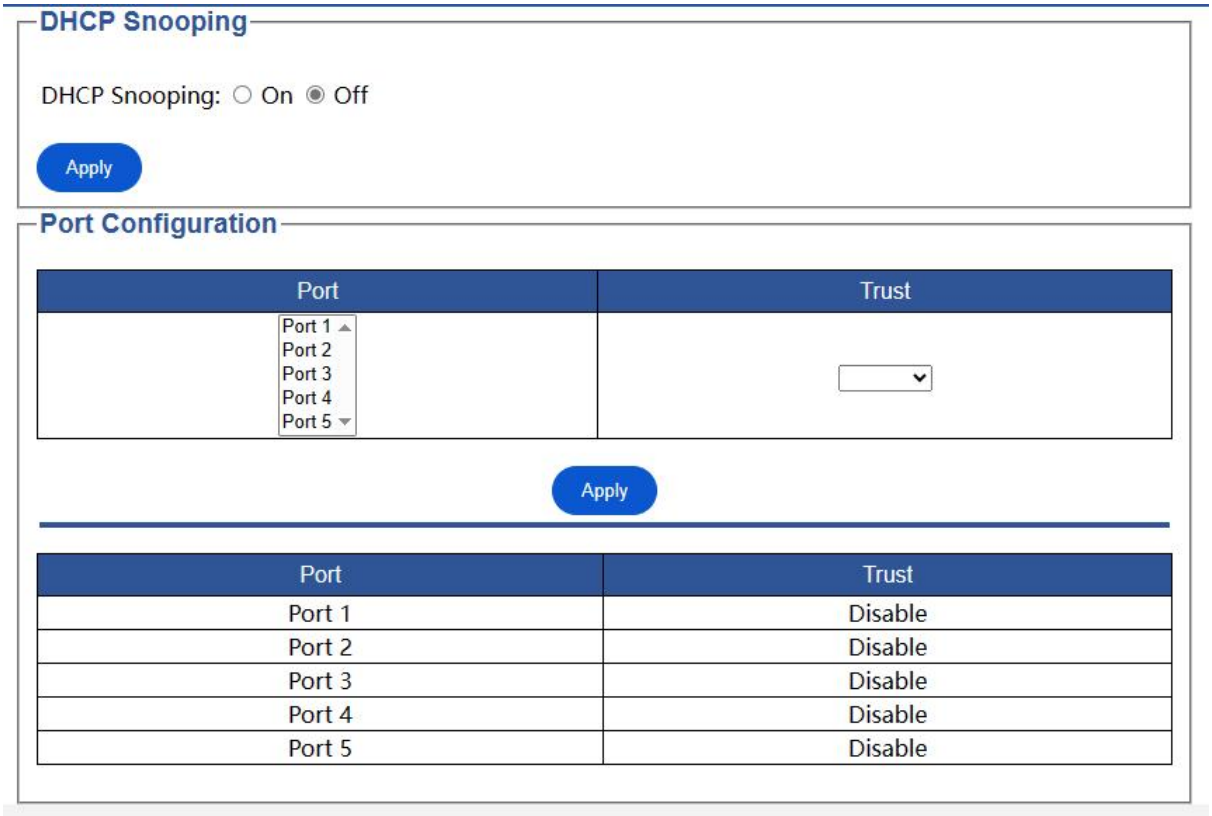
parameter description:

Port: When digital, the access port is the corresponding physical port, and the CPU is the device's own port or management MAC.

Attention:

When the port is bound to a static MAC, the port will be in a bound state: the port will turn off MAC address learning, and the device after binding the MAC cannot communicate on other ports, and other devices cannot communicate normally when accessing the port.

5.5 DHCP Snooping

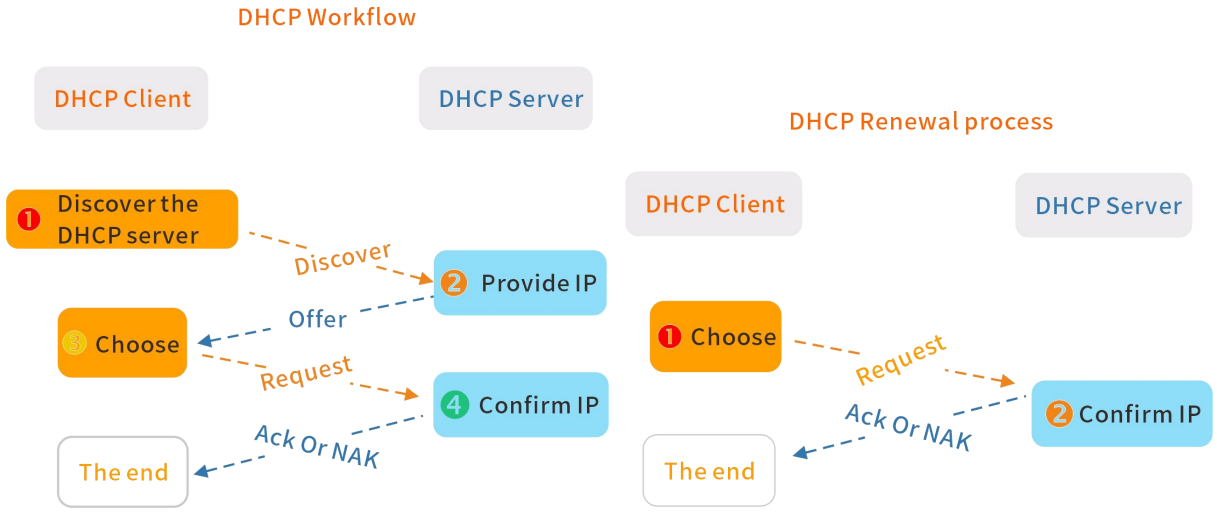


Attention: It is recommended to turn on the DHCP listening switch after configuring the relevant parameters.

*DHCP snooping is used to ensure that the DHCP client side obtains an Internet Protocol Address from a legitimate DHCP server.

About DHCP Snooping:

DHCP Snooping is a security feature of DHCP (Dynamic Host Configuration Protocol), which is used to ensure that the DHCP client side obtains the Internet Protocol Address from the legitimate DHCP server. By configuring the "trusted/untrusted" working mode of the device interface: set the interface directly or indirectly connected to the legitimate DHCP server to the trusted interface, and set the other interfaces to the untrusted interface. After that, the DHCP response message received from the "untrusted (trust disabled) " interface will be directly discarded, which can effectively prevent the attack of the DHCP Server impersonator.



As shown in the figure, after enabling the DHCP Snooping function, packets from untrusted ports (Offer or ACK, NAK) will be discarded.

parameter description:

Parameter	Description
Port	Select the port to be set, and press the ctrl key to perform multiple selection operations.
trust	When port trust is set to "enabled", a trusted DHCP server device (* router) can be accessed at this port. When there are illegal DHCP devices (such as routers) on the "disabled" port, devices connected to other ports will only obtain the correct

	Internet Protocol Address from the DHCP server (router) connected to the trusted port.

Enter or select and 

click to execute the action.

6. Basic specifications

Item	Parameter
Power Specifications	AC input 100-240V 50/60Hz
Network media and transmission distance	1000Base-T: 4 pairs of Super Class 5 (Cat5e) or above UTP/STP (≤ 100m) 100Base-TX: 2 pairs of 5 (Cat5) or above UTP/STP (≤100m) 10Base-TX: 2 pairs of 5（Cat5e）or above UTP/STP(≤250m)
basic function	Complies with IEEE 802.3 Ethernet and IEEE 802.3u Fast Ethernet protocol standards Compatible with IEEE 802.3af/at compliant POE-powered devices store and forward MAC automatic learning and aging IEEE802.3X Full Duplex Flow Control and Backpressure Half Duplex Flow Control
Ethernet protocols and standards	IIEEE 802.3 Ethernet Media Access Control Protocol IEEE 802.3i 10BASE-T Ethernet IEEE 802.3u 100BASE-TX Fast Ethernet IEEE 802.3ab 1000BASE-T Gigabit Ethernet IEEE802.3z 1000Base-X SFP interface IEEE 802.3x Flow Control
data transfer rate	Ethernet 10Mbps half duplex, 20Mbps full duplex Fast Ethernet 100Mbps half duplex, 200Mbps full duplex Gigabit Ethernet 2000Mbs Full Duplex

Items marked with*are selected according to different product models

7. Exit

The device only supports web login on one PC or mobile phone at the same time. If you need to switch between different terminals or different browsers, you need to click the "Exit" button in the logged-in browser to perform a safe exit operation, or wait 3 minutes before logging in.

8. FAQ

1、How to activate the Mini Program with the device password;

■ Log in to the web for the new device first, and then bind it to the cloud (APP or Mini Program):

Log in to the web page and set a password. When binding the device to the cloud APP later, you need to enter the password set by the web page at the activation code.

■ The new device is bound to the cloud (APP or Mini Program) first, and then logged in to the WEB:

When adding a device through the Mini Program, enter the device activation code as the device password. After the addition is completed, you can log in to the web later to use the password.

■ Unbound cloud device Forgot password, reset password:

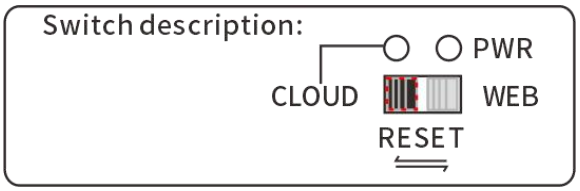
If there is a function switch, reset the device with a quick toggle switch, see the next description;

No function switch version, you can contact the after-sales service, and a special PC software tool will be provided to reset the device password through this tool.

2、How to reset the device password (including a complete device reset)?

Second gear function switch:

RESET: The switch is at the WEB position. Within 1 second, pull it to CLOUD and then back to WEB. The switch will restart and restore the factory settings.



3、After configuring DHCP Snooping, there is no how to discover the device in the DHCP client side of the router, how to deal with it?

Confirm that the router connection is a DHCP Snooping trust port, and that vlan is not configured or the default vlan port.

When unsure, you need to reset the device or use an alternate IP 10.0.0.10 reconfigure DHCP Snooping.

Please note: V6 does not support the web version